

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

C. Li  
China Telecom  
O. Havel  
A. Olariu  
Huawei Technologies  
P. Martinez-Julia  
NICT  
J. Nobre  
UFRGS  
D. Lopez  
Telefonica, I+D  
February 22, 2022

Intent Classification  
draft-irtf-nmrg-ibn-intent-classification-06

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) and is not issued by the IETF and is not an IETF standard.

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 August 22, 2022.

#### Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction.....	4
1.1. Research activities.....	4
1.2. Standards and open source activities.....	5
1.3. Scope.....	6
2. Acronyms.....	7
3. Definitions.....	8
4. Abstract Intent Requirements.....	8
4.1. What is Intent?.....	8
4.2. Intent Solutions and Intent Users.....	9
4.3. Benefits of Intents for Different Stakeholders.....	11
4.4. Intent Types that need to be supported.....	12
5. Functional Characteristics and Behaviour.....	13
5.1. Abstracting Intent Operation.....	13
5.2. Intent User Types.....	14
5.3. Intent Scope.....	15
5.4. Intent Network Scope.....	15
5.5. Intent Abstraction.....	16
5.6. Intent Life-cycle.....	16
5.7. Autonomous Driving Levels.....	16
6. Intent Classification.....	17
6.1. Intent Classification Methodology.....	18
6.2. Intent Taxonomy.....	21
6.3. Intent Classification for Carrier Solution.....	23
6.3.1. Intent Users and Intent Types.....	23
6.3.2. Intent Categories.....	27
6.3.3. Intent Classification Example.....	27
6.4. Intent Classification for Data Center Network Solutions.....	31
6.4.1. Intent Users and Intent Types.....	31
6.4.2. Intent Categories.....	35
6.4.3. Intent Classification Example.....	35
6.5. Intent Classification for Enterprise Solution.....	39
6.5.1. Intent Users and Intent Types.....	39
6.5.2. Intent Categories.....	41
7. Conclusions.....	43
8. Security Considerations.....	43
9. IANA Considerations.....	43
10. Contributors.....	44
11. Acknowledgments.....	44
12. Informative References.....	44

## 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 RG. During the document's lifecycle it received many positive expressions of support and detailed reviews beyond the authors. Only in the last call period it received more than 12 positive expressions of support and more than 5 detailed reviews. It is published for informational purposes.

### 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 [Bezahaf19], 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:

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

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:

- o 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.
- o Intent-Based Network: A network that can be managed using intent.
- o Policy: A set of rules that governs the choices in behaviour of a system.
- o 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. .

- o 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.
- o 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%.
- o 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:

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

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

- o simplify and automate network operations
- o simplify definitions of network services
- o provide simple customer APIs for value added services (operators)
- o be informed if the network or service is not behaving as requested
- o enable automatic optimization and correction for selected scenarios
- o 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:

- o build their own network services with their own policies via simple interfaces, without becoming networking experts
- o 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:

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

- o for configuring and monitoring policies, alarms generation for non-compliance, auto-recovery
  - o for design models and policies for network and network service design
  - o for design workflows, models and policies for operational task intents
- o Operational task intents
  - o for network migration
  - o for device replacements
  - o for network software upgrades
  - o 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}

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

- o 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.
- o 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.

- o 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.

- o 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.
- o 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:

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

- o 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.
- o 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:

- o 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.
- o 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.

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

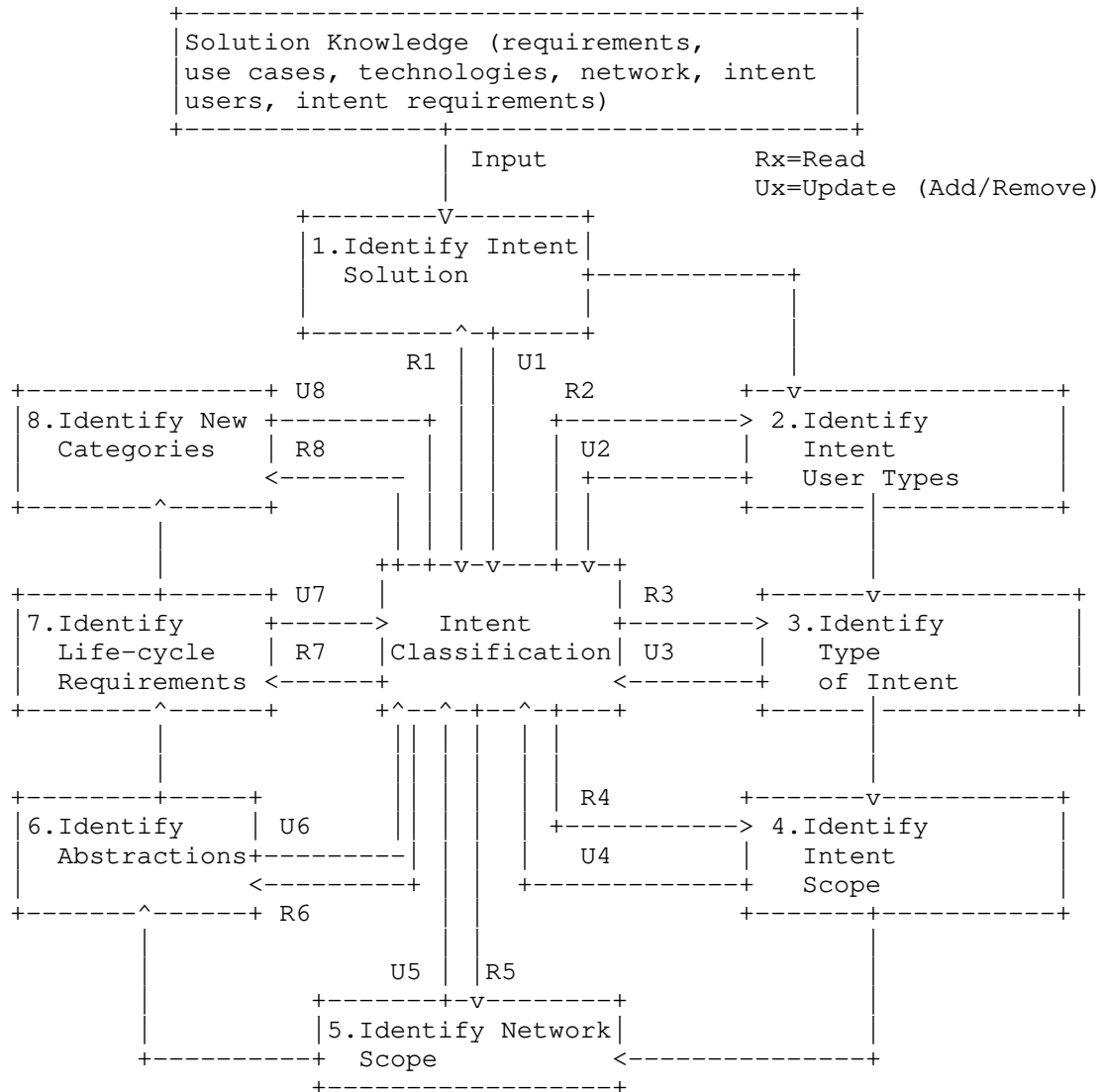


Figure 1 - Intent Classification Methodology

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.

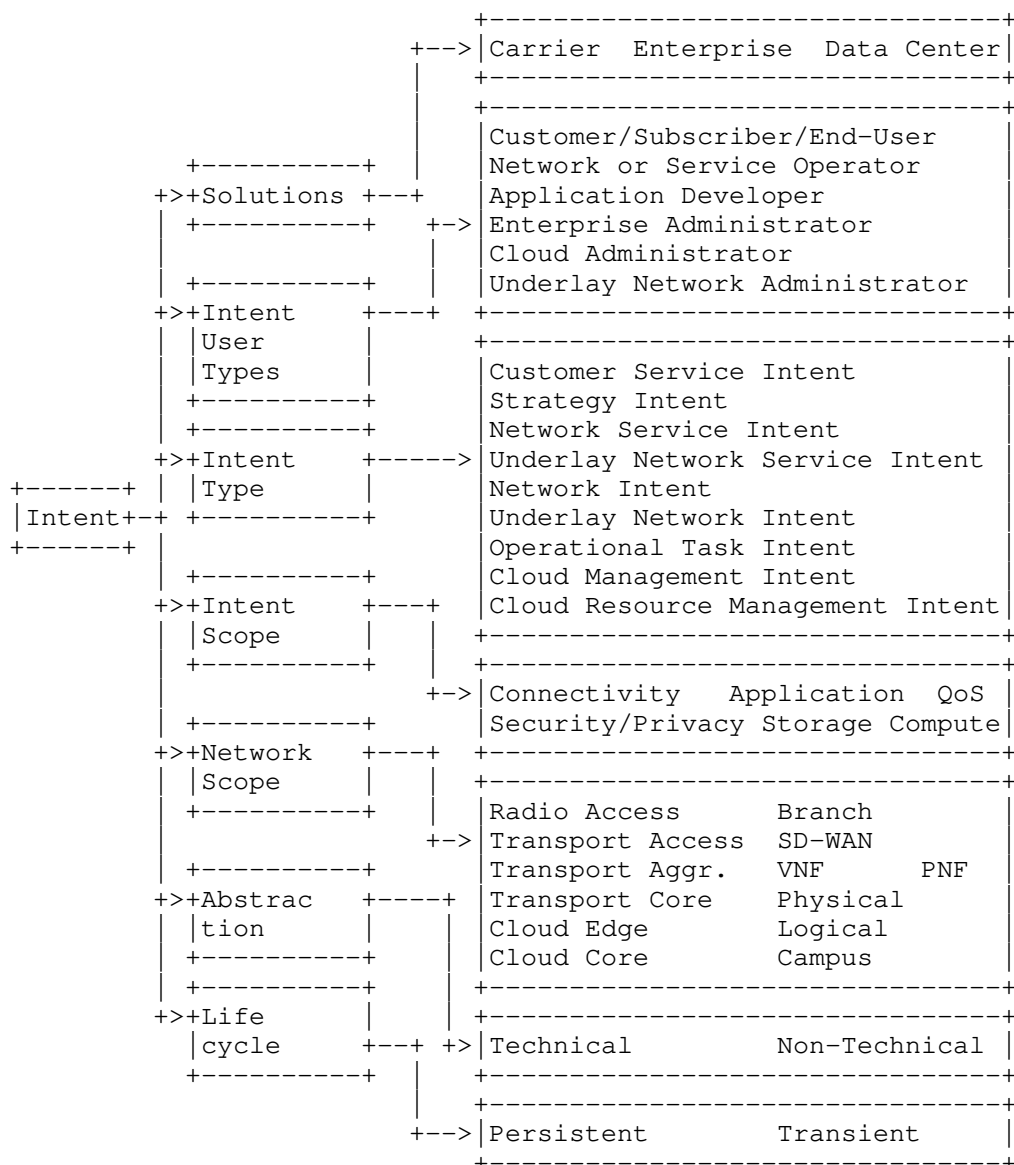


Figure 2 - Intent Taxonomy

### 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:

- o Intent Scope: C1=Connectivity, C2=Security/Privacy, C3=Application, C4=QoS
- o Network Scope:
  - o Network Domain: C1=Radio Access, C2=Transport Access, C3=Transport Aggregation, C4=Transport Core, C5=Cloud Edge, C6=Cloud Core)
  - o Network Function (NF) Scope: C1=VNFs, C2=PNFs
- 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)

### 6.3.3. 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																
	Operational 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 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



Application Developer		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%.
	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:

- o Intent Scope: C1=Connectivity, C2=Security/Privacy, C3=Application, C4=QoS
- o Network (Net) Scope: C1=Campus, C2=Branch, C3=SD-WAN
- 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)

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											



## 10. Contributors

The following people all contributed to creating this document:

Xueyuan Sun, China Telecom  
Will (Shucheng) Liu, Huawei  
Ying Chen, China Unicom  
John Strassner, Huawei  
Weiping Xu, Huawei  
Richard Meade, Huawei

## 11. Acknowledgments

Special thanks to Xueyuan Sun from China Telecom for significant contributions to this document, and to Will (Shucheng) Liu from Huawei for contributions and guidance.

This document has benefited from reviews, suggestions, comments and proposed text provided by the following members, listed in alphabetical order: Mehdi Bezhaf, 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] Bezhaf, 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.
- [Bezhafl9] Bezhaf, 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., Kravlevska, 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](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](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](http://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/](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-sup-  
generic-policy-info-model/?include\\_text=1](https://datatracker.ietf.org/doc/draft-ietf-sup-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





Internet Research Task Force  
Internet-Draft  
Intended status: Informational  
Expires: September 6, 2022

D. Chen  
H. Yang  
K. Yao  
China Mobile  
G. Fioccola  
Huawei Technologies  
March 05, 2022

Network measurement intent - one of IBN use cases  
draft-yang-nmrg-network-measurement-intent-04

Abstract

As an important technical means to detect network state, network measurement has attracted more and more attention in the development of network. However, the current network measurement technology has the problem that the measurement method and the measurement purpose cannot match well. To solve this problem, this memo introduces network measurement intent, namely the process of realizing user or network operator to allocate network states as needed. And it can be as a specified user case of intent based network.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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 <https://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 September 6, 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Definitions and Acronyms . . . . .	3
3. Connections to Existing Documents . . . . .	3
4. Overview . . . . .	5
5. Concrete Examples . . . . .	7
5.1. SLA measurement intent . . . . .	8
5.2. Clustered performance measurement intent . . . . .	10
6. Classification of NMI . . . . .	11
6.1. Static NMI . . . . .	12
6.2. Dynamic NMI . . . . .	12
7. Summary . . . . .	12
8. Security Considerations . . . . .	12
9. IANA Considerations . . . . .	13
10. References . . . . .	13
10.1. Normative References . . . . .	13
10.2. Informative References . . . . .	13
Authors' Addresses . . . . .	13

## 1. Introduction

With the rapid development of the current network, the scale of the network is getting larger and larger, while users' requirements for the network are getting higher and higher. At the same time, network resources are increasingly restrained. In order to realize the efficient allocation of network resources, it is necessary to understand the running state of the network, and network measurement, as a technical means to detect the network, has been paid of more and more attention. The continuous development of network measurement technology has also satisfied the higher and higher precision of network perception. However, both the traditional network measurement technology and the network telemetry technology, which

has emerged with the development of software-defined network in recent years, need to occupy the network resources when detecting the network state and feeding back the detection results. Therefore, to some extent, the choice of network measurement methods, in addition to different accuracy of measurement results, will also cause different degrees of burden to the network.

In order to balance the accuracy of network measurement results with the network load, it is very important to choose the appropriate network measurement method according to the different requirements of network measurement. As a result, accurate on-demand network measurement technology is becoming more and more important. At the same time, the development of Intent based Network (IBN) enables the network to be configured according to users' or network administrators' intent. Therefore, we can combine network measurement with IBN, that is, the users' or network administrators' perceived demand for network state is regarded as network measurement intent.

We want to use the network measurement intent to achieve network performance acquisition based on user/network administrator intent-based, verify whether network measurement results meet the measurement intent, and further improve the accuracy of the configuration in IBN.

## 2. Definitions and Acronyms

CLI: Command-line Interface.

IBN: Intent based Network.

Policy: A set of rules that governs the choices in behavior of a system.

NMI: Network Measurement Intent, refers to based on user/network operator's demand for network status, and automatically collect network status information on demand.

SLA: Service Level Agreement.

## 3. Connections to Existing Documents

As the rise of IBN, different groups have different definitions of intent. For example, ONF [ONOS] defines intent is represented as a list of CLI modes that allows users to pass low-level details on the network; and there are two active RG drafts in the NMRG right now, Intent-Based Networking - Concepts and Definitions, [I-D.irtf-nmr-ibn-concepts-definitions] solves the problem that

"What is an intent?"

and[I-D.irtf-nmrg-ibn-intent-classification] solves the problem "Given a specific intent, how to parse/disassemble it from different angles?".

Naturally, the question that needs to be solved after concept definition should be "How to realize an specific intent?". The classification draft can be considered as the first step of realization of a given intent, however, it is not enough. Some other issues should be clarified, like "whether the input intent is valid or not?" , "What would the IBN system do when the result is not acceptable?", "If the result is not acceptable, does human/operator interference required?"... We should take a specific IBN use case for illustration of the realization procedure, so we will take the network measurement intent as an example.

Referring to the taxonomy of intent proposed in[I-D.irtf-nmrg-ibn-concepts-definitions], the network measurement intent can be classified into different subgroups.

Solution: the intent could cover carrier and data center.

Intent user type: customer.

Intent type: customer service intent.

Intent scope: Application, QoS.

Network scope: Radio Access, Transport, Edge, Core.

Abstraction: Non-technical.

Lifecycle Requirements: transient.

In order to combine the NMI with the existing drafts of IBN, in this document we define the components of the NMI processing process as follows:

- o NMI Recognition and Acquisition
- o NMI Translation
- o NMI Policy
- o NMI Orchestration and pre-Verification
- o Data Collection and Analytics

- o NMI Compliance Assessment

#### 4. Overview

As mentioned above, NMI refers to the on-demand measurement of the network state based on the user/network operators' perceived intent of the network state. We will present the detailed process of it within each part and take the measurement of busy network performances as a simple example.

- o NMI Recognition and Acquisition.

- \* In this function, NMI will be recognized by "ingesting" users' or network operators' measurement intent. They have the ability to identify the NMI of a certain network performance that users want to measure, such as delay, jitter, etc., and at the same time allow users to express the NMI of network performance in a variety of interactive ways to ensure the accuracy of the identification of the NMI. To achieve this functionality, such an interaction requires the use of the intent-northbound interface defined in the IBN.

- o NMI Translation.

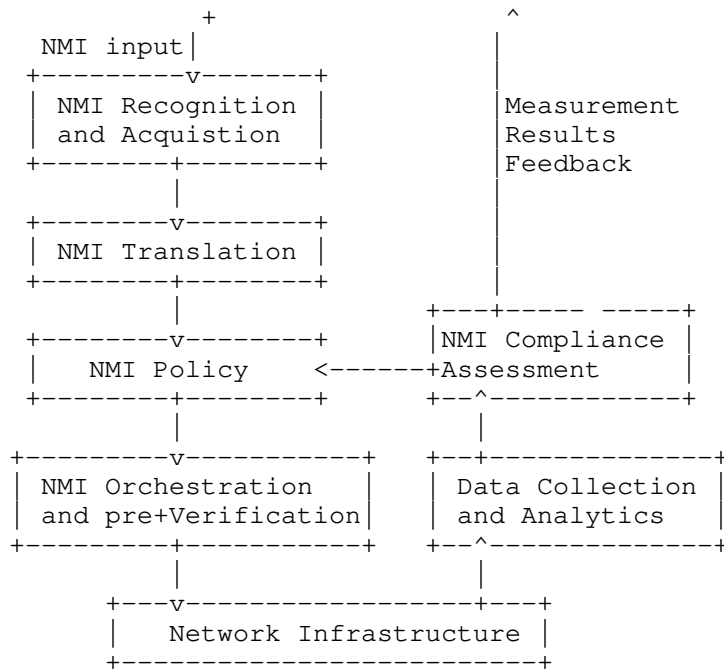
- \* In this function, NMI needs to be translated into corresponding measurement policy, which includes but is not limited to network performance parameters to be measured (such as delay, jitter, and packet loss), time period to be measured, and measurement precision. For a simple example, in the measurement of busy network performances, due to dynamic changes such as daily network bandwidth occupancy rate, the period of network busy time is not fixed. As a result, NMI Policy generated by NMI Translation can determine the threshold when the network state is busy on the same day based on the historical data learned by AI.

- o NMI Policy

- \* In this function, NMI policy needs to be translated into actions and requests taken against the specified network element. Therefore, NMI policy generated by NMI Translation must be executable, that is, corresponding underlying network devices must be able to support policy execution.. If the generated policy cannot be executed by the underlying device, the policy needs to be adjusted. And if the measurement results cannot meet the requirements, the policy also needs to be adjusted.

- o NMI Orchestration and pre-Verification.
  - \* In this function, according to the previous NMI Translation and NMI Policy step, NMI Orchestration and pre-Verification determines the measurement scheme according to the measurement policy generated by NMI Policy, and pre-verifies whether the measurement scheme is feasible.
  - \* Take busy time network measurement as an example, except for choosing of measurement schemes and contents, it also needs to determine whether the network is busy according to the current network state. In addition, this function performs automatic network deployment, such as in CLI mode.
- o Data Collection and Analytics.
  - \* In NMI, data collection and analysis should be based on the selected measurement scheme and the content to be measured that determined in previous steps, automatically realize the collection on demand, and generate corresponding data analysis results.
- o NMI Compliance Assessment.
  - \* At the end, this function verifies whether the results meets the requirement and whether the NMI is satisfied. If either of the two conditions is not satisfied, the NMI should be modified and re-enter the NMI Policy.

And the measurement flow diagram is shown as the following figure:



## 5. Concrete Examples

In this section, we will take SLA measurement intent as an example to illustrate each step of the process.

With the development of measurement technology in recent years, network measurement can be divided into active measurement, passive measurement and a combination of active and passive measurement. As mentioned above, no matter which measurement technology will occupy network resources. For example, if the transmission frequency of active measurement message is too fast, it will occupy too much bandwidth resources and affect the normal operation of actual business. While if the transmission frequency is too slow, some instantaneous network anomalies will be missed and the network status cannot be accurately reflected. Passive measurement requires real-time collection of actual business data. If the sampling rate is too high, a large amount of data will be accumulated in a short time. The analysis system for real-time analysis of these data needs strong processing capacity; if the sampling rate is too low, some network anomalies will also be omitted.

How to balance and accurately measure the network state, especially the abnormal network affecting the service, while occupying as little network bandwidth as possible, and the processing capacity of the

data analysis system is not high, this is the function that the NMI scheme based on IBN should realize.

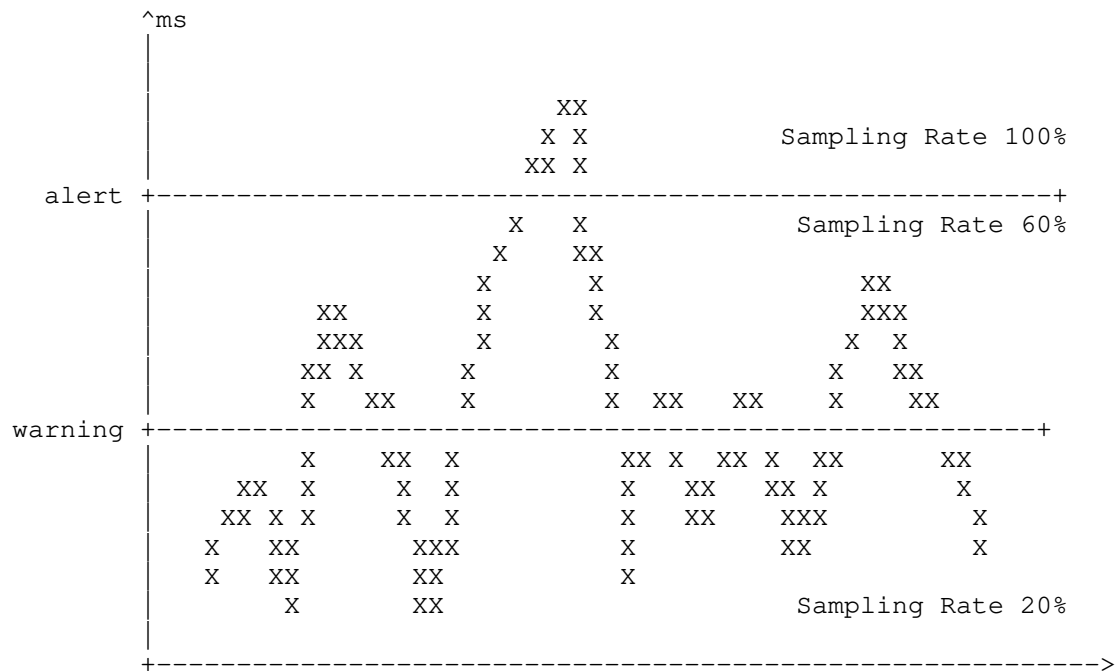
In this section, we will consider two examples to illustrate each step of the process.

#### 5.1. SLA measurement intent

Taking network SLA performance index -- time delay measurement as an example, the simple schematic diagram is as follows, different thresholds, warning value and alert value should be set for network delay in advance. When the delay value is below warning, the network is normal and the business is normal. When the delay is between warning value and alert value, the network fluctuation is abnormal, but the business is normal. When the delay exceeds the alert value, both the network and business are abnormal. For delay in different thresholds, different measurement strategies should be adopted:

- o When the network delay exceeds the alert value, or when the historical data predict that the delay will exceed the alert value, passive measurement requires 100% sampling of business data, and the transmission frequency of active measurement is modulated to the maximum. At the same time, the log and alarm data of the whole network equipment are collected to realize the most fine-grained measurement of the network, locate the root cause of the problem and repair the network in time.
- o When the network delay exceeds warning value but is lower than alert value, passive measurement samples 60% of business data, and the transmission message frequency of the active measurement is adjusted to the median value, and the running state data of some key devices in the network is collected synchronously.
- o When the network delay is less than warning value, passive measurement data is sampled at 20%, and active measurement message frequency is adjusted to the lowest, and the network equipment running state of key nodes can be collected as needed.





Based on the above SLA time delay index measurement, different thresholds adopt different measurement strategies, the concrete steps of SLA measurement intent are as follows:

- o In NMI Recognition and Acquisition, SLA measurement intent is recognized, and business requirements and performance metrics are identified by interacting with users. Then the NMI Recognition and Acquisition module inputs the SLA measurement intent into the NMI Translation module.
- o The NMI Translation module combines the SLA measurement intent with the measurement policy in NMI Policy, and outputs the executable measurement policy, such as the message transmission frequency of active measurement, the sampling rate of passive measurement, the collection range of equipment running state, etc.
- o The NMI Orchestration and pre-Verification module arranges the measurement policy into the specific configuration and execution time of each device in the tested network. The NMI Orchestration and pre-Verification module verifies the implementation of the policy in the equipment and preanalyzes the measurement results.
- o The Data Collection and Analysis module will collect the measurement data according to the requirements of the previous

step, make a simple analysis of the collected data, and then send the collected measurement data to the NMI Compliance Assessment module. After that, it feedback the measurement results to the user to complete the closed loop of the measurement task.

- o According to the change of delay data in the measured data, the NMI Compliance Assessment module notifies the NMI Orchestration and pre-Verification module to modify the execution time of the policy in time, and at the same time updates the measured results to the delay history database to improve the accuracy of delay prediction. The NMI Compliance Assessment module evaluates whether the actual measurement results are in line with the user's intent. If they are, the results will be fed back. If they are not, the NMI Policy module will be informed to adjust the policy, and then the measurement will be restarted.

## 5.2. Clustered performance measurement intent

The desired approach is to accurately measure the network state, especially when there are some issues affecting the service, but at the same time, reduce the resources to be employed to achieve the desired accuracy.

In this regard, the Clustered Alternate-Marking framework [RFC8889] adds flexibility to Performance Management (PM), because it can reduce the order of magnitude of the packet counters. This allows the NMI Orchestration and pre-Verification module to supervise, control, and manage PM in large networks.

RFC 8889 [RFC8889] introduces the concept of cluster partition of a network. The monitoring network can be considered as a whole or split into clusters that are the smallest subnetworks (group-to-group segments), maintaining the packet loss property for each subnetwork. The clusters can be combined in new connected subnetworks at different levels, forming new clusters, depending on the level of detail to achieve.

The clustered performance measurement intent represents the spatial accuracy, that is the size of the subnetworks to consider for the monitoring. It is possible to start without examining in depth and, in case of necessity, the "network zooming" approach can be used.

This approach called "network zooming" and can be performed in two different ways:

1. change the traffic filter and select more detailed flows;

2. activate new measurement points by defining more specified clusters.

The network-zooming approach implies that some filters, rules or flow identifiers are changed. But these changes must be done in a way that do not affect the performance. Therefore there could be a transient time to wait once the new network configuration takes effect. Anyway, if the performance issue is relevant, it is likely to last for a time much longer than the transient time.

The concrete steps of the clustered performance measurement intent are as follows:

- o In NMI Recognition and Acquisition, the clustered performance measurement intent is recognized. Then the NMI Recognition and Acquisition module inputs the clustered performance measurement intent into the NMI Translation module.
- o The NMI Translation module analyzes the clustered performance measurement intent and outputs the executable measurement policy, such as network partition and the spatial accuracy for the monitoring.
- o The NMI Orchestration and pre-Verification module arranges and calibrates the measurement with the specific configuration to split the whole network into clusters at different levels.
- o The Data Collection and Analysis module collects the measurement data from the different clusters, and then send these data to the NMI Compliance Assessment module. It verifies the performance for each cluster and send the measurement results to the user.
- o The NMI Compliance Assessment module, in case a cluster is experiencing a packet loss or the delay is high, notifies the NMI Orchestration and pre-Verification module to modify the cluster partition of the network for further investigation. The network configuration can be immediately modified in order to perform a new partition of the network but only for the cluster with bad performance. In this way, the problem can be localized with successive approximation up to a flow detailed analysis. This is the so-called "closed loop" performance management.

## 6. Classification of NMI

In this section, we divide the network measurement intent into static NMI and dynamic NMI according to different requirement characteristics.

### 6.1. Static NMI

Static NMI refers to the measurement purposes remain unchanged and is independent of the network state/external environment. Static NMI can be translated into determined network performance indicator values, such as concrete delay values, network bandwidth occupancy, throughput and so on.

Because the static NMI can be translated into the measurement of the determined network performance parameters, the whole process is relatively simple and error-prone, and only needs to verify whether the measurement results meet the requirements.

### 6.2. Dynamic NMI

Dynamic NMI refers to the measurement purpose remains unchanged but the measurement process changes dynamically according to the network state/external environment. Dynamic NMI can also be translated into the measurement of determined network performance parameters, however, the values of network performance parameters will change with the changes of network states and external environment.

For example, the measurement of busy network performances mentioned in the previous. Although the corresponding network parameters for judging whether the network is busy are determined, the corresponding network parameters have different values according to different network states and external environments.

Due to the dynamic nature of dynamic NMI, its processing process is more complex than static NMI. It is not only necessary to verify the accuracy of demand analysis, but also to verify whether the final measurement results meet the requirements.

## 7. Summary

This memo introduces the network measurement intent, and give two concrete examples to illustrate the process of network measurement intent. On the basis of existing intent drafts, this memo can be used as a use case for IBN. NMI is a big and typical use case of IBN, and the classification of different examples of NMI may vary.

## 8. Security Considerations

TBD.

## 9. IANA Considerations

This document has no requests to IANA.

## 10. References

### 10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC8889] Fioccola, G., Ed., Cociglio, M., Sapio, A., and R. Sisto, "Multipoint Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8889, DOI 10.17487/RFC8889, August 2020, <<https://www.rfc-editor.org/info/rfc8889>>.

### 10.2. Informative References

- [I-D.irtf-nmrg-ibn-concepts-definitions]  
Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", draft-irtf-nmrg-ibn-concepts-definitions-06 (work in progress), December 2021.
- [I-D.irtf-nmrg-ibn-intent-classification]  
Li, C., Havel, O., Olariu, A., Martinez-Julia, P., Nobre, J. C., and D. R. Lopez, "Intent Classification", draft-irtf-nmrg-ibn-intent-classification-06 (work in progress), February 2022.

## Authors' Addresses

Danyang Chen  
China Mobile  
Beijing 100053  
China

Email: [chendanyang@chinamobile.com](mailto:chendanyang@chinamobile.com)

Hongwei Yang  
China Mobile  
Beijing 100053  
China

Email: yanghongwei@chinamobile.com

Kehan Yao  
China Mobile  
Beijing 100053  
China

Email: yaokehan@chinamobile.com

Giuseppe Fioccola  
Huawei Technologies  
Riesstrasse, 25  
Munich 80992  
Germany

Email: giuseppe.fioccola@huawei.com

Internet Research Task Force  
Internet-Draft  
Intended status: Informational  
Expires: 6 September 2022

C. Zhou  
H. Yang  
X. Duan  
China Mobile  
D. Lopez  
A. Pastor  
Telefonica I+D  
Q. Wu  
Huawei  
M. Boucadair  
C. Jacquenet  
Orange  
5 March 2022

Digital Twin Network: Concepts and Reference Architecture  
draft-zhou-nmrg-digitaltwin-network-concepts-07

Abstract

Digital Twin technology has been seen as a rapid adoption technology in Industry 4.0. The application of Digital Twin technology in the networking field is meant to develop various rich network applications and realize efficient and cost effective data driven network management and accelerate network innovation.

This document presents an overview of the concepts of Digital Twin Network, provides the basic definitions and a reference architecture, lists a set of application scenarios, and discusses the benefits and key challenges of such technology.

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 <https://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 6 September 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
2.1. Acronyms & Abbreviations . . . . .	3
2.2. Definitions . . . . .	4
3. Introduction and Concepts of Digital Twin Network . . . . .	4
3.1. Background of Digital Twin . . . . .	4
3.2. Digital Twin for Networks . . . . .	5
3.3. Definition of Digital Twin Network . . . . .	6
4. Benefits of Digital Twin Network . . . . .	9
4.1. Optimized Network Total Cost of Operation . . . . .	10
4.2. Optimized Decision Making . . . . .	10
4.3. Safer Assessment of Innovative Network Capabilities . . . . .	10
4.4. Privacy and Regulatory Compliance . . . . .	11
4.5. Customized Network Operation Training . . . . .	11
5. Challenges to Build Digital Twin Network . . . . .	11
6. A Reference Architecture of Digital Twin Network . . . . .	13
7. Interaction with IBN . . . . .	16
8. Sample Application Scenarios . . . . .	17
8.1. Human Training . . . . .	17
8.2. Machine Learning Training . . . . .	17
8.3. DevOps-Oriented Certification . . . . .	18
8.4. Network Fuzzing . . . . .	18
9. Research Perspectives: A Summary . . . . .	18
10. Security Considerations . . . . .	18
11. Acknowledgements . . . . .	19
12. IANA Considerations . . . . .	19
13. Open issues . . . . .	19
14. Informative References . . . . .	20
Appendix A. Change Logs . . . . .	22
Authors' Addresses . . . . .	23



## 1. Introduction

The fast growth of network scale and the increased demand placed on these networks require them to accommodate and adapt dynamically to customer needs, implying a significant challenge to network operators. Indeed, network operation and maintenance are becoming more complex due to higher complexity of the managed networks and the sophisticated services they are delivering. As such, providing innovations on network technologies, management and operation will be more and more challenging due to the high risk of interfering with existing services and the higher trial costs if no reliable emulation platforms are available.

A Digital Twin is the real-time representation of a physical entity in the digital world. It has the characteristics of virtual-reality interrelation and real-time interaction, iterative operation and process optimization, full life-cycle and comprehensive data-driven network infrastructure. Currently, digital twin has been widely acknowledged in academic publications. See more in Section 3.

A digital twin for networks platform can be built by applying Digital Twin technologies to networks and creating a virtual image of physical network facilities (called herein, emulation). Basically, the digital twin for networks is an expansion platform of network simulation. The main difference compared to traditional network management systems is the interactive virtual-real mapping and data driven approach to build closed-loop network automation. Therefore, a digital twin network platform is more than an emulation platform or network simulator.

Through the real-time data interaction between the physical network and its twin network(s), the digital twin network platform might help the network designers to achieve more simplification, automatic, resilient, and full life-cycle operation and maintenance. More specifically, the digital twin network can, thus, be used to develop various rich network applications and assess specific behaviors (including network transformation) before actual implementation in the physical network, tweak the network for better optimized behavior, run 'what-if' scenarios that cannot be tested and evaluated easily in the physical network. In addition, service impact analysis tasks can also be facilitated.

## 2. Terminology

### 2.1. Acronyms & Abbreviations

IBN: Intent-Based Networking

IA: Artificial Intelligence

CI/CD: Continuous Integration / Continuous Delivery

ML: Machine Learning

OAM: Operations, Administration, and Maintenance

PLM: Product Lifecycle Management

## 2.2. Definitions

This document makes use of the following terms:

**Digital Twin:** a virtual instance of a physical system (twin) that is continually updated with the latter's performance, maintenance, and health status data throughout the physical system's life cycle.

**Digital twin network:** a digital twin that is used in the context of networking. This is also called, digital twin for networks. See more in Section 3.3.

## 3. Introduction and Concepts of Digital Twin Network

### 3.1. Background of Digital Twin

The concept of the "twin" dates to the National Aeronautics and Space Administration (NASA) Apollo program in the 1970s, where a replica of space vehicles on Earth was built to mirror the condition of the equipment during the mission [Rosen2015].

In 2003, Digital Twin was attributed to John Vickers by Michael Grieves in his product lifecycle management (PLM) course as "virtual digital representation equivalent to physical products" [Grieves2014]. Digital twin can be defined as a virtual instance of a physical system (twin) that is continually updated with the latter's performance, maintenance, and health status data throughout the physical system's life cycle [Madni2019]. By providing a living copy of physical system, digital twins bring numerous advantages, such as accelerated business processes, enhanced productivity, and faster innovation with reduced costs. So far, digital twin has been successfully applied in the fields of intelligent manufacturing, smart city, or complex system operation and maintenance to help with not only object design and testing, but also management aspects [Tao2019].

Compared with 'digital model' and 'digital shadow', the key difference of 'digital twin' is the direction of data between the physical and virtual systems [Fuller2020]. Typically, when using a digital twin, the (twin) system is generated and then synchronized using data flows in both directions between physical and digital components, so that control data can be sent, and changes between the physical and digital objectives and systems are automatically represented. This behavior is unlike a 'digital model' or 'digital shadow', which are usually synchronized manually, lacking of control data, and might not have a full cycle of data integrated.

At present (2022), there is no unified definition of digital twin framework. The industry, scientific research institutions, and standards developing organizations are trying to define a general or domain-specific framework of digital twin. [Natis-Gartner2017] proposed that building a digital twin of a physical entity requires four key elements: model, data, monitoring, and uniqueness. [Tao2019] proposed a five-dimensional framework of digital twin {PE, VE, SS, DD, CN}, in which PE represents physical entity, VE represents virtual entity, SS represents service, DD represents twin data, and CN represents the connection between various components. [ISO-2021] issued a draft standard for digital twin manufacturing system, and proposed a reference framework including data collection domain, device control domain, digital twin domain, and user domain.

### 3.2. Digital Twin for Networks

Communication networks can provide a solid foundation for implementing various 'digital twin' applications. At the same time, in the face of increasing business types, scale and complexity, a network itself also needs to use digital twin technology to seek better solutions beyond physical network. Since 2017, the application of digital twin technology in the field of communication networks has gradually been researched. Some examples are listed below.

In academy, [Dong2019] established the digital twin of 5G mobile edge computing (MEC) network, used the twin offline to train the resource allocation optimization and normalized energy-saving algorithm based on reinforcement learning, and then updated the scheme to MEC network. [Dai2020] established a digital twin edge network for mobile edge computing system, in which a twin edge server is used to evaluate the state of entity server, and the twin mobile edge computing system provides data for training offloading strategy. [Nguyen2021] discusses how to deploy a digital twin for complex 5G networks. [Hong2021] presents a digital twin platform towards automatic and intelligent management for data center networks, and then proposes a simplified the workflows of network service

management. In addition, international workshops dedicated to digital twin in network field have already appeared, such as IEEE DTPI 2021 - Digital Twin Network Online Session [DTPI2021], or are being proposed such as IEEE NOMS 2022 - TNT workshop [TNT2022].

Although the application of digital twin technology in networking has started, the research of digital twin for networks technology is still in its infancy. Current applications focus on specific scenarios (such as network optimization), where network digital twin is just used as a network simulation tool to solve the problem of network operation and maintenance. Combined with the characteristics of digital twin technology and its application in other industries, this document believes that digital twin network can be regarded as an organic whole of the overall network system and become a general architecture involving the whole life cycle of physical network in the future, serving the application of network innovative technologies such as network planning, construction, maintenance and optimization, improving the automation and intelligence level of the network.

### 3.3. Definition of Digital Twin Network

So far, there is no standard definition of "digital twin network" within the networking industry. This document defines "digital twin network" as a virtual representation of the physical network. Such virtual representation of the network is meant to be used to analyze, diagnose, emulate, and then control the physical network based on data, models, and interfaces. To that aim, a real-time and interactive mapping is required between the physical network and its virtual twin network.

Referring the characteristics of digital twin in other industries and the characteristics of the networking itself, the digital twin network should involve four key elements: data, mapping, models and interfaces as shown in Figure 1.

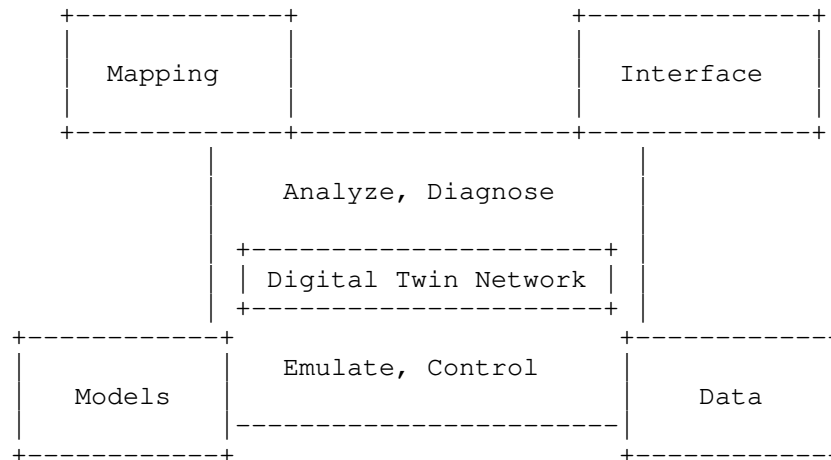


Figure 1: Key Elements of Digital Twin Network

**Data:** A digital twin network should maintain historical data and/or real time data (configuration data, operational state data, topology data, trace data, metric data, process data, etc.) about its real-world twin (i.e. physical network) that are required by the models to represent and understand the states and behaviors of the real-world twin.

The data is characterized as the single source of "truth" and populated in the data repository, which provides timely and accurate data service support for building various models.

**Models:** Techniques that involve collecting data from one or more sources in the real-world twin and developing a comprehensive representation of the data (e.g., system, entity, process) using specific models. These models are used as emulation and diagnosis basis to provide dynamics and elements on how the live physical network operates and generates reasoning data utilized for decision-making.

Various models such as service models, data models, dataset models, or knowledge graph can be used to represent the physical network assets and, then, instantiated to serve various network applications.

**Interfaces:** Standardized interfaces can ensure the interoperability of digital twin network. There are two major types of interfaces:

- \* The interface between the digital twin network platform and the physical network infrastructure.

- \* The interface between digital twin network platform and applications.

The former provides real-time data collection and control on the physical network. The latter helps in delivering application requests to the digital twin network platform and exposing the various platform capabilities to applications.

**Mapping:** Used to identify the digital twin and the underlying entities and establish a real-time interactive relation between the physical network and the twin network or between two twin networks. The mapping can be:

- \* One to one (pairing, vertical): Synchronize between a physical network and its virtual twin network with continuous flows.
- \* One to many (coupling, horizontal): Synchronize among virtual twin networks with occasional data exchange.

Such mappings provide a good visibility of actual status, making the digital twin suitable to analyze and understand what is going on in the physical network. It also allows using the digital twin to optimize the performance and maintenance of the physical network.

The digital twin network constructed based on the four core technology elements can analyze, diagnose, emulate, and control the physical network in its whole life cycle with the help of optimization algorithms, management methods, and expert knowledge. One of the objectives of such control is to master the digital twin network environment and its elements to derive the required system behavior, e.g., provide:

- \* repeatability: that is the capacity to replicate network conditions on-demand.
- \* reproducibility: i.e., the ability to replay successions of events, possibly under controlled variations.

Note: Real-time interaction is not always mandatory for all twins. When testing some configuration changes or trying some innovative techniques, the digital twins can behave as a simulation platform without the need of real time telemetry data. And even in this scenario, it is better to have interactive mapping capability so that the validated changes can be tested in real network whenever required by the testers. In most other cases (e.g., network optimization, network fault recovery), real-time interaction between virtual and real network is mandatory. This way, digital twin network can help achieve the goal of autonomous network or self-driven network.

#### 4. Benefits of Digital Twin Network

Digital twin network can help enabling closed-loop network management across the entire lifecycle, from deployment and emulation, to visualized assessment, physical deployment, and continuous verification. By doing so, network operators and end-users to some extent, as allowed by specific application interfaces, can maintain a global, systemic, and consistent view of the network. Also, network operators and/or enterprise user can safely exercise the enforcement of network planning policies, deployment procedures, etc., without jeopardizing the daily operation of the physical network.

The main difference between digital twin network and simulation platform is the use of interactive virtual-real mapping to build closed-loop network automation. Simulation platforms are the predecessor of the digital twin network, one example of such a simulation platform is network simulator [NS-3], which can be seen as a variant of digital twin network but with low fidelity and lacking for interactive interfaces to the real network. Compared with those classical approaches, key benefits of digital twin network can be summarized as follows:

- 1) Using real-time data to establish high fidelity twins, the effectiveness of network simulation is higher; then the simulation cost will be relatively low.
- 2) The impact and risk on running networks is low when automatically applying configuration/policy changes after the full analysis and required verifications (e.g., service impact analysis) within the twin network.
- 3) The faults of the physical network can be automatically captured by analyzing real-time data, then the correction strategy can be distributed to the physical network elements after conducting adequate analysis within the twins to complete the closed-loop automatic fault repair.

The following subsections further elaborate such benefits in details.

#### 4.1. Optimized Network Total Cost of Operation

Large scale networks are complex to operate. Since there is no effective platform for simulation, network optimization designs have to be tested on the physical network at the cost of jeopardizing its daily operation and possibly degrading the quality of the services supported by the network. Such assessment greatly increases network operator's Operational Expenditure (OPEX) budgets too.

With a digital twin network platform, network operators can safely emulate candidate optimization solutions before deploying them in the physical network. In addition, operator's OPEX on the real physical network deployment will be greatly decreased accordingly at the cost of the complexity of the assessment and the resources involved.

#### 4.2. Optimized Decision Making

Traditional network operation and management mainly focus on deploying and managing running services, but hardly support predictive maintenance techniques.

Digital twin network can combine data acquisition, big data processing, and AI modeling to assess the status of the network, but also to predict future trends, and better organize predictive maintenance. The ability to reproduce network behaviors under various conditions facilitates the corresponding assessment of the various evolution options as often as required.

#### 4.3. Safer Assessment of Innovative Network Capabilities

Testing a new feature in an operational network is not only complex, but also extremely risky. Service impact analysis is required to be adequately achieved prior to effective activation of a new feature.

Digital twin network can greatly help assessing innovative network capabilities without jeopardizing the daily operation of the physical network. In addition, it helps researchers to explore network innovation (e.g., new network protocols, network AI/ML applications) efficiently, and network operators to deploy new technologies quickly with lower risks. Take AI/ ML application as example, it is a conflict between the continuous high reliability requirement (i.e., 99.999%) and the slow learning speed or phase-in learning steps of AI/ML algorithms. With digital twin network, AI/ML can complete the learning and training with the sufficient data before deploying the model in the real network. This would encourage more network AI innovations in future networks.



#### 4.4. Privacy and Regulatory Compliance

The requirements on data confidentiality and privacy on network providers increase the complexity of network management, as decisions made by computation logics such as an SDN controller may rely upon the packet payloads. As a result, the improvement of data-driven management requires complementary techniques that can provide a strict control based upon security mechanisms to guarantee data privacy protection and regulatory compliance. This may range from flow identification (using the archetypal five-tuple of addresses, ports and protocol) to techniques requiring some degree of payload inspection, all of them considered suitable to be associated to an individual person, and hence requiring strong protection and/or data anonymization mechanisms.

With strong modeling capability provided by the digital twin network, very limited real data (if at all) will be needed to achieve similar or even higher level of data-driven intelligent analysis. This way, a lower demand of sensitive data will permit to satisfy privacy requirements and simplify the use of privacy-preserving techniques for data-driven operation.

#### 4.5. Customized Network Operation Training

Network architectures can be complex, and their operation requires expert personnel. Digital twin network offers an opportunity to train staff for customized networks and specific user needs. Two salient examples are the application of new network architectures and protocols or the use of "cyber-ranges" to train security experts in threat detection and mitigation.

### 5. Challenges to Build Digital Twin Network

According to [Hu2021], the main challenges in building and maintaining digital twins can be summarized as the following five aspects:

- \* Data acquisition and processing
- \* High-fidelity modeling
- \* Real-time, two-way connection between the virtual and the real twins
- \* Unified development platform and tools
- \* Environmental coupling technologies

Compared with other industrial fields, digital twin in networking field has its unique characteristics. On one hand, network elements and system have higher level of digitalization, which implies that data acquisition and virtual-real connection are relatively easy to achieve. On the other hand, there are many kinds of network elements and topologies in the network field; and the complex giant system of network carries a variety of business services. So, the construction of a digital twin network system needs to consider the following major challenges:

**Large scale challenge:** A digital twin of large-scale networks will significantly increase the complexity of data acquisition and storage, the design and implementation of relevant models. The requirements of software and hardware of the digital twin network system will be even more constraining. Therefore, efficient and low cost tools in various fields should be required. Take data as an example, massive network data can help achieve more accurate models. However, to lower the cost of virtual-real communication and data storage, efficient tools on data collection and data compression methods must be used.

**Interoperability:** Due to the inconsistency of technical implementations and the heterogeneity of vendor technologies, it is difficult to establish a unified digital twin network system with a common technology in a network domain. Therefore, it is needed firstly to propose a unified architecture of digital twin network, in which all components and functionalities are clear to all stakeholders; then define standardized and unified interfaces to connect all network twins via ensuring necessary compatibility.

**Data modeling difficulties:** Based on large-scale network data, data modeling should not only focus on ensuring the accuracy of model functions, but also has to consider the flexibility and scalability to compose and extend as required to support large scale and multi-purpose applications. Balancing these requirements further increases the complexity of building efficient and hierarchical functional data models. As an optional solution, straightforwardly clone the real network using virtualized resources is feasible to build the twin network when the network scale is relatively small. However, it will be of unaffordable resource cost for larger scales network. In this case, network modeling using mathematical abstraction or leveraging the AI algorithms will be more suitable solutions.

**Real-time requirements:** Network services normally have real-time requirements, the processing of model simulation and verification through a digital twin network will increase the service latency. Meanwhile, the real-time requirements will further increase

performance requirements on the system software and hardware. Moreover, it is also challenge to keep network digital twins in sync given the nature of distributed systems and propagation delays. To address these requirements, the function and process of the data model need to be based on automated processing mechanism under various network application scenarios. On the one hand, it is needed to design a simplified process to reduce the time cost for tasks in network twin as much as possible; on the other hand, it is recommended to define the real-time requirements of different applications, and then match the corresponding computing resources and suitable solutions as needed to complete the task processing in the twin.

Security risks: A digital twin network has to synchronize all or subset of the data related to involved physical networks in real time, which inevitably augments the attack surface, with a higher risk of information leakage, in particular. On one hand, it is mandatory to design more secure data mechanism leveraging legacy data protection methods, as well as innovative technologies such as block chain. On the other hand, the system design can limit the data (especially raw data) requirement on building digital twin network, leveraging innovative modeling technologies such as federal learning.

In brief, to address the above listed challenges, it is important to firstly propose a unified architecture of digital twin network, which defines the main functional components and interfaces (Section 6). Then, relying upon such an architecture, it is required to continue researching on the key enabling technologies including data acquisition, data storage, data modeling, interface standardization, and security assurance.

## 6. A Reference Architecture of Digital Twin Network

Based on the definition of the key digital twin network technology elements introduced in Section 3.3, a digital twin network architecture is depicted in Figure 2. This digital twin network architecture is broken down into three layers: Application Layer, Digital Twin Layer, and Physical Network Layer.

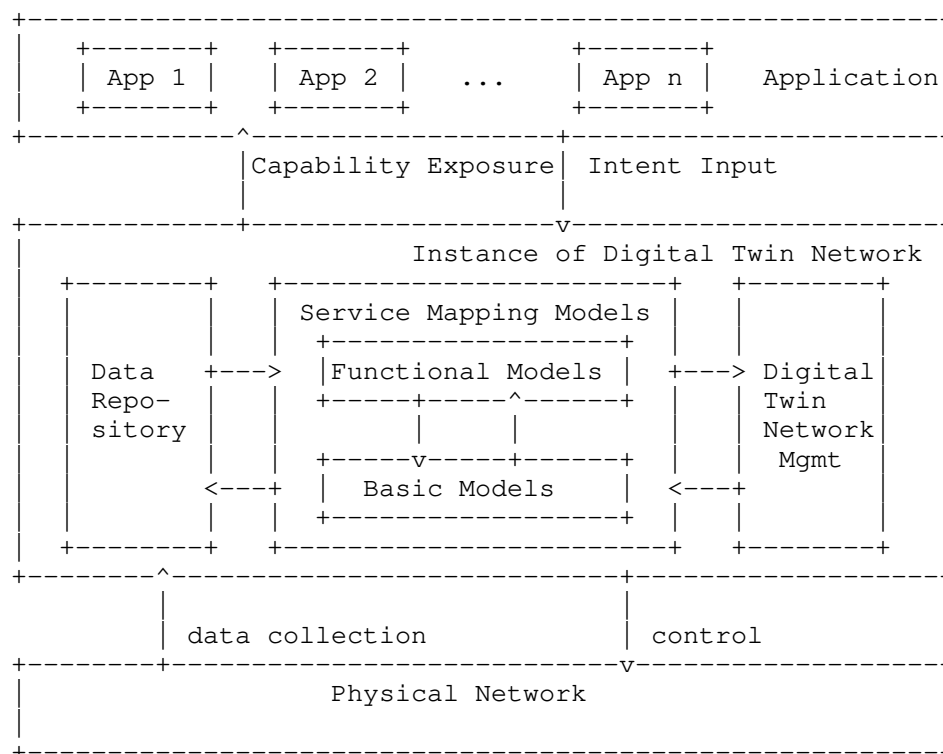


Figure 2: Reference Architecture of Digital Twin Network

**Physical Network:** All or subset of network elements in the physical network exchange network data and control messages with a network digital twin instance, through twin-physical control interfaces. The physical network can be a mobile access network, a transport network, a mobile core, a backbone, etc. The physical network can also be a data center network, a campus enterprise network, an industrial Internet of Things, etc.

The physical network can span across a single network administrative domain or multiple network administrative domains.

This document focuses on the IETF related physical network such as IP bearer network and datacenter network.

**Digital Twin Layer:** This layer includes three key subsystems: Data Repository subsystem, Service Mapping Models subsystem, and Digital Twin Network Management subsystem.

One or multiple digital twin network instances can be built and maintained:

- \* Data Repository subsystem is responsible for collecting and storing various network data for building various models by collecting and updating the real-time operational data of various network elements through the twin southbound interface, and providing data services (e.g., fast retrieval, concurrent conflict handling, batch service) and unified interfaces to Service Mapping Models subsystem.
- \* Service Mapping Models complete data modeling, provide data model instances for various network applications, and maximizes the agility and programmability of network services. The data models include two major types: basic and functional models.
  - Basic models refer to the network element model(s) and network topology model(s) of the network digital twin based on the basic configuration, environment information, operational state, link topology and other information of the network element(s), to complete the real-time accurate characterization of the physical network.
  - Functional models refer to various data models used for network analysis, emulation, diagnosis, prediction, assurance, etc. The functional models can be constructed and expanded by multiple dimensions: by network type, there can be models serving for a single or multiple network domains; by function type, it can be divided into state monitoring, traffic analysis, security exercise, fault diagnosis, quality assurance and other models; by network lifecycle management, it can be divided into planning, construction, maintenance, optimization and operation. Functional models can also be divided into general models and special-purpose models. Specifically, multiple dimensions can be combined to create a data model for more specific application scenarios.

New applications might need new functional models that do not exist yet. If a new model is needed, 'Service Mapping Models' subsystem will be triggered to help creating new models based on data retrieved from 'Data Repository'.

- \* Digital Twin Network Management fulfils the management function of digital twin network, records the life-cycle transactions of the twin entity, monitors the performance and resource consumption of the twin entity or even of individual models, visualizes and controls various elements of the network digital twin, including topology management, model management and security management.

Notes: 'Data collection' and 'change control' are regarded as southbound interfaces between virtual and physical network. From implementation perspective, they can optionally form a sub-layer or sub-system to provide common functionalities of data collection and change control, enabled by a specific infrastructure supporting bi-directional flows and facilitating data aggregation, action translation, pre-processing and ontologies.

Application Layer: Various applications (e.g., Operations, Administration, and Maintenance (OAM)) can effectively run over a digital twin network platform to implement either conventional or innovative network operations, with low cost and less service impact on real networks. Network applications make requests that need to be addressed by the digital twin network. Such requests are exchanged through a northbound interface, so they are applied by service emulation at the appropriate twin instance(s).

## 7. Interaction with IBN

Implementing Intent-Based Networking (IBN) is an innovative technology for life-cycle network management. Future networks will be possibly Intent-based, which means that users can input their abstract 'intent' to the network, instead of detailed policies or configurations on the network devices.

[I-D.irtf-nmrg-ibn-concepts-definitions] clarifies the concept of "Intent" and provides an overview of IBN functionalities. The key characteristic of an IBN system is that user intent can be assured automatically via continuously adjusting the policies and validating the real-time situation.

IBN can be envisaged in a digital twin network context to show how digital twin network improves the efficiency of deploying network innovation. To lower the impact on real networks, several rounds of adjustment and validation can be emulated on the digital twin network platform instead of directly on physical network. Therefore, digital twin network can be an important enabler platform to implement IBN systems and speed up their deployment.

## 8. Sample Application Scenarios

Digital twin network can be applied to solve different problems in network management and operation.

### 8.1. Human Training

The usual approach to network OAM with procedures applied by humans is open to errors in all these procedures, with impact in network availability and resilience. Response procedures and actions for most relevant operational requests and incidents are commonly defined to reduce errors to a minimum. The progressive automation of these procedures, such as predictive control or closed-loop management, reduce the faults and response time, but still there is the need of a human-in-the-loop for multiples actions. These processes are not intuitive and require training to learn how to respond.

The use of digital twin network for this purpose in different network management activities will improve the operators performance. One common example is cybersecurity incident handling, where "cyber-range" exercises are executed periodically to train security practitioners. Digital twin network will offer realistic environments, fitted to the real production networks.

### 8.2. Machine Learning Training

Machine Learning requires data and their context to be available in order to apply it. A common approach in the network management environment has been to simulate or import data in a specific environment (the ML developer lab), where they are used to train the selected model, while later, when the model is deployed in production, re-train or adjust to the production environment context. This demands a specific adaption period.

Digital twin network simplifies the complete ML lifecycle development by providing a realistic environment, including network topologies, to generate the data required in a well-aligned context. Dataset generated belongs to the digital twin network and not to the production network, allowing information access by third parties, without impacting data privacy.

### 8.3. DevOps-Oriented Certification

The potential application of CI/CD models network management operations increases the risk associated to deployment of non-validated updates, what conflicts with the goal of the certification requirements applied by network service providers. A solution for addressing these certification requirements is to verify the specific impacts of updates on service assurance and SLAs using a digital twin network environment replicating the network particularities, as a previous step to production release.

Digital twin network control functional block supports such dynamic mechanisms required by DevOps procedures.

### 8.4. Network Fuzzing

Network management dependency on programmability increases systems complexity. The behavior of new protocol stacks, API parameters, and interactions among complex software components are examples that imply higher risk to errors or vulnerabilities in software and configuration.

Digital twin network allows to apply fuzzing testing techniques on a twin network environment, with interactions and conditions similar to the production network, permitting to identify and solve vulnerabilities, bugs and zero-days attacks before production delivery.

## 9. Research Perspectives: A Summary

Research on digital twin network has just started. This document presents an overview of the digital twin network concepts and reference architecture. Looking forward, further elaboration on digital twin network scenarios, requirements, architecture, and key enabling technologies should be investigated by the industry, so as to accelerate the implementation and deployment of digital twin network.

## 10. Security Considerations

This document describes concepts and definitions of digital twin network. As such, the following security considerations remain high level, i.e., in the form of principles, guidelines or requirements.

Security considerations of the digital twin network include:

- \* Secure the digital twin system itself.



- \* Data privacy protection.

Securing the digital twin network system aims at making the digital twin system operationally secure by implementing security mechanisms and applying security best practices. In the context of digital twin network, such mechanisms and practices may consist in data verification and model validation, mapping operations between physical network and digital counterpart network by authenticated and authorized users only.

Synchronizing the data between the physical and the digital twin networks may increase the risk of sensitive data and information leakage. Strict control and security mechanisms must be provided and enabled to prevent data leaks.

## 11. Acknowledgements

Many thanks to the NMRG participants for their comments and reviews. Thanks to Daniel King, Quifang Ma, Laurent Ciavaglia, Jerome Francois, Jordi Paillisse, Luis Miguel Contreras Murillo, Alexander Clemm, Qiao Xiang, Ramin Sadre, Pedro Martinez-Julia, Wei Wang, Zongpeng Du, and Peng Liu.

Diego Lopez and Antonio Pastor were partly supported by the European Commission under Horizon 2020 grant agreement no. 833685 (SPIDER), and grant agreement no. 871808 (INSPIRE-5Gplus).

## 12. IANA Considerations

This document has no requests to IANA.

## 13. Open issues

- \* The draft focuses on concept and architecture of digital twin network, not including enabling technologies. Actually, each 'enabling technology' is worth of a separate draft to study in details in future. A decision is needed that whether to add a section to describe the enabling technologies in brief.
- \* Related to above issue, if section of enabling technologies is added, recent technologies (e.g. Network connectivity, Real-time data communication, Collaboration management, conflict detection and resolution, etc.) recently discussed in the IRTF/IETF should be described.
- \* In section of 'Sample Application Scenarios', to dig deeper into one or two use cases.

- \* On the research side, the idea behind digital twin networks is reminiscent of earlier work from the 1990s that should be referenced/acknowledged. Examples include the Shadow MIB concept, Inductive Modeling Technique, etc.

#### 14. Informative References

- [Dai2020] Dai, Y. Dai., Zhang, K. Zhang., Maharjan, S. Maharjan., and Yan Zhang. Zhang, "Deep Reinforcement Learning for Stochastic Computation Offloading in Digital Twin Networks. IEEE Transactions on Industrial Informatics, vol. 17, no. 17", August 2020.
- [Dong2019] Dong, R. Dong., She, C. She., HardjawanaLiu, W. Hardjawana., Li, Y. Li., and B. Vucetic. Vucetic, "Deep Learning for Hybrid 5G Services in Mobile Edge Computing Systems: Learn from a Digital Twin. IEEE Transactions on Wireless Communications, vol. 18, no. 10", July 2019.
- [DTPI2021] "IEEE International Conference on Digital Twins and Parallel Intelligence - Digital Twin Network Session, <https://www.dtpi.org/video/10>", July 2021.
- [Fuller2020] Fuller, A. Fuller., Fan, Z., Day, C., and C. Barlow, "Digital Twin: Enabling Technologies, Challenges and Open Research," in IEEE Access, vol. 8, pp. 108952-108971", 2020.
- [Grieves2014] Grieves, M. Grieves., "Digital twin: Manufacturing excellence through virtual factory replication", 2003, <<https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf>>.
- [Hong2021] Hong, H., Wu, Q., Dong, F., Song, W., Sun, R., Han, T., Zhou, C., and H. Yang, "NetGraph: An Intelligent Operated Digital Twin Platform for Data Center Networks. In ACM SIGCOMM 2021 Workshop on Network-Application Integration (NAI' 21), Virtual Event, USA. ACM, New York, NY, USA", 2021.
- [Hu2021] Hu, W., Zhang, T., Deng, X., Liu, Z., and J. Tan, "Digital twin: a state-of-the-art review of its enabling technologies, applications and challenges. Journal of Intelligent Manufacturing and Special Equipment, Vol. 2 No. 1, pp. 1-34", 2021.

- [I-D.irtf-nmrg-ibn-concepts-definitions]  
Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", Work in Progress, Internet-Draft, draft-irtf-nmrg-ibn-concepts-definitions-06, 15 December 2021, <<https://www.ietf.org/archive/id/draft-irtf-nmrg-ibn-concepts-definitions-06.txt>>.
- [ISO-2021] ISO, "Digital Twin manufacturing framework - Part 2: Reference architecture: ISO/CD 23247-2. <https://www.iso.org/standard/78743.html>", 2021.
- [Madni2019]  
Madni, A. Madni., Madni, C. Madni., and S. Lucero. Lucero, "Leveraging digital twin technology in model-based systems engineering. Systems, vol. 7, no. 1, p. 7", January 2019.
- [Natis-Gartner2017]  
Natis, Y. Natis., Velosa, A. Velosa., and W. R. Schulte. Schulte, "Innovation insight for digital twins - driving better IoT-fueled decisions. <https://www.gartner.com/en/documents/3645341>", 2017.
- [Nguyen2021]  
Nguyen, H. X. Nguyen., Trestian, R. Trestian., To, D. To., and M. Tatipamula. Tatipamula, "Digital Twin for 5G and Beyond. IEEE Communications Magazine, vol. 59, no. 2", February 2021.
- [NS-3] "Network Simulator, NS-3. <https://www.nsnam.org/>".
- [Roson2015]  
Rosen, R. Rosen., Wichert, G. Von Wichert., Lo, G. Lo., and K.D. Bettenhausen. Bettenhausen, "About the importance of autonomy and DTs for the future of manufacturing. IFAC-Papersonline, Vol. 48, pp. 567-572.", 2015.
- [Tao2019] Tao, F. Tao., Zhang, H. Zhang., Liu, A. Liu., and A. Y. C. Nee. Nee, "Digital Twin in Industry: State-of-the-Art. IEEE Transactions on Industrial Informatics, vol. 15, no. 4.", April 2019.
- [TNT2022] "IEEE International workshop on Technologies for Network Twins, <https://sites.google.com/view/tnt-2022/>", 2022.

## Appendix A. Change Logs

v06 - v07: Addressed reviewer's comments from adoption call, including below major changes.

- \* Resequenced the sections via adding more subsections on concepts of digital twin network, removing the 'Requirements Language' section, and moving ahead the 'Challenges' section.
- \* Cited more papers, or industrial information on digital twin concepts and digital twin for networks.
- \* Added more information on describing the challenges and key characteristics digital twin network.
- \* Removed previous open issue on investigating related digital twin network work and identify the differences and commonalities, and added several new open issues for future studys.
- \* Other Editorial changes.

v05 - v06: Addressed comments form meeting and maillist, to request adoptoin call.

- \* Remove acronym DTN to avoid conflict with 'Delay Tolerant Network';
- \* Elaborate the descriptoin of Digital Twin Network architecture that supports multiple instances;
- \* Other Editorial changes.

04 - v05

- \* Clarify the difference between digital twin network platform and traditional network management system;
- \* Add more references of researches on applying digital twin to network field;
- \* Clarify the benefit of 'Privacy and Regulatory Compliance';
- \* Refine the description of reference architecture;
- \* Other Editorial changes.

v03 - v04

- \* Update data definition and models definitions to clarify their difference.
- \* Remove the orchestration element and consolidated into control functionality building block in the digital twin network.
- \* Clarify the mapping relation (one to one, and one to many) in the mapping definition.
- \* Add explanation text for continuous verification.

v02 - v03

- \* Split interaction with IBN part as a separate section.
- \* Fill security section;
- \* Clarify the motivation in the introduction section;
- \* Use new boilerplate for requirements language section;
- \* Key elements definition update.
- \* Other editorial changes.
- \* Add open issues section.
- \* Add section on application scenarios.

#### Authors' Addresses

Cheng Zhou  
China Mobile  
Beijing  
100053  
China  
Email: zhouchengyjy@chinamobile.com

Hongwei Yang  
China Mobile  
Beijing  
100053  
China  
Email: yanghongwei@chinamobile.com

Xiaodong Duan  
China Mobile  
Beijing  
100053  
China  
Email: duanxiaodong@chinamobile.com

Diego Lopez  
Telefonica I+D  
Seville  
Spain  
Email: diego.r.lopez@telefonica.com

Antonio Pastor  
Telefonica I+D  
Madrid  
Spain  
Email: antonio.pastorperales@telefonica.com

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

Mohamed Boucadair  
Orange  
Rennes 35000  
France  
Email: mohamed.boucadair@orange.com

Christian Jacquenet  
Orange  
Rennes 35000  
France  
Email: christian.jacquenet@orange.com