IETF-125 NMRG Meeting

Use Cases and Practices for Intent-Based Networking (draft-irtf-nmrg-ibn-usecases-03)

March 16, 2026
Shenzhen in China

Kehan Yao, Danyang Chen, Jaehoon Paul Jeong, Qin Wu,
Chungang Yang, Luis M. Contreras, and Giuseppe Fioccola

Major Updates of from 02 Version to 03 Version

- Version-03: draft-irtf-nmrg-ibn-usecases-03
  - https://datatracker.ietf.org/doc/draft-irtf-nmrg-ibn-usecases/

- This version has addressed all the remaining comments of Jérôme Francois (NMRG Chair) during the RG adoption call (November 26, 2024).

Major Updates between 02 Version and 03 Version

Table of Contents

Table of Contents

Jerome's Comments (1/3)

- Adding References to technologies mentioned in Section 2 (A Methodology for Building IBN Systems)
  - This is done.
- Usage of IBN Methodology in Section 2 for Use Cases in Section 3
  - This is done.
  - Section 3.9 (IBN Methodology Usage on IBN Use Cases) is added to specify which methodology steps are used for each use case.
- Self-contained Explanation for Each Use Case
  - This is done.
  - Some drafts will be developed as separate documents.

3.9. IBN Methodology Usage on IBN Use Cases

This section analyzes how the IBN methodology is applied to each IBN use case in Section 3. Figure 15 shows a table for the IBN methodology analysis for IBN use cases in Section 3. In the table, C1 through C8 represent the construction numbers of IBN the construction of an IBN system in Section 2.2. The "X" in the table refers to a construction number supported by each IBN use case, such as C1: Intent Translation, C2: Policy Translation, C3: Policy Verification, C4: Policy Deployment, C5: Policy Monitoring, C6: Policy Validation, C7: Policy Optimization, and C8: Intent Report.

Section Number	Use Case	Construction Number							
		C1	C2	C3	C4	C5	C6	C7	C8
3.1.1	IBN for Service Function Chaining	X	X	X	X	X	X		
3.1.2	IBN for SRv6 Networks		X	X	X	X	X	X	X
3.2	IBN for Guaranteeing SLA		X	X	X	X	X	X	
3.3	IBN for Cloud-Based Security System		X	X	X	X	X	X	X
3.4	IBN for IoT Device Management in 5G		X	X	X	X	X	X	X
3.5	IBN for Sofware-Defined Vehicle	X	X	X	X	X	X	X	X
3.6	IBN for Interconnection	X	X	X	X	X	X	X	X
3.7	IBN for IETF Network Slices	X	X	X	X	X	X	X	X
3.8	IBN for Green Service Management	X	X	X	X	X	X	X	X

Figure 15: IBN Methodology Analysis for IBN Use Cases

Jerome's Comments (2/3)

- Relation between RFC9315 (concepts) and IBN System in Section 2
  - This is done.
  - Section 2.3 (Mapping between IBN System and Intent Life Cycle) is added.
- Relation with RFC9316 (Taxonomy) and IBN Use Cases in Section 3
  - This is done.
  - Section 3.10 (Intent Taxonomy Usage on IBN Use Cases) is added to specify what types the intent taxonomy components of each use case are.
- Enhancement of Section 4 (Practice Learnings) Section
  - This is done.
  - Added Cloud-Based Security System with I2NSF as another use case for learnings with numerical or qualitative results along with SFC use case.

3.10. Intent Taxonomy Usage on IBN Use Cases

This section analyzes how the intent taxonomy in [RFC9316] can be applied to each use case in Section 3. Figure 16 shows a diagram of Intent Taxonomy for the IBN Methodology Analysis for IBN use cases in Section 3. In this diagram, an Intent has seven intent components as follows:

* A: Intent Solution
* B: Intent User Type
* C: Intent Type
* D: Intent Scope
* E: Network Scope
* F: Abstraction
* G: Life Cycle

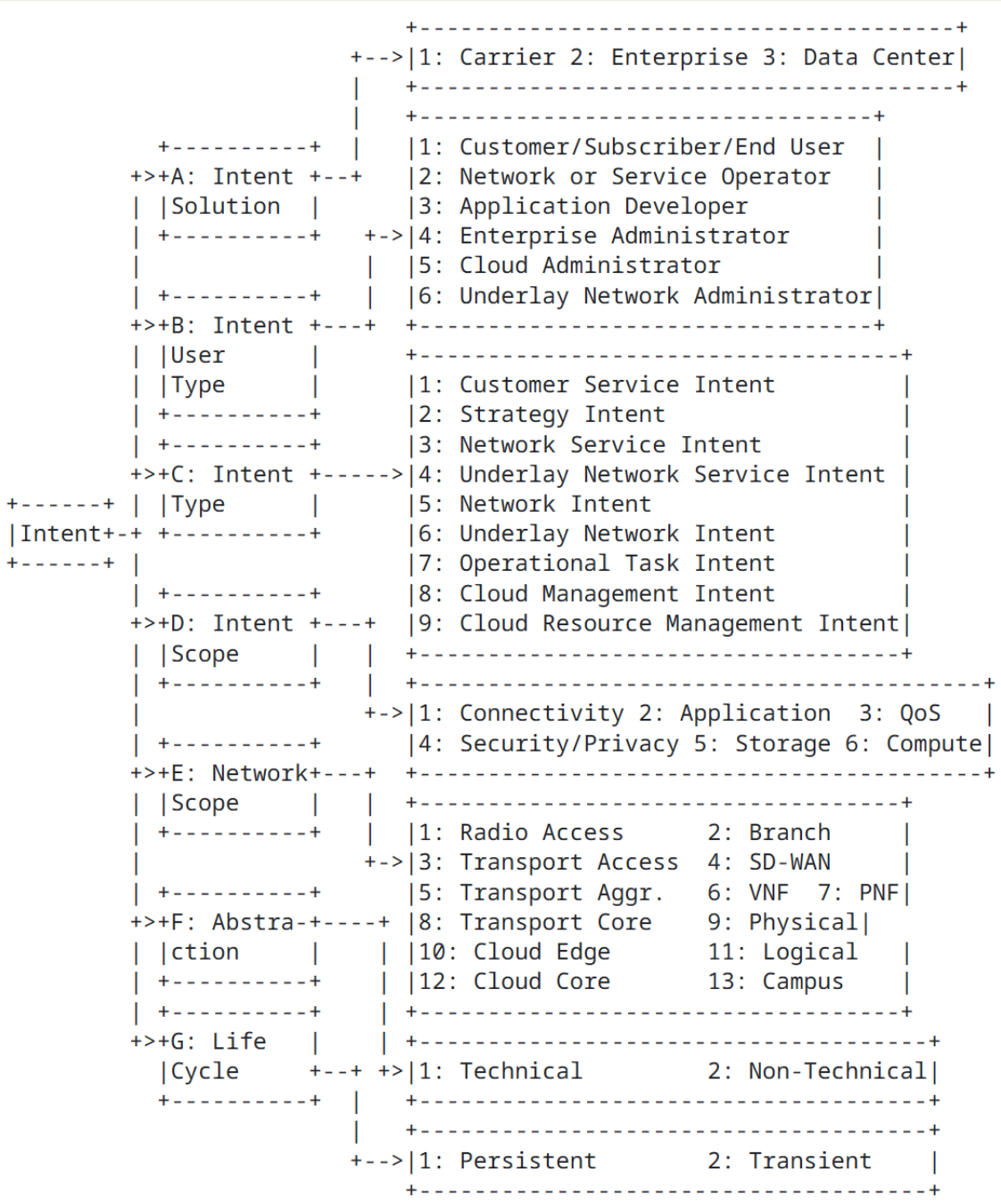


Figure 16: Intent Taxonomy

For the other use cases in Figure 17, the intent taxonomy per use case can be interpreted in the same way with the above use case of "IBN for Service Function Chaining".

Section Number	Use Case	Intent Taxonomy A	B	C	D	E	F	G
3.1.1	IBN for Service Function Chaining	1	2	3	2	4	1	1
3.1.2	IBN for SRv6 Networks	1	6	6	1	8	1	1
3.2	IBN for Guaranteeing SLA	2	4	5	3	4	1	1
3.3	IBN for Cloud-Based Security System	2	4	3	4	10	2	1
3.4	IBN for IoT Device Management in 5G	2	1	1	2	6	2	2
3.5	IBN for Sofware-Defined Vehicle	2	3	1	2	6	2	1
3.6	IBN for Interconnection	1	2	3	2	3	1	1
3.7	IBN for IETF Network Slices	1	6	6	3	4	1	1
3.8	IBN for Green Service Management	2	1	1	2	9	2	1

Figure 17: Intent Taxonomy Analysis for IBN Use Cases

Second, Cloud-Based Security System (called CBSS) in Section 3.3 showed the following three challenges:

1. Security Intent Translation: A natural-language security intent needs to be translated into a high-level security policy according to the I2NSF Consumer-Facing YANG Data Model [I-D.ietf-i2nsf-consumer-facing-interface-dm]. This intent translation should use the syntax of the YANG data model even where a train dataset with security policies is small. To detect a hallucinated high-level security policy, the generated policy is double checked againt the syntax this YANG data model [Hallucination-Mitigation].

2. Security Policy Conflict Handling: A new security policy can conflict with an existing security policy, so the new security policy can be overlapped with the existing security policy or contradict with the existing security policy, which may invalidate the effect of the existing security policy. There are four kinds of security policy conflicts in [Security-Misconfiguration] such as Shadowing Conflict, Correlation Conflict, Redundancy Conflict, and Generalization Conflict. These conflicts should be resolved after an intent is translated into a high-level security policy.

3. Dynamic Security Policy Enforcement: It takes time to detect whether a traffic flow is related to a security attack or not. For a certain time period, a malicious traffic flow needs to be observed to see whether it has a negative impact on a target network. According to the severity of the impact of a traffic flow, the treatment of the traffic flow at network forwarding elements (e.g., router and switch) should be adapted dynamically and proactively by an adaptive decision-making (e.g., partial packet dropping and rerouting) in Security Controller in the I2NSF framework [ICSC].

Jerome's Comments (3/3)

- Difference between Verification and Validation
  - This is done.
  - In Section 2.2, Policy Verification and Policy Validation are explained.
- More Freedom for Intent Translator with not only GUI (templates) but also Non-GUI tools
  - This is done.
  - In Section 2.2, LLMs (e.g., Flan-T5 and GPT-3) and DSLs (e.g., Nile and NEMO) can be used as a Non-GUI tool.
- Balanced and Consistent Explanation among Use Cases
  - This is done.
  - Enhanced the On-Path Telemetry Use Case in Section 3.2 (IBN for Guaranteeing Service-Level Agreement).

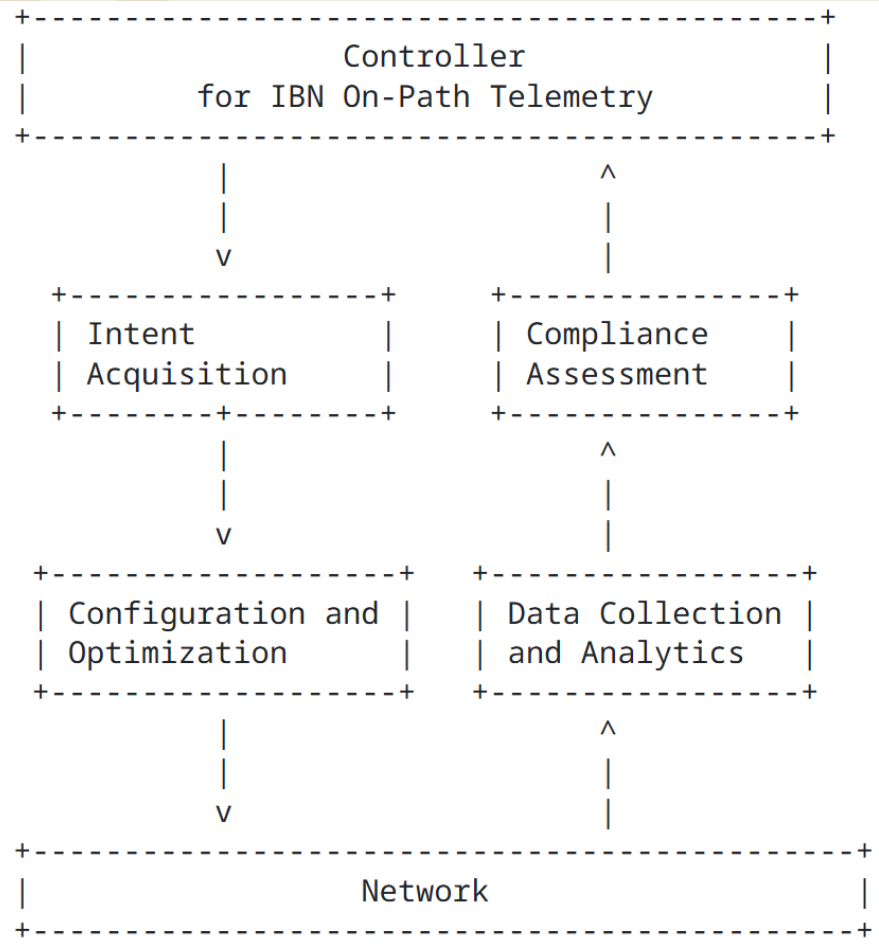


Figure 4: A Traffic Monitoring System with IBN-Based On-Path Telemetry

In Figure 4, the Controller for IBN On-Path Telemetry configures the monitoring of the network according to a specific performance measurement intent. For this monitoring, either AltMark or IOAM can be used. Then it collects data and analytics from the selected methodology (e.g., AltMArk and IOAM) in order to verify the compliance with the intent.

An Intent Acquisition Module acquires an intent as an SLA request from a network administrator. The intent is a specific SLA request for a target network in terms of performance parameter values. The Intent Acquisition Module gives the intent to a Configuration-and-Optimization Module.

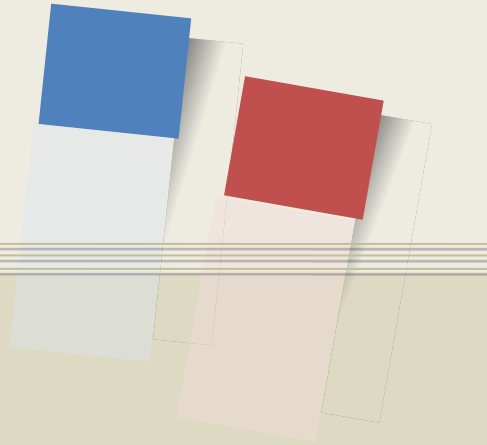
The Configuration-and-Optimization Module translates the intent into a network configuration and a measurement policy, such as network partition and a spatial accuracy needed for network monitoring. Both the network configuration and the measurement policy are deployed into network clusters (i.e., subnetworks) in the target network, having forwarding elements (e.g., routers and switches). For the configuration, the YANG Data Model for the Alternate Marking Method [I-D.ydt-ippm-alt-mark-yang] can be used.

A Data-Collection-and-Analytics Module collects measurement data from the different network clusters in the target network, and then validates the actual performance for each cluster against the required performance according to the intent. For the collection of the measurement data, the On-path Telemetry YANG Data Model [I-D.fz-ippm-on-path-telemetry-yang] or the IPFIX Alternate-Marking Information [I-D.ietf-opsawg-ipfix-alt-mark] can be used.

Next Steps

- This version has addressed all comments of Jérôme Francois (NMRG Chair).
- Authors will enhance this draft through the reviews of the RG members before IETF-126 meeting (July 2026).
- We aim at the RG last call in IETF-126 meeting (July 2026).

Thanks and Any Comments?



Contact: Jaehoon Paul Jeong
(pauljeong@skku.edu)