Network Management Research Group
Internet-Draft
Intended status: Informational
Expires: 11 December 2025

J. Jeong, Ed.
Y. Ahn
M. Gu
Sungkyunkwan University
Y. Kim
Soongsil University
J. Park
ETRI

9 June 2025

Intent-Based Network Management Automation in 5G Networks
draft-jeong-nmrg-ibn-network-management-automation-06

Abstract

This document describes Network Management Automation (NMA) of cellular network services in 5G networks. For NMA, it proposes a framework empowered with Intent-Based Networking (IBN). The NMA in this document deals with a closed-loop network control, network intent translator, and network management audit. To support these three features in NMA, it specifies an architectural framework with system components and interfaces. Also, this framework can support the use cases of NMA in 5G networks such as the data aggregation of Internet of Things (IoT) devices, network slicing, and the Quality of Service (QoS) in Vehicle-to-Everything (V2X).

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 11 December 2025.

Copyright Notice

Table of Contents

1. Introduction

5G networks are evolutionary mobile networks over 4G networks in terms of high speed, wide bandwidth, high frequency bands, massive device connectivity, low energy consumption, and intelligence. Especially, the intelligence will be a key feature to understand the intents of users and automate network management fully. 5G networks are designed and implemented on the experience from 4G networks and new technologies which include Software-Defined Networking (SDN) [RFC7149] and Network Functions Virtualization (NFV) [ETSI-NFV][ETSI-NFV-Release-2] along with mmWave for low delivery delay, high data speed, and large network capacity [TS-23.501].

The support of network intelligence is one of the main goals of 5G networks. The network intelligence can provide the 5G networks with Network Management Automation (NMA) for a self-driving network that optimizes and adjusts itself by minimizing the interaction with humans (e.g., network administrators and users).

Intent-Based Networking (IBN) is a feasible approach that can provide the 5G networks with the NMA services [RFC9315] [TS-28.312][TR-28.812]. The concept of IBN enables a closed-loop network control architecture [RFC9315] that can adapt to the current status of a target network by collecting and analyzing monitoring data from Network Functions (NFs). NFs can be either Virtual Network Functions (VNFs), Cloud-Native Network Functions (CNFs) or Physical Network Functions (PNFs) in cloud and edge computing environments. In the 3rd Generation Partnership Project (3GPP), Network Data Analytics Function (NWDAF) is defined to collect and analyze monitoring data from multiple VNFs and PNFs in cellular networks [TS-23.288][TS-29.520].

For the intelligent NMA services, this document proposes an architectural framework that combines the IBN and NWDAF to the 5G networks with Artificial Intelligence (AI) and Machine Learning (ML). The framework allows a network intent from either a network operator or user, which is expressed in the form in [TS-28.312], to be translated into a network policy by a Network Intent Translator (NIT) [I-D.yang-i2nsf-security-policy-translation]. A Natural Language Processing (NLP) technique can be used to design and implementation of such an NIT [USENIX-ATC-Lumi]. For the intent translation, the data model mapping between a network indent data model and a network policy needs to be performed by a data model mapper in advance [I-D.yang-i2nsf-security-policy-translation]. The translated network policy can be used to remotely configure NFs running on top of VNFs, CNFs or PNFs in order to enforce the commanded intent in a target network (e.g., 5G Networks). Also, it also collects and analyzes the monitoring data from VNFs, CNFs and PNFs such that the network policy can be verified and optimized to satisfy the requests for the network intent.

Therefore, the NMA in this document deals with closed-loop network control, network intent translator, and network management audit. To support these three features in NMA, it specifies an architectural framework with system components and interfaces. In addition, this framework can support the use cases of NMA in 5G networks such as the data aggregation of Internet of Things (IoT) devices, network slicing, and the Quality of Service (QoS) in Vehicle-to-Everything (V2X). Especially, this document shows a use case of IoT in 5G networks such as the data collection and analysis of IoT devices.

2. Terminology

This document uses the terminology described in [RFC8329], [I-D.ietf-i2nsf-applicability], and [I-D.jeong-i2nsf-security-management-automation]. In addition, the following terms are defined below:

* 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 [RFC9315].

* Network Management Automation (NMA): It enforces a network intent from a user (or administrator) into a target network system. The network intent can be translated into the corresponding network policy by a network intent translator (NIT) and dispatched to appropriate NFs. Through the monitoring of the NFs, the activity and performace of the NFs is monitored and analyzed. If needed, the network rules of the network policy are augmented or new network rules are generated and configured to appropriate NFs.

* Network Intent Translator (NIT): It translates a network intent to a network policy that can be understood and configured by an NF for a specific network service, such as the data aggregation of Internet of Things (IoT) devices, network slicing, and the Quality of Service (QoS) provisioning in Vehicle-to-Everything (V2X) communications.

* Feedback-Based Network Management (FNM): It means that a network service is evolved by updating a network policy (having network rules) and adding new network rules for detected network problems by processing and analzing the monitoring data of NFs.

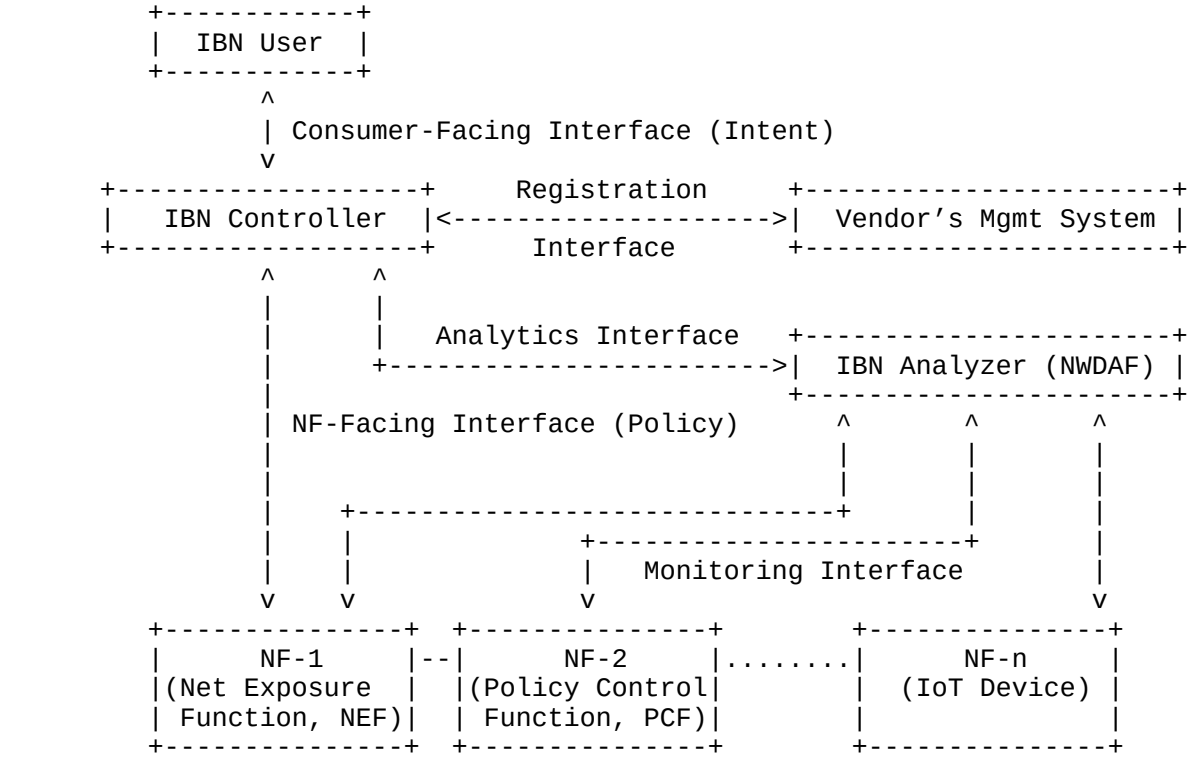

Figure 1: Network Management Automation in IBN Framework for 5G Networks

3. Network Management Automation in IBN Framework for 5G Networks

This section describes an IBN framework for 5G networks. Note that this IBN Framework is based on the Framework for Interface to Network Security Functions (I2NSF) [RFC8329][I-D.jeong-i2nsf-security-management-automation]. As shown in Figure 1, an IBN User can use network functions by delivering network intents, which specify network requirements and goals that the IBN User wants to enforce, to the IBN Controller via the Consumer-Facing Interface (CFI).

3.1. Components with IBN Framework for Network Management Automation

The following are the system components for the IBN framework for network management automation in 5G networks.

* IBN User: An entity that delivers a network intent to IBN Controller. It is assumed that a network intent is constructed by the intent data model in the 3GPP intent document [TS-28.312].

* IBN Controller: An entity that controls and manages other system components in the IBN framework. It translates a network intent into the corresponding network policy and selects appropriate NFs to execute the network rules of the network policy.

* Vendor's Management System (VMS): An entity that provides an image of of a virtualized NF for a network service to the IBN framework, and registers the capability and access information of an NF with IBN Controller.

* Network Function (NF): An entity that is a Virtual Network Function (called VNF), Cloud-Native Network Function (CNF), and Physical Network Function (called PNF) which is also called Cloud-native Network Function, for a specific network service such as the data aggregation of IoT devices, network slicing, and the QoS provisioning in V2X communications.

* IBN Analyzer: An entity that collects monitoring data from NFs and analyzes such data for checking the activity and performance of the NFs using machine learning techniques (e.g., Deep Learning [Deep-Learning]). IBN Analyzer can be a Network Data Analytics Function (NWDAF) in 5G networks [TS-23.288][TS-29.520]. If there is a suspicious network problem (e.g., traffic congestion and QoS degradation) for the target network or NF, IBN Analyzer delivers a report of the augmentation or generation of network rules to IBN Controller.

For IBN-based network services with Feedback-Based Network Management (FNM), IBN Analyzer is a key IBN component for the IBN framework [RFC9315] to collect monitoring data from NFs and analyzing the monitoring data. The actual implementation of the analysis of monitoring data is out of the scope of this document.

3.2. Interfaces for the IBN Framework

The following are the interfaces for the IBN framework. Note that the interfaces can be modeled with YANG [RFC6020] or YAML [YAML] and network policies are delivered through either RESTCONF [RFC8040] or NETCONF [RFC6241]. In addition, according to 3GPP specifications, REST API [REST] can be supported for those interfaces.

* Consumer-Facing Interface: An interface between IBN User and IBN Controller for the delivery of a network intent [I-D.ietf-i2nsf-consumer-facing-interface-dm].

* NF-Facing Interface: An interface between IBN Controller and an NF (e.g., Network Exposure Function (NEF) in 5G Core Network) for the delivery of a network policy [I-D.ietf-i2nsf-nsf-facing-interface-dm].

* Registration Interface: An interface between a VMS and IBN Controller for the registration of an NF's capability and access information with the IBN Controller or the query of an NF for a required low-level network policy [I-D.ietf-i2nsf-registration-interface-dm].

* Monitoring Interface: An interface between an NF and IBN Analyzer for collecting monitoring data from an NF to check the activity and performance of an NF for a possible network problem [I-D.ietf-i2nsf-nsf-monitoring-data-model].

* Analytics Interface: An interface between IBN Analyzer and IBN Controller for the delivery of an analytics report of the augmentation or generation of network rules to IBN Controller, which lets IBN Controller apply the report for network rules to its network policy management [I-D.lingga-i2nsf-analytics-interface-dm].

For IBN-based network services with FSM, Analytics Interface is a key interface in the IBN framework to deliver an analytics report of the augmentation or generation of network rules to IBN Controller through the analysis of the monitoring data from NFs.

4. Network Intent Translator

To facilitate Network Intent Translation, IBN Controller needs to have a Network Intent Translator (NIT) that performs the translation of a network intent (called intent) into the corresponding network policy (called policy). For the automatic NIT services, the IBN framework needs to bridge an intent data model and a policy data model in an automatic manner [I-D.yang-i2nsf-security-policy-translation]. Note that an intent data model is for the IBN Consumer-Facing Interface, and a policy data model is for the IBN NF-Facing Interface.

Figure 2 shows automatic mapping of intent and policy data models for network policies. Automatic Data Model Mapper takes an intent data module for the Consumer-Facing Inteface and a policy data module for the NF-Facing Interface. It then constructs a mapping table associating the data attributes (or variables) of the intent data module with the corresponding data attributes (or variables) of the policy data module. Also, it generates a set of production rules of the grammar for the construction of an XML (or JSON) file of network policy rules.

Figure 3 shows the procedure of network intent translation. A network policy translator is a component of IBN Controller. The translator consists of three components such as Data Model Mapper, Policy Data Extractor, Policy Data Converter, and Policy Generator.

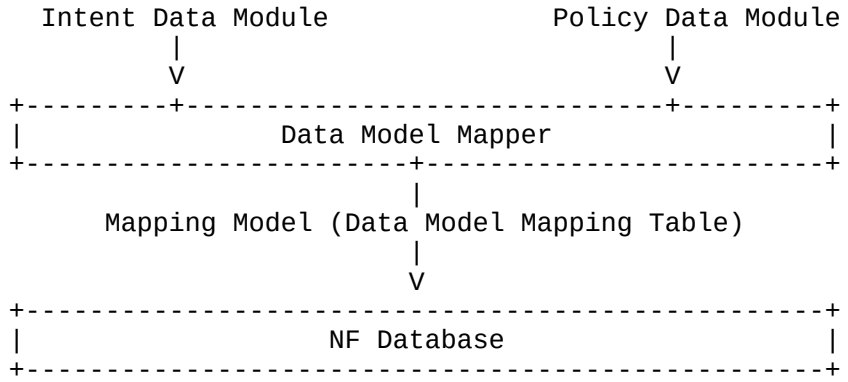

Figure 2: Automatic Mapping of Intent and Policy Data Models

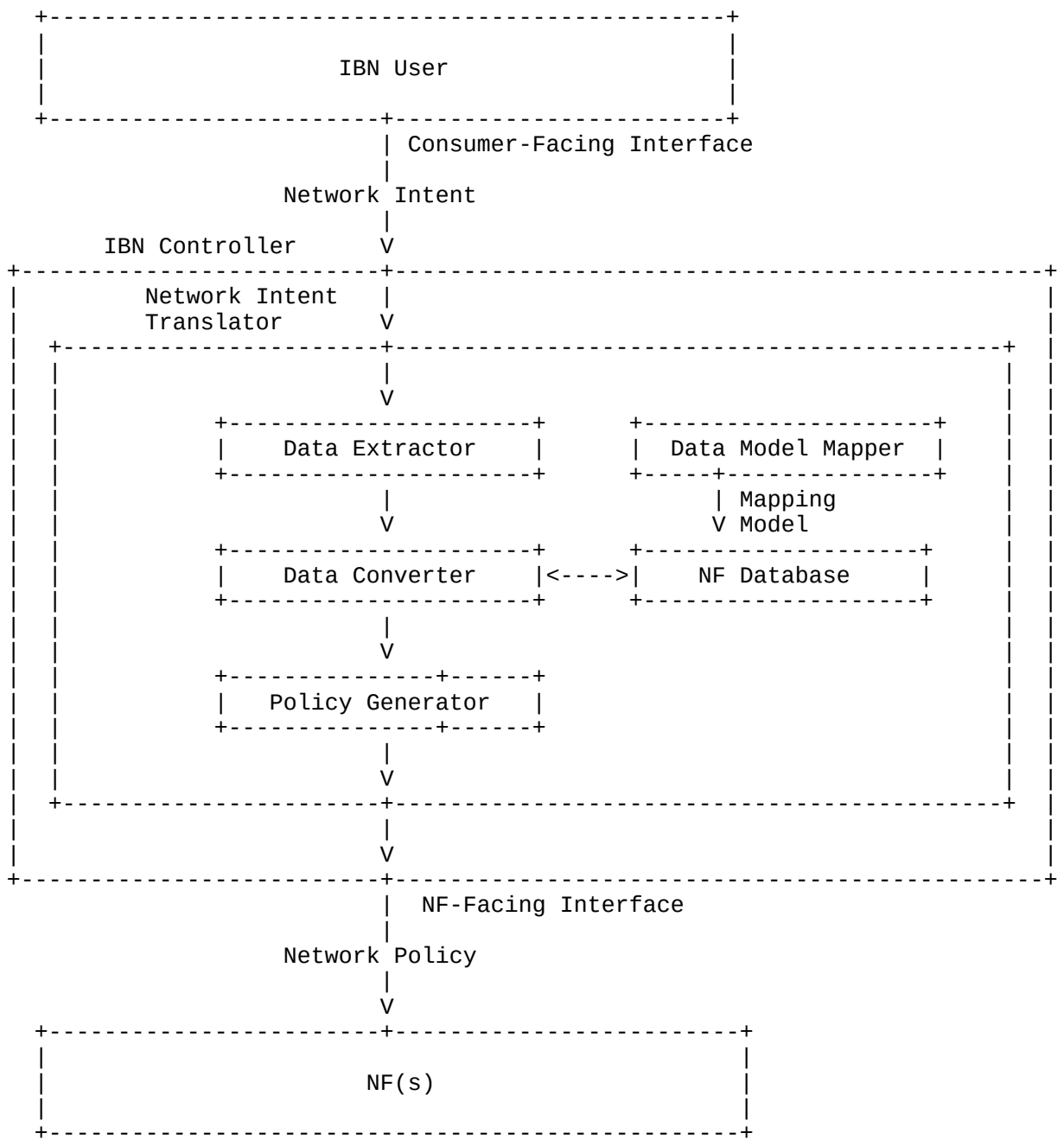

Figure 3: Network Intent Translation

Data Model Mapper maps the attributes and their values of a network intent to the corresponding attributes and their values of a network policy. Note that the values of a network intent may involve a human language and must be converted to an appropriate value for a network policy (e.g., employees -> 192.0.1.0/24).

Data Extractor extracts the values of the attributes related to the network intent that was delivered by an IBN User to an IBN Controller through the Consumer-Facing Interface [I-D.ietf-i2nsf-consumer-facing-interface-dm].

Data Converter converts the values of the network intent's attributes into the values of the corresponding network policy's attributes to generate the network policy [I-D.ietf-i2nsf-nsf-facing-interface-dm].

Policy Generator generates the corresponding network policy that is delivered by the IBN Controller to an appropriate NF through NF-Facing Interface [I-D.ietf-i2nsf-nsf-facing-interface-dm].

5. Network Audit System

The IBN framework is weak to both an insider attack and a supply chain attack since it trusts in NFs provided by VMS and assumes that NFs work for their network services appropriately [I-D.ietf-i2nsf-applicability].

To detect the malicious activity of either an insider attack by a malicious VMS or a supply chain attack by a compromised VMS, a network audit system is required by the IBN framework. This network audit system can facilitate the non-repudiation of configuration commands and monitoring data generated in the IBN framework.

A network audit system has the following four main objectives:

* To check the existence of a network policy, a management system, and its procedures;

* To identify and understand the existing vulnerabilities and risks of either an insider attack or a supply chain attack;

* To review existing network controls on operational and administrative issues;

* To provide recommendations and corrective actions to IBN Controller for further network and security improvement.

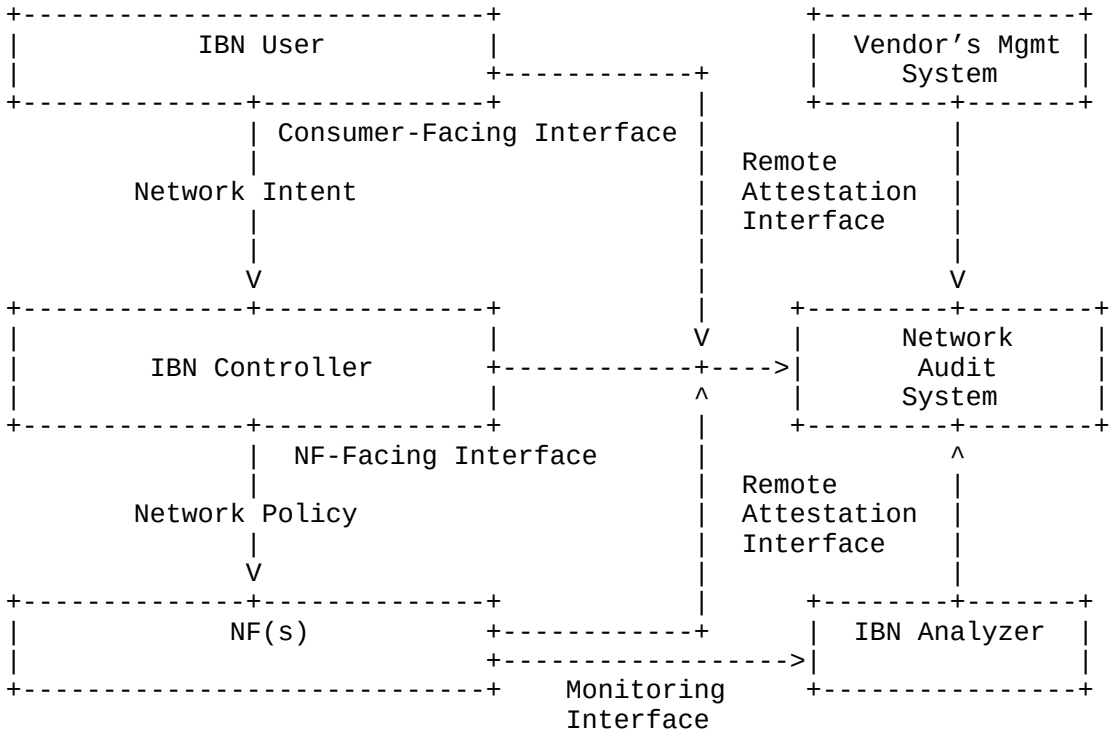

Figure 4: Activity Auditing with Network Audit System

Figure 4 shows activity auditing with a network audit system in the IBN framework. All the components in the IBN framwork report its activities (such as configuration commands and monitoring data) to Network Audit System as transactions through Remote Attestation Interface [I-D.yang-i2nsf-remote-attestation-interface-dm]. The network audit system can analyze the reported activities from the IBN components to detect malicious activities such as an insider attack and a supply chain attack. Note that such a network audit system can be implemented by remote attestation [I-D.ietf-rats-architecture][I-D.yang-i2nsf-remote-attestation-interface-dm] or Blockchain [Bitcoin]. The details of the implementation of the network audit system are out of the scope of this document.

In order to determine a minimum set of controls required to reduce the risks from either an insider attack or a supply chain attack, the network audit system should analyze the activities of all the components in the IBN framework periodically, evaluate possible risks, and take an action to such risks since vulnerabilities and threats may change in different environments over time.

6. A Use Case of IoT Device Data Aggregation

This section describes a use case where a policy of IoT device data aggregation is set up in the IBN framework for 5G networks.

Figure 5 shows the procedure of the enforcement for an IoT device data aggregation intent in the IBN Framework as follows:

1. IBN User sends a Network Intent Request to IBN Controller.

2. IBN Controller translates the request with its Network Intent Translator (called NIT). The NIT identifies NFs (i.e., IoT Devices) for the request after the steps of Data Extraction and Data Conversion.

3. If the NFs are available for the requested network policy, go to the step of Policy Generation in NIT. If the NFs are unavailable for the requested network policy, go to the next step.

4. IBN Controller sends an NF Query Request to Vendor’s Management System (called VMS) to find an appropriate NF for the request network policy.

5. If there is such an NF registered with VMS, VMS sends an NF Initializtion Request to Cloud (or Edge Server) to initialize the NF.

6. Cloud (or Edge Server) forwards the NF Initializtion Request to the appropriate NF to let it initialize itself.

7. The NF performs an initialization to perform a task for a network policy in 5G networks.

8. The NF sends an NF Initialization Response to Cloud (or Edge Server) to tell Cloud (or Edge Server) its readiness to perform a task.

9. Cloud (or Edge Server) forwards the NF Initialization Response to VMS to tell an NF’s readiness to perform a task.

10. VMS sends an NF Query Response to IBN Controller to tell an NF’s readiness to perform a task along with the network access information for the NF.

11. IBN Controller performs the step of Policy Generation in its NIT along with the network access information of an appropriate NF(s).

12. IBN Controller sends a Network Policy Request to the appropriate NF.

13. The NF performs the configration in the given Network Policy Request to perform the requested task (e.g., sensing and reporting).

14. The NF sends a Network Policy Response to IBN Controller to tell its readiness to perform the requested task.

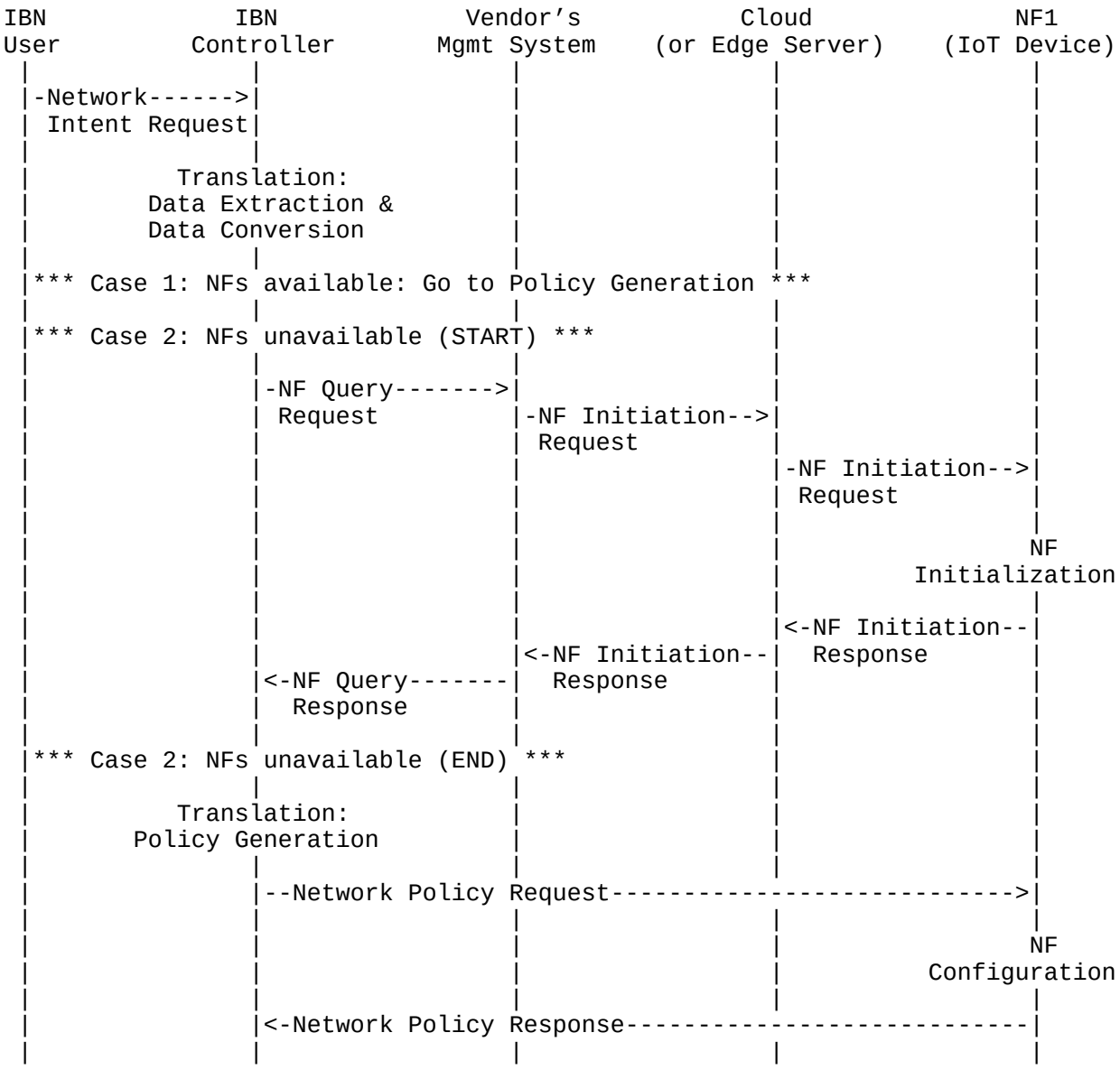

Figure 5: Procedure of an IoT Device Data Aggregation Intent Enforcement in the IBN Framework

Figure 6 shows the procedure of the reporting for IoT device data aggregation in the IBN Framework as follows:

1. NF1 (as an IoT Device) sends its Sensing Data to IBN Analyzer (as an NWDAF).

2. NF2 (as an IoT Device) sends its Sensing Data to IBN Analyzer (as an NWDAF).

3. IBN Analyzer performs Sensing Data Aggregation and analyzes the aggregated sensing data through Machine Learning (ML) techniques. It then generates a Sensing Report for IBN Controller.

4. IBN Analyzer sends a Sensing Report to IBN Controller.

5. IBN Controller analyzes the Sensing Report for a further action. If a further action is needed, it updates the existing network policy or generates a new network policy.

6. IBN Controller sends the report for the further action to IBN User optionally if the reporting is needed.

7. For the further action, IBN Controller sends an Updated NF Policy Request or a New NF Policy Request to the appropriate NF(s).

8. The appropriate NF(s) reconfigures the Updated NF Policy or configures the new NF Policy in its own system.

9. The appropriate NF(s) sends an Updated NF Policy Response or a New NF Policy Response to IBN Controller.

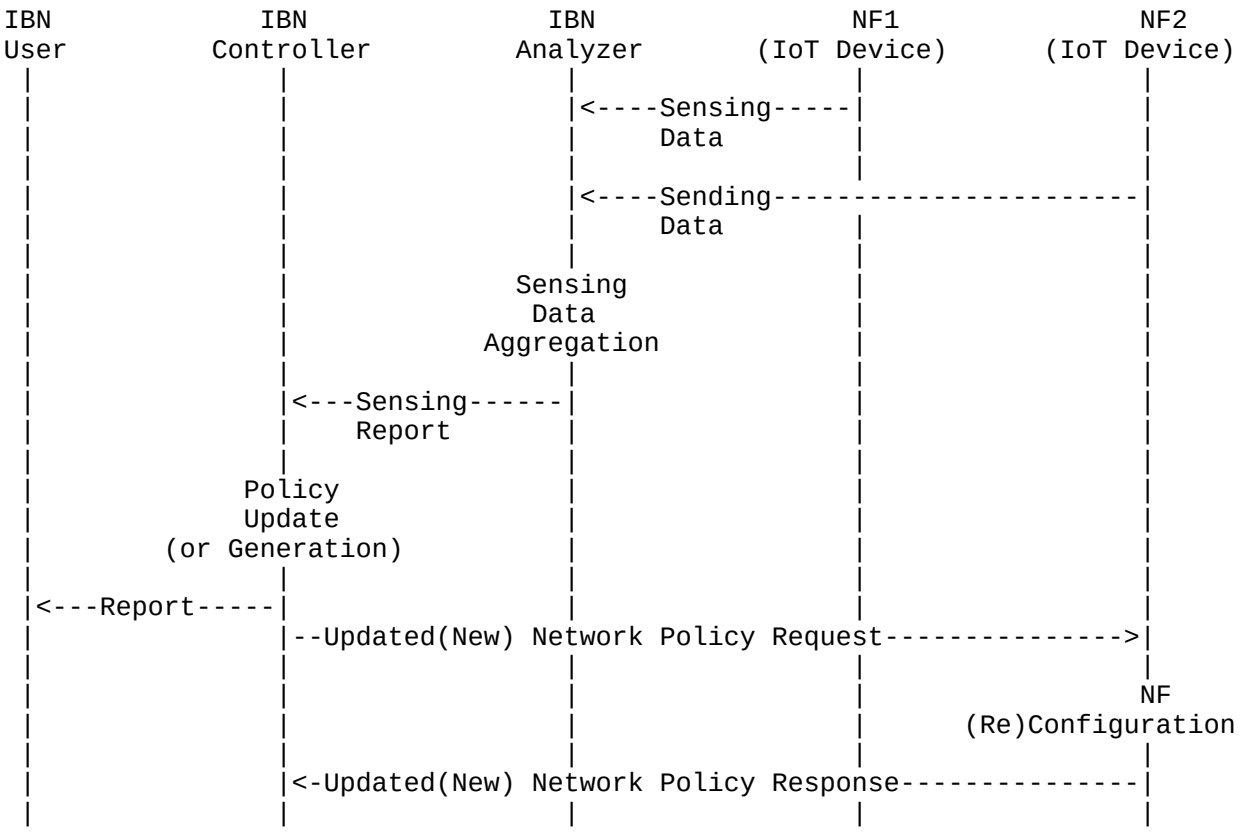

Figure 6: Procedure of IoT Device Data Aggregation Reporting in the IBN Framework

7. IANA Considerations

This document does not require any IANA actions.

8. Security Considerations

The same security considerations for the IBN framework [RFC8329] are applicable to this document.

The development and introduction of IBN Analyzer and Network Audit System in the IBN Framework may create new security concerns that have to be anticipated at the design and specification time. The usage of machine learning to analyze monitoring data of malicious NFs may add a risk to its model to be attacked (e.g., adversarial attack) and can result in a bad security policy that is deployed into the IBN system.

9. References

9.1. Normative References

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8329] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, DOI 10.17487/RFC8329, February 2018, <https://www.rfc-editor.org/info/rfc8329>.

[RFC9315] Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", RFC 9315, DOI 10.17487/RFC9315, October 2022, <https://www.rfc-editor.org/info/rfc9315>.

9.2. Informative References

[I-D.ietf-i2nsf-consumer-facing-interface-dm] Jeong, J. P., Chung, C., Ahn, T., Kumar, R., and S. Hares, "I2NSF Consumer-Facing Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-consumer-facing-interface-dm-31, 15 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-consumer-facing-interface-dm-31>.

[I-D.ietf-i2nsf-nsf-facing-interface-dm] Kim, J. T., Jeong, J. P., Jung-Soo, J., Hares, S., and Q. Lin, "I2NSF Network Security Function-Facing Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-nsf-facing-interface-dm-29, 1 June 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-nsf-facing-interface-dm-29>.

[I-D.ietf-i2nsf-registration-interface-dm]
Hyun, S., Jeong, J. P., Roh, T., Wi, S., and J. Jung-Soo, "I2NSF Registration Interface YANG Data Model for NSF Capability Registration", Work in Progress, Internet-Draft, draft-ietf-i2nsf-registration-interface-dm-26, 10 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-registration-interface-dm-26>.

[I-D.ietf-i2nsf-nsf-monitoring-data-model]
Jeong, J. P., Lingga, P., Hares, S., Xia, L., and H. Birkholz, "I2NSF NSF Monitoring Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-nsf-monitoring-data-model-20, 1 June 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-nsf-monitoring-data-model-20>.

[I-D.lingga-i2nsf-analytics-interface-dm]
Lingga, P., Jeong, J. P., and Y. Choi, "I2NSF Analytics Interface YANG Data Model for Closed-Loop Security Control in the I2NSF Framework", Work in Progress, Internet-Draft, draft-lingga-i2nsf-analytics-interface-dm-04, 26 July 2024, <https://datatracker.ietf.org/doc/html/draft-lingga-i2nsf-analytics-interface-dm-04>.

[I-D.ietf-i2nsf-applicability]
Jeong, J. P., Hyun, S., Ahn, T., Hares, S., and D. Lopez, "Applicability of Interfaces to Network Security Functions to Network-Based Security Services", Work in Progress, Internet-Draft, draft-ietf-i2nsf-applicability-19, 3 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-applicability-19>.

[I-D.jeong-i2nsf-security-management-automation]
Jeong, J. P., Lingga, P., Jung-Soo, J., Lopez, D., and S. Hares, "An I2NSF Framework for Security Management Automation in Cloud-Based Security Systems", Work in Progress, Internet-Draft, draft-jeong-i2nsf-security-management-automation-08, 26 July 2024, <https://datatracker.ietf.org/doc/html/draft-jeong-i2nsf-security-management-automation-08>.

[I-D.yang-i2nsf-security-policy-translation]
Jeong, J. P., Lingga, P., and J. Yang, "Guidelines for Security Policy Translation in Interface to Network Security Functions", Work in Progress, Internet-Draft, draft-yang-i2nsf-security-policy-translation-16, 7 February 2024, <https://datatracker.ietf.org/doc/html/draft-yang-i2nsf-security-policy-translation-16>.

[I-D.ietf-rats-architecture]
Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-architecture-22, 28 September 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-architecture-22>.

[I-D.yang-i2nsf-remote-attestation-interface-dm]
Yang, P., chenmeiling, Su, L., Lopez, D., Jeong, J. P., and L. Dunbar, "I2NSF Remote Attestation Interface YANG Data Model", Work in Progress, Internet-Draft, draft-yang-i2nsf-remote-attestation-interface-dm-01, 5 June 2022, <https://datatracker.ietf.org/doc/html/draft-yang-i2nsf-remote-attestation-interface-dm-01>.

[YAML] Ingerson, B., Evans, C., and O. Ben-Kiki, "Yet Another Markup Language (YAML) 1.0", Available: https://yaml.org/spec/history/2001-05-26.html, October 2023.

[TS-23.501]
"System Architecture for the 5G System (5GS)", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144, September 2023.

[TS-28.312]
"Intent Driven Management Services for Mobile Networks", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554, September 2023.

[TR-28.812]
"Study on Scenarios for Intent Driven Management Services for Mobile Networks", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3553, December 2020.

[TS-23.288]
"Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579, September 2023.

[TS-29.520]
"Network Data Analytics Services", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3355, September 2023.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, March 2014, <https://www.rfc-editor.org/rfc/rfc7149>.

[ETSI-NFV] "Network Functions Virtualisation (NFV); Architectural Framework", Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf, December 2014.

[ETSI-NFV-Release-2]
"Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Architectural Framework Specification", Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/006/02.01.01_60/gs_nfv006v020101p.pdf, January 2021.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", Available: https://bitcoin.org/bitcoin.pdf, May 2009.

[USENIX-ATC-Lumi]
Jacobs, A., Pfitscher, R., Ribeiro, R., Ferreira, R., Granville, L., Willinger, W., and S. Rao, "Hey, Lumi! Using Natural Language for Intent-Based Network Management", USENIX Annual Technical Conference, Available: https://www.usenix.org/conference/atc21/presentation/jacobs, July 2021.

[REST] Fielding, R. and R. Taylor, "Principled Design of the Modern Web Architecture", ACM Transactions on Internet Technology, Vol. 2, Issue 2,, Available: https://dl.acm.org/doi/10.1145/514183.514185, May 2002.

[Deep-Learning]
Goodfellow, I., Bengio, Y., and A. Courville, "Deep Learning", Publisher: The MIT Press, URL: https://www.deeplearningbook.org/, November 2016.

Appendix A. Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. RS-2024-00398199 and RS-2022-II221015).

Appendix B. Contributors

This document is made by the group effort of NMRG, greatly benefiting from inputs and texts by Linda Dunbar (Futurewei) and Susan Hares (Huawei). The authors sincerely appreciate their contributions.

The following are coauthors of this document:

Jiwon Suh
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: sjw6136@skku.edu
URI: http://iotlab.skku.edu/people-Ji-Won-Suh.php

Yiwen Shen
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: chrisshen@skku.edu
URI: https://chrisshen.github.io/

Patrick Lingga
Department of Electrical & Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: patricklink@skku.edu
URI: http://iotlab.skku.edu/people-Patrick-Lingga.php

Yunchul Choi
Standards & Open Source Research Division
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu
Daejeon
34129
Republic of Korea
Phone: +82 42 860 5978
Email: cyc79@etri.re.kr

Appendix C. Changes from draft-jeong-nmrg-ibn-network-management-automation-05

The following changes are made from draft-jeong-nmrg-ibn-network-management-automation-05:

* This version is submitted for the maintanance of draft-jeong-nmrg-ibn-network-management-automation.

Authors' Addresses

Jaehoon Paul Jeong (editor)
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Yoseop Ahn
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: ahnjs124@skku.edu
URI: http://iotlab.skku.edu/people-Ahn-Yoseop.php

Mose Gu
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: rna0415@skku.edu
URI: http://iotlab.skku.edu/people-Moses-Gu.php

Younghan Kim
School of Electronic Engineering
Soongsil University
369, Sangdo-ro, Dongjak-gu
Seoul
06978
Republic of Korea
Phone: +82 10 2691 0904
Email: younghak@ssu.ac.kr

Jung-Soo Park
Standards & Open Source Research Division
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu
Daejeon
34129
Republic of Korea
Phone: +82 42 860 6514
Email: pjs@etri.re.kr