

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 19 April 2026

M. Boucadair  
Orange  
L. M. Contreras  
O. G. D. Dios  
Telefonica  
T. Graf  
Swisscom  
R. Rahman  
Equinix  
16 October 2025

An Update of Operators Requirements on Network Management Protocols and  
Modelling  
draft-ietf-nmop-rfc3535-20years-later-01

Abstract

The IAB organized an important workshop to establish a dialog between network operators and protocol developers, and to guide the IETF focus on work regarding network management. The outcome of that workshop was documented in the "IAB Network Management Workshop" (RFC 3535) which was instrumental for developing NETCONF and YANG, in particular.

20 years later, it is time to evaluate what has been achieved since then and identify the operational barriers for making these technologies widely implemented. Also, this document captures new requirements for network management operations.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at  
<https://github.com/boucadair/rfc3535-20years-later>.

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 19 April 2026.

## Copyright Notice

Copyright (c) 2025 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. Observations and New Requirements . . . . .	4
2.1. On the Importance of Data Models . . . . .	4
2.2. Fragmented Ecosystem . . . . .	6
2.3. The Network Becomes Consumable . . . . .	6
2.4. Network APIfication . . . . .	6
2.5. Lack of Profiling . . . . .	7
2.6. Lack of Agile Process for (The Maintenance of) YANG Modules . . . . .	7
2.7. Integration Complexity . . . . .	8
2.8. YANG-formatted Data Manipulation . . . . .	9
2.9. Translation and Mapping Between Service/Network and Device Models . . . . .	9
2.10. (In)Consistent Data Structures in Network Protocols for Data Export . . . . .	9
2.11. Proprietary YANG Modules, CLI, and Limited Abstraction .	10
2.12. Distinct Networks, Distinct Management Requirements . .	11
2.13. Implications of External Dependency . . . . .	11
2.14. Too Much Time Between Publication of New Networking Functionality and the Associated YANG . . . . .	12
2.15. Lack of Implementation of Proposed Solutions . . . . .	12
2.16. Tooling & Skills . . . . .	13
2.16.1. Integration with "native" IT Tooling . . . . .	13
2.16.2. IETF Support for Better YANG Integration . . . . .	13
2.16.3. Open-source Tools . . . . .	13

2.16.4. Skills . . . . .	13
2.17. New Service Approaches . . . . .	14
2.18. Many Solutions for the Same Problem, but Lack of Clear Applicable Guidance . . . . .	14
3. Updated Operators' Requirements . . . . .	14
3.1. Summary . . . . .	14
3.2. Categorization . . . . .	17
3.3. Overall New Requirements Levels: Operators View . . . . .	19
3.4. Collaborative Prioritization . . . . .	20
4. Security Considerations . . . . .	20
5. IANA Considerations . . . . .	21
6. Informative References . . . . .	21
Appendix A. Assessment of RFC 3535 Operator Requirements . . . . .	30
A.1. Detailed Analysis . . . . .	30
A.2. Summary . . . . .	33
Appendix B. Assessment of RFC 3535 Recommendations . . . . .	34
B.1. Detailed Analysis . . . . .	34
B.2. Summary . . . . .	37
Acknowledgments . . . . .	38
Contributors . . . . .	38
Authors' Addresses . . . . .	38

## 1. Introduction

The IAB organized a workshop (June 4-June 6, 2002) to establish a dialog between network operators and protocol developers, and to guide the IETF to focus on work regarding network management. The outcome of that workshop was documented in the "IAB Network Management Workshop" [RFC3535] which was instrumental for developing NETCONF [RFC6241] and YANG [RFC6020][RFC7950].

Since the publication of [RFC3535] major advances were achieved in the Network Management area, such as (but not limited to):

- \* NETCONF [RFC6241]
- \* YANG [RFC7950]
- \* RESTCONF [RFC8040]
- \* SDN & Programmable Networks [RFC7149][RFC7426]
- \* Automation [RFC8969]
- \* Virtualization [RFC8568]
- \* Containerization [I-D.ietf-bmwg-containerized-infra]

- \* Intent-based [RFC9315]
- \* Network APIs
- \* Models for management of services, networks, and devices [RFC8199][RFC8309]
- \* Telemetry [RFC9232]
- \* JSON Encoding of Data Modeled with YANG [RFC7951]
- \* CoAP Management Interface (CORECONF) [I-D.ietf-core-comi]
- \* YANG to CBOR mapping [RFC9254]
- \* YANG Schema Item Identifier (YANG SID) [I-D.ietf-core-sid]

See also "An Overview of the IETF Network Management Standards" [RFC6632].

More than 20 years later, new requirements on network management operations are emerging from the operators. This document captures these requirements that reflect the progress in this area.

The document also provide an assessment of the RFC3535 recommendations (Appendix A) and to what extent that roadmap was driving network management efforts within the IETF, in particular (Appendix B).

## 2. Observations and New Requirements

### 2.1. On the Importance of Data Models

An appealing aspect about network automation techniques is that they almost apply to any kind of network. From that perspective, the functional component of a network automation framework that probably matters the most, and independent of the underlying interfaces and protocols, are the data models. Concretely, data models are instrumental in the automation of networks, especially that they can provide closed-loop control for adaptive and deterministic service creation, delivery, and maintenance.

Data models can be used to derive required configuration information for both network and service components, and state information that will be monitored and tracked. Likewise, they can be used during the service/network management life cycle (e.g., service instantiation, provisioning, optimization, monitoring, diagnostic, and assurance).

More than three decades of "Internet standardization" have shown that the specification of data models is not that straightforward. This is because of at least two major reasons:

- \* For more than 30 years, legacy network equipment manufacturers have considered their technology as a competitive advantage, thereby leading to proprietary, vendor-specific, data models and the burden of vendor lock-ins. For example, there are more YANG proprietary modules than standarized ones.
- \* Over the same period, operators have also developed their savoir-faire as a key competitive advantage. Such savoir-faire had to rely upon these proprietary data models. Operators were reluctant in the past to share their design and management practices.

The situation has changed since network "softwarization" strategies have been disclosed by vendors and operators. From a business standpoint, network "softwarization" is seen as a major transformation effort by operators, because of the flexibility and the "a la carte" approach that is promoted by "X-as-a-service" (XaaS) designs, "X" being network, platform, Network Slice, etc.

XaaS designs assume the availability of data models that are dynamically instantiated (along with a set of relevant policies) as a function of the "X" (and its design, for that matter). \*XaaS services cannot be designed, delivered, and operated without data models.\* Standard data models are thus key as they allow to:

- \* Ease mapping among many (network/service) layers.
- \* Ease data correlation from distinct sources.
- \* Nullify (soften) CLI specifics to vendors.
- \* Support both top-down and bottom-up approaches:
- \* Accurate control loops for adaptive and deterministic service creation, delivery, and maintenance.
- \* Feed an intelligence that will drive appropriate actions to adjust the current status to align with the intended status.

OPS-REQ-STRENGTHEN-DM: Network softwarization can only happen with a strong, committed standardization effort, complemented by active involvement in open-source projects that facilitate access to code.

Particularly, \*without data models, a Network API is essentially

useless\* (see also Section 2.4).

## 2.2. Fragmented Ecosystem

The current YANG device models ecosystem is *\*fragmented\**: some standards models are defined through the IETF, while similar ones are defined in other forums such as Openconfig or ONF. Unlike service and network models, IETF-defined device models are not widely implemented.

OPS-REQ-DM-RATIONALIZE: There is a need to rationalize this space and avoid redundant efforts.

## 2.3. The Network Becomes Consumable

Network connectivity can support tailored services in terms of Service Level Objectives (SLOs), for instance, by means of Network Slice Services [RFC9543]. This approach of "consuming" the network flexibly and dynamically is made possible by enabling means of exposing network capabilities to either internal or external applications. Then, network management is no longer limited to collect network status information, but it should be now extended to permit the exposure of resources, capabilities, functionality, and associated information (e.g., inventory based data).

OPS-REQ-EASE-EXPOSURE: Focus on protocols and data models to expose network/service capabilities, network-wide services, and related operations.

OPS-REQ-NW-API-DISCOVERY: Define a reference approach/process for service exposure discovery (APIs discovery).

## 2.4. Network APIfication

APIs are getting momentum as means of interworking between parties, also at the time of providing network services. As an example, [I-D.ramseyer-grow-peering-api] defines an API for dynamically establishing BGP peering sessions between Autonomous Systems of different administrative domains. That same objective is also covered by the YANG data model defined in [I-D.ietf-opsawg-teas-attachment-circuit] as exemplified in Appendix A.10. Tools such as YANG/OpenAPI transforms are key to leverage existing data models and allow for better integration and mapping to actual realization models.

OPS-REQ-DM-API: Readily available API specifications could be generalized from YANG modules for fast development, prototyping, and validation.

## 2.5. Lack of Profiling

Many NETCONF-related features are (being) specified by the IETF, but these features are not widely supported (e.g., YANG-Push [RFC8639]).

OPS-REQ-GUIDE-AND-PROFILE: The target application/applicability of a network management approach should be documented (e.g., edit profile documents that outline a set of recommendations for core/key features, along with appropriate justifications, will help foster more implementations that meet operators' needs). This also covers security management aspects of network management. Additionally, consider independent compliance suites to validate functions/features/etc.

OPS-REQ-ARCH: Need to promote more arch and framework documents to exemplify the intended use.

Examples of such profile documents are the various RFCs that were published by the Behavior Engineering for Hindrance Avoidance (behave) WG [BCP127]. Another approach could be to consider a model similar to the "Roadmap for Transmission Control Protocol (TCP) Specification Documents" [RFC7414]. Such a document would serve as a guide and reference for implementers and others seeking information on 'NETCONF/RESTCONF/YANG'-related RFCs.

OPS-REQ-REASSESS: Additionally, reassessing the value of some IETF proposals compared to competing or emerging solutions (e.g., gRPC vs. YANG-Push) would be beneficial.

## 2.6. Lack of Agile Process for (The Maintenance of) YANG Modules

RFCs might not be suited for documenting YANG modules (it takes much too long, especially for updates). In the meantime, there is a need for "reference models" and "sufficiently stable models".

An hybrid approach might be investigated for documenting IETF-endorsed YANG modules, such as considering an RFC to describe the initial module sketch and objectives and an official IETF repository for maintaining intermediate YANG versions.

By drawing a parallel between YANG data models and the concept of ontology used in the field of Semantic Web, the topic of YANG module maintenance could greatly benefit from proven methodologies in knowledge engineering such as [LOT2019] and automatic documentation tools like [Widoco2017].

OPS-REQ-QUICK-BUT-WELL: Develop a more agile process for the

development and maintenance of YANG modules in the IETF. RFCs might not be suited for documenting YANG modules.

## 2.7. Integration Complexity

Section 3 of [RFC3535] describes a set of network operator requirements. One of the requirements is the ease of use which, according to Section 3.2 of [RFC6244], is addressed by NETCONF and YANG. For configuration this holds true, for network observability it is unfortunately not yet. This has been confirmed with a set of network operators asking how long it takes from subscribing YANG data to make it accessible to the operator. Minutes, Hours, Days, or Weeks. None of them answered Minutes or Hours. All of them responded Days or Weeks. Hinting manual post processing of YANG data.

Collecting YANG metrics from networks is already a struggle due to late arrival of [RFC8639], [RFC8640], [RFC8641], [I-D.ietf-netconf-https-notif], and [I-D.ietf-netconf-udp-notif] for configured subscription transport protocols which defined YANG-Push in the industry. This caused network vendors to implement alternative solutions to collect real-time streaming data in the meanwhile, such as gNMI which was proposed in 2018 in [I-D.openconfig-rtgwg-gnmi-spec] to the IETF but not followed up on. Unfortunately, these implementations differ between network Operating Systems due to the lack of standardization, specifically for the metadata which would ensure machine readability.

When a set of network operators were asked to where operational YANG data needs to be integrated to, the answer homogeneously was Apache Kafka Message Broker and Time Series Databases. There is a need to specify how YANG-Push can be integrated into Apache Kafka and references needed YANG-Push extensions and YANG schema registry development. The YANG-Push extensions addressing needs to make YANG-Push messages machine readable and against semantic validate able to ensure a consistent data processing.

Another challenge is that the subscribed YANG data referenced with datastore-subtree-filter or datastore-xpath-filter breaks semantic integrity which needs to be addressed by either updating Section 4 of [RFC8641] or proposing a new YANG module being used at the YANG-Push receiver.

OPS-REQ-INTEGRATION: Consider approaches to ease integration by-design (e.g., protocols and data models).



## 2.8. YANG-formatted Data Manipulation

The use of a flat tree hierarchy in YANG models may induce some performance issues compared to other graph models. This can be the case, for example, during a path calculation on a network topology. Different approaches using graph theory and compatible with YANG are currently available, but require further experimentation to generalize their adoption. For instance, OpenDaylight [ODL] implements an in-memory connected graph version of YANG-based data to enable fast breadth-first search (BFS).

OPS-REQ-Y2KG: Need for a reference specification to translate YANG-based data into the knowledge graph (KG).

For example, [I-D.marcas-nmop-knowledge-graph-yang] and [I-D.tailhardat-nmop-incident-management-noria] discuss YANG-2-KG proposals to leverage automated reasoning and graph traversal techniques.

OPS-REQ-SCALE: Consider approaches for YANG models to scale.

## 2.9. Translation and Mapping Between Service/Network and Device Models

Navigating among multiple levels of the hierarchy (service, network, device) relies currently on proprietary solutions to graft and translate between two layers. There is no programmatic approach to ensure lossless mappings.

OPS-REQ-LOSSLESS: Consider programmatic approaches to ensure lossless mappings between service/network/device data models. Means to detect, characterize, and expose loss may be considered. Note that lossless mapping is an enabler for support of deterministic verification, auditing, and tracing back along layers/models.

## 2.10. (In)Consistent Data Structures in Network Protocols for Data Export

Network Telemetry, as described in [RFC9232], involve a set of protocols. Due to the different requirements, one Network Telemetry protocol doesn't address all needs. This is mainly due to the nature of the subscribed data. BGP Monitoring Protocol (BMP) [RFC7854] adds monitoring and tracing capabilities natively to the BGP process to minimize the processing overhead. While IPFIX [RFC7011][RFC7012] can be applied according to [RFC5472] to gain visibility into the data and forwarding planes, due to the amount of data, sampling as defined in [RFC5476] and applied to IPFIX in [RFC5477] and aggregation as defined in [RFC7015] for IPFIX is needed to reduce the amount of

exposed data. While YANG-Push focuses on exposing already YANG modelled data, which eases the correlation among network configuration and operational data.

[RFC9232] is an informational document and does not specify what these Network Telemetry protocols should have in common to ensure consistent data structures for data export. While data types are fairly good aligned, a lack of metadata standardization among the Network Telemetry protocols is observed. In particular describing from where the metrics has been exported from and timestamping. In Section 4.2 of [RFC7854] timestamps are optional and sysName [RFC1213] is only carried in the BMP initiation message (Section 4.3 of [RFC7854]), while the message header of IPFIX defined in Section 4.3 of [RFC7011] lacks the sysName definition.

The lack of information from where the data is being pushed from is only known to the Network Telemetry data collection due to the transport session being established from the network node exporting the information. When Network Telemetry messages are being transformed and forwarded, this information is being lost. Therefore, it is common among network operators to augment sysName and other metadata at the data collection.

The same common principle applies to when observation timestamping is missing in the Network Telemetry message. Since the data collection is the closest element to the network, a time stamp is added to give the network operator at least the information when the Network Telemetry message was collected. However, since Network Telemetry addresses real-time streaming needs, this is often not accurate enough for data correlation.

OPS-REQ-REUSABILITY: Consider approach to ensure reuse/consistent data structure.

## 2.11. Proprietary YANG Modules, CLI, and Limited Abstraction

Leveraging on pluggins, proprietary YANG models or even CLI is still the rule in many operations, sometimes forced by the need of operating legacy infrastructures.

The complexity of developing and maintaining these means of operation is huge, as it is required to cover many OS and vendors along the lifetime of the network device.

Network models for the realization of services provide some "level" of abstraction and then automation.

## 2.12. Distinct Networks, Distinct Management Requirements

From the time [RFC3535] was released up to now, new kind of services and applications have been developed and deployed over the time, with very diverse, and some times contradicting, requirements. Those services have been engineered on top of multi-service networks for the sake of efficiency and simplicity, accommodating such a variety of needs. As a result, services requiring mobility, data replication, large capacity, adaptability, multi-path support, determinism, etc., coexist on the same shared network, needing from it mechanisms for graceful operation.

Likewise, such diversity of services also require different management capabilities. For example, session continuity, distribution trees, traffic engineering, congestion status notification, reordering, or on-time delivery impose very different management needs to be satisfied.

This reality is different from the one existing at the time of [RFC3535], and as such, the new identified needs can require from novel approaches to guarantee the aforementioned co-existence of services.

OPS-REQ-NEW-NEED: Some networks have specific network management requirements such as the need for asynchronous operations or constraints on data compactness. An example of such networks is Delay-Tolerant Networking (DTN) [RFC838] or DetNet [RFC8557].

## 2.13. Implications of External Dependency

Networks are being updated to abandon the silo approach from the past towards an increasing convergence. Specifically, there are trends towards a tighter interaction and integration of different technologies previously considered as totally separated from an operational perspective. Examples of that trends are the IP and Optical integration (e.g., the introduction of colored interfaces on routers), or the extension of deterministic-behavior features to Layer 3 networks. This kind of convergence in most cases creates dependencies on the conventional network management features, which require to incorporate or integrate functionality from other technological domains.

Such convergence is also reflected on the need of interacting and interworking with distinct network parts participating in the end-to-end service delivery. Mobile access, fixed access, data center, enterprise, radio functional split (i.e., fronthaul and midhaul), neutral exchanges, intensive data networks (e.g., scientific academic networks), content distribution, etc., represent network parts constituent of end-to-end services that can impose dependencies of the management of an intermediate network.

OPS-REQ-UNSILO: The convergence observed in recent years also implies the need for an up-to-date refresh of management capabilities and tools for conventional networks.

It highlights the necessity to handle the heterogeneity of data, configuration, and network management/requirements.

From a YANG perspective, this involves easily mapping and relating the data models used to manage each specific segment.

Resolving such issue could draw on insights from parallel technical fields such as knowledge engineering practices and concepts associated with Linked Data in the Semantic Web, areas where it is common to manage problems of heterogeneity and data reconciliation across various application domains.

#### 2.14. Too Much Time Between Publication of New Networking Functionality and the Associated YANG

For example, [RFC8667] (IS-IS extensions for SR) was published in December 2019, while [I-D.ietf-isis-sr-yang] will be published ~5 years after.

OPS-REQ-TIMELY-DM: Consider having YANG as part of the protocol specification/change where possible, or have the YANG document progress in parallel. That may slow down the protocol specification, though.

#### 2.15. Lack of Implementation of Proposed Solutions

New solutions proposed by WGs such as NETMOD and NETCONF very often lack an implementation or only have a partial implementation. The situation has improved with the last hackathons (e.g., for YANG-Push), but these solutions became RFCs without a known implementation:

- \* YANG-Push [RFC8641]

- \* Schema-mount [RFC8528]

\* NMDA [RFC8342]

Schema-mount allegedly has only one known implementation because of the complexity of the solution. That means the IETF most likely spent lots of cycles for something which won't be deployed ever.

While hackathons have improved the situation, the availability of implementation is concerning. For open-source, 'sysrepo'/'libyang' are decent choices.

OPS-REQ-READILTY-IMPLEM: It is tempting to consider mandating at least one implementation. However, there were areas which imposed in the past rules for implementations for I-Ds to be published as PS (e.g., [RFC1264]), but these rules were relaxed for reasons described, e.g., [RFC4794] and left it to the WGs to decide about the actual measures to put in place. To date, only IDR WG has clear guidance on two implementations.

## 2.16. Tooling & Skills

### 2.16.1. Integration with "native" IT Tooling

OPS-REQ-IT-INTEGRATION: There is a need to ease the integration of low-level/network-oriented solution with native "IT tooling" (e.g., "https://opentelemetry.io/").

### 2.16.2. IETF Support for Better YANG Integration

OPS-REQ-IETF-TOOLS Ease exposure of libraries and host tools (e.g., yangkit) to ease integration.

### 2.16.3. Open-source Tools

While there are open-source implementations for NETCONF (e.g., NETOPEER), the gRPC/gNMI suite seems to have more support for tools on the client side. For example, "ygot" generates structures from YANG models and these can easily be used by a client to configure a device with gNMI. NETCONF is not supported though (we need the XML tags).

OPS-REQ-CLIENT-TOOLS: Focus on tooling is needed, especially on the client side.

### 2.16.4. Skills

The IETF is not the expert community in data engineering. The experts are in the data industry. Without them, integration in data processing chains like Data Mesh is going to be a challenge.

OPS-REQ-BRIDGE: Create an eco-system where data and networking engineers can collaborate.

## 2.17. New Service Approaches

The virtualization trend have made possible to dynamically instantiate Service Functions (SFs) in distributed compute facilities in the form of virtual machines or containers, as micro-services. The instantiation of the SFs is governed by cloud management systems, as it is the connectivity among the different instances or micro-services. That connectivity is typically realized by using overlay mechanisms, without any further interaction with the network. However, this approach seems to be insufficient for future services demanding stringent requirements in terms of SLOs.

OPS-REQ-GLUE: The distinct approaches followed in both the compute and the network environments makes necessary to define suitable mechanisms for enabling an efficient interplay, while highly automating the overall service delivery procedure.

## 2.18. Many Solutions for the Same Problem, but Lack of Clear Applicably Guidance

There are several solutions that were standardized for network management purposes. For example, management of ACLs by means to BGP FlowSpec [RFC8955][RFC8956] or by means of NETCONF/YANG [RFC8519]. There is no cross referencing between the two standards or delimits its applicability scope vs the other approach.

Likewise, BGP FlowSpec did not reuse the IPFIX Information Elements.

OPS-REQ-GUIDANCE: The target application/applicability of a network management approach should be integrated in the specification itself.

## 3. Updated Operators' Requirements

### 3.1. Summary

OPS-REQ-STRENGTHEN-DM: Network softwarization can only happen with a strong, committed standardization effort, complemented by active involvement in open-source projects that facilitate access to code.

OPS-REQ-DM-RATIONALIZE: Rationalize this space and avoid redundant efforts (in almost all layers (IP, optic, etc.)). Unlike service and network models, Standard-based device models are not widely implemented.

OPS-REQ-QUICK-BUT-WELL: Develop a more agile process for the development and maintenance of YANG modules in the IETF. RFCs might not be suited for documenting YANG modules.

OPS-REQ-GUIDE-AND-PROFILE: The target application/applicability of a network management approach should be documented (e.g., edit profile documents that outline a set of recommendations for core/key features, along with appropriate justifications, will help foster more implementations that meet operators' needs). This also covers security management aspects of network management. Additionally, consider independent compliance suites to validate functions/features/etc.

OPS-REQ-ARCH: Need to promote more arch and framework documents to exemplify the intended use.

OPS-REQ-EASE-EXPOSURE: Focus on protocols and data models to expose network/service capabilities, network-wide services, and related operations.

OPS-REQ-TIMELY-DM: Consider having YANG as part of the protocol specification/change where possible, or have the YANG document progress in parallel.

OPS-REQ-READILY-IMPLEM: The availability of implementation is concerning. Consider catalyst approaches to trigger more (open) implementations, especially during the development of protocols/extensions.

OPS-REQ-DM2API: Readily available API specifications should be generalized from YANG modules for fast development, prototyping, and validation.

OPS-REQ-NW-API-DISCOVERY: Define a reference approach/process for service exposure discovery (APIs discovery).

OPS-REQ-REASSESS: Reassess the value of some IETF proposals, including compared to competing or emerging solutions (e.g., gNMI).

OPS-REQ-BRIDGE: Create an eco-system where data and networking engineers can collaborate.

OPS-REQ-INTEGRATION: Consider approaches to ease integration by-design (e.g., protocols and data models). The integration covers both horizontal and vertical realms. For example, there is a lack of enablement of this integration across standard bodies that operators are left to solve.

OPS-REQ-LOSSLESS: Consider programmatic approaches to ensure lossless mappings between service/network/device data models. Means to detect, characterize, and expose loss may be considered. Note that lossless mapping is an enabler for support of deterministic verification, auditing, and tracing back along layers/models.

OPS-REQ-REUSABILITY: Consider approaches to ensure reuse/consistent data structure across various NM segments. This will ease correlating data learned from different means (IPFIX, BMP, SYSLOG, etc.).

OPS-REQ-SCALE: Consider approaches for YANG models to scale + protocol considerations (transactions, touches, etc.). Specifically, address Telemetry scalability enhancements.

OPS-REQ-UNSILO: Necessity to handle the heterogeneity of data, configuration, and network management/requirements. Resolving such issue could draw on insights from parallel technical fields such as knowledge engineering practices and concepts associated with Linked Data in the Semantic Web, areas where it is common to manage problems of heterogeneity and data reconciliation across various application domains.

OPS-REQ-IT-INTEGRATION: There is a need to ease the integration of low-level/network-oriented solution with native "IT tooling" (e.g., "<https://opentelemetry.io/>").

OPS-REQ-ITER: Need a velocity and approach to standardisation that allows for business goals to be incrementally realised.

OPS-REQ-Y2KG: Need for reference specifications to translate YANG-based data into the knowledge graph. Sample use cases to illustrate the intended use should be considered as well.

OPS-REQ-TOOLS: Focus on tooling is needed, especially on the client side. There is a need for tools that are easy to use. Likewise, there is need for support for multiple friendly, stable, and feature-rich libraries for programming languages.

OPS-REQ-IETF-TOOLS: Ease exposure of libraries and host tools (e.g., yangkit) to ease integration.

OPS-REQ-NEW-NEED: Some networks have specific network management requirements such as the need for asynchronous operations or constraints on data compactness.

OPS-REQ-GLUE: Distinct approaches followed in both the compute and



the network environments make necessary to define suitable mechanisms for enabling an efficient interplay, while highly automating the overall service delivery procedure.

### 3.2. Categorization

The following table provides a classification of the requirements listed in Section 3.1. It specifically tags whether a requirement:

- \* Belongs to Data modeling (DM)
- \* Requires protocol work (Protocol)
- \* Impacts deployability of standardized approaches (Deployability)
- \* Has implications on integration effort by operators (Integration)
- \* Requires some adaptation to an SDO process (SDO Process)
- \* Allows better coordination (Collaboration & Cooperation)
- \* Is relevant to skills transformations (Skills)

NEW Ops Requirement Label	DM	Protocol	Deployability	Integration	SDO Process	Collaboration & Cooperation	Skills
OPS-REQ-STRENGTHEN-DM	X		X				
OPS-REQ-DM-RATIONALIZE	X		X		X	X	
OPS-REQ-QUICK-BUT-WELL	X	X	X				
OPS-REQ-GUIDE-PROFILE	X	X	X				
OPS-REQ-ARCH		X	X				
OPS-REQ-EASE-	X	X	X	X			

EXPOSURE								
OPS-REQ-TIMELY-DM	X		X					
OPS-REQ-READILY-IMPLEM	X	X	X		X			
OPS-REQ-DM-API			X					
OPS-REQ-NW-API-DISCOVERY			X	X				
OPS-REQ-REASSESS		X						
OPS-REQ-BRIDGE						X	X	
OPS-REQ-INTEGRATION			X	X	X			
OPS-REQ-LOSSLESS			X	X	X			
OPS-REQ-REUSABILITY		X		X	X			
OPS-REQ-SCALE	X	X						
OPS-REQ-UNSILO			X	X				
OPS-REQ-IT-INTEGRATION			X	X				
OPS-REQ-ITER					X	X		
OPS-REQ-Y2KG			X	X				
OPS-REQ-TOOLS			X	X				X

OPS-REQ-IETF-TOOLS					X		X
OPS-REQ-NEW-NEED		X					
OPS-REQ-GLUE				X			X

Table 1

### 3.3. Overall New Requirements Levels: Operators View

The following table provides the requirement level of Section 3.1 from an operator perspective.

NEW Ops Requirement Label	Overall Level
OPS-REQ-STRENGTHEN-DM	Strong
OPS-REQ-DM-RATIONALIZE	Strong
OPS-REQ-QUICK-BUT-WELL	Strong
OPS-REQ-GUIDE-AND-PROFILE	Nice to have
OPS-REQ-ARCH	Strong
OPS-REQ-EASE-EXPOSURE	Strong
OPS-REQ-TIMELY-DM	Strong
OPS-REQ-READILY-IMPLEM	Strong
OPS-REQ-DM2API	Strong
OPS-REQ-NW-API-DISCOVERY	Nice to have
OPS-REQ-REASSESS	Strong
OPS-REQ-BRIDGE	Strong
OPS-REQ-INTEGRATION	Strong
OPS-REQ-LOSSLESS	Nice to have

OPS-REQ-REUSABILITY	Strong
OPS-REQ-SCALE	Strong
OPS-REQ-UNSILO	Strong
OPS-REQ-IT-INTEGRATION	Nice to have
OPS-REQ-ITER	Strong
OPS-REQ-Y2KG	Nice to have
OPS-REQ-TOOLS	Strong
OPS-REQ-IETF-TOOLS	Nice to have
OPS-REQ-NEW-NEED	Nice to have
OPS-REQ-GLUE	Nice to have

Table 2

### 3.4. Collaborative Prioritization

TBC to reflect the priorities set by the WG.

((Including Rob's Inputs))

- \* Move much faster (OPS-REQ-QUICK-BUT-WELL, OPS-REQ-TIMELY-DM)
- \* Implement minimal functionality, not bells and whistles (OPS-REQ-GUIDE-AND-PROFILE, OPS-REQ-ITER)
- \* Have running code (OPS-REQ-READILY-IMPLEM, OPS-REQ-TOOLS)
- \* Have vendors and operators on board at the time of developing the solution independent compliance suite to validate things.
- \* Need to coorelating data learned from different means (IPFIX, BMP, Models)

### 4. Security Considerations

This document does not define any protocol or architecture.

## 5. IANA Considerations

This document has no IANA actions.

## 6. Informative References

- [BCP127] Best Current Practice 127,  
<<https://www.rfc-editor.org/info/bcp127>>.  
At the time of writing, this BCP comprises the following:
- Audet, F., Ed. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, DOI 10.17487/RFC4787, January 2007, <<https://www.rfc-editor.org/info/rfc4787>>.
- Perreault, S., Ed., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, DOI 10.17487/RFC6888, April 2013, <<https://www.rfc-editor.org/info/rfc6888>>.
- Penno, R., Perreault, S., Boucadair, M., Ed., Sivakumar, S., and K. Naito, "Updates to Network Address Translation (NAT) Behavioral Requirements", BCP 127, RFC 7857, DOI 10.17487/RFC7857, April 2016, <<https://www.rfc-editor.org/info/rfc7857>>.
- [I-D.iab-nemops-workshop-report]  
Hardaker, W. and D. Dhody, "Report from the IAB Workshop on the Next Era of Network Management Operations (NEMOPS)", Work in Progress, Internet-Draft, draft-iab-nemops-workshop-report-04, 29 August 2025, <<https://datatracker.ietf.org/doc/html/draft-iab-nemops-workshop-report-04>>.
- [I-D.ietf-bmwg-containerized-infra]  
Ngc, T. M., Rao, S., Lee, J., and Y. Kim, "Considerations for Benchmarking Network Performance in Containerized Infrastructures", Work in Progress, Internet-Draft, draft-ietf-bmwg-containerized-infra-07, 1 July 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-bmwg-containerized-infra-07>>.
- [I-D.ietf-core-comi]  
Veillette, M., Van der Stok, P., Pelov, A., Bierman, A., and C. Bormann, "CoAP Management Interface (CORECONF)", Work in Progress, Internet-Draft, draft-ietf-core-comi-20, 6 May 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-core-comi-20>>.

`[I-D.ietf-core-sid]`

Veillette, M., Pelov, A., Petrov, I., Bormann, C., and M. Richardson, "YANG Schema Item iDentifier (YANG SID)", Work in Progress, Internet-Draft, draft-ietf-core-sid-24, 22 December 2023, <<https://datatracker.ietf.org/doc/html/draft-ietf-core-sid-24>>.

`[I-D.ietf-isis-sr-yang]`

Litkowski, S., Qu, Y., Lindem, A., Chen, H., and J. Tantsura, "A YANG Data Model for IS-IS Segment Routing over the MPLS Data Plane", Work in Progress, Internet-Draft, draft-ietf-isis-sr-yang-31, 6 May 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-isis-sr-yang-31>>.

`[I-D.ietf-netconf-https-notif]`

Jethanandani, M. and K. Watsen, "An HTTPS-based Transport for YANG Notifications", Work in Progress, Internet-Draft, draft-ietf-netconf-https-notif-15, 1 February 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-https-notif-15>>.

`[I-D.ietf-netconf-udp-notif]`

Feng, A. H., Francois, P., Zhou, T., Graf, T., and P. Lucente, "UDP-based Transport for Configured Subscriptions", Work in Progress, Internet-Draft, draft-ietf-netconf-udp-notif-23, 14 October 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-udp-notif-23>>.

`[I-D.ietf-opsawg-ntw-attachment-circuit]`

Boucadair, M., Roberts, R., de Dios, O. G., Barguil, S., and B. Wu, "A Network YANG Data Model for Attachment Circuits", Work in Progress, Internet-Draft, draft-ietf-opsawg-ntw-attachment-circuit-16, 23 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-ntw-attachment-circuit-16>>.

`[I-D.ietf-opsawg-teas-attachment-circuit]`

Boucadair, M., Roberts, R., de Dios, O. G., Barguil, S., and B. Wu, "YANG Data Models for Bearers and 'Attachment Circuits'-as-a-Service (ACaaS)", Work in Progress, Internet-Draft, draft-ietf-opsawg-teas-attachment-circuit-20, 23 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-teas-attachment-circuit-20>>.

- [I-D.marcas-nmop-knowledge-graph-yang]  
Martinez-Casanueva, I. D., Rodrguez, L. C., and P. Martinez-Julia, "Knowledge Graphs for YANG-based Network Management", Work in Progress, Internet-Draft, draft-marcas-nmop-knowledge-graph-yang-05, 21 October 2024, <<https://datatracker.ietf.org/doc/html/draft-marcas-nmop-knowledge-graph-yang-05>>.
- [I-D.openconfig-rtgwg-gnmi-spec]  
Shakir, R., Shaikh, A., Borman, P., Hines, M., Lebsack, C., and C. Morrow, "gRPC Network Management Interface (gNMI)", Work in Progress, Internet-Draft, draft-openconfig-rtgwg-gnmi-spec-01, 5 March 2018, <<https://datatracker.ietf.org/doc/html/draft-openconfig-rtgwg-gnmi-spec-01>>.
- [I-D.ramseyer-grow-peering-api]  
Aguado, C., Griswold, M., Ramseyer, J., Servin, A., and T. Strickx, "Peering API", Work in Progress, Internet-Draft, draft-ramseyer-grow-peering-api-06, 4 November 2024, <<https://datatracker.ietf.org/doc/html/draft-ramseyer-grow-peering-api-06>>.
- [I-D.tailhardat-nmop-incident-management-noria]  
Tailhardat, L., Troncy, R., Chabot, Y., Ramparany, F., and P. Folz, "Knowledge Graphs for Enhanced Cross-Operator Incident Management and Network Design", Work in Progress, Internet-Draft, draft-tailhardat-nmop-incident-management-noria-02, 15 May 2025, <<https://datatracker.ietf.org/doc/html/draft-tailhardat-nmop-incident-management-noria-02>>.
- [LOT2019] Poveda-Villalon, M., Fernandez-Izquierdo, A., Fernandez-Lopez, M., and R. Garcia-Castro, "LOT: An industrial oriented ontology engineering framework", 2022, <<https://doi.org/10.1016/j.engappai.2022.104755>>.
- [ODL] "Graph Model Overview", 2023, <<https://docs.opendaylight.org/projects/bgpcep/en/latest/graph/graph-user-guide-graph-model.html#>>.
- [RFC1213] McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", STD 17, RFC 1213, DOI 10.17487/RFC1213, March 1991, <<https://www.rfc-editor.org/rfc/rfc1213>>.

- [RFC1264] Hinden, R., "Internet Engineering Task Force Internet Routing Protocol Standardization Criteria", RFC 1264, DOI 10.17487/RFC1264, October 1991, <<https://www.rfc-editor.org/rfc/rfc1264>>.
- [RFC3084] Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R., and A. Smith, "COPS Usage for Policy Provisioning (COPS-PR)", RFC 3084, DOI 10.17487/RFC3084, March 2001, <<https://www.rfc-editor.org/rfc/rfc3084>>.
- [RFC3159] McCloghrie, K., Fine, M., Seligson, J., Chan, K., Hahn, S., Sahita, R., Smith, A., and F. Reichmeyer, "Structure of Policy Provisioning Information (SPPI)", RFC 3159, DOI 10.17487/RFC3159, August 2001, <<https://www.rfc-editor.org/rfc/rfc3159>>.
- [RFC3317] Chan, K., Sahita, R., Hahn, S., and K. McCloghrie, "Differentiated Services Quality of Service Policy Information Base", RFC 3317, DOI 10.17487/RFC3317, March 2003, <<https://www.rfc-editor.org/rfc/rfc3317>>.
- [RFC3318] Sahita, R., Ed., Hahn, S., Chan, K., and K. McCloghrie, "Framework Policy Information Base", RFC 3318, DOI 10.17487/RFC3318, March 2003, <<https://www.rfc-editor.org/rfc/rfc3318>>.
- [RFC3535] Schoenwaelder, J., "Overview of the 2002 IAB Network Management Workshop", RFC 3535, DOI 10.17487/RFC3535, May 2003, <<https://www.rfc-editor.org/rfc/rfc3535>>.
- [RFC3571] Rawlins, D., Kulkarni, A., Ho Chan, K., Bokaemper, M., and D. Dutt, "Framework Policy Information Base for Usage Feedback", RFC 3571, DOI 10.17487/RFC3571, August 2003, <<https://www.rfc-editor.org/rfc/rfc3571>>.
- [RFC4794] Fenner, B., "RFC 1264 Is Obsolete", RFC 4794, DOI 10.17487/RFC4794, December 2006, <<https://www.rfc-editor.org/rfc/rfc4794>>.
- [RFC5472] Zseby, T., Boschi, E., Brownlee, N., and B. Claise, "IP Flow Information Export (IPFIX) Applicability", RFC 5472, DOI 10.17487/RFC5472, March 2009, <<https://www.rfc-editor.org/rfc/rfc5472>>.



- [RFC5476] Claise, B., Ed., Johnson, A., and J. Quittek, "Packet Sampling (PSAMP) Protocol Specifications", RFC 5476, DOI 10.17487/RFC5476, March 2009, <<https://www.rfc-editor.org/rfc/rfc5476>>.
- [RFC5477] Dietz, T., Claise, B., Aitken, P., Dressler, F., and G. Carle, "Information Model for Packet Sampling Exports", RFC 5477, DOI 10.17487/RFC5477, March 2009, <<https://www.rfc-editor.org/rfc/rfc5477>>.
- [RFC5706] Harrington, D., "Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions", RFC 5706, DOI 10.17487/RFC5706, November 2009, <<https://www.rfc-editor.org/rfc/rfc5706>>.
- [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/rfc/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/rfc/rfc6241>>.
- [RFC6244] Shafer, P., "An Architecture for Network Management Using NETCONF and YANG", RFC 6244, DOI 10.17487/RFC6244, June 2011, <<https://www.rfc-editor.org/rfc/rfc6244>>.
- [RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 6353, DOI 10.17487/RFC6353, July 2011, <<https://www.rfc-editor.org/rfc/rfc6353>>.
- [RFC6632] Ersue, M., Ed. and B. Claise, "An Overview of the IETF Network Management Standards", RFC 6632, DOI 10.17487/RFC6632, June 2012, <<https://www.rfc-editor.org/rfc/rfc6632>>.
- [RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <<https://www.rfc-editor.org/rfc/rfc7011>>.

- [RFC7012] Claise, B., Ed. and B. Trammell, Ed., "Information Model for IP Flow Information Export (IPFIX)", RFC 7012, DOI 10.17487/RFC7012, September 2013, <<https://www.rfc-editor.org/rfc/rfc7012>>.
- [RFC7015] Trammell, B., Wagner, A., and B. Claise, "Flow Aggregation for the IP Flow Information Export (IPFIX) Protocol", RFC 7015, DOI 10.17487/RFC7015, September 2013, <<https://www.rfc-editor.org/rfc/rfc7015>>.
- [RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <<https://www.rfc-editor.org/rfc/rfc7149>>.
- [RFC7414] Duke, M., Braden, R., Eddy, W., Blanton, E., and A. Zimmermann, "A Roadmap for Transmission Control Protocol (TCP) Specification Documents", RFC 7414, DOI 10.17487/RFC7414, February 2015, <<https://www.rfc-editor.org/rfc/rfc7414>>.
- [RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC7426, January 2015, <<https://www.rfc-editor.org/rfc/rfc7426>>.
- [RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <<https://www.rfc-editor.org/rfc/rfc7854>>.
- [RFC7860] Merkle, J., Ed. and M. Lochter, "HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3", RFC 7860, DOI 10.17487/RFC7860, April 2016, <<https://www.rfc-editor.org/rfc/rfc7860>>.
- [RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <<https://www.rfc-editor.org/rfc/rfc7950>>.
- [RFC7951] Lhotka, L., "JSON Encoding of Data Modeled with YANG", RFC 7951, DOI 10.17487/RFC7951, August 2016, <<https://www.rfc-editor.org/rfc/rfc7951>>.
- [RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <<https://www.rfc-editor.org/rfc/rfc8040>>.

- [RFC8199] Bogdanovic, D., Claise, B., and C. Moberg, "YANG Module Classification", RFC 8199, DOI 10.17487/RFC8199, July 2017, <<https://www.rfc-editor.org/rfc/rfc8199>>.
- [RFC8299] Wu, Q., Ed., Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN Service Delivery", RFC 8299, DOI 10.17487/RFC8299, January 2018, <<https://www.rfc-editor.org/rfc/rfc8299>>.
- [RFC8309] Wu, Q., Liu, W., and A. Farrel, "Service Models Explained", RFC 8309, DOI 10.17487/RFC8309, January 2018, <<https://www.rfc-editor.org/rfc/rfc8309>>.
- [RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <<https://www.rfc-editor.org/rfc/rfc8341>>.
- [RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <<https://www.rfc-editor.org/rfc/rfc8342>>.
- [RFC838] Smallberg, D., "Who talks TCP?", RFC 838, DOI 10.17487/RFC0838, January 1983, <<https://www.rfc-editor.org/rfc/rfc838>>.
- [RFC8466] Wen, B., Fioccola, G., Ed., Xie, C., and L. Jalil, "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery", RFC 8466, DOI 10.17487/RFC8466, October 2018, <<https://www.rfc-editor.org/rfc/rfc8466>>.
- [RFC8519] Jethanandani, M., Agarwal, S., Huang, L., and D. Blair, "YANG Data Model for Network Access Control Lists (ACLs)", RFC 8519, DOI 10.17487/RFC8519, March 2019, <<https://www.rfc-editor.org/rfc/rfc8519>>.
- [RFC8528] Bjorklund, M. and L. Lhotka, "YANG Schema Mount", RFC 8528, DOI 10.17487/RFC8528, March 2019, <<https://www.rfc-editor.org/rfc/rfc8528>>.
- [RFC8557] Finn, N. and P. Thubert, "Deterministic Networking Problem Statement", RFC 8557, DOI 10.17487/RFC8557, May 2019, <<https://www.rfc-editor.org/rfc/rfc8557>>.

- [RFC8568] Bernardos, CJ., Rahman, A., Zuniga, JC., Contreras, LM., Aranda, P., and P. Lynch, "Network Virtualization Research Challenges", RFC 8568, DOI 10.17487/RFC8568, April 2019, <<https://www.rfc-editor.org/rfc/rfc8568>>.
- [RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", RFC 8639, DOI 10.17487/RFC8639, September 2019, <<https://www.rfc-editor.org/rfc/rfc8639>>.
- [RFC8640] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Dynamic Subscription to YANG Events and Datastores over NETCONF", RFC 8640, DOI 10.17487/RFC8640, September 2019, <<https://www.rfc-editor.org/rfc/rfc8640>>.
- [RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <<https://www.rfc-editor.org/rfc/rfc8641>>.
- [RFC8667] Previdi, S., Ed., Ginsberg, L., Ed., Filsfils, C., Bashandy, A., Gredler, H., and B. Decraene, "IS-IS Extensions for Segment Routing", RFC 8667, DOI 10.17487/RFC8667, December 2019, <<https://www.rfc-editor.org/rfc/rfc8667>>.
- [RFC8791] Bierman, A., Bjorklund, M., and K. Watsen, "YANG Data Structure Extensions", RFC 8791, DOI 10.17487/RFC8791, June 2020, <<https://www.rfc-editor.org/rfc/rfc8791>>.
- [RFC8955] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <<https://www.rfc-editor.org/rfc/rfc8955>>.
- [RFC8956] Loibl, C., Ed., Raszuk, R., Ed., and S. Hares, Ed., "Dissemination of Flow Specification Rules for IPv6", RFC 8956, DOI 10.17487/RFC8956, December 2020, <<https://www.rfc-editor.org/rfc/rfc8956>>.
- [RFC8969] Wu, Q., Ed., Boucadair, M., Ed., Lopez, D., Xie, C., and L. Geng, "A Framework for Automating Service and Network Management with YANG", RFC 8969, DOI 10.17487/RFC8969, January 2021, <<https://www.rfc-editor.org/rfc/rfc8969>>.

- [RFC9132] Boucadair, M., Ed., Shallow, J., and T. Reddy.K, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", RFC 9132, DOI 10.17487/RFC9132, September 2021, <<https://www.rfc-editor.org/rfc/rfc9132>>.
- [RFC9144] Clemm, A., Qu, Y., Tantsura, J., and A. Bierman, "Comparison of Network Management Datastore Architecture (NMDA) Datastores", RFC 9144, DOI 10.17487/RFC9144, December 2021, <<https://www.rfc-editor.org/rfc/rfc9144>>.
- [RFC9182] Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., Munoz, L., and A. Aguado, "A YANG Network Data Model for Layer 3 VPNs", RFC 9182, DOI 10.17487/RFC9182, February 2022, <<https://www.rfc-editor.org/rfc/rfc9182>>.
- [RFC9232] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", RFC 9232, DOI 10.17487/RFC9232, May 2022, <<https://www.rfc-editor.org/rfc/rfc9232>>.
- [RFC9254] Veillette, M., Ed., Petrov, I., Ed., Pelov, A., Bormann, C., and M. Richardson, "Encoding of Data Modeled with YANG in the Concise Binary Object Representation (CBOR)", RFC 9254, DOI 10.17487/RFC9254, July 2022, <<https://www.rfc-editor.org/rfc/rfc9254>>.
- [RFC9291] Boucadair, M., Ed., Gonzalez de Dios, O., Ed., Barguil, S., and L. Munoz, "A YANG Network Data Model for Layer 2 VPNs", RFC 9291, DOI 10.17487/RFC9291, September 2022, <<https://www.rfc-editor.org/rfc/rfc9291>>.
- [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/rfc/rfc9315>>.
- [RFC9456] Vaughn, K., Ed., "Updates to the TLS Transport Model for SNMP", RFC 9456, DOI 10.17487/RFC9456, November 2023, <<https://www.rfc-editor.org/rfc/rfc9456>>.
- [RFC9543] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "A Framework for Network Slices in Networks Built from IETF Technologies", RFC 9543, DOI 10.17487/RFC9543, March 2024, <<https://www.rfc-editor.org/rfc/rfc9543>>.

[Widoco2017]

Garijo, D., "WIDOCO: a wizard for documenting ontologies", 2017, <<http://dgarijo.com/papers/widoco-iswc2017.pdf>>.

## Appendix A. Assessment of RFC 3535 Operator Requirements

### A.1. Detailed Analysis

Section 3 of [RFC3535] includes the following recommendations:

#### 3535-OPS-REQ-EASE-USE:

| Ease of use is a key requirement for any network management  
| technology from the operators point of view.

\*Status Update\*: This is still a valid requirement. It is even exacerbated with the amount of techniques and extensions that were specified since then.

#### 3535-OPS-REQ-CONFIG-OPS-SEPARATE:

| It is necessary to make a clear distinction between configuration  
| data, data that describes operational state and statistics. Some  
| devices make it very hard to determine which parameters were  
| administratively configured and which were obtained via other  
| mechanisms such as routing protocols.

\*Status Update\*: This requirement was taken into account when designing IETF solutions. Specifically, datastores are a fundamental concept in NETCONF/YANG (e.g., [RFC8342]).

#### 3535-OPS-REQ-CONFIG-OPS-FETCH-SEPARATE:

| It is required to be able to fetch separately configuration data,  
| operational state data, and statistics from devices, and to be  
| able to compare these between devices.

\*Status Update\*: This is supported by NETCONF and RESTCONF.

#### 3535-OPS-REQ-NETWORK-NOT-DEVICE:

| It is necessary to enable operators to concentrate on the  
| configuration of the network as a whole rather than individual  
| devices.

\*Status Update\*: Protocols such as NETCONF supports means to handle

transactions at the level of a network. For example, a controller can establish parallel sessions with a set of devices and make use of confirmed commit.

Also, [RFC8969] describes how YANG/RESTCONF/YANG can be used to manage a network and map it to involves underlying functions/nodes. Several service and network data models are required for this aim.

The IETF defined in the past models to manage few services such as VPN at both service and network levels (e.g., the Layer 2 Service Model (L2SM) [RFC8466], the Layer 3 Service Model (L3SM) [RFC8299], the Layer 2 Network Model (L2NM) [RFC9291], and the Layer 3 Network Model (L3NM) [RFC9182]).

A similar effort is currently ongoing for handling attachment circuits at both service and network layers (e.g., [I-D.ietf-opsawg-teas-attachment-circuit], [I-D.ietf-opsawg-ntw-attachment-circuit]).

More effort is still needed in this area.

#### 3535-OPS-REQ-NETWORK-WIDE-TRANSACTIONS:

| Support for configuration transactions across a number of devices  
| would significantly simplify network configuration management.

\*Status Update\*: This feature is supported by NETCONF.

#### 3535-OPS-REQ-CONFIG-DIFF:

| Given configuration A and configuration B, it should be possible  
| to generate the operations necessary to get from A to B with  
| minimal state changes and effects on network and systems. It is  
| important to minimize the impact caused by configuration changes.

\*Status Update\*: This feature is supported by NETCONF.

#### 3535-OPS-REQ-CONFIG-DUMP-RESTORE:

| A mechanism to dump and restore configurations is a primitive  
| operation needed by operators. Standards for pulling and pushing  
| configurations from/to devices are desirable.

\*Status Update\*: This feature is supported by NETCONF.

#### 3535-OPS-REQ-CONFIG-CONSISTENCY-CHECK:

| It must be easy to do consistency checks of configurations over  
| time and between the ends of a link in order to determine the  
| changes between two configurations and whether those  
| configurations are consistent.

\*Status Update\*: A mechanism is specified in [RFC9144].

#### 3535-OPS-REQ-CONFIG-NETWORK-WIDE-SCHEMA:

| Network wide configurations are typically stored in central  
| master databases and transformed into formats that can be pushed  
| to devices, either by generating sequences of CLI commands or  
| complete configuration files that are pushed to devices. There  
| is no common database schema for network configuration, although  
| the models used by various operators are probably very similar.  
| It is desirable to extract, document, and standardize the common  
| parts of these network wide configuration database schemas.

\*Status Update\*: Covered by current implementations.

#### 3535-OPS-REQ-TXT-PROCESSING-TOOLS:

| It is highly desirable that text processing tools such as diff,  
| and version management tools such as RCS or CVS, can be used to  
| process configurations, which implies that devices should not  
| arbitrarily reorder data such as access control lists.

\*Status Update\*: This is deployment-specific.

#### 3535-OPS-REQ-ACCESS-CONTROL-OPS-CENTRIC:

| The granularity of access control needed on management interfaces  
| needs to match operational needs. Typical requirements are a  
| role-based access control model and the principle of least  
| privilege, where a user can be given only the minimum access  
| necessary to perform a required task.

\*Status Update\*: Role-based Access Control (RBAC) is supported by  
existing implementation. Also, the IETF defined [RFC8341] for  
this purpose.

#### 3535-OPS-REQ-ACCESS-CONTROL-CHECKS:

| It must be possible to do consistency checks of access control  
| lists across devices.

\*Status Update\*: This is implementation-specific.



## 3535-OPS-REQ-CONFIG-SEPARATE-DISTRIB-ACTIV:

It is important to distinguish between the distribution of configurations and the activation of a certain configuration. Devices should be able to hold multiple configurations.

\*Status Update\*: This is supported by existing NETCONF methods.

## 3535-OPS-REQ-ACCESS-CONTROL-BOTH-DATA-TASK:

SNMP access control is data-oriented, while CLI access control is usually command (task) oriented. Depending on the management function, sometimes data-oriented or task-oriented access control makes more sense. As such, it is a requirement to support both data-oriented and task-oriented access control.

\*Status Update\*: This is supported by [RFC8341].

## A.2. Summary

RFC3535 Ops Requirement Label	Status
3535-OPS-REQ-EASE-USE	Still Applicable
3535-OPS-REQ-CONFIG-OPS-SEPARATE	A solution was standarized
3535-OPS-REQ-CONFIG-OPS-FETCH-SEPARATE	A solution was standarized
3535-OPS-REQ-NETWORK-NOT-DEVICE	Protocol (OK), DM (Still Applicable)
3535-OPS-REQ-NETWORK-WIDE-TRANSACTIONS	A solution was standarized
3535-OPS-REQ-CONFIG-DIFF	A solution was standarized
3535-OPS-REQ-CONFIG-DUMP-RESTORE	A solution was standarized
3535-OPS-REQ-CONFIG-CONSISTENCY-CHECK	Implementation-specific
3535-OPS-REQ-CONFIG-NETWORK-WIDE-SCHEMA	Still Applicable
3535-OPS-REQ-TXT-PROCESSING-TOOLS	Deployment-specific

3535-OPS-REQ-ACCESS-CONTROL-OPS-CENTRIC	Implementation-specific
3535-OPS-REQ-ACCESS-CONTROL-CHECKS	Implementation-specific
3535-OPS-REQ-CONFIG-SEPARATE-DISTRIB-ACTIV	A solution was standarized
3535-OPS-REQ-ACCESS-CONTROL-BOTH-DATA-TASK	A solution was standarized

Table 3

## Appendix B. Assessment of RFC 3535 Recommendations

### B.1. Detailed Analysis

Section 6 of [RFC3535] includes the following recommendations:

#### 3535-RECO-STOP-MANDATE-MIB:

The workshop recommended that the IETF stop forcing working groups to provide writable MIB modules. It should be the decision of the working group whether they want to provide writable objects or not.

**\*Status Update\*:** In 2014, the IESG published a statement Writable MIB Module, which states that:

SNMP MIB modules creating and modifying configuration state should only be produced by working groups in cases of clear utility and consensus to use SNMP write operations for configuration, and in consultation with the OPS ADs/MIB doctors.

#### 3535-RECO-MIB-INVESTIGATE:

The workshop recommended that a group be formed to investigate why current MIB modules do not contain all the objects needed by operators to monitor their networks.

**\*Status Update\*:** No such a group was formed in the IETF.

#### 3535-RECO-SNMP-WG4MONITORING:

| The workshop recommended that a group be formed to investigate why  
| the current SNMP protocol does not satisfy all the monitoring  
| requirements of operators.

\*Status Update\*: No such a group was formed in the IETF.

#### 3535-RECO-FOCUS-IETF-CONFIG-MECHANISMS:

| The workshop recommended, with strong consensus from both protocol  
| developers and operators, that the IETF focus resources on the  
| standardization of configuration management mechanisms.

\*Status Update\*: The IETF specified NETCONF [RFC6241], RESTCONF [RFC8040], CORECONF [I-D.ietf-core-comi], and YANG.

YANG is a transport-independent data modeling language. It can be used independently of NETCONF/RESTCONF. For example, YANG can be used to define abstract data structures [RFC8791] that can be manipulated by other protocols (e.g., [RFC9132]).

#### 3535-RECO-FOCUS-XML:

| The workshop recommended, with strong consensus from the operators  
| and rough consensus from the protocol developers, that the  
| IETF/IRTF should spend resources on the development and  
| standardization of XML-based device configuration and management  
| technologies (such as common XML configuration schemas, exchange  
| protocols and so on).

\*Status Update\*: This recommendation was followed in base specifications. This recommendation was also mirrored in other documents such as [RFC5706].

However, the IETF integrated support for other encoding such as JSON.

#### 3535-RECO-NO-HTTP:

| The workshop recommended, with strong consensus from the operators  
| and rough consensus from the protocol developers, that the  
| IETF/IRTF should not spend resources on developing HTML-based or  
| HTTP-based methods for configuration management.

\*Status Update\*: The IETF deviated from this recommendation, e.g., RESTCONF [RFC8040] or CoAP Management Interface (CORECONF) [I-D.ietf-core-comi].

#### 3535-RECO-MAINTAIN-SMI-SPPI:

| The workshop recommended, with rough consensus from the operators  
| and strong consensus from the protocol developers, that the IETF  
| should continue to spend resources on the evolution of the  
| SMI/SPPI data definition languages as being done in the SMIng  
| working group.

\*Status Update\*: SMIng WG was concluded in 2003-04-04.

#### 3535-RECO-IETF2FIX-MIB:

| The workshop recommended, with split consensus from the operators  
| and rough consensus from the protocol developers, that the IETF  
| should spend resources on fixing the MIB development and  
| standardization processs.

\*Status Update\*: The IETF dedicated some resources to fix some SNMP shortcomings with a focus on security (e.g., Transport Layer Security (TLS) Transport Model for the SNMP [RFC6353] or [RFC9456], HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3 [RFC7860]).

Section 6 of [RFC3535] also includes the following but without tagging them as recommendations:

#### 3535-MISC-NO-CIM:

| The workshop had split consensus from the operators and rough  
| consensus from the protocol developers, that the IETF should not  
| focus resources on CIM extensions.

\*Status Update\*: The IETF didn't dedicate any resources on CIM extensions.

#### 3535-MISC-ABANDON-PIB:

| The workshop had rough consensus from the protocol developers  
| that the IETF should not spend resources on COPS-PR development.  
| So far, the operators have only very limited experience with  
| COPS-PR. In general, however, they felt that further development  
| of COPS-PR might be a waste of resources as they assume that  
| COPS-PR does not really address their requirements.

\*Status Update\*: The IETF has reclassified COPS Usage for Policy Provisioning [RFC3084] to Historic status.

#### 3535-MISC-ABANDON-COPS-PR:

The workshop had rough consensus from the protocol developers that the IETF should not spend resources on SPPI PIB definitions. The operators had rough consensus that they do not care about SPPI PIBs.

**\*Status Update\*:** The IETF has reclassified Structure of Policy Provisioning Information [RFC3159], as well as three Policy Information Bases ([RFC3317], [RFC3318], and [RFC3571]) to Historic status.

## B.2. Summary

RFC3535 Recommendation Label	Status
3535-RECO-STOP- MANDATE-MIB	Done, IESG Statement on Writable MIB Module (2014)
3535-RECO-MIB- INVESTIGATE	No such a group was formed
3535-RECO-SNMP- WG4MONITORING	No such a group was formed
3535-RECO-FOCUS-IETF- CONFIG-MECHANISMS	NETCONF/RESTCONF/CORECONF/YANG/COMI/ etc.
3535-RECO-FOCUS-XML	The recommendation was followed
3535-RECO-NO-HTTP	The IETF deviated from this recommendation, e.g., RESTCONF or CoAP Management Interface (CORECONF)
3535-RECO-MAINTAIN- SMI-SPPI	SMIng WG was concluded in 2003-04-04
3535-RECO-IETF2FIX- MIB	The IETF dedicated resources to fix some SNMP shortcomings with a focus on security
3535-MISC-NO-CIM	The IETF didn't dedicate any resources on CIM extensions
3535-MISC-ABANDON- COPS-PR	The IETF has reclassified COPS-PR to Historic status
3535-MISC-ABANDON-PIB	The IETF has reclassified SPPI, as

	well as three PIBs to Historic	
	status	
+-----+	+-----+	+-----+

Table 4

#### Acknowledgments

Thanks to Christian Jacquenet and Jean-Michel Combes for their inputs.

Thanks to Benot Claise and Alex Clemm for the comments.

Many of the requirements were extracted from contributions to the IAB Next Era of Network Management Operations (NEMOPS) Workshop [I-D.iab-nemops-workshop-report].

Thanks to Ian Farrer, Brad Peters, Chongfeng Xie, and Qin Wu for their contribution to consolidate the requirements.

#### Contributors

Lionel Tailhardat  
Orange  
Email: lionel.tailhardat@orange.com

#### Authors' Addresses

Mohamed Boucadair  
Orange  
Email: mohamed.boucadair@orange.com

Luis M. Contreras  
Telefonica  
Email: luismiguel.contrerasmurillo@telefonica.com

Oscar Gonzalez de Dios  
Telefonica  
Email: oscar.gonzalezdedios@telefonica.com

Thomas Graf  
Swisscom  
Email: thomas.graf@swisscom.com

Reshad Rahman  
Equinix  
Email: rrahman@equinix.com