

Operationalizing Network & Service abstractionNs (ONSEN) Problem Statement

Benoît Claise

March 17th 2026

IAB Workshop on the Next Era of Network Management Operations (NEMOPS)

- Review the outcome documented in RFC3535 over the past 20 years. (*December 3-5, 2024*)
- RFC3535, “Overview of the 2002 IAB Network Management Workshop”:
 - This leads to the NETCONF and then NETMOD WG creation

draft-iab-nemops-workshop-report-04

Network Working Group
Internet-Draft

W. Hardaker

Intended status: Informational

D. Dhody

Expires: 2 March 2026

29 August 2025

Report from the IAB Workshop on the Next Era of Network Management
Operations (NEMOPS)

draft-iab-nemops-workshop-report-04

Abstract

The "Next Era of Network Management Operations (NEMOPS)" workshop was convened by the Internet Architecture Board (IAB) from December 3-5, 2024, as a three-day online meeting. It builds on a previous 2002 workshop, the outcome of which was documented in RFC 3535, identifying 14 operator requirements for consideration in future network management protocol design and related data models, along with some recommendations for the IETF. Much has changed in the Internet's operation and technological foundations since then. The NEMOPS workshop reviewed the past outcomes and discussed any operational barriers that prevented these technologies from being widely implemented. With the industry, network operators and protocol engineers working in collaboration, the workshop developed a suggested plan of action and network management recommendations for the IETF and IRTF. Building on RFC 3535, this document provides the report of the follow-up IAB workshop on Network Management.

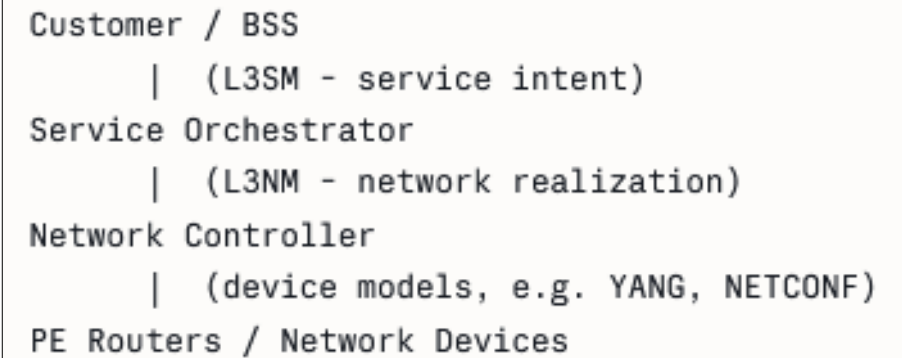
NEMOPS: One key ONSSEN-related Observation

```
It was noted that IETF's focus should be on defining abstract/  
service-level data models since it is the only thing the  
community may ever agree on.
```

Report from the IAB Workshop on the Next Era of Network Management Operations (NEMOPS):

<https://datatracker.ietf.org/doc/draft-iab-nemops-workshop-report/>

Service Models are Hard to Operate



- IETF has produced numerous YANG service data models (e.g., L3SM, L3NM, L2SM, etc.) for automating connectivity services.
 - So not a lack of models
- However, operators report persistent challenges in “using” these models in production.
 - In consistent, scalable, and automated way.
 - In multi-vendor, multi-domain environments.
- In practice, APIs generated from similar YANG models often differ in service semantics, complicating integration across systems, vendors, and deployment environments.

L3SM Reusability?

- Exercise in draft-xie-onsen-problem-statement:
Can we have a new “data-intensive workloads transmission” based on L3SM?
=> requires on-demand, ultra-high bandwidth, predictable completion times (deterministic scheduling), dynamic workflows
- L3SM:
 - Lacks concept of “temporary” (assumes all connectivity is persistent)
 - Lacks dynamic bandwidth (only fixed bandwidth values set at service creation)
 - Lacks integration with SLOs like latency, jitter, or guaranteed throughput.
 - Lacks built-in mechanisms to integrate slice service templates
- L3SM difficult to be reused

High Levels of Duplication between the Service Models

```

module: ietf-l2vpn-svc
  +--rw l2vpn-svc
    +--rw vpn-profiles
      | +--rw valid-provider-identifiers
      |   +--rw cloud-identifier* string{cloud-access}?
      |   +--rw qos-profile-identifier* string
      |
      ...
    +--rw vpn-services
      | +--rw vpn-service* [vpn-id]
      |   +--rw vpn-id                               svc-id
      |   +--rw vpn-svc-type?                         identityref
      |   +--rw customer-name?                       string
      |   +--rw svc-topo?                             identityref
      |
      ...
    +--rw sites
      +--rw site* [site-id]
      +--rw site-id                               string
      +--rw site-vpn-flavor?                       identityref
      +--rw devices
      | +--rw device* [device-id]
      |   +--rw device-id       string
      |   +--rw location
      |
      ...
    +--rw vpn-policies
      | +--rw vpn-policy* [vpn-policy-id]
      |   +--rw vpn-policy-id   string
      |
      ...
  
```

```

module: ietf-l3vpn-svc
  +--rw l3vpn-svc
    +--rw vpn-profiles
      | +--rw valid-provider-identifiers
      |   +--rw cloud-identifier* [id] {cloud-access}?
      |
      ...
    +--rw vpn-services
      | +--rw vpn-service* [vpn-id]
      |   +--rw vpn-id                               svc-id
      |   +--rw customer-name?                       string
      |   +--rw vpn-service-topology?               identityref
      |   +--rw cloud-accesses {cloud-access}?
      |     | +--rw cloud-access* [cloud-identifier]
      |
      ...
    +--rw sites
      +--rw site* [site-id]
      +--rw site-id                               svc-id
      |
      ...
      +--rw devices
      | +--rw device* [device-id]
      |   +--rw device-id       svc-id
      |
      ...
    +--rw vpn-policies
      | +--rw vpn-policy* [vpn-policy-id]
      |   +--rw vpn-policy-id   svc-id
      |   +--rw entries* [id]
      |
      ...
  
```

- If offers both types of services, must manage two separate models with a large amount of duplicated information.
- What about a new service, duplicate again?

IETF Service Models & OSS/BSS Integration Challenge

- **Challenge**

- How to integrate easily YANG-based service abstractions with external systems (OSS/BSS, Orchestration)

- **The Reality**

- Operators may purchase commercial OSS products with TMF-aligned OpenAPIs.
- These commercial products cannot natively consume diverse, vendor-specific YANG-based network service models.

IETF Service Models & OSS/BSS Integration Challenge (Model)

- Misalignment between Layers
- **The Problem:** Service abstractions may not cleanly map to underlying network capabilities. Network models may expose parameters without clear service-level semantics.
- Operator needs to define its own API
 - (see the figure)

```
{
  "externalId": "VPN-ORDER-001",
  "description": "VPN service order",
  "orderItem": [
    {
      "id": "1",
      "action": "add",
      "service": {
        "name": "VPN Service",
        "description": "VPN Service for customer",
        "category": "Dedicated line",
        "state": "active",
        "serviceSpecification": {
          "id": "VPN-service-spec",
          "href":
"http://catalog.example.com/serviceSpecification/
          "name": "VPN Service Specification",
          "version": "1.0"
        },
        "serviceCharacteristic": [
          {
            "name": "MemberCount",
            "value": 3
          },
          {
            "name": "StartTime",
            "value": "2026-04-01T09:00:00Z"
          }
        ]
      }
    }
  ]
}
```

Fragmented Lifecycles Challenge

- Operational workflows (instantiation, monitoring, modification, decommissioning) are fragmented and handled inconsistently
- Examples:
 - Activation time.
 - Service duration and expiration.
 - Rollback behavior.

Limited Observability/Operational Data

- Current service models focus on configuration but poor at providing feedback on the outcome.
- There are limited standardized mechanisms for reporting what the current provisioning status for a requested service over its lifecycle.
- Inability to observe the current status of provisioned services (e.g., through active service health-checking)

• Ex: L3SM

```
    +--ro actual-site-start?      yang:date-and-time
    +--ro actual-site-stop?      yang:date-and-time
```

- **The Impact:**

- Preventing closed-loop automation.
- It increases reliance on manual monitoring and troubleshooting to verify that the service intent is actually being met.

Conclusions:

- Service models are important
- But there are challenges, as demonstrated
 - NEMOPS IAB challenges
 - draft-xie-onsen-problem-statement
 - draft-lambrechts-onsen-svc-yang
 - Some more challenges in the draft
- We could really do better in coordinating those services models and solving those challenges

Q&A
Thanks