ETSI GS NFV-IFA 040 V4.3.1 (2022-05)

Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGS/NFV-IFA040ed431

Keywords
container, interface, management, NFV,
orchestration, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies the NFV object model for OS container management and orchestration. The present document also specifies requirements on the list of services to be offered by architectural elements providing the Container Infrastructure Service Management (CISM) and Container Image Registry (CIR) functions described in ETSI GR NFV-IFA 029 [i.2] and on the interfaces for exposing these services to NFV-MANO and other consuming entities.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Functional requirements specification".

[2] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; VNF Descriptor and Packaging Specification".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ETSI GR NFV-IFA 029: "Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"".

[i.3] Void.

[i.4] ETSI GS NFV 006: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Architectural Framework Specification".

[i.5] ETSI GR NFV-IFA 038: "Network Functions Virtualisation (NFV) Release 4; Architectural framework; Report on network connectivity for container-based VNF".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.1] and the following apply:

Compute MCIO (MCIO-C): MCIO which declarative descriptor specifies compute infrastructure resource requests

containerized workload: VNF or VNF component designed to be deployed and managed on Container Infrastructure Service (CIS) instances

namespace: logical grouping for a particular set of identifiers, resources, policies and authorizations

namespace quota: upper limit on specific types of resources that can be used by one or more Managed Container Infrastructure Objects within the scope of a namespace

Network MCIO (MCIO-N): MCIO which declarative descriptor specifies network infrastructure resource requests.

OS container: virtualisation container utilizing a shared Operating System (OS) kernel of its host

NOTE: The host providing the shared OS kernel can be a physical compute node or another virtualisation container.

Storage MCIO (MCIO-S): MCIO which declarative descriptor specifies storage infrastructure resource requests

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.1] and the following apply:

CIR	Container Image Registry
MCIO-C	Compute MCIO
MCIO-N	Network MCIO
MCIO-S	Storage MCIO
OS	Operating System
RBAC	Role-Based Access Control

4 Overview and framework for OS container management and orchestration

4.1 Introduction

The NFV-MANO architectural framework described in ETSI GS NFV 006 [i.4] identifies the following functional blocks/entities:

- NFV Orchestrator (NFVO);
- VNF Manager (VNFM); and
- Virtualised Infrastructure Manager (VIM).

ETSI GR NFV-IFA 029 [i.2] identifies the following functions required for the management and orchestration of OS containers:

- Container Infrastructure Service Management (CISM); and
- Container Image Registry (CIR).

The CISM is responsible for maintaining the containerized workloads as Managed Container Infrastructure Objects (MCIOs).

The CIR is responsible for storing and maintaining information of OS container software images.

The functional requirements for the CISM and the CIR specified in ETSI GS NFV-IFA 010 [1] shall apply.

The requirements for the VNF Package and the information elements for the VNFD to support OS container management and orchestration specified in ETSI GS NFV-IFA 011 [2] shall apply.

The present document specifies the requirements on the list of services to be provided by the CISM and the CIR, and on the management services interfaces to expose these services to other NFV-MANO functional entities and/or external entities outside NFV-MANO.

4.2 Framework

4.2.1 Overview

The CISM and CIR functions provide one or more management capabilities which can be invoked by using one or more management service interfaces.

The services for the management and orchestration of OS containers are exposed via management service interfaces by the CISM and CIR functions as specified in the present document. The management service interfaces can be consumed by:

- Other NFV-MANO functional entities; and/or
- Consumers outside NFV-MANO.

The CISM and CIR functions produce the management service interfaces, which are invoked by consumers within an NFV-MANO functional entity and/or within an external entity outside NFV-MANO.

4.2.2 CISM function and CISM services

The CISM function offers multiple types of CISM services, i.e. OS container management services or other services, which are exposed by the OS container management service interfaces or other service interfaces respectively. More than one instance of an OS container management service interface is possible to cater for the possibility to expose different versions of a type of OS container management service interface. Other services than the OS container management services that may be offered by the CISM are not specified in the present document.

Figure 4.2.2-1 illustrates an example of the relationship between the different concepts introduced in the present clause.

The CISM function acts as the producer of three specific instances of OS container management services and their associated OS container management service interfaces plus one instance of another CISM service and its associated service interface. In this example, the types of CISM services are: "OS container management service A", "OS container management service B", "CISM service C", and "OS container management service D". The instance of "OS container management service D" is available and accessible via the same type of OS container management service interface, but through different interface instances providing different API endpoints. As an example, the API endpoints can provide different paths indicating the support of different versions of the same type of OS container management service interface. The example in figure 4.2.2-1 also shows three consumer instances, namely "NFV-MANO functional entity X", "NFV-MANO functional entity Y", and "external entity Z". Each consumer instance may access one or more CISM services via their respective service interfaces.

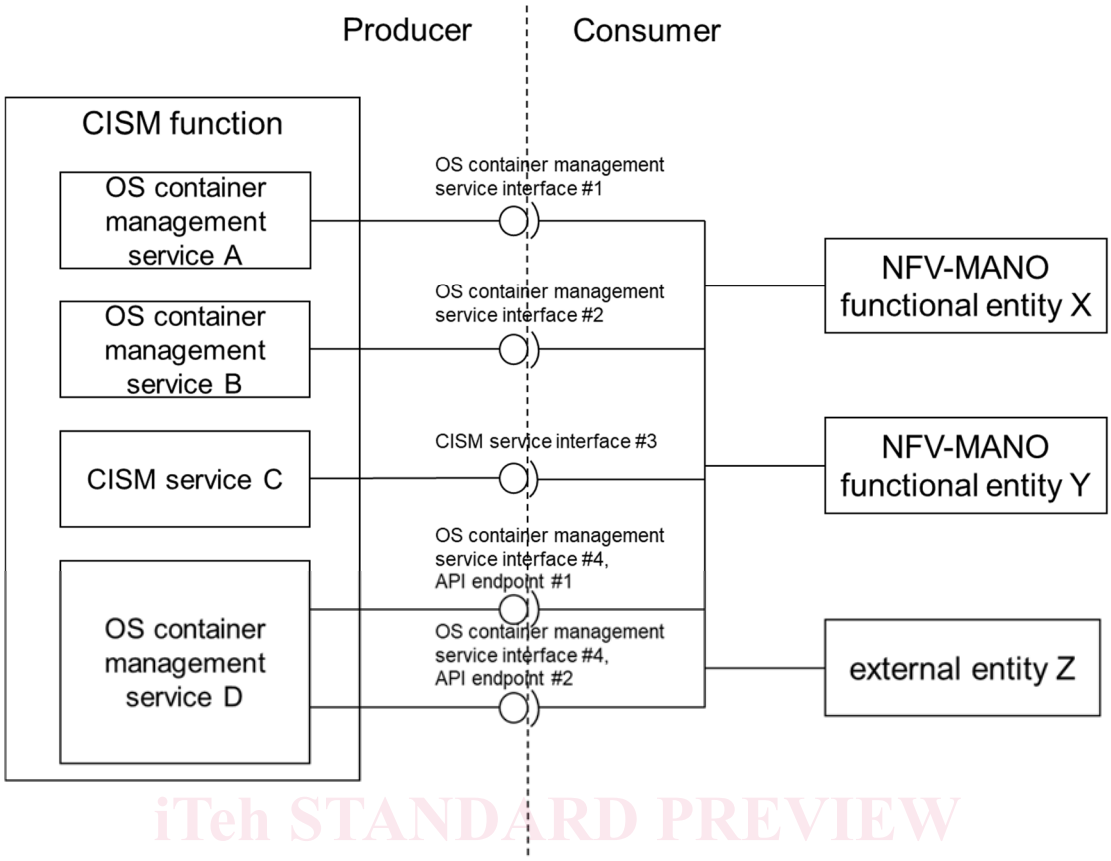

Figure 4.2.2-1: Example of CISM function, CISM services, OS container management service interfaces, and consumers

4.2.3 CIR function and CIR services

The CIR function offers multiple types of OS container image management services, which are exposed by the OS container image management service interfaces. More than one instance of an OS container image management service interface is possible to cater for the possibility to expose different versions of a type of OS container image management service interface.

Figure 4.2.3-1 illustrates an example of the relationship between the different concepts introduced in the present clause.

The CIR function acts as the producer of three specific instances of OS container image management services and their associated OS container image management service interfaces. In this example, the types of CIR services are: "OS container image management service A", "OS container image management service B", and "OS container image management service C". The instance of "OS container image management service C" is available and accessible via the same type of OS container image management service interface, but through different interface instances providing different API endpoints. As an example, the API endpoints can provide different paths indicating the support of different versions of the same type of OS container image management service interface. The example in figure 4.2.3-1 also shows three consumer instances, namely "NFV-MANO functional entity X", "NFV-MANO functional entity Y", and "external entity Z". Each consumer instance may access one or more OS container image management services via their respective OS container image management service interfaces.

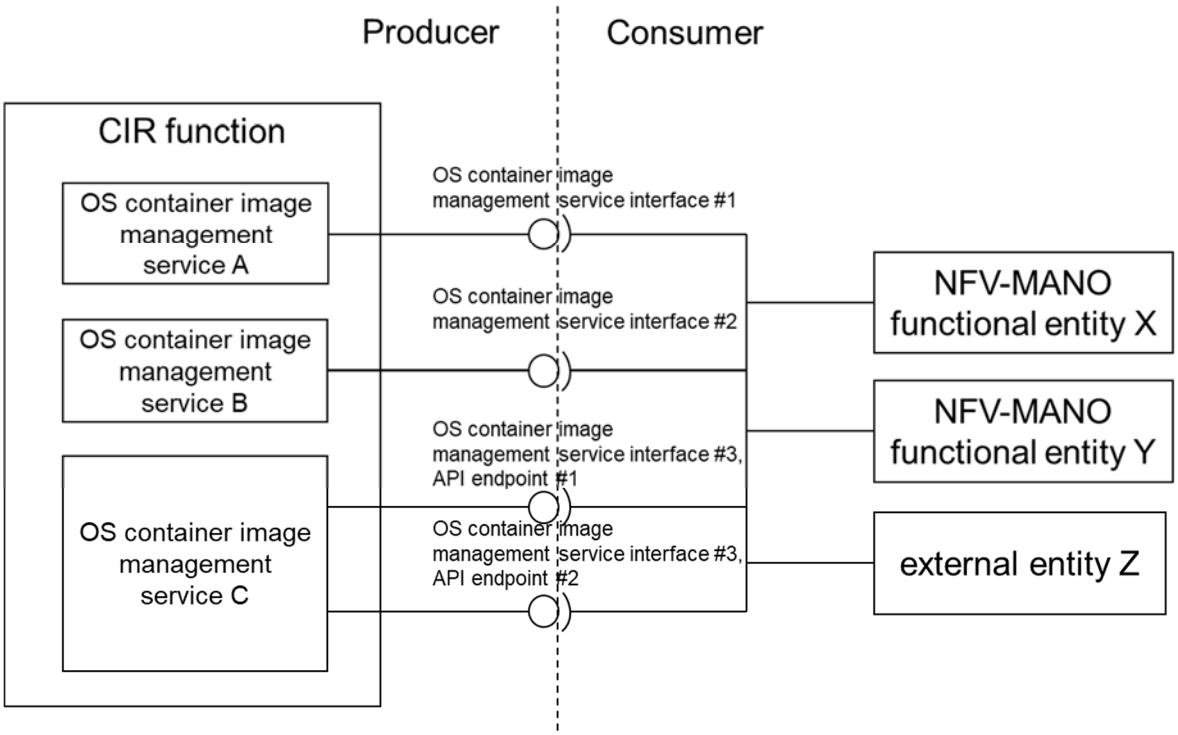

Figure 4.2.3-1: Example of CIR function, OS container image management services, OS container image management service interfaces, and consumers

5 OS container NFV object model

5.1 Introduction

Clause 5 of the present document specifies the NFV object model for OS container management and orchestration. It describes and specifies abstract NFV objects related to OS container management and orchestration. It also specifies the relationship of these abstract NFV objects to the information models of NFV-MANO. The terms for these abstract NFV objects are used in the subsequent clauses of the present document to specify generic requirements on the services and management service interfaces exposed by the CISM and the CIR. The abstract NFV objects are also expected to be used in specifications profiling APIs of de-facto standard solutions, to map the abstract NFV objects to objects of the specific de-facto standard solution.

Some of the abstract NFV objects for OS container management and orchestration have been introduced in ETSI GR NFV-IFA 029 [i.2], but are formally specified in the present document.

5.2 Managed objects

5.2.1 Managed Container Infrastructure Object

5.2.1.1 Purpose

A Managed Container Infrastructure Object (MCIO) is an abstract NFV object for OS container management and orchestration, introduced by ETSI GR NFV-IFA 029 [i.2]. It is an object managed and exposed by the CISM, characterized by the desired and actual state of a containerized workload, including its requested and allocated infrastructure resources and applicable policies. The desired state of an MCIO is specified in a declarative descriptor which may include references to OS container images. This declarative descriptor is interpreted by the CISM.

Different types of MCIOs with different requested infrastructure resources exist. An MCIO is created by the CISM by allocating its requested infrastructure resources on Container Infrastructure Service (CIS) instances. Dependent on its type, the creation of an MCIO may include the deployment of an OS container image. MCIOs are lifecycle managed via change requests on their desired state, utilizing a modified declarative descriptor sent to the CISM, which adapts the infrastructure resource allocations according to the changed infrastructure resource requests.

5.2.1.2 Relationship to the existing NFV-MANO information model

Dependent on its type, an MCIO is represented by a corresponding object in the existing NFV-MANO information model. An MCIO requesting compute and/or storage infrastructure resources is mapped to a VNF Component (VNFC). An MCIO requesting network infrastructure resources for VNF external connectivity is mapped to an applicable sub-class of a Connection Point (CP). Figure 5.2.1.2-1 illustrates the mapping of an MCIO to the existing NFV-MANO logical objects.

NOTE 1: There is no MCIO type equivalent to an internal Virtual Link (VL).

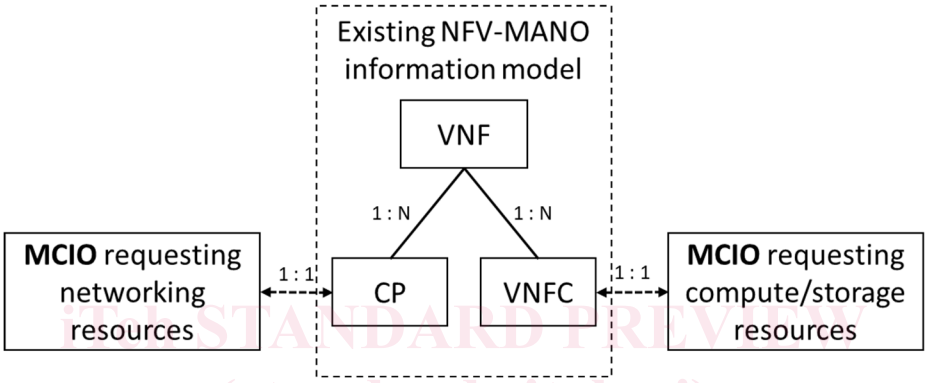

Figure 5.2.1.2-1: MCIO logical model mapping

Properties of an MCIO described in declarative descriptors and relevant being exposed to NFV-MANO are mirrored in attributes of the descriptors of the corresponding objects of the existing NFV-MANO information model. Properties of an MCIO requesting compute and/or storage infrastructure resources are described in attributes of the VDU information element of the VNF Descriptor. Properties of an MCIO requesting network infrastructure resources for VNF external connectivity are described in attributes of applicable sub-classes of the CPD information element of the VNF Descriptor. Figure 5.2.1.2-2 illustrates the specification of an MCIO's properties in enhanced NFV-MANO descriptor objects.

NOTE 2: Properties of MCIO's requesting network infrastructure resources cannot be used to specify requirements on the network infrastructure resources to be used for internal VLs.

NOTE 3: The declarative descriptor of an MCIO cannot be used to specify requirements equivalent to those specified for a VduCP that is not re-exposed as an external CP.

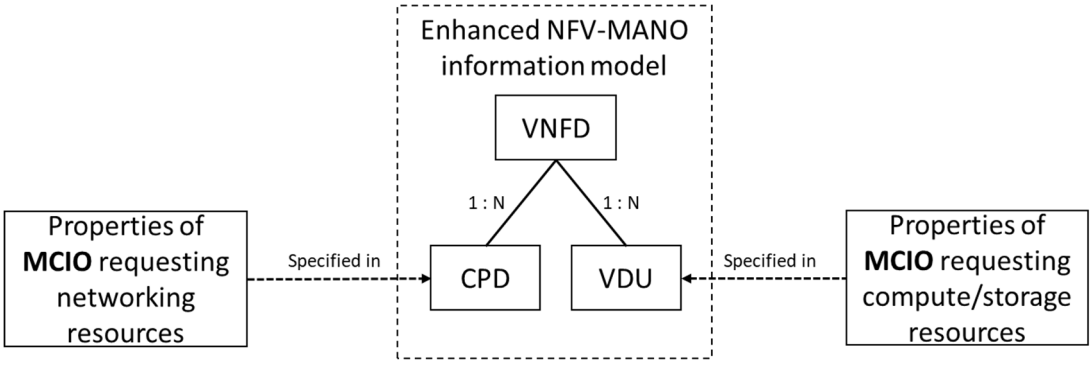

Figure 5.2.1.2-2: MCIO's properties specification

The above defined relationships in between the MCIO, their descriptors, and the NFV IM enables the interoperability of containerized workloads management with NFV management and orchestration. On the one hand, the information contained in NFV descriptors, artefacts and the VNF and NS runtime information held by NFV-MANO, that relates to MCIOs, enable the VNFM and NFVO of NFV-MANO to process relevant resources requirements, and perform the lifecycle, fault and performance management of VNF or VNF components, when these are realized by a set of OS containers. On the other hand, the mapped MCIO, their descriptors and the produced services by the CISM enable the VNFM and NFVO to request the relevant management of the containerized workloads to be deployed and managed on CIS instances.

NOTE 4: While the NFVO and VNFM do not manage individual OS containers, resources information related to OS containers such as images or resource requests can be exchanged and/or visible to the NFVO and VNFM for other purposes such as resources granting, capacity management, namespace management, etc.

5.2.2 Managed Container Infrastructure Object Package

5.2.2.1 Purpose

A Managed Container Infrastructure Object Package (MCIOP) is a hierarchical aggregate of information objects for OS container management and orchestration, introduced by ETSI GR NFV-IFA 029 [i.2]. The aggregate of information objects includes declarative descriptors and configuration files for one or multiple Managed Container Infrastructure Objects (MCIOs).

Configuration files typically specify values for parameters defined in the declarative descriptors. The MCIO configurable parameters are represented by key-value pairs. All the keys corresponding to MCIO configurable parameters are specified in the configuration files. The configuration files may contain values for some of the parameters. The other values are not specified in the configuration files but injected during the related containerized workload management. Furthermore, the values provided in the configuration files may also be overwritten by injecting values.

The MCIOP, representing aggregated containerized workloads, is used to instantiate and maintain containerized workloads and provide a higher abstraction level than individual MCIO declarative descriptors used by the CISM, declaring the relationships among the MCIOs, as addressed in ETSI GR NFV-IFA 029 [i.2].

5.2.2.2 Relationship to the existing NFV-MANO information model

The VNF Package contains both the VNFD and one or multiple MCIOPs. The VNFD and its constituent VDUs are the descriptor objects to instantiate the VNF and its constituent VNFCs. In this context, both the containerized VNF and the containerized VNFCs are regarded as containerized workloads. A containerized workload uses MCIOs during its lifecycle, which are created and maintained by using the declarative descriptors and configuration files for the respective MCIO in the MCIOP.

The relationship between an MCIOP and the existing NFV-MANO information model is shown in figure 5.2.2.2-1. The VNFD of a containerized VNF has references to one or multiple MCIOPs which contain declarative descriptors and configuration files for MCIOs consumed by the containerized VNF.

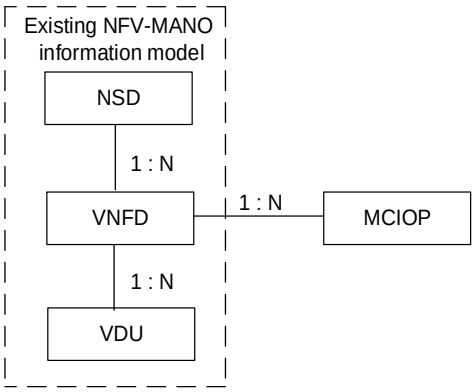

Figure 5.2.2.2-1: MCIOP logical model mapping