International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3150
(09/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

High-level technical characteristics of network softwarization for IMT-2020

Recommendation ITU-T Y.3150

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3150

High-level technical characteristics of network softwarization for IMT-2020

Summary

Recommendation ITU-T Y.3150 describes how network softwarization, whose usefulness is globally recognized, and its most typical substantiation, network slicing, contribute to International Mobile Telecommunications-2020 systems. Recommendation ITU-T Y.3150 explores network slicing from two viewpoints: vertical and horizontal aspects. Recommendation ITU-T Y.3150 further describes network slicing for mobile fronthaul and backhaul, introduction to advanced data-plane programmability and capability exposure. These descriptions are expected to lead to the detailed study of these technical characteristics.

This edition contains: i) a change in the basic model, which contains software-defined networking, network functions virtualization, cloud computing and other technical environments; and ii) security considerations for network slicing. In addition, information on hierarchical orchestration is included.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3150	2020-09-29	13	11.1002/1000/14399

Keywords

IMT-2020, network slicing, network softwarization.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3150

High-level technical characteristics of network softwarization for IMT-2020

1 Scope

This Recommendation describes high-level characteristics of network softwarization for non-radio parts of International Mobile Telecommunications-2020 (IMT-2020). This Recommendation explores network slicing from two viewpoints: vertical and horizontal aspects. After reviewing each aspect, this Recommendation further describes network slicing for mobile fronthaul (FH) and backhaul (BH), introduction to advanced data-plane programmability and capability exposure, whose technical characteristic descriptions are expected to lead to their detailed study.

Detailed technical features (e.g., signalling specifications) lie outside the scope of this Recommendation.

This edition mainly includes descriptions of: i) an updated reference model showing relations with software-defined networking/network functions virtualization (SDN/NFV) and cloud computing; and ii) security considerations for network slicing. Supplementary information regarding orchestration is given.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network.*

[ITU-T Y.3102] Recommendation ITU-T Y.3102 (2018), *Framework of the IMT-2020 network.*

[ITU-T Y.3105] Recommendation ITU-T Y.3105 (2018), *Requirements of capability exposure in the IMT-2020 network*.

[ITU-T Y.3108] Recommendation ITU-T Y.3108 (2019), *Capability exposure function in IMT-2020 networks*.

[ITU-T Y.3111] Recommendation ITU-T Y.3111 (2017), *IMT-2020 network management and orchestration framework.*

[ITU-T Y.3112] Recommendation ITU-T Y.3112 (2018), *Framework for the support of network slicing in the IMT-2020 network*.

[ITU-T Y.3151] Recommendation ITU-T Y.3151 (2019), *High-level technical characteristics of network softwarization for IMT-2020 – Part: SDN.*

[ITU-T Y.3152] Recommendation ITU-T Y.3152 (2019), *Advanced data plane programmability for IMT-2020*.

[ITU-T Y.3153] Recommendation ITU-T Y.3153 (2019), *Network slice orchestration and management for providing network services to 3rd party in the IMT-2020 network.*

[ITU-T Y.3154] Recommendation ITU-T Y.3154 (2020), *Resource pooling for scalable network slice service management and orchestration in the IMT-2020 network*.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-R M.2083] Recommendation ITU-R M.2083 (2015), *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 backhaul [ITU-T Y.3100]: A network path between base station systems and a core network.

3.1.2 control plane [b-ITU-T Y.2011]: The set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control.

3.1.3 data plane [b-ITU-T Y.2011]: The set of functions used to transfer data in the stratum or layer under consideration.

3.1.4 fronthaul [ITU-T Y.3100]: A network path between centralized radio controllers and remote radio units of a base station function.

3.1.5 network function [ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

NOTE 1 – Network functions include but are not limited to network node functionalities, e.g., session management, mobility management and transport functions, whose functional behaviour and interfaces are defined.

NOTE 2 – Network functions can be implemented on a dedicated hardware or as virtualized software functions.

NOTE 3 – Network functions are not regarded as resources, but rather any network functions can be instantiated using the resources.

3.1.6 network functions virtualization (NFV) [b-ETSI GS NFV 003]: Principle of separating network functions from the hardware they run on by using virtual hardware abstraction.

3.1.7 network slice [ITU-T Y.3100]: A logical network that provides specific network capabilities and network characteristics.

NOTE 1 – Network slices enable the creation of customized networks to provide flexible solutions for different market scenarios which have diverse requirements, with respect to functionalities, performance and resource allocation.

NOTE 2 – A network slice may have the ability to expose its capabilities.

NOTE 3 – The behaviour of a network slice is realized via network slice instance(s).

3.1.8 network slice blueprint [ITU-T Y.3100]: A complete description of the structure, configuration and work flows on how to create and control a network slice instance during its life cycle.

NOTE – A network slice template can be used synonymously with a network slice blueprint.

3.1.9 network slice instance [ITU-T Y.3100]: An instance of network slice, which is created based on network slice blueprint.

NOTE 1 – A network slice instance is composed of a set of managed run-time network functions, and physical/logical/virtual resources to run these network functions, forming a complete instantiated logical network to meet certain network characteristics required by the service instance(s).

NOTE 2 – A network slice instance may also be shared across multiple service instances provided by the network operator. A network slice instance may be composed of none, one or more sub-network slice instances which may be shared with another network slice instance.

3.1.10 network softwarization [ITU-T Y.3100]: An overall approach for designing, implementing, deploying, managing and maintaining network equipment and/or network components by software programming.

NOTE – Network softwarization exploits the nature of software such as flexibility and rapidity all along the lifecycle of network equipment and/or components, for the sake of creating conditions that enable the re-design of network and services architectures, the optimization of costs and processes, self-management and bring added values in network infrastructures.

3.1.11 orchestration [ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructure by optimization criteria.

3.1.12 physical resource [ITU-T Y.3100]: A physical asset for computation, storage and/or networking.

NOTE – Components, systems and equipment can be regarded as physical resources.

3.1.13 virtual resource [b-ITU-T Y.3011]: An abstraction of physical or logical resource, which may have different characteristics from the physical or logical resource and whose capability may be not bound to the capability of the physical or logical resource.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 management: In the context of IMT-2020, the processes aiming at fulfilment, assurance, and billing of services, network functions, and resources in both physical and virtual infrastructure including compute, storage, and network resources. A network path between base station systems and a core network.

NOTE – Based on [ITU-T Y.3100].

3.2.2 virtualized network function: A network function whose functional software is decoupled from hardware, and runs on virtual machine(s).

NOTE – Based on [ITU-T Y.3321].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BH	Backhaul
BSS	Business Support System
CMUD	Create, Monitor, Update and Delete
CN	Core Network
DNS	Domain Name System

eMBB	enhanced Mobile Broadband
EM	Element Management
EMS	Element Management System
FCAPS	Fault, Configuration, Accounting, Performance and Security
FH	Fronthaul
GTP	General packet radio service Tunnelling Protocol
ICT	Information and Communication Technology
IMT-2020	International Mobile Telecommunications-2020
Inf&NF-M	Infrastructure and Network Function Management
IoT	Internet of Things
IP	Internet Protocol
LCM&O	Lifecycle Management and Orchestration
L*n*	Layer *n*
mMTC	massive Machine Type Communication
NAT	Network Address Translation
NEM	Network Element Management
NF	Network Function
NFV	Network Functions Virtualization
NFVI	NFV infrastructure
NFV-MANO	NFV-Management and Orchestration
NFVO	NFV Orchestration
NSO	Network Service Orchestration
OLT	Optical Line Terminal
OSS	Operations Support System
PNF	Physical Network Function
RAN	Radio Access Network
RO	Resource Orchestration
SDN	Software-Defined Networking
URLLC	Ultra-Reliable and Low Latency Communication
VIM	Virtualized Infrastructure Management
VNF	Virtualized Network Function
VNFM	Virtualized Network Function Management

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

6 Introduction to network softwarization for IMT-2020

Network softwarization is an overall approach for the design, implementation, deployment, management and maintenance of network equipment and network components by software. It exploits software features such as flexibility and rapidity throughout the lifecycle of network equipment or components, for the sake of creating conditions that enable the re-design of network and service architectures, optimize costs and processes, enable self-management and add value to network infrastructures.

Figure 6-1 shows how network softwarization contributes to the IMT-2020 network, whose requirements are specified in [ITU-T Y.3101]. With network softwarization, underlying heterogeneous physical infrastructure is abstracted as network, computing and storage resources. With management and orchestration, these resources and functions form multiple isolated networks as network slices. Individual network slices can have specific characteristics that reflect various different requirements derived from application and services.

[ITU-T Y.3102] shows the concept of network slice in IMT-2020 networks. In addition, [ITU-T Y.3112] introduces use-cases, functional and performance aspects, and high-level requirements for network slicing.

Key components to realize network softwarization are SDN, NFV and cloud computing, which are described in clause 6.1.

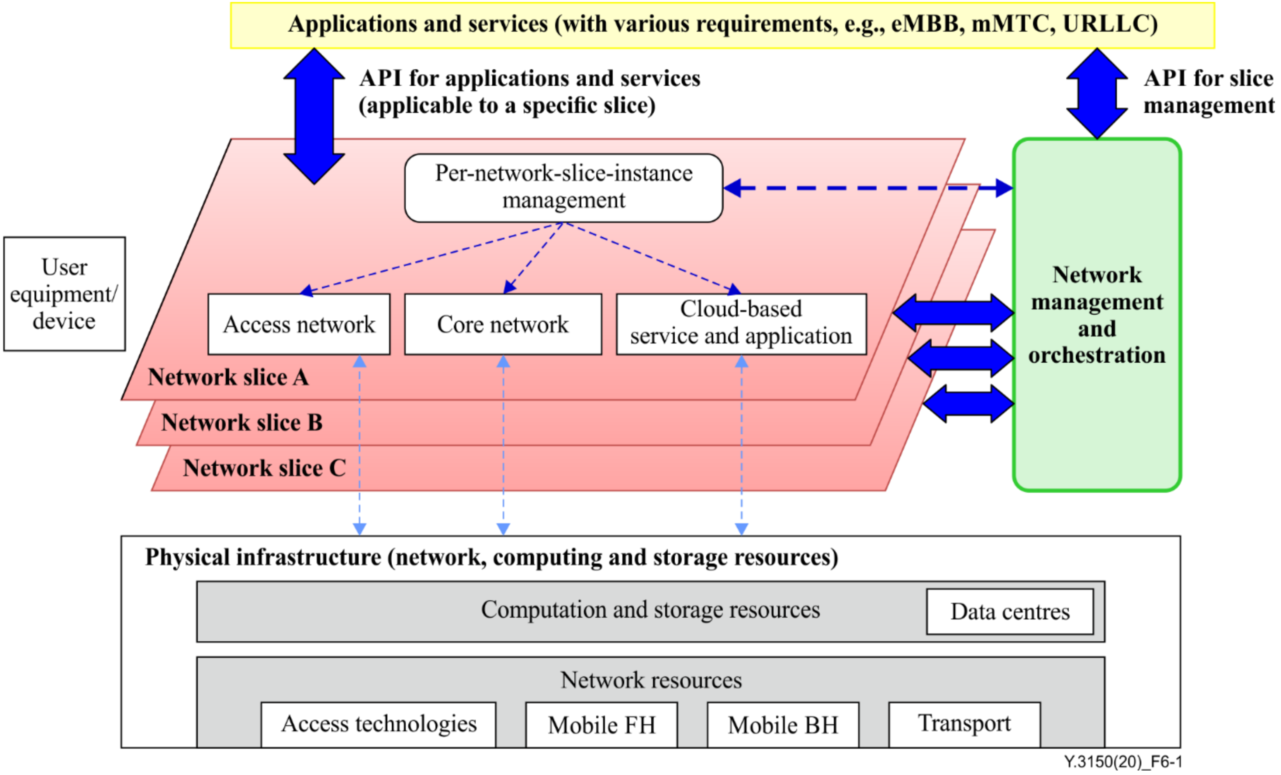

Applications and services (with various requirements, e.g., eMBB, mMTC, URLLC)
API for applications and services (applicable to a specific slice)
API for slice management
Per-network-slice-instance management
User equipment/ device
Access network
Core network
Cloud-based service and application
Network slice A
Network slice B
Network slice C
Network management and orchestration
Physical infrastructure (network, computing and storage resources)
Computation and storage resources
Data centres
Network resources
Access technologies
Mobile FH
Mobile BH
Transport
Y.3150(20)_F6-1

Figure 6-1 – Network softwarization for IMT-2020

6.1 Underlying technologies for softwarization

Together with SDN, NFV and cloud computing technologies, network softwarization is established for rapid service creation especially new services.

6.1.1 SDN

SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data centre. The goal of SDN is to allow network engineers and administrators to respond quickly to changing business requirements. In a software-defined network, a network administrator can shape traffic from a centralized control console without having to touch individual switches, and can deliver services to wherever they are needed in the network, regardless of what specific devices a server or other device is connected to. The key technologies are functional separation, network virtualization and automation through programmability.

Recommendations in the ITU-T Y.3300 series cover this technology area.

6.1.2 NFV

NFV offers a new way to design, deploy and manage networking services. NFV decouples the network functions (NFs) from proprietary hardware appliances such as network address translation (NAT), firewalling, intrusion detection, domain name system (DNS), and caching. All NFs can run in software.

It is designed to consolidate and deliver the networking components needed to support a fully virtualized infrastructure – including virtual servers, storage and even other networks. It is applicable to any data plane processing or control plane function in both wired and wireless network infrastructure.

NOTE – ETSI GS NFV series standards mainly cover this technology area.

6.1.3 Cloud computing

Cloud computing technologies in telecommunication infrastructure bring both new opportunities for service offers and challenges from the management perspective. One important challenge for telecommunication operators is efficient management of cloud computing, taking into account the legacy management system framework and ensuring customer satisfaction including end-to-end quality of service.

Cloud computing is different from traditional telecommunication networks because it does not expose individual elements to the telecommunication management system. Moreover, cloud computing does not distinguish between management operations carried out on behalf of the customer and network operator.

ITU-T Y.3500 series Recommendations cover this technology area.

6.2 Potential use cases supported by network softwarization

In the IMT-2020 era, a variety of changes in the information and telecommunication environment and social requirements impacting on network infrastructure should be taken into account. Typical examples of these are as follows.

- Video traffic already dominates mobile communication traffic and is still increasing. This requires the network architecture to have an efficient video-on-demand delivery mechanism in terms of network or server congestion reduction and shorter response times.
- In many countries, disaster resilience, which is the ability both to maintain service and recover from disruption, is a key concern. Since network systems are a part of the lifeline infrastructure, they are expected to be robust. Increased network flexibility, such as dynamic network resource allocation helps, respond to this demand.
- The Internet of things (IoT) and big data processing are booming. Future networks, including the IMT-2020 network, should provide functions that support efficient IoT communication and big data-processing systems.
- One of the expectations for IMT-2020 is the realization of ultra-low latency. Total design including data processing and service provision is necessary to fulfil this expectation.
- SDN and NFV are expanding as possible key technologies for application to future networks including the IMT-2020 network. Data plane programmability, which enables change of

action of data-forwarding devices by programming, and the usage of open source software are involved in this perspective.

These wide varieties of objective can be achieved via network softwarization. With the adoption of SDN and NFV, software programmability of network nodes will in turn makes it feasible to run information processing and service software on network nodes as a new concept called in-network computing.

7 Vertical aspects

This clause describes technical characteristics of network softwarization (including network slicing) in terms of different levels of abstraction, of which a range is from physical infrastructure, virtual resources, and virtualized NFs and to network slices, in managed network domain(s) and their interactions.

In this Recommendation, these are referred to as vertical aspects.

7.1 Basic model for providing network slices

7.1.1 Overview

From the vertical viewpoint, the IMT-2020 network providing network slices can be modelled by the three key functional entities shown in Figure 7-1.

– Network slice customers: request the creation of network slice instances based on their service requirements and use the instances provided.

– Network slice lifecycle management and orchestration (LCM&O): provides and manages network slice instances based on requests from network slice customers.

– Network slice support: assists the network slice LCM&O by preparing individual components of network slice instances and arranging them according to network slice LCM&O requests. The components of network slice instances consist of NFs and resources. Network element management (NEM), which manages individual network slice instance, can be included if explicitly required.

NOTE 1 – Details of the network slice LCM&O are given in [ITU-T Y.3111] and [ITU-T Y.3153].

NOTE 2 – Appendix I provides details about the configuration of network slice support. Appendix II provides the relationship of the models in this Recommendationwith that of ETSI NFV.

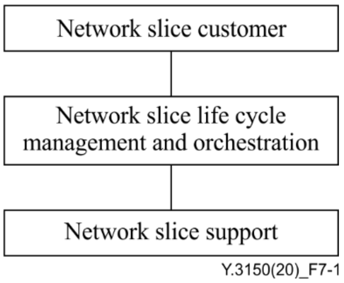


Figure 7-1 – Basic model for providing network slices

Figure 7-2 illustrates details of the network slice support functional entity. Network slice support contains a combination of four technical environments: an SDN environment; an NFV environment; a cloud computing environment; and the other environment for providing a network slice instance.

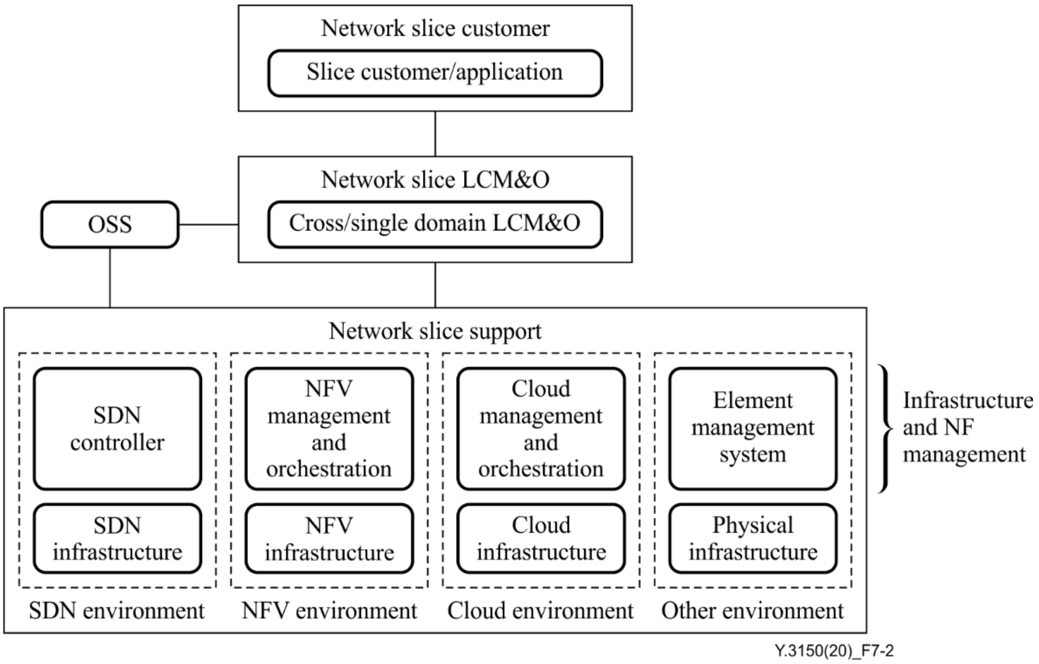


Figure 7-2 – Details of network slice support

The key components in Figure 7-2 are as follows.

– Slice customer/application: requests network services (NSs) by using network slicing.

– Operations support system (OSS): is an operational system used by telecommunication services.

– Cross- and single domain LCM&O: manages and orchestrates te processes of network slice instances. The types of management target of the network slice LCM&O are classified as a single network domain or multiple network domains. Cross- and single domain LCM&O can have a hierarchical structure. For example, multiple single domain LCM&O may hierarchically work under the control of one cross-domain LCM&O. Typical managed domains in IMT-2020 networks are access network, core network (CN) and transport network [ITU-T Y.3153].

– SDN environment:

a) SDN controller: provides a means to program, orchestrate, control and manage the SDN infrastructure;

b) SDN infrastructure: represents physical network resources for control and management by an SDN controller.

– NFV environment:

a) NFV management and orchestration: provides a means to program, orchestrate, control and manage the NFV infrastructure (NFVI);

b) NFVI: represents objects to be orchestrated and managed to provide NFV resources and virtualized network functions (VNFs).

– Cloud environment:

a) cloud management and orchestration: provides a means to program, orchestrate, control and manage cloud services and applications;

b) cloud infrastructure: represent physical computing and storage resources, which enable to be accessed through software abstraction.

– Other environment:

a) element management system (EMS): manages physical network functions (PNFs);

b) other infrastructure: represents PNFs, which do not belong to SDN/NFVI.

– Infrastructure and network function management (Inf&NF-M): is a logical representative of management capabilities in the network slice support consisting of the SDN controller, the NFV management and orchestration, the cloud management and orchestration and the EMS (See clause 7.2).

NOTE 3 – One or multiple types of technical environments can be involved in a single managed domain.

NOTE 4 – Appendix IV considers role sharing of the hierarchical functions.

7.1.2 SDN environment for network slice support

The SDN environment in network slice support consists of an SDN controller and SDN infrastructure (e.g., an SDN-controlled local area network bridge, a layer 3 (L3) forwarding switch and an optical line terminal (OLT)). It provides control, management and orchestration functions for a network slice using virtual resources in the SDN infrastructure [ITU-T Y.3151].

NOTE 1 – The SDN controller and the SDN infrastructure can be realized in NFVI as VNFs. Variations of implementation of virtualized SDN controllers and SDN applications are listed in Appendix V.

Transport SDN is an underlying technology that provides connectivity of functionality and an overall bandwidth guarantee on an instantiated network slice.

NOTE 2 – The role of transport networks in the context of IMT-2020 is briefly introduced in Appendix V.

7.1.3 NFV environment for network slice support

The NFV environment in network slice support is roughly divided into NFV-management and orchestration (NFV-MANO) and NFVI. NFV-MANO and the NFVI operate in cooperation and realize VNFs including provision, control and management functions with the virtualization of physical resources on computing, network and storage.

NOTE – [b-ETSI GS NFV 002] and [b-ETSI GS NFV-INF 005] introduce a ground concept of NFV and details of NFV functionalities, respectively. Especially, management functions in the NFVI are assumed to be the same as ETSI management and orchestration (MANO) [b-ETSI GS NFV-IFV 009].

7.1.4 Cloud environment for network slice support

The cloud environment contains cloud management and orchestration functionalities and a cloud infrastructure. The cloud management functionality encompasses the set of management capabilities that are required in order to manage and control cloud services. The cloud orchestration functionality conducts coordination, aggregation and composition of multiple service components, and provides a common interface to access to cloud services that are implemented in software. The cloud infrastructure is where the resources reside. This includes equipment typically used in a data centre, such as servers, networking switches and routers, and storage devices, as well as the corresponding non-cloud-specific software that runs on servers and other equipment, such as host operating systems, hypervisors, device drivers and generic systems management software [ITU-T Y.3502].

NOTE – The cloud management, cloud service orchestration and cloud infrastructure in this Recommendation can be mapped to the OSS functional components, access and service layer functional components and resource layer functional components specified in [ITU-T Y.3502].

7.1.5 Other environment for network slice support

The other environment consists of physical network nodes and links that have not undergone virtualization. The nodes provide specific network functions (NFs; e.g., hardware routers, switches, firewalls, load balancers and session border controllers).

7.1.6 Open source for network slice support

Several well-known open source projects relevant to network slicing are in progress at the time of publication. Especially, open source software for network slice LCM&O, the SDN controller and NFV management and orchestration is a key part of the implementation of network slicing. Recently, network standardization is tending to incorporate open source development as a part of proof of concept. [b-ITU-T Y-Suppl.44] provides a snapshot of the field in 2017.

7.2 Management for network slicing

To provide components needed for a network slice instance (i.e., resources, NFs and NEMs), each environment in the network slice support contains its own Inf&NF-M.

NOTE 1 – When multiple technical environments are embedded in a single managed domain, detailed logical mapping between the Inf&NF-M and each environment is not treated in this Recommendation. For example, a top-level SDN controller may manage both an SDN environment and the other environments.

The Inf&NF-M is responsible for the following three-level management.

– Infrastructure and resource level:

a) fault, configuration, accounting, performance and security (FCAPS) management of infrastructure;

b) create, monitor, update and delete (CMUD) virtual resources or the allocation of physical resources;

c) FCAPS management of the assigned resources.

– NF level:

a) CMUD of NF instances and NEM instances;

b) FCAPS management of assigned NF instances and NEM instances.

– Network slice level:

a) CMUD of network slice instances;

b) FCAPS management of network slice instances.

[ITU-T Y.3154] introduces typical processes of network slice LCM&O by using a resource pool mechanism.

NOTE 2 – Appendix I shows examples of relevant interactions between the Inf&NF-M and the network slice LCM&O. In addition, Appendix III provides example procedures and flows for slice instance creation.

NOTE 3 – The possible interface between the network slice LCM&O and the Inf&NF-M are introduced in [ITU-T Y.3111].

7.3 Network slicing for access networks – mobile fronthaul and backhaul

According to the survey conducted by ITU-T FG IMT-2020 [b-ITU-T Y.Sup 44], network slicing receives broader acceptance from the industry. The initial focus of network slicing is on its application to the CN of the IMT-2020 network. This Recommendation focuses on another point: the use of network slicing in the access network of the IMT-2020 network, which consists of mobile FH and BH. To identify key capabilities in this application, this clause starts with expected capabilities and benefits of network softwarization for FH and BH. Two new key features are identified.

7.3.1 Expected capabilities and benefits

This clause describes expected capabilities and benefits of network softwarization on FH and BH for tackling typical problems. The IMT-2020 network goes along with the following three service categories: the enhanced mobile broadband (eMBB); massive machine type communication (mMTC); and ultra-reliable and low latency communication (URLLC), described in [ITU-R M.2083]. The typical problems in the categories are as follows.

– Huge and fluctuating power consumption in eMBB services:

To support eMBB, a large number of small cells and a lot of their links are required. The first issue is huge power consumption of them. The second issue is the limited small number of users (and devices) in the cells. Therefore, efficient statistical multiplexing effect cannot be expected in this case. In other words, the fluctuation of power consumption may be large.

In this circumstance, if (1) some radio stations are in a sleeping mode when the adjacent cell's or macro cell's radio station can cover others' areas and (2) network elements in FH and BH have a sleep or power reduction mode according to the change of network traffic, power consumption can be reduced drastically. Network softwarization mechanisms are expected to have capabilities to make use of these characteristics on FH and BH with the dynamic resource allocation for network slices.

– Data traffic overflow in mMTC services:

Even if traffic volume from each device for mMTC is small, the number of the devices may be very large. When there is no traffic control, burst user data traffic may flow from the huge number of devices to a termination node, which may be placed around FH and BH. To prevent the overflow, it is highly expected that suitable resource allocation is conducted in both data plane and control plane in network slice instances.

– Delay in control plane in URLLC services:

When a terminal in URLLC services with high bandwidth is moving from a cell to an adjacent cell, the resource (e.g., bandwidth) dedicated to the original cell and its connecting link should be re-allocated immediately to another link connecting to the adjacent cell. If this re-allocation is conducted by only the centralized network slice LCM&O, there must be a large control traffic between cells and the centralized network slice LCM&O. In such a case, if some controllability is delegated to local controllers in FH and BH, the controllers could re-allocate the resources by their own decision. This delegation and localization can reduce certain delay in control traffic.

7.3.2 Required new functionalities

The following two functional sets are expected when network slicing is applied to FH and BH in the IMIT-2020 network.

– Functionalities for low power mode operation:

It is observed that existing SDN technologies for transport (e.g., [b-ONF TR-527]) do not consider functions to operate underlying physical resources with different modes of operation in terms of electric power consumption. Some functionality should be prepared so that the network LCM&O can control physical resources to meet different power-consumption requirements. Specifically, the network slice LCM&O should be able to collect information about the capabilities of possible modes of operation that are available in the underlying physical resources. Based on this information, the network slice LCM&O can choose the best mode of operation and change modes if necessary.

– Functionalities for updating the resource allocation using statistical traffic information:

Existing SDN technologies for transport (e.g., [b-ONF TR-527]) include functions to allocate the resources. The allocation is done by specifying a ratio to the given physical resources. For example, when the physical link bandwidth (i.e., physical resource) is 1 Gbit/s and 300 Mbit/s of the bandwidth is planned to allocate to some use, it is specified by 30%. The allocation is fixed regardless of its actual use. To change the allocation, the network slice LCM&O modifies the setting (i.e., ratio). To adjust the allocated resource close enough to the real use, the network slice LCM&O should modify the setting frequently.

Some functionality should be provided to allow the underlying physical resources and its controller to run autonomously so that its resource allocation can change automatically. For example, when actual usage approaches the upper limit of allocated resource, the autonomous mechanism increases the allocated resource automatically. Similarly, when the actual usage decreases, the allocated resource is reduced accordingly. For this operation, a target range of usage ratio is given and statistical traffic information is used. This functionality provides benefits of (1) providing automatic power saving and (2) smooth sharing of unused resources with other virtual paths. This autonomous mechanism mitigates the burden of the orchestrator.

NOTE – Other standardization development organizations have already designed some application programming interfaces (APIs) that can be used in CMUD functionalities. Information about the APIs specified in ONF is given in [b-ONF TR-527]. Through work in FG IMT-2020, the above functionalities were identified that are not supported by the existing APIs. The detailed analysis is given in the gap analysis performed by FG-IMT2020 [b-ITU-T FG IMT-2020].

[ITU-T Y.3151] gives details of the network softwarization approach to FH and BH from the viewpoint of SDN transport networks.

7.4 Advanced data plane programmability

Network softwarization technologies including SDN, NFV, network slicing and their extensions are expected to support IMT-2020 networks. Current SDN technologies primarily focus on the programmability of the control plane, and existing SDN protocol specifications reflect a "bottom-up" design process in which the capabilities of the forwarding plane are determined by fixed function chips with built-in knowledge of existing network protocols. For supporting new protocols and architectures driven by use cases in IMT-2020 networks, further work in the data plane is needed.

Data plane programmability as an underlying technology for network softwarization enhances the SDN with more agility and flexibility to meet the requirements of IMT-2020 networks. Via data plane programmability technology, network operators benefit from the "top-down" design process by defining the network processing behaviour in a high-level language. In other words, data plane programmability enables operators to define specific data plane protocol (including packet format) and to support extended network functionalities. It brings the smooth evolution from existing protocols to future proof protocols. The network hypervisor provides resource slicing and isolation over the programmable data plane. Data plane programmability leads to automation and orchestration, which let developers integrate applications tightly with the network such that every stage of development can be accelerated. Therefore, programmability of IMT-2020 networks should be extended vertically from the control plane to the data plane.

[ITU-T Y.3152] introduces a framework, which includes requirements and an architectural overview, of data plane programmability.

8 Horizontal aspects

This clause describes technical characteristics of network softwarization (including network slicing) in terms of network-wide aspects. In this Recommendation, these are referred to as horizontal aspects.

8.1 Basic horizontal view of network slices

Network slices may be requested to concatenate to fully meet service requirements. Horizontal aspects of network softwarization on network slicing mean the control and management of network slice instances through multiple network infrastructure domains. An infrastructure domain is identified from the viewpoints of: i) characteristics of a network; or ii) management of a group of components of the infrastructure segment. Consideration of both vertical and horizontal aspects of network capabilities is important for network softwarization to realize agility, flexibility and scalability of NSs.

NOTE – An infrastructure domain is involved in network slice support described in clause 7.

Figure 8-1 shows an image of horizontal aspects of network slicing when each network slice is managed within an infrastructure domain that contains network, computer and storage resources.

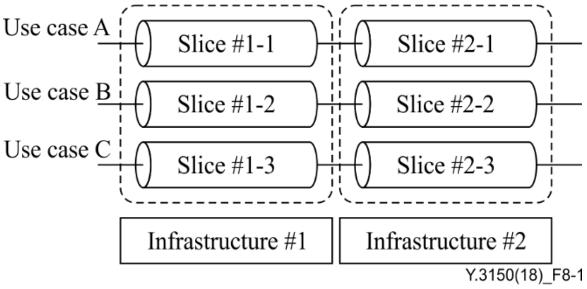


Figure 8-1 – A schematic diagram of network slices dependent on infrastructures

NOTE 1 – A set of connected network slices in Figure 8-1 (e.g., slice #1-1 + slice #2-1) can be regarded as a network slice. In this case, individual slices in Figure 8-1 (e.g., slice #1-1) may be called a sub-network slice [ITU-T Y.3102]. On the other hand, Third Generation Partnership Project (3GPP) specifications such as [b-ETSITS 128.530] called it a network slice subnet.

Figure 8-2 illustrates an example of network slicing in the IMT-2020 network based on Figure 8-1. In Figure 8-2, infrastructure domains are separated as a mobile FH, a mobile BH and a CN. Individual network slices are logically connected for specific NSs such as eMBB and mMTC.

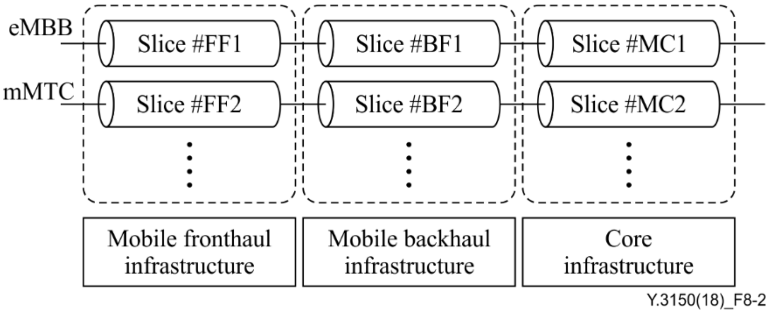


Figure 8-2 – An example of network slicing for IMT-2020 network

The administrators of different infrastructure domains may be a single network operator or service provider.

Figure 8-3 shows an example of the usage of network slicing for roaming services.

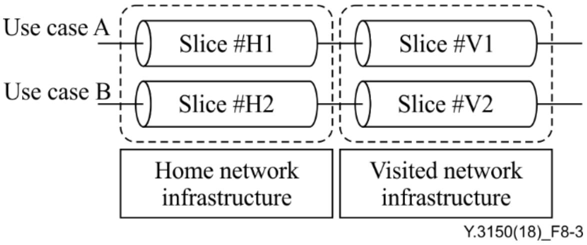


Figure 8-3 – A possible usage of network slicing for roaming

There are several variations of roaming use-cases. For example, the functionalities of a home network can be expanded to a visited network infrastructure (i.e., one of another operator) through network slicing, and a roaming service in the visited network controlled by the home network side.

There is another case of network slicing. A network slice can be used for multiple services simultaneously, when it is called a shared network slice. On the other hand, a network slice for single service use is called a dedicated network slice. Figure 8-4 shows an image of the concept mapping a shared network slice "Slice #2-1" and dedicated network slices "Slice #1-1" and "Slice #1-2". To support network slice mapping, a network slice type indicator [ITU-T Y.3112] is properly handled between two infrastructures. The mapping of the general packet radio service tunnelling protocol (GTP) tunnel information [ITU-T Y.3102] is also necessary.

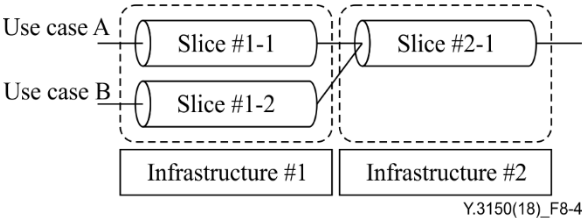


Figure 8-4 – A schematic diagram of shared and dedicated network slices

8.2 Capability exposure and APIs

The IMT-2020 network will accommodate many and various types of devices, which belong to different industries. New diverse use cases will need to be supported by the network. The new use cases are expected to come with a wide variety of requirements on the network. For example, there will be different requirements for functionality such as charging, policy control, security and mobility. Some use cases such as eMBB may require application-specific mobility and policy control, while other use cases can be handled with simpler mobility or policies. The use cases will also have huge differences in performance requirements.

Capability exposure based on network softwarization enables an operator to create a customized network (e.g., a network slice) to provide optimized solutions for different market scenarios that have diverse requirements (e.g., in the areas of functionality and performance).

High-level operational requirements are as follows:

– the IMT-2020 system is required to be able to customize NFs within a network slice dynamically based on the variation of third party (e.g., enterprises, service providers and content providers) demands;

– the IMT-2020 network is required to support dynamic utilization of resources (for computation, networking and storage) within a network slice as per third party application requirements, which are subject to the policy of the operator.

Detailed requirements for capability exposure are specified in [ITU-T Y.3105].

Figure 8-5 is an overview of capability exposure for network slice management.

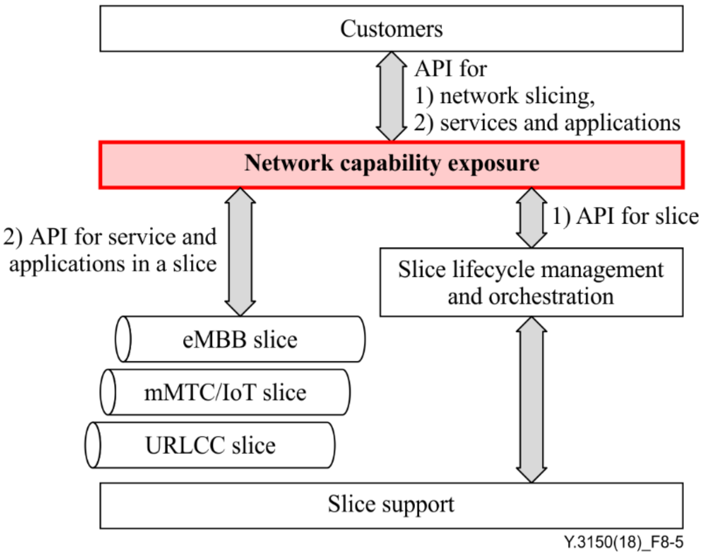

Customers
API for
1) network slicing,
2) services and applications
Network capability exposure
2) API for service and applications in a slice
1) API for slice
Slice lifecycle management and orchestration
eMBB slice
mMTC/IoT slice
URLCC slice
Slice support
Y.3150(18)_F8-5

Figure 8-5 – Capability exposure for network slicing

Use case 1: The creation or instantiation of a network slice triggered by a third party

1) The third party indicates functionality and performance requirements to create a network slice instance via a network slice building API. In terms of implementation, a network slice template may be sent by the API. This template contains parameters to describe functionality and performance requirements.

2) The network capability exposure function transfers the network slice creation request to a network slice LCM&O.

3) The network slice LCM&O authorizes the creation request of the network slice to meet the functionality and performance requirements based on the agreement between the operator and the third party. If the request is allowed, the network slice LCM&O forwards resource requirements to network slice support and accordingly the network slice support allocates the resources required (hardware and software) to create or instantiate the dedicated network slice.

Use case 2: The dynamic modification of functionality and performance configuration of a network slice

1) The third party indicates a modification of functionality or performance for a pre-created network slicing via a network slice modification API. The modification may be triggered due to lack of resources or new functions needed by the third party in the network slice. In terms of implementation, a network slice template may be sent by the API. This template contains parameters to describe the functionality and performance modification requirement.

2) The network capability exposure function transfers the network slice modification request to the network slice LCM&O.

3) The network slice LCM&O authorizes the request for functionality and performance modification based on the agreement between the operator and the third party. If the request is allowed, the network slice LCM&O forwards resource requirements to network slice support, which accordingly re-allocates the resources required (hardware and software) to modify the dedicated slice.

Authorization between a network slice customer and a network capability exposure platform is needed. The detailed functional architecture of capability exposure in the control plane of IMT-2020 networks is specified in [ITU-T Y.3108].

Network slice support manages and orchestrates resources, which results in the deployment of network slice functions including network connectivity.

9 Security considerations

First, general security requirements for networks based on the Internet protocol (IP) in [ITU-T Y.2701] and for IMT-2020 systems in [ITU-T Y.3101] are fundamentals for network softwarization.

Second, network softwarization consists of SDN, NFV and cloud computing techniques; therefore, security threats in each technical field should be taken care of.

Security and privacy issues related to cloud computing services and some issues identified may occur in network softwarization environments using network virtualization techniques. The issues described in [ITU-T X.1601], which introduces a general security framework for cloud computing, should be considered during planning and designing networks to mitigate issues.

In addition, network softwarization usually applies centralized control based on the separation of the control and data planes. With a centralized SDN controller, the impact of security issues related to the scalability and resilience of the control plane (e.g., a denial-of-service or distributed denial-of-service attack) can be higher than those faced by a single router. [ITU-T X.1038] identifies the security threats to the SDN application layer, SDN control layer, SDN resource layer, application-control interface and resource-control interface, according to the framework of SDN [ITU-T Y.3300]. Possible security countermeasures to these issues should be examined.

Appendix I

Example details of network slice support

(This appendix does not form an integral part of this Recommendation.)

I.1 Basic model

Clause 7.1 describes a basic model for providing network slices. This appendix introduces a detailed example of configuration of a functional entity network slice support introduced in clause 7.1.1. Figure I.1 is an overview of the model. Network slice support is composed of infrastructure and Inf&NF-M. Inf&NF-M contains infrastructure management (InfM) and network function management (NFM).

InfM is connected with infrastructures and manages their FCAPS. InfM connects with slice LCM&O from which it receives information to create, monitor, update and delete resources over infrastructures that are dedicated to a slice instance. InfM manages FCAPS of the resources. InfM is also connected to NFM.

NFM connects with slice LCM&O and InfM. NFM is responsible for CMUD of NFs and NEMs using the resources given by InfM. NFs and NEMs are dedicated to each slice instance. NFM is responsible for FCAPS management of NFs and NEMs. For these purposes, FCAPS information is exchanged with InfM.

Resources, NFs and NEMs are allocated and used in a network slice instance. The dotted lines in Figure I.1 represent this instantiation.

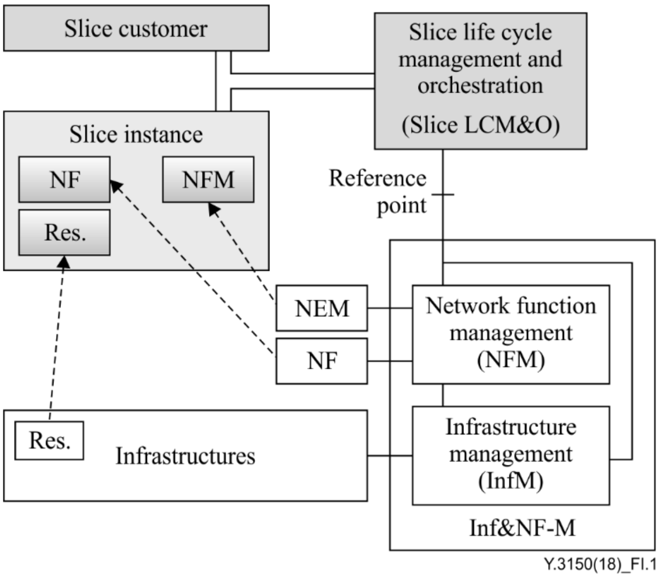


Figure I.1 – Basic model for providing slices with slice support

I.2 Interactions between network slice LCM&O and Inf&NF-M

The following are the possible interactions between a network slice LCM&O and an Inf&NF-M in Figure I.1.

– Interaction for FCAPS management of infrastructure: Network slice LCM&O gives management policies for infrastructures to the Inf&NF-M. In the case of fault management, management policies may represent the required level of reliability assurance and associated mechanisms (e.g., mean time to repair and specific redundancy mechanisms). Network slice support provides infrastructure information (e.g., infrastructure fault alarms) to network slice LCM&O.

- Interaction for CMUD of virtual resources: Network slice LCM&O sends messages for CMUD of virtual resources, which are used for virtualized NFs or NEMs, to the Inf&NF-M.
- Interaction for FCAPS management of virtual resources: Network slice LCM&O gives virtual resource management policies to the Inf&NF-M. Network slice support sends information about the virtual resources needed for network slice LCM&O (e.g., resource fault alarms) to the network slice LCM&O;
- Interaction for CMUD of virtualized NFs and NEMs: Network slice LCM&O sends messages for CMUD of virtualized NFs or NEMs to the Inf&NF-M. Virtualized NFs are created using resources according to the configuration information embedded in the messages.
- Interaction for FCAPS of virtualized NFs and NEMs: Network slice LCM&O gives management policies for virtualized NFs and NEMs to the Inf&NF-M. Network slice support provides information about virtualized NFs and NEMs needed for FCAPS (e.g., NF or NEM fault alarms) to the network slice LCM&O.

For NF level management, the information exchanged between network slice LCM&O and Inf&NF-M can be treated in an implementation- and hardware-agnostic way. On the other hand, for infrastructure and resource level management, information exchanged between Inf&NF-M and infrastructures depends on their technologies.

Appendix II

Relationship of the models in this Recommendation with that of ETSI NFV

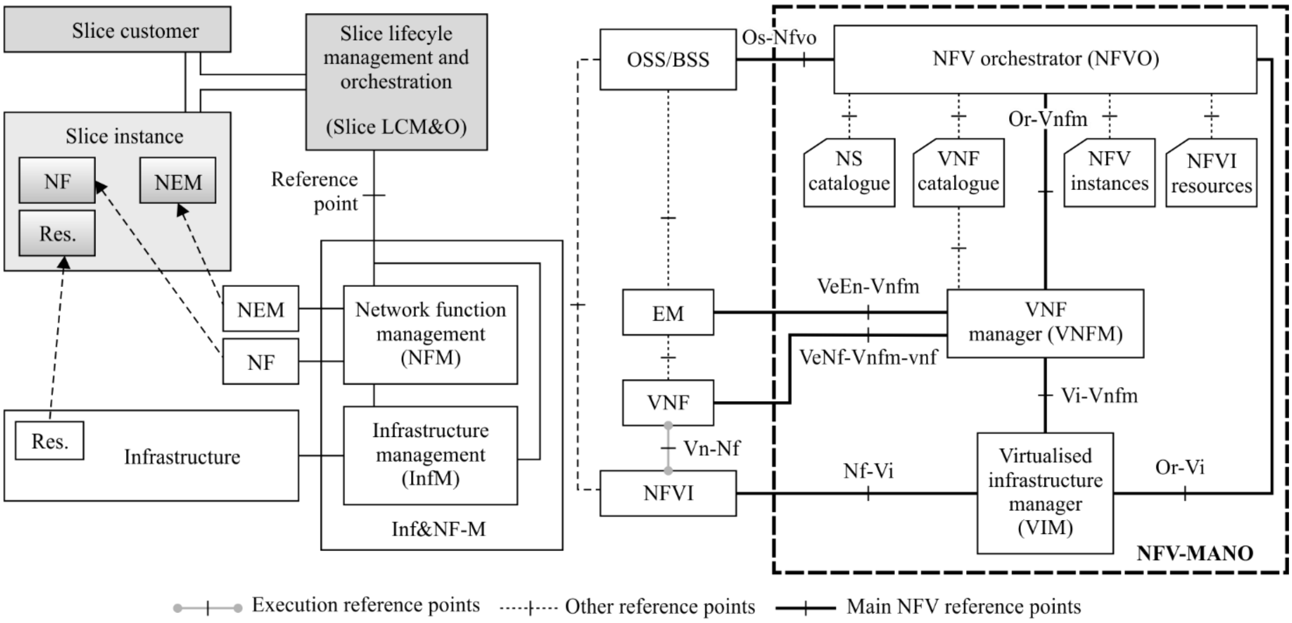
(This appendix does not form an integral part of this Recommendation.)

The ETSI NFV model is shown on the right side of Figure II.1. This technology provides virtual resources, VNFs and element management (EM).

The relationship of the models in this Recommendation with that of ETSI NFV is described in this Appendix.

Table II.1 reviews the models specified in this Recommendation and ETSI specification in terms of objectives, relations and functions. In addition, an example of a candidate configuration is shown in Figure II.2, in which the ETSI-NFV scheme can be mapped over the model described in clause 7.1.

When the models in this Recommendation apply to or include the ETSI NFV mechanism, some adaptation should be considered (as shown in Figure II.2).



Y.3150(18)_FII.1

Figure II.1 – The model shown in Figure I.1 (left) and the ETSI-NFV model (right)

Table II.1 – Comparison between the models in this Recommendation model and that of ETSI-NFV

	Recommendation ITU-T Y.3150	**ETSI-NFV**
Target	Providing a network slice	Providing a network service
Definitions of the target objects	**network slice instance** [ITU-T Y.3100]: An instance of network slice, which is created based on network slice blueprint. Note 1 – A network slice instance is composed of a set of managed run-time network functions, and physical/logical/virtual resources to	**network service** (NS) [b-ETSI GS NFV 003]: composition of network functions and/or network service(s), defined by its functional and behavioural specification. Note – The network service contributes to the behaviour of the higher layer service, which is characterized by at least

Table II.1 – Comparison between the models in this Recommendation model and that of ETSI-NFV

	Recommendation ITU-T Y.3150	ETSI-NFV
	run these network functions, forming a complete instantiated logical network to meet certain network characteristics required by the service instance(s). Note 2 – A network slice instance may also be shared across multiple service instances provided by the network operator. A network slice instance may be composed of none, one or more sub-network slice instances which may be shared with another network slice instance	performance, dependability, and security specifications. The end-to-end network service behaviour is the result of the combination of the individual network function behaviours as well as the behaviours of the network infrastructure composition mechanism
	A network slice instance includes its management function. This management function is accessible by slice customers (via capability exposure). Network service in the ETSI-NFV model is not clear on this point atthe time of publication of this Recommendation	
Who orders the lifecycle management for network slice instance or network service to slice LCM&O or NFV orchestration (NFVO)?	Slice customer via capability exposure	OSS/BSS via OSS/BSS-NFV management and orchestration. This reference point is used for network service lifecycle management. (See clause 7.3.7 of [b-ETSI GS NFV 002])
Transport network functions	– Transport network functions are also a kind of NF. – They are managed by NFM. – Slice Customer can configure the functions by using NEM	(Under study in ITU-T) They are described by using examples (e.g., vSwitch). (See clause 4.1 of [b-ETSI GS NFV-IFA 003] and [b-ETSI GS NFV-INF 005])
Information exchanged between slice LCM&O and InfM (in [ITU-T Y.3150]) or NFVO and virtualized infrastructure management (VIM; in ETSI)	InfM – CMUD for resources – FCAPS for resources – FCAPS for infrastructure (physical systems)	VIM – CMUD for resources – FCAPS for resources [b-ETSI GS NFV-IFA 005]

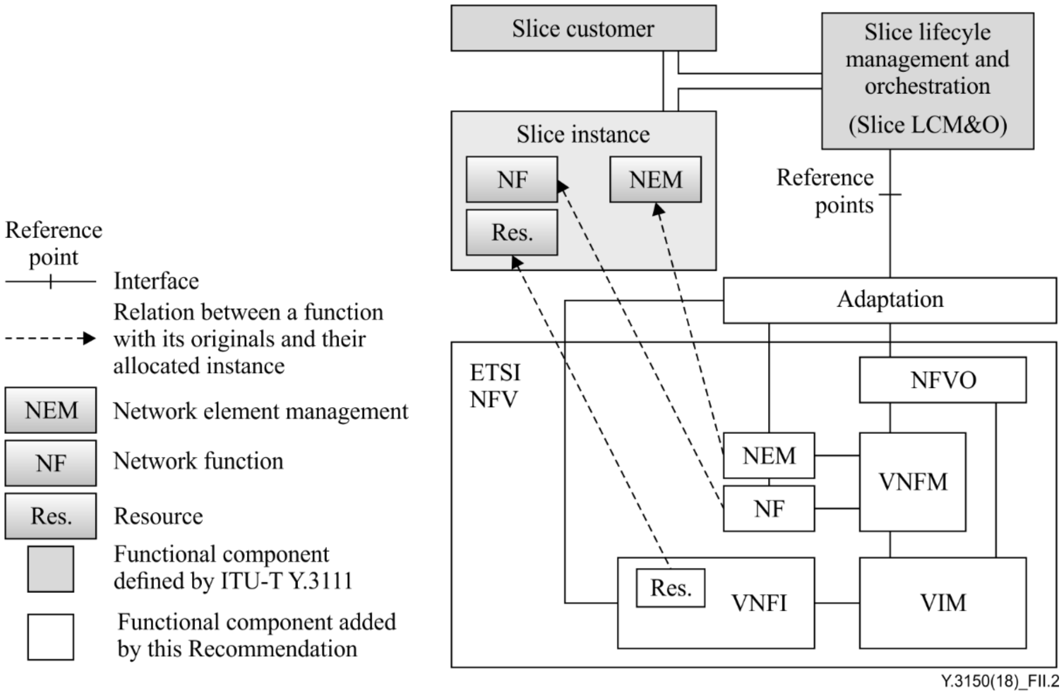

Slice customer
Slice lifecyle management and orchestration
(Slice LCM&O)
Slice instance
NF
NEM
Res.
Reference points
Reference point
Interface
Relation between a function with its originals and their allocated instance
NEM
Network element management
NF
Network function
Res.
Resource
Functional component defined by ITU-T Y.3111
Functional component added by this Recommendation
Adaptation
ETSI NFV
NFVO
NEM
NF
VNFM
Res.
VNFI
VIM
Y.3150(18)_FII.2

Figure II.2 – An example of a configuration of a slice instance when logical resources are assumed to be provided by the ETSI NFV scheme

Appendix III

Example procedures and flows for slice instance creation

(This appendix does not form an integral part of this Recommendation.)

Clause 7.1 introduces the basic model for allocating and providing resources, NFs and NEMs which are used for network slice instances. This appendix describes examples of procedures and relevant flows for network slice instance creation.

In this appendix, slice support is composed of infrastructure and Inf&NF-M, which contains InfM and NFM (See Appendix I).

InfM manages FCAPS of infrastructures based on information given by slice LCM&O. NFM is responsible for CUMD and FCAPS management of NFs and NEMs.

– Step (1): Slice customer (A) requests slice LCM&O (B) to provide a slice instance for a specific use case.

– Step (2): Slice LCM&O (B) designs a slice instance using a slice instance blueprint.

– Step (3): Slice LCM&O (B) requests Inf&NF-M (C) to provide dedicated resources; NFs and NEMs are needed for the slice instance.

– Step (4): In the Inf&NF-M (C), infrastructure management (C1) orders infrastructures (D) to allocate and assign resources to dedicate to the slice instance.

Steps (1) to (4) are depicted in Figure III.1.

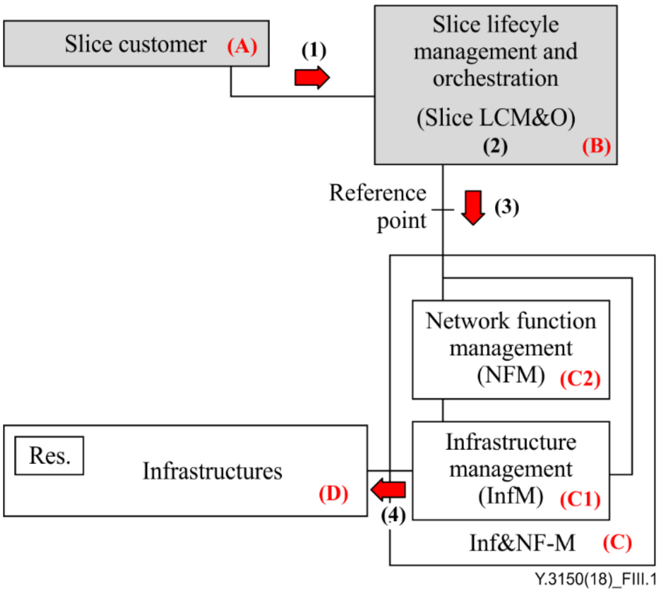


Figure III.1 – An example flow of slice instance creation (steps 1 to 4)

– Step (5): NFM (C2) creates and configures NFs (E) and NEMs (F) over the resources in infrastructure (D) dedicated to the requested slice instance.

See Figure III.2.

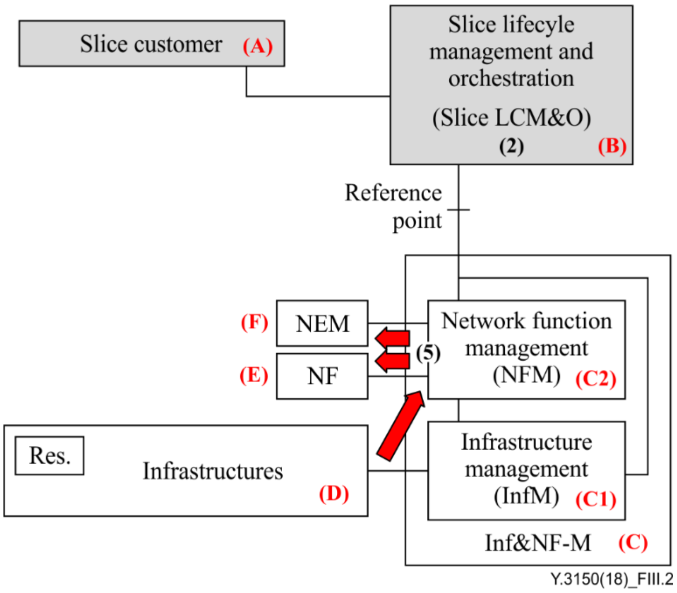


Figure III.2 – An example flow of slice instance creation (step 5)

– Step (6): Slice LCM&O (B) creates and configures the slice instance (G) using the resources (G1), NFs (G2), and NEM (G3), which are provided by Inf&NF-M (C).

See Figure III.3.

NOTE – Creation and configuration of slice instances conduct the setting or operation of the infrastructure from the real hardware point of view.

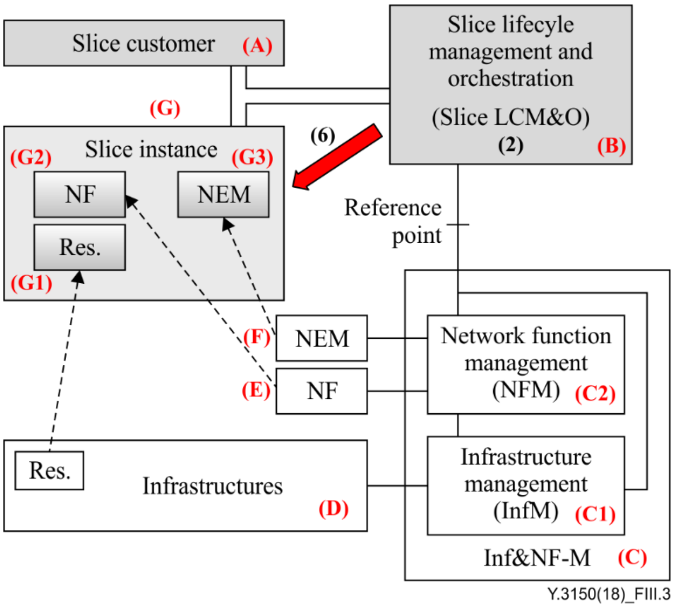


Figure III.3 – An example flow of slice instance creation (step 6)

Appendix IV

Considerations of multiple orchestrations

(This appendix does not form an integral part of this Recommendation.)

IV.1 Background

SDN and NFV have promoted scenarios in which L2 to L7 NFs and services (i.e., from a software switch or router to a software middle-box) can be delivered as software running on virtual machines either centralized in the cloud or distributed in clusters of DCs located at the edge of the network.

In IMT-2020 networks, network softwarization enables the deployment of different mobile NFs as virtualized entities. These virtual mobile NFs also include the radio access network (RAN; i.e., cloud RAN) and the CN that can be run in the cloud infrastructure [b-Martin].

In addition, transport SDN also focuses on centralized control and management of L0 to L2 NFs in order to expand applicability of SDN technologies to all network layers and domains [b-ITU-T G.7702].

In this situation, the term orchestration has been widely used in the various contexts with slightly different meanings.

In this Recommendation, there are hierarchized orchestrators in Figure 7-2, which consists of a slice orchestrator, SDN controller and NFV management and orchestration. This appendix considers their functionalities and interrelations.

IV.2 The goal and roles of orchestration

The general goal of orchestration is to streamline and optimize frequent and repeatable processes to ensure accurate and quick deployment of software in a large and complex information and communication technology (ICT) system. See clause 3.1.11 for the ITU-T definition of orchestration

To put it simply, orchestration is the term for the arranging and coordination of multiple automated tasks at once, which ultimately results in a consolidated process or workflow.

In addition, from the functionality viewpoint, orchestration implies two main roles.

– Service alignment: An orchestrator aligns business requests with applications, data and infrastructure. The orchestration process determines the policies and service levels through automated workflows, provisioning etc.

– Resource control and management: The orchestration also provides centralized control and management of the resource pool. For example, orchestration reduces the time and effort for deployment of multiple instances of a single application.

IV.3 Examples of orchestrations

There is a variety of usage of the term orchestration in different contexts. Examples follow.

– Service orchestration: is responsible for setting up and managing individual services in a network in the most resource-effective manner.

- Cloud orchestration: is the use of softwarization technology to manage interconnections and interactions among workloads on public and private cloud infrastructures. It connects automated tasks into a cohesive workflow to accomplish a goal, with permissions oversight and policy enforcement.
- Network orchestration: allows network operators to establish their own gateways, routers and security groups through software configuration files or policies that are written in a language that a control plane can understand.
- Some recent network orchestration tools implement a network-aware function that enables analysis to decide how to deploy specific resources in order to realize optimal network performance.
- Resource orchestration: determines which ICT resources are requested, resource interdependency and resource configurations. The orchestration can automatically create and configure all resources for automatic deployment, operation and maintenance.

IV.4 Orchestration in SDN controller

An SDN controller programs (i.e., dynamically designs and changes) a data-plane by automated decisions about the network if traffic congestion, faults in devices or security problems occur.

SDN orchestration is one abilities of the SDN controller that programs automated behaviours in a network to coordinate SDN-enabled networking hardware and software elements to support applications and services via APIs [ITU-T Y.3300].

NOTE – SDN orchestration can use a number of network protocols including OpenFlow and IP-based networking, such as the border gateway protocol and network configuration protocol.

In an SDN network, there may be a hierarchy of SDN controllers. Each controller orchestrates its clients' resources [b-ITU-T G.7702].

See Figure IV.1.

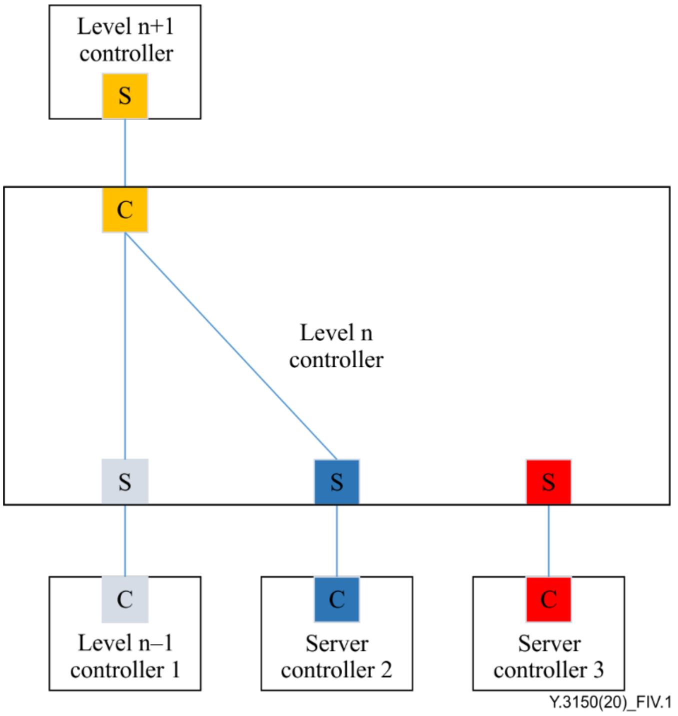


Figure IV.1 – Client and server relationships in the SDN architecture [b-ITU-T G.7702]

IV.5 ETSI NFV management and orchestration

ETSI NFV-MANO consists of three functions: NFV orchestration, VNF management (VNFM) and VIM.

NOTE – An NS consists of multiple VNFs, virtual links, VNF forwarding graph and PNFs.

- NFVO: is responsible for:
  i) network service orchestration (NSO): lifecycle management of NSs;
  ii) resource orchestration (RO): the orchestration of NFVI resources across multiple VIMs.
- VNFM: is responsible for lifecycle management (creation, deletion and scale-in and out) and monitoring of VNFs;
- VIM: is responsible for controlling and managing the NFVI computation, storage and networking resources.

NFVO functionality consists of several components, such as NSO and RO functions [b-ETSI GS NFV-IFA 009].

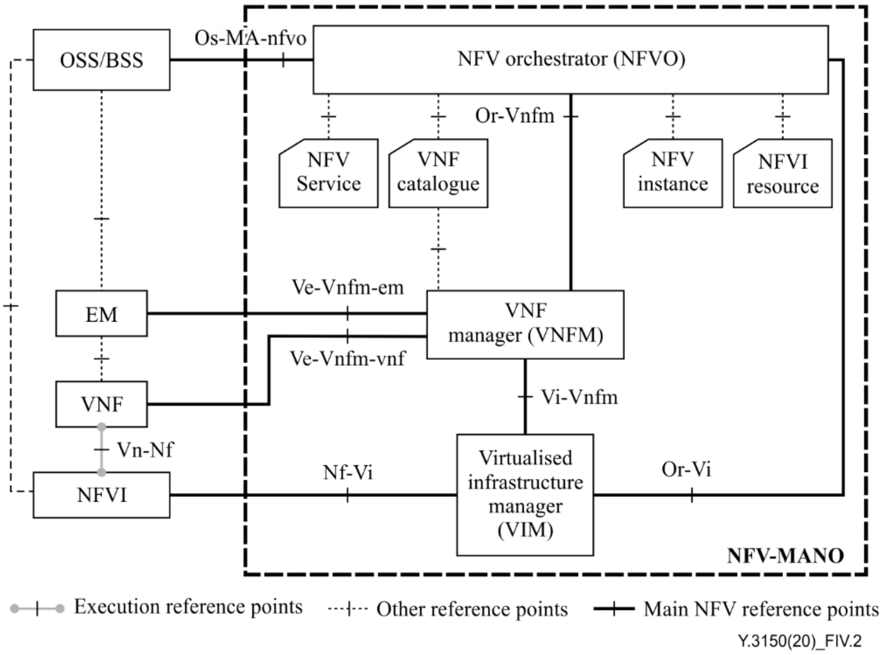


Figure IV-2 – The NFV-MANO architectural framework with reference points

IV.6 Hierarchy and ubiquity of orchestrations

The variations in orchestration described in clauses IV.2 to IV.5 are briefly summarized as follows:

- service level, application level or resource level orchestration;

  NOTE 1 – For example, MANO functions regarding NSs, VNFs and resources can be deemed to be service level, application level and resource level orchestrations, respectively.
- single domain/multi- (cross-)domain orchestration;
- upper (meta)/lower (sub) orchestration;
- single layer or multi-layer orchestration.

  NOTE 2 – For example, the orchestration of both an SDN controller in L3 (i.e., IP networks) and another SDN controller in L1-2 (e.g., MPLS networks and optical networks) is a multi-layer orchestration case.

To realize scalability and flexibility of orchestration (e.g., vendor-agnostic and technology agnostic approach), it is not a good idea that the slice orchestrator in Figure 7-2 directly manage all physical and virtual resources because of the processing burden of data exchanged through lots of interfaces. Each orchestrator therefore takes care of its targeted NSs, applications and physical or virtual resources in this Recommendation.

- Slice orchestrator (Meta): receives business requests from customers or upper applications, offers service requests to SDN and NFV environments, and controls and manages them both. The orchestrator gets an abstracted and simplified view of whole network slice instances.
- SDN controller (Sub): orchestrates SDN-enabled physical or virtual resources. The controller shields the complexity of the SDN network from the slice orchestrator.
- NFV management and orchestration (Sub): has responsibility for the control and management of NSs, VNFs and NFVI.

Appendix V

Considerations of deployment location of SDN controllers

(This appendix does not form an integral part of this Recommendation.)

V.1 Possible SDN deployment in an IMT-2020 system

[b-ITU.T TR GSTR-TN5G] introduces an example of the interaction between a 3GPP management system and a transport network management system as shown in Figure V.1, in which each transport network (TN) within or between different network domain(s) such as RAN and CN)is assumed to be managed by a transport management system, which may contain a single or multiple SDN controller(s).

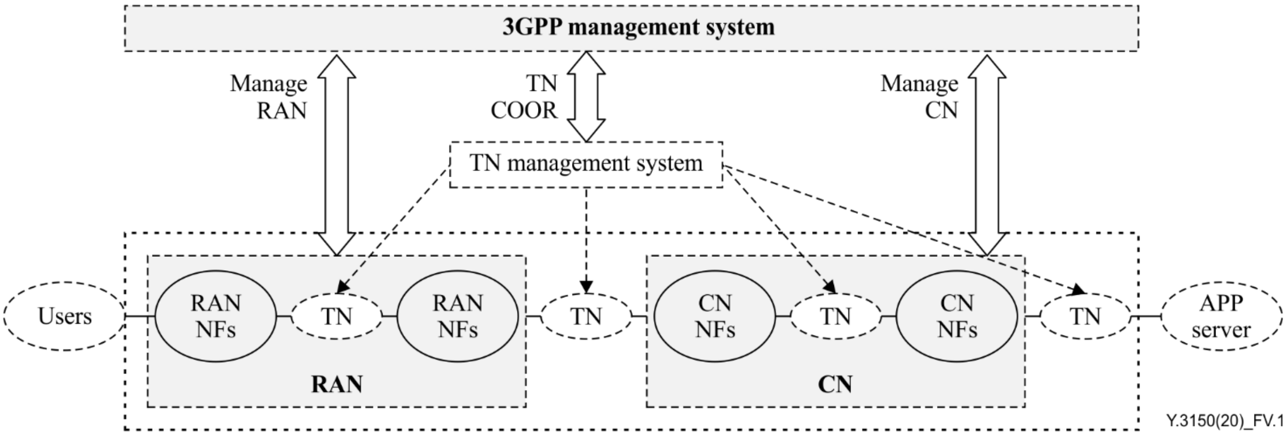


Figure V.1 – Example of the interaction between the 3GPP management system and the transport network management system as per [b-ETSI TS 128.530]

V.2 Variations of SDN deployment in an NFV environment

In a network infrastructure consisting of both SDN and NFV environments, there is a variety of locations where an SDN controller can be implemented. [b-Arfaoui] introduces the following deployment possibility for NFV environments (see Appendix II for details of the ETSI NFV model).

– As part of VIM: When using open source software, this is the typical position where VIM allocates computation resources, then contacts the SDN controller through its northbound interface to allocate network resources.

– As a VNF or a PNF: This position implies that its life-cycle is managed by the VNFM. In such a position, this VNF may perform only control plane functions.

– As part of the NFVI: In this position, it would act as a network hypervisor providing virtualized networks on top of the physical resources.

– As part of the operations support system/business support system (OSS/BSS): OSS/BSS is where the services are defined, and is directly connected to NFVO in the NFV reference architecture. At this position, the SDN controller would not react at the millisecond scale being therefore dedicated to rather static and high-level tasks.

SDN applications can be also located in several locations:

– As a VNF/PNF: If the SDN applications are implemented as VNFs, the SDN controller could also be implemented as a VNF/PNF to reduce the latency to communicate to both entities.

– As part of VIM: If SDN applications are implemented inside VIM, the SDN controller can also be integrated within VIM to reduce the latency.

- As part of element management (EM): As EM embeds SDN applications, it is worth implementing the SDN controller as a VNF. This is to manage it from the SDN application, which is now part of the EM, and hence reduce the latency.
- As part of the OSS/BSS: If SDN applications are embedded at the OSS/BSS level it is preferable to locate the SDN controller at this level and not at an infrastructure level to reduce the latency.

Bibliography

[b-ITU-T G.7702] Recommendation ITU-T G.7702 (2018), *Architecture for SDN control of transport networks*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[b-ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.3111] Recommendation ITU-T Y.3111 (2017), *IMT-2020 network management and orchestration framework*.

[b-ITU-T Y.3321] Recommendation ITU-T Y.3321 (2015), *Requirements and capability framework for NICE implementation making use of software-defined networking technologies*.

[b-ITU-T Y-Suppl.44] ITU-T Y-series Recommendations – Supplement 44 (2017), *Standardization and open source activities related to network softwarization of IMT-2020*.

[b-ITU-T FG IMT-2020] ITU-T Focus Group (2017), *IMT-2020 Deliverables*.

[b-ITU-T TR GSTR-TN5G] Technical Report ITU-T GSTR-TN5G (2018), *Transport network support of IMT-2020/5G*.

[b-ETSI GS NFV 002] ETSI GS NFV 002 V1.2.1 (2014), *Network functions virtualisation (NFV); Architectural framework.*

[b-ETSI GS NFV 003] ETSI GS NFV 003 V1.5.1 (2020), *Network functions virtualisation (NFV); Terminology for main concepts in NFV.*

[b-ETSI GS NFV-IFA 003] ETSI GS NFV-IFA 003 V2.4.1 (2018), *Network functions virtualisation (NFV) release 2; Acceleration technologies; vSwitch benchmarking and acceleration specification*.

[b-ETSI GS NFV-IFA 005] ETSI GS NFV-IFA 005 V3.4.1 (202016), *Network functions virtualisation (NFV) release 3; Management and orchestration; Or-Vi reference point – Interface and information model specification*.

[b-ETSI GS NFV-INF 005] ETSI GS NFV-INF 005 V1.1.1 (2014), *Network functions virtualisation (NFV); Infrastructure; Network domain*.

[b-ETSI GS NFV-IFA 009] ETSI GS NFV-IFA 009 V1.1.1 (2016), *Network functions virtualisation (NFV); Management and orchestration; Report on architectural options*.

[b-ETSI TS 128.530] ETSI TS 128 530 V16.3.0 (2020), *5G; Management and orchestration; Concepts, use cases and requirements*.

[b-Arfaoui] Arfaoui, G., Sánchez-Vilchez, J.M., Wary, J.-P. (2017). Security and resilience in 5G: Current challenges and future directions, 8 pp. In: *2017 IEEE Trustcom/BigDataSE/ICESS*.

[b-Martin]	Martin, B., Gharbaoui, M., Cerutti, I., Castoldi, P. (2016). Network and datacenter resource orchestration strategies for mobile virtual networks over telco clouds. In: *18th International Conference on Transparent Optical Networks* (ICTON 2016), pp. 1673-6. Piscataway, NJ; IEEE. DOI: 10.1109/ICTON.2016.7550703
[b-ONF TR-527]	Open Networking Foundation Technical Recommendation 527 (2016), *Functional requirements for transport API*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020