International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3150

(01/2018)

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

International Telecommunication Union

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.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

With the global recognition of the usefulness of network slicing technology, which is the most typical substantiation of the network softwarization approach, this Recommendation describes how network softwarization and network slicing contribute to IMT-2020 systems. It explores network slicing from two viewpoints: vertical and horizontal aspects. The Recommendation further describes network slicing for mobile fronthaul/backhaul, introduction to advanced data-plane programmability, and capability exposure. These technical characteristic descriptions are expected to lead to their detailed study.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3150	2018-01-13	13	11.1002/1000/13468

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 part of IMT-2020. It explores network slicing from two viewpoints: vertical and horizontal aspects. After overviewing in each aspect, the Recommendation further describes network slicing for mobile fronthaul/backhaul, introduction to advanced data-plane programmability, and capability exposure, whose technical characteristic descriptions are expected to lead to their detailed study.

The detailed technical features (e.g., signalling specifications) are out of the scope of this Recommendation.

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

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

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

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

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

3.1.3 management [ITU-T Y.3100]: 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.

3.1.4 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.

3.1.5 network functions virtualization [b-GS-NFV003]: principle of separating network functions from the hardware they run on by using virtual hardware abstraction.

3.1.6 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).

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

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

3.1.8 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.

3.1.9 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 natures of software such as flexibility and rapidity all along the lifecycle of network equipment/components, for the sake of creating conditions enabling the re-design of network and services architectures, optimizing costs and processes, enabling self-management and bringing added values in network infrastructures.

3.1.10 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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BH	Backhaul
CMUD	Create, Monitor, Update and Delete
DNS	Domain Name System
DPP	Data Plane Programmability
eMBB	enhanced Mobile Broadband
FCAPS	Fault, Configuration, Accounting, Performance and Security
FH	Fronthaul
IMT-2020	International Mobile Telecommunications for 2020
Inf&NF-M	Infrastructure and NF Management
IoT	Internet of Things
LCM&O	Lifecycle Management and Orchestration
MBH	Mobile Backhaul
MFH	Mobile Fronthaul
mMTC	massive Machine Type Communication
NAT	Network Address Translation
NE	Network Element
NetSoft	Network Softwarization
NFV	Network Functions Virtualization
RAN	Radio Access Network
SDN	Software Defined Networking
SDO	Standards Developing Organization
UE	User Equipment
URLLC	Ultra-Reliable and Low Latency Communication
VNF	Virtual Network Function

5 Conventions

None.

6 Introduction to network softwarization for IMT-2020

Network softwarization is an overall approach for designing, implementing, deploying, managing and maintaining network equipment and network components by software. It exploits the natures of software such as flexibility and rapidity all along the lifecycle of network equipment/components, for the sake of creating conditions enabling the re-design of network and services architectures, optimizing costs and processes, enabling self-management and bringing added values in network infrastructures.

Figure 6-1 shows how network softwarization contributes to 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.

Key components to realize this are SDN, NFV and cloud computing, which are described in the next sub-clause.

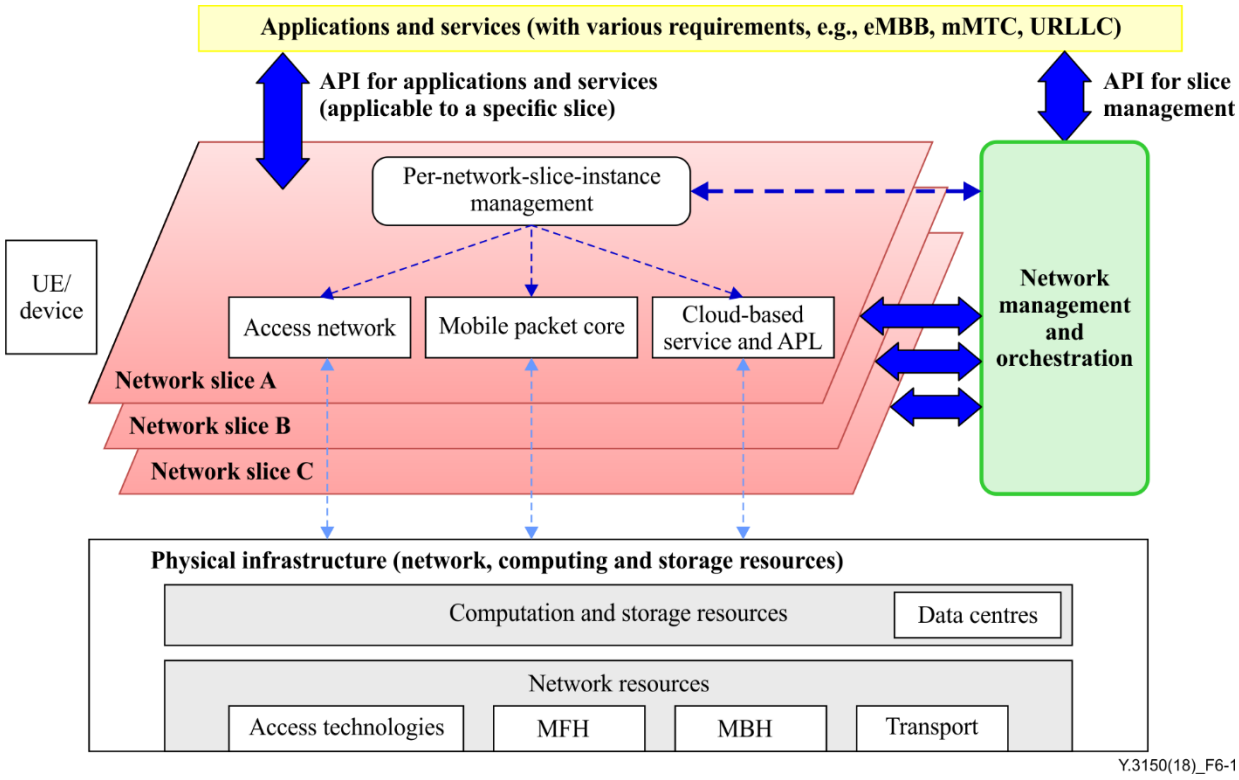

Figure 6-1 – Network softwarization for IMT-2020

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 Software-defined networking (SDN)

Software-defined networking (SDN) is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualised 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.

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

6.1.2 Network functions virtualization (NFV)

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

It is designed to consolidate and deliver the networking components needed to support a fully virtualised 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.

6.1.3 Cloud computing

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

Cloud computing is different from traditional telecommunication networks since 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 customer and network operator.

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

6.2 Potential use cases supported by network softwarization

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

1. Video traffic already dominates the mobile communication traffic and still increasing. This requires the network architecture having efficient video-on-demand delivery mechanism in terms of network/server congestion reduction and shorter response time.
2. In many countries, disaster resilience is a key concern. Since network systems are a life line infrastructure, they are expected to be robust. Increased network flexibility helps respond this request.
3. IoT and big data processing are booming. Future networks including IMT-2020 network should provide with functions that fit to efficient big data processing systems.
4. One of the expectations for IMT-2020 is the low latency. Total design including data processing and service provisioning is necessary to fulfil this expectation.
5. SDN and NFV are expanding as possible key technologies for future networks including IMT-2020 network.

The flexibility covering these wide varieties of objectives can be achieved via network softwarization. With the adoption of SDN and NFV, software programmability of network nodes will expand, which in turn makes it feasible to run information processing and service software on network nodes.

7 Vertical aspects

This clause describes technical characteristics of network softwarization (including network slicing) in terms of different levels of abstraction (ranging from physical infrastructure, virtualised resources, virtualised network functions and to network slices) 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, IMT-2020 system for providing network slices can be modelled by the three key functional entities as shown in Figure 7-1.

Slice customers request creation of network slices (instances) based on their service requirements and use the provided instance.

Slice lifecycle management and orchestration (slice LCM&O) provides and manages network slices (instances) based on the request from a slice customer.

Slice support assists slice LCM&O by gathering individual components of a slice and arranging them to respond to slice LCM&O's request and the corresponding slice customer's demand. The components of a slice and its instances consist of network functions (NFs) and resources. Network element management (NEM) can be included if explicitly required.

This clause further describes the slice support and its interaction with slice LCM&O across R1.

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

NOTE 2 – Appendix I provides details about configuration of slice-support. Appendix II provides the relation with ETSI NFV model.

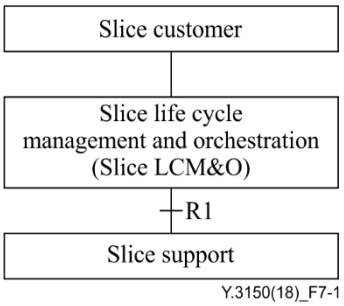

Figure 7-1 – Basic model for providing network slices

7.1.2 Slice support

For providing the components needed for a slice instance (i.e., resources, NFs and NEMs), the slice support includes at least the following:

Infrastructure: This represents objects to be managed to provide resources, NFs, and NEMs.

Manager for infrastructure and NF (Inf&NF-M): This is responsible for the following functions.

Infrastructure and resource aspects:

(f1) fault, configuration, accounting, performance and security (FCAPS) management of infrastructure

(f2) create, monitor, update and delete (CMUD) of resources

(f3) FCAPS management of resources

Network function aspects

(f4) CMUD of NFs and NEMs

(f5) FCAPS management of NFs and NEMs

7.1.3 Interactions between slice LCM&O and slice support

The following are the possible interactions between slice LCM&O and slice support.

(i-1) Interaction for FCAPS management of infrastructure

From slice LCM&O to slice support, management policies for infrastructures are given. (In the case of fault management, the management policies represent required level of reliability assurance and associated mechanisms (e.g., mean time to repair and specific redundancy mechanisms).) From slice support to slice LCM&O, information of infrastructure is provided (e.g., fault alarms of the infrastructure).

(i-2) Interaction for CMUD of resources

From slice LCM&O to slice support, messages are sent for CMUD of the resources, which are used for NFs or NEMs.

(i-3) Interaction for FCAPS management of resources

From slice LCM&O to slice support, resource management policies are given. From slice support to slice LCM&O, information of resources needed for slice LCM&O is sent (e.g., fault alarms of the resources).

(i-4) Interaction for CMUD of NFs and NEMs

From slice LCM&O to slice support, messages are sent for CMUD of NFs or NEMs. NFs are created using resources according to the configuration information embedded in the messages.

(i-5) Interaction for FCAPS of NFs and NEMs

From slice LCM&O to slice support, management policies for NFs and NEMs are given. From slice support to slice LCM&O, information of NFs and NEMs needed for FCAPS is provided (e.g., fault alarms of NFs or NEMs).

The information exchanged between slice LCM&O and Inf&NF-M and information exchanged between Inf&NF-M and infrastructure may be different. The former information can be described in the same way (i.e., implementation- and hardware-agnostic) and the latter information depends on the technologies of the infrastructure.

NOTE 1 – Appendix III provides example procedures and flows for slice instance creation.

NOTE 2 – The interface between slice LCM&O and Inf&NF-M corresponds to the interface Se identified in [ITU-T Y.3111]. The detailed information and messages exchanged between slice LCM&O and Inf&NF-M are for further study.

7.2 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 slicing is on its application to the core network. This Recommendation focuses on another point: the use of slicing in the access network of the IMT-2020 network, which consists of mobile fronthaul (FH) and backhaul (BH). To identify key capabilities in this application, this clause starts with expected capabilities and benefits of network softwarization for FH/BH. Two new key features are identified.

7.2.1 Expected capabilities and benefits

The description in this clause 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].

(A) Expected capabilities and benefits of NetSoft on FH/BH for eMBB

– Reduction of the huge and fluctuating power consumption caused by a large number of small cells

To support eMBB, a large number of small cells are foreseen and a lot of links to them are also required. The first issue is huge power consumption of them.

Second, since a cell size is small, the number of users (and devices) in a cell is small. Statistical multiplexing effect, which usually makes changing behaviours easy to manage, cannot be expected. 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 covers the area and (2) network elements (NEs) for FH/BH have a sleep or power reduction mode according to the traffic, power

consumption can be reduced drastically. NetSoft mechanisms are expected to have capabilities to make use of these characteristics on FH/BH with the dynamic resource allocation for slices.

(B) Expected capabilities and benefits of NetSoft on FH/BH for mMTC

– Avoidance of overflow caused by user data traffic and control signal processing

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 devices to a termination node, which may be placed around FH/BH. The FH/BH is expected to transfer the data. This applies to the control signal processing as well. To prevent overflow, suitable resource allocation is expected for the both data plane and control plane in the slice instances.

(C) Expected capabilities and benefits of NetSoft on FH/BH for URLLC

– Controllability delegation from orchestrator to the controller in the FH/BH

When a terminal for URLCC 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 a distant orchestrator and the orchestration covers reallocation of all terminals, large traffic for this control will flow. In such a case, if some controllability is delegated to the local controller, the controller could reallocate the resources (instead of orchestrator) by its own decision. This delegation and localization can reduce delay and control traffic. The controllability for the reallocation is expected to be transferred from orchestrator to the controller in FH/BH.

7.2.2 Required new functionalities

The following two functionalities are expected when network slicing is applied to mobile fronthaul and backhaul.

a) Functionalities for the 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 orchestrator can control physical resources to meet different power-consumption requirements. Specifically, the orchestrator 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 orchestrator can choose the best mode of operation and change modes if necessary.

b) 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 it 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 orchestrator modifies the setting (i.e., ratio). To adjust the allocated resource close enough to the real use, the orchestrator 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 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 a) providing automatic power saving

and b) smooth sharing of unused resources with other virtual paths. This autonomous mechanism mitigates the burden of the orchestrator.

NOTE – Other SDOs already designed some APIs, which can be used in the CMUD functionalities. Information about the APIs specified in ONF is given in [b-ONF TR-527]. Through Phase 1 work in FG IMT-2020, the above functionalises 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].

7.3 Advanced data plane programmability

Network softwarization technologies including SDN, NFV, slicing and their extensions are expected to support IMT-2020 mobile 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 (DPP) 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.

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 be concatenated each other to fully meet service requirements. Horizontal aspects of network softwarization and slicing mean control and management of network slices through multiple network infrastructure segments. An infrastructure segment is separated from the viewpoints of i) characteristics of a network and/or ii) administrative purpose to manage a group of components of the infrastructure segment. Consideration on both vertical and horizontal aspects of network capabilities is important for network softwarization to realize agility, flexibility and scalability of network services.

NOTE – An infrastructure segment can be represented by "slice support" described in clause 7.

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

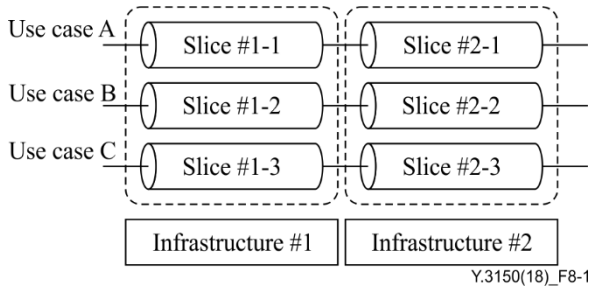

Figure 8-1 – An image on network slices depending on infrastructures

NOTE 1 – A set of connected slices for a use case in this figure (e.g., slice #1-1 + slice #2-1) can be regarded as a "network slice". In this case, individual slices in the Figure (e.g., slice #1-1) may be called as a "sub-network slice".

Figure 8-2 illustrates an example of network slicing for IMT-2020 network based on Figure 8-1. In this figure, infrastructure segments are separated as a mobile fronthaul, backhaul and core network. Individual network slices, which attribute to the independent infrastructures, are logically connected for different services such as eMBB and mMTC.

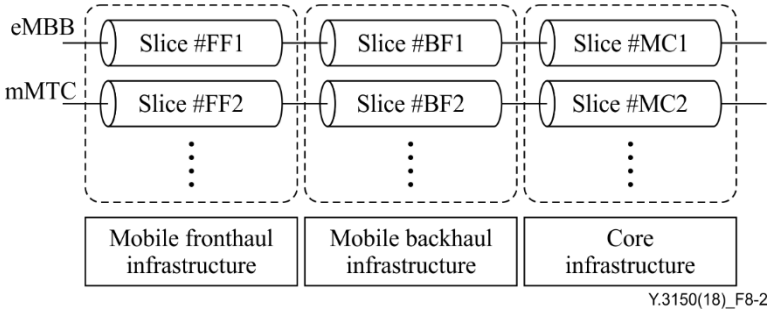

Figure 8-2 – An example of network slicing for IMT-2020 network

Administrators of individual infrastructure segments may not be a single network operator/service provider. Figure 8-3 shows an example of the usage of network slicing for roaming services.

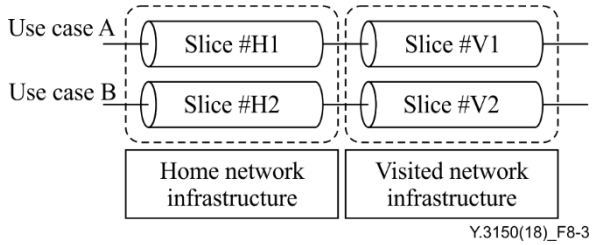

Figure 8-3 – A possible usage of network slicing for roaming

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

NOTE 2 – There is another example of network slicing. A network slice can be used for multiple services simultaneously, and it is called as "shared network slice". On the other hand, a network slice for the purpose of single service is named as "dedicated" network slice. Figure 8-4 shows an image of the concept combining a shared network slice "Slice #2-1" and dedicated network slices "Slice #1-1" and "Slice #1-2".

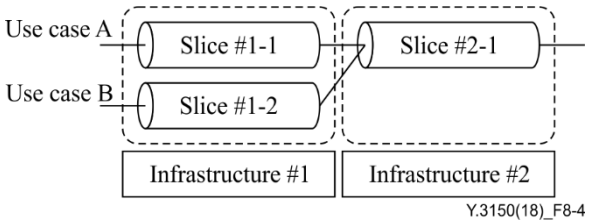

Figure 8-4 – An image on shared and dedicated network slices

8.2 Capability exposure and APIs

IMT-2020 system will accommodate a lot of 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 high variety of requirements on the network. For example, there will be different requirements on functionality such as charging, policy control, security, mobility etc. Some use cases such as enhanced Mobile Broadband (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 the operator to create customised network (e.g., a network slice) to provide optimized solutions for different market scenarios which have diverse requirements, e.g., in the areas of functionality and performance.

The potential operational requirements are as follows:

- The IMT-2020 system is required to be able to customize the network functions within a slice dynamically based on the variation of the third party (e.g., enterprises, service providers, contents providers, etc.) demands.
- The IMT-2020 system is required to also support dynamic utilization of resources (compute, network and storage resources) within a slice as per the third party application requirement, subject to operator's policy.

Figure 8-5 illustrates the capability exposure architecture for slice management.

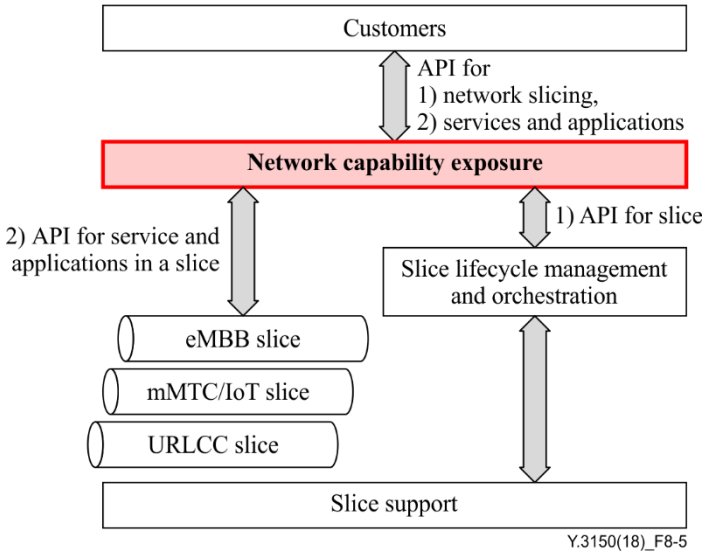

Figure 8-5 Capability Exposure for network slicing

Use Case 1: The creation or instantiation of a slice triggered by the third party

1. The third party indicates the functionality and performance requirements to create a slice via slice building API. In terms of implementation, a service template profile may be sent to by the API. And this template contains parameters to describe the functionality and performance requirements.
2. The network capability exposure function transfers the above slice building request to the slice lifecycle management and orchestration (slice LCM&O).
3. The slice lifecycle management and orchestration (slice LCM&O) authorizes the creation request of the 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 slice LCM&O forwards resource requirement to slice support and accordingly the Slice support allocate the required resource (hardware and software) to create or instantiate the dedicated slice.

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

1. The third party indicates the modification of functionality or performance for a pre-created slicing via slice modification API. The modification may be triggered for the reason of lack of resource or new function needed by the third party in the slice. In terms of implementation, a service template profile may be sent to by the API. And this temple contains the parameters to describe the functionality and performance modification requirement.
2. The network capability exposure function transfers the above slice modification request to the slice LCM&O.
3. The slice LCM&O authorizes the request of functionality and performance modification based on the agreement between the operator and the third party. If the request is allowed, the slice LCM&O forwards resource requirement to the slice support and accordingly the slice support re-allocates the required resources (hardware and software) to modify the dedicated slice.

Authorization between slice customer and network capability exposure platform is needed. Slice support can act as the resource management and orchestration, which realizes the deployment of network slice functions including network connectivity. Transport SDN is an underlying technology of providing the overall bandwidth guarantee on an instantiated network slice.

Appendix I

Example details of slice-support

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

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

The InfM is connected with the infrastructures and manages FCAPS of infrastructures. The InfM connects with slice LCM&O and receives the information from slice LCM&O to creates, monitors, updates and deletes resources over the infrastructures which are dedicated for a slice instance. The InfM manages FCAPS of the resources. The InfM is also connected with NFM.

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

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

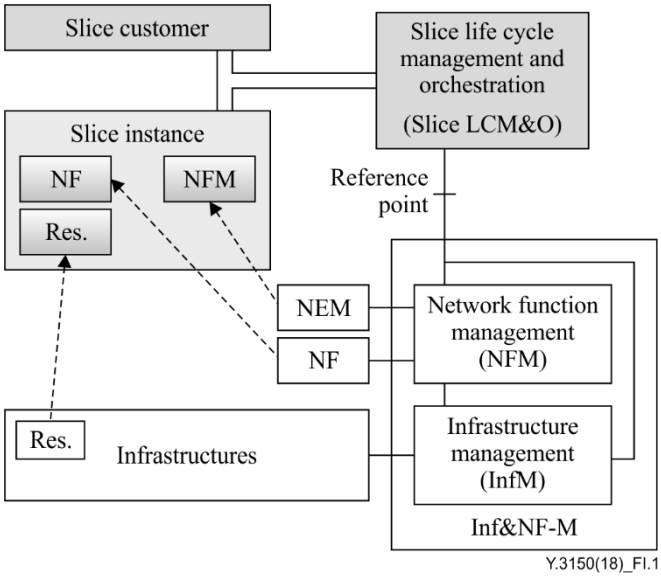

Figure I.1 – Basic model for providing slices with slice support

Appendix II

Consideration on the relationship with ETSI NFV model

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

ETSI NFV (network functions virtualization) model is shown in the right side of Figure II.1. This technology provides virtual resources, virtualised network functions (VNFs) and element managements (EMs).

The relationship with ETSI NFV model 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 candidate configuration is shown in Figure II.2 in which ETSI-NFV scheme can be mapped over the model described in clause 7.1.

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

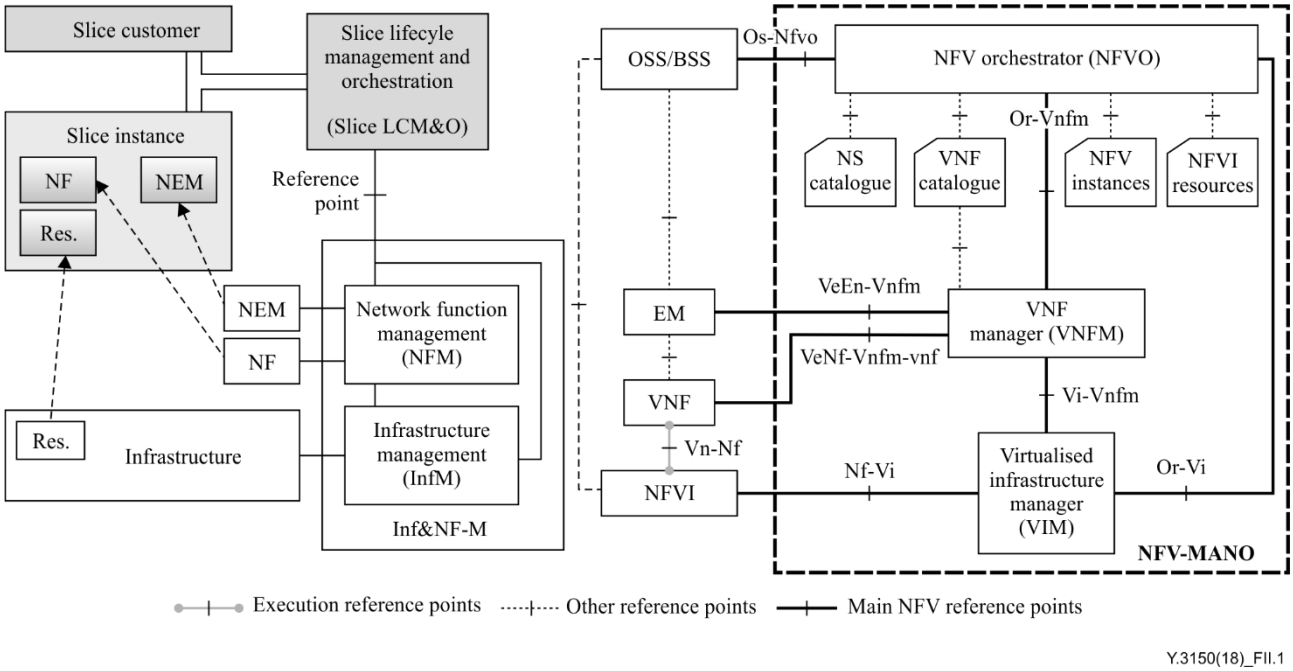

Figure II.1 – The model shown in Figure I.1 (left) and the ETSI-NFV model (right)

Table II.1 – Comparison between this Recommendation model and ETSI-NFV model

	Recommendation ITU-T Y.3150	ETSI-NFV
Target	Providing for "network slice"	Providing for "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 [b-ETSI_GS_NFV003]: composition of Network Functions and 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 performance, dependability, and security

Table II.1 – Comparison between this Recommendation model and ETSI-NFV model

	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.	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 inside. This management function can be accessible by slice customers (via capability exposure). Network service in ETSI-NFV model is not clear for this point as of the publication of this Recommendation.	
Who orders the lifecycle management for network slice instance or network service to slice LCM&O or NFVO	Slice customer via capability exposure	OSS/BSS via Os-Ma. This reference point is used for network service lifecycle management. (see clause 7.3.7 in [b-ETSI_GS_NFV 002]).
Transport network functions	– Transport network functions are also a kind of NFs. – 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 in [b-ETSI GS NFV-IFA003] and [b-ETSI GS NFV-INF005])
Information exchanged between slice LCM&O and InfM (in ITU-T Y.3150) / NFVO and 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-IFA005]

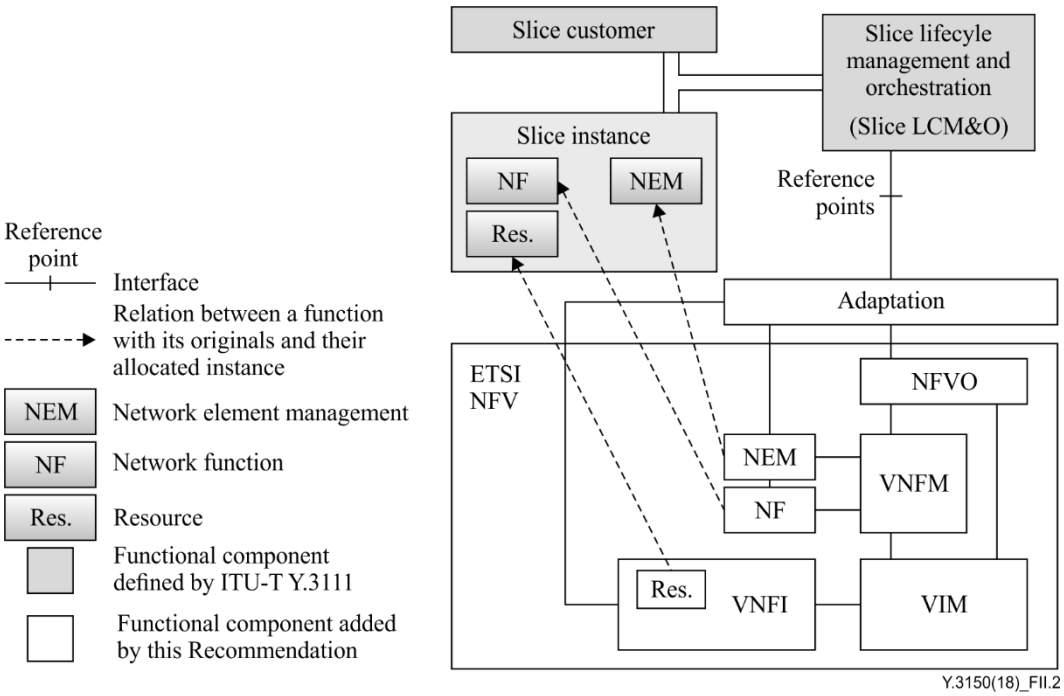

Figure II.2 – An example configuration for a slice instance when logical resources are assumed to be provided by ETSI NFV scheme

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 on procedures and relevant flows for network slice instance creation.

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

The InfM manages FCAPS of infrastructures based on information given by slice LCM&O. The NFM has a responsible on 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 blue print.

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

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

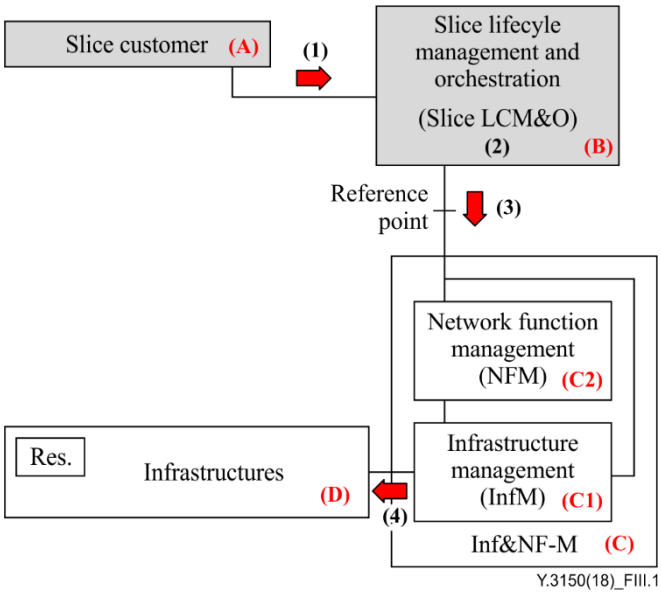

Figure III.1 – An example flow of slice instance creation (steps 1 to 4)

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

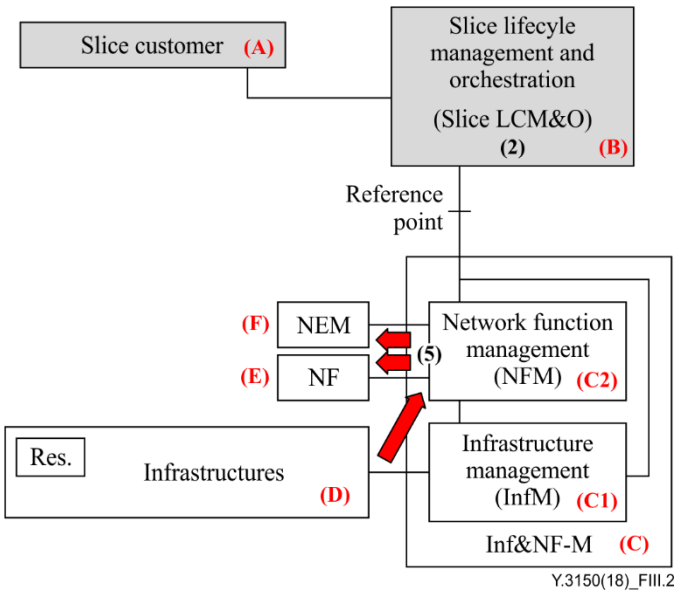

Figure III.2 – An example flow of slice instance creation (step 5)

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).

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

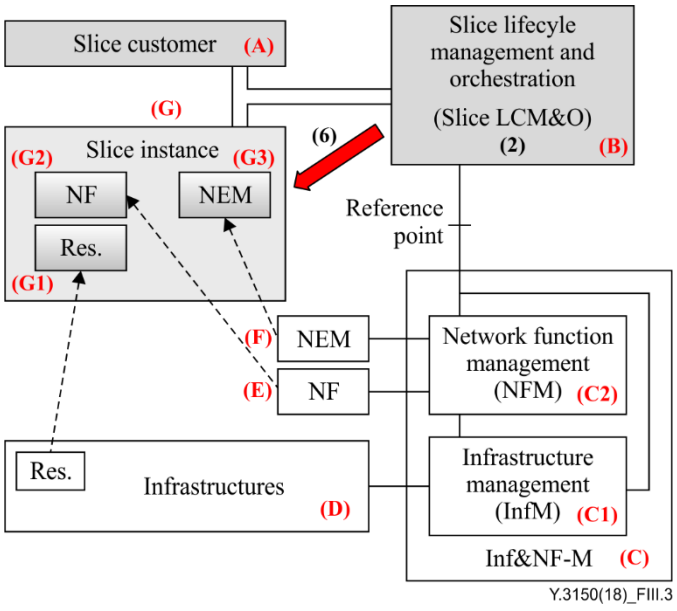

Figure III.3 – An example flow of slice instance creation (step 6)

Bibliography

[b-ITU-T Y.Sup 44] ITU-T Supplement 44 to Y.3100 series (2017), *Standardization and open source activities on network softwarization of IMT-2020*.

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

[b-ETSI GS NFV 002] ETSI GS NFV 002 (2014), *Network Functions Virtualisation (NFV); Architectural Framework*.

[b-ETSI GS NFV 003] ETSI GS NFV 003 (2014), *Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV*.

[b-ETSI GS NFV-IFA003] ETSI GS NFV-IFA003 (V2.1.1 (2016-04)), *Network Functions Virtualisation (NFV); Acceleration Technologies; vSwitch Benchmarking and Acceleration Specification*.

[b-ETSI GS NFV-INF005] ETSI GS NFV-INF005 (V1.1.1 (2014-12)), *Network Functions Virtualisation (NFV); Infrastructure; Network Domain*.

[b-ETSI GS NFV-IFA005] ETSI GS NFV-IFA005 (V2.1.1 (2016-04)), *Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vi reference point – Interface and Information Model Specification*.

[b-ONF TR-527] ONF TR-527 (2016), *Functional Requirements for Transport API*, June 10.

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, 2018