International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3102

(05/2018)

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

Future networks

Framework of the IMT-2020 network

Recommendation ITU-T Y.3102

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.3102

Framework of the IMT-2020 network

Summary

Recommendation ITU-T Y.3102 provides the framework for overall non-radio aspects of the IMT-2020 network. Following an introduction to the key features of the IMT-2020 network, architectural design considerations and framework of the IMT-2020 network are provided.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3102	2018-05-29	13	11.1002/1000/13610

Keywords

Access network agnostic common core network, framework, IMT-2020, network architecture, network function, network service framework, network slice.

[*] 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.3102

Framework of the IMT-2020 network

1 Scope

This Recommendation provides the framework for overall non-radio aspects of the IMT-2020 network. Following an introduction to the key features of the IMT-2020 network, architectural design considerations and framework of the IMT-2020 network are provided.

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.3110] Recommendation ITU-T Y.3110 (2017), *IMT-2020 network management and orchestration requirements.*

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

[ITU-T Y.3150] Recommendation ITU-T Y.3150 (2018), *High-level technical characteristics of network softwarization for IMT-2020.*

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

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

3.1.3 IMT-2020 [ITU-T Y.3100]: Systems, system components, and related technologies that provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

NOTE – [b-ITU-R M.1645] defines the framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000 for the radio access network.

3.1.4 logical resource [b-ITU-T Y.3011]: An independently manageable partition of a physical resource, which inherits the same characteristics as the physical resource and whose capability is bound to the capability of the physical resource.

NOTE – "independently" means mutual exclusiveness among multiple partitions at the same level.

3.1.5 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.

3.1.6 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.

3.1.7 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 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 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 infrastructures by optimization criteria.

3.1.10 PDU session [ITU-T Y.3100]: In the context of IMT-2020, an association between a user equipment (UE) and a data network that provides a protocol data unit (PDU) connectivity service.

NOTE – The type of the association includes IP type, non-IP type and Ethernet type.

3.1.11 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.

3.1.12 user plane [b-ITU-T Y.2011]: A synonym for data plane.

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 not be bound to the capability of the physical or logical resource.

NOTE – "different characteristics" means simplification or extension of the resource characteristics. "different characteristics" allows the virtual resource to expose access or control methods different from the original physical or logical resource.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF	Application Function
AN	Access Network
ASF	Authentication Server Function
BRAS	Broadband Remote Access Server
CDN	Content Delivery Network
CEF	Capability Exposure Function
CN	Core Network
CM	Connection Management
CP	Control Plane
CPE	Customer Premises Equipment
CSCF	Call Session Control Function
eMBB	enhanced Mobile Broadband
GBR	Guaranteed Bit Rate
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GTP	GPRS Tunnelling Protocol
HM	Handover Management
IMS	IP Multimedia Subsystem
IMT-2020	International Mobile Telecommunication 2020
IWF	Interworking Function
LAN	Local Area Network
MEC	Mobile Edge Computing
MGCF	Media Gateway Control Function
MPLS	Multiprotocol Label Switching
MTC	Machine Type Communications
NACF	Network Access Control Function
NAS	Non-Access Stratum
NF	Network Function
NFI	Network Function Instance
NFR	Network Function Registry function
NFV	Network Function Virtualization
NS	Network Slice
NSI	Network Slice Instance
NSSF	Network Slice Selection Function
PCF	Policy Control Function

PDU	Protocol Data Unit
PGW	Packet data network Gateway
RAN	Radio Access Network
PCF	Policy Control Function
QoS	Quality of Service
RAT	Radio Access Technology
RM	Registration Management
RRC	Radio Resource Control
SDN	Software Defined Networking
SGW	Serving Gateway
SM	Session Management
SMF	Session Management Function
UE	User Equipment
UP	User Plane
UPF	User Plane Function
UPM	User Plane Management
URLLC	Ultra-Reliable Low Latency Communications
USM	Unified Subscription Management function
VPLMN	Visited Public Land Mobile Network
VPLS	Virtual Private LAN Service

5 Conventions

None.

6 Introduction to the key features of the IMT-2020 network

The IMT-2020 network will enable a variety of services, including enhanced mobile broadband (eMBB) services, massive machine type communications (MTC) based services and ultra-reliable low latency communications (URLLC) based services [ITU-T Y.3101], on an infrastructure of network and computing resources.

Among the numerous features of the IMT-2020 network, the following are specific key features which characterize the IMT-2020 network:

– distributed architecture based on softwarized network functions,

– access network agnostic common core network,

– network slicing.

6.1 Distributed architecture based on softwarized network functions

By virtue of softwarization and pervasive deployment of computing infrastructure with connectivity and storage, as described in [ITU-T Y.3150], network functions can be instantiated on demand. This brings to the IMT-2020 network architecture a shift in terms of network deployment paradigm from the deployment of network entities with fixed functionalities such as packet data network gateways (PGWs) or serving gateways (SGWs) to the instantiation of network functions as necessary.

The IMT-2020 network is required to enable the provisioning of diverse services by instantiating network functions as appropriate on the infrastructure of network and computing resources.

A network function can be instantiated more than once (i.e., network function instances), e.g., to provide a given service to different geographical areas or to provide redundancy and scalability.

The distributed architecture based on softwarized network functions allows on-demand flexible deployment of the necessary network functions and programmable network configuration. Modular network function design (e.g., separation of mobility management and session management control functions) is desirable to enable flexible network function deployment and programmable network configuration.

6.2 Access network agnostic common core network

In order to enable service providers to provide different services without building a separate end-to-end network for each service, an access network agnostic common core network is required.

The IMT-2020 network provides diverse services with different access networks using the access network agnostic common core network.

Separate access networks can be deployed based on the appropriate set of network functions and employed technologies. For example, access networks for vertical industries (i.e., smart manufacturing, power grids, intelligent transport, smart home environments, etc.) may require specific network functions and technologies. These access networks may employ industry specific communication, control and management technologies and architectures, which likely differ from the typical IP-based technologies and architectures of wireline and mobile access networks. Furthermore, the IMT-2020 network is also required to cope with other emerging services.

The IMT-2020 core network is generally composed of common network functions and service specific network functions.

The common core network functions are required to support the basic IMT-2020 network service framework for network services, including registration management, connection management, session management, user plane management and handover management. A high-level description of the IMT-2020 common core network functions is provided in clause 8.1.

The service specific core network functions are required to support specific services. For example, public warning services and mission critical services for utilities and railways require service specific network functions such as IP multimedia subsystem (IMS) based call session control function (CSCF) and media gateway control function (MGCF) [b-3GPP TS 23.228].

6.3 Network slicing

Network operators have traditionally provisioned multiple different networks to cope with their market requirements and business strategies. Each of these networks has been optimized to different requirements in terms of service characteristics, functionalities, performance and isolation aspects. Network slicing enables IMT-2020 network operators to create logically partitioned networks providing customised solutions for different market and business scenarios.

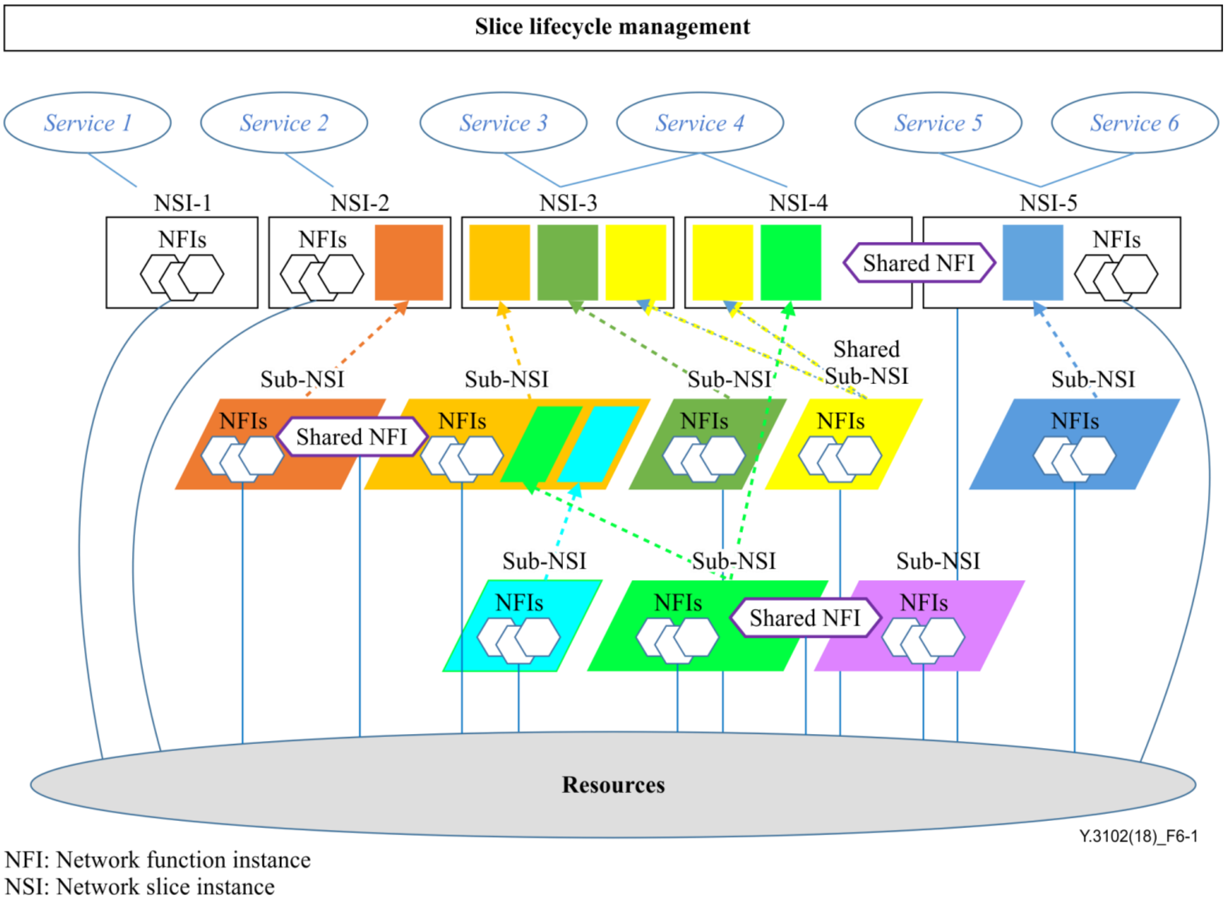
In a typical IMT-2020 network deployment making usage of network slicing, the services are provided in the context of each network slice. Each network slice can provide customized solutions enabling the support of different application services such as eMBB, MTC and URLLC.

Network operators may also deploy, e.g., for different customer groups or geographical locations, multiple instances of a given network slice, i.e., network slice instances, delivering the same features.

A network slice instance (NSI) is composed of a set of network function instances (NFIs) running over the allocated resources. An NSI constitutes a logical network that provides specific network capabilities and characteristics. Even when a network slice instance is statically defined, allocated resources together with their configuration may vary over time because of on-demand resource re-allocation or scaling.

Network slice instances are created and managed by network slice life-cycle management functions. These functions deal with orchestration, control and management of network slice, network functions and resources during network slice life-cycle. ITU-T Recommendations [ITU-T Y.3110] and [ITU-T Y.3111] provide more details about the IMT-2020 network slice life-cycle management functions.

Figure 6-1 introduces the conceptual overview of network slicing in the IMT-2020 network.



NFI: Network function instance
NSI: Network slice instance

Figure 6-1 – Conceptual overview of network slicing in the IMT-2020 network

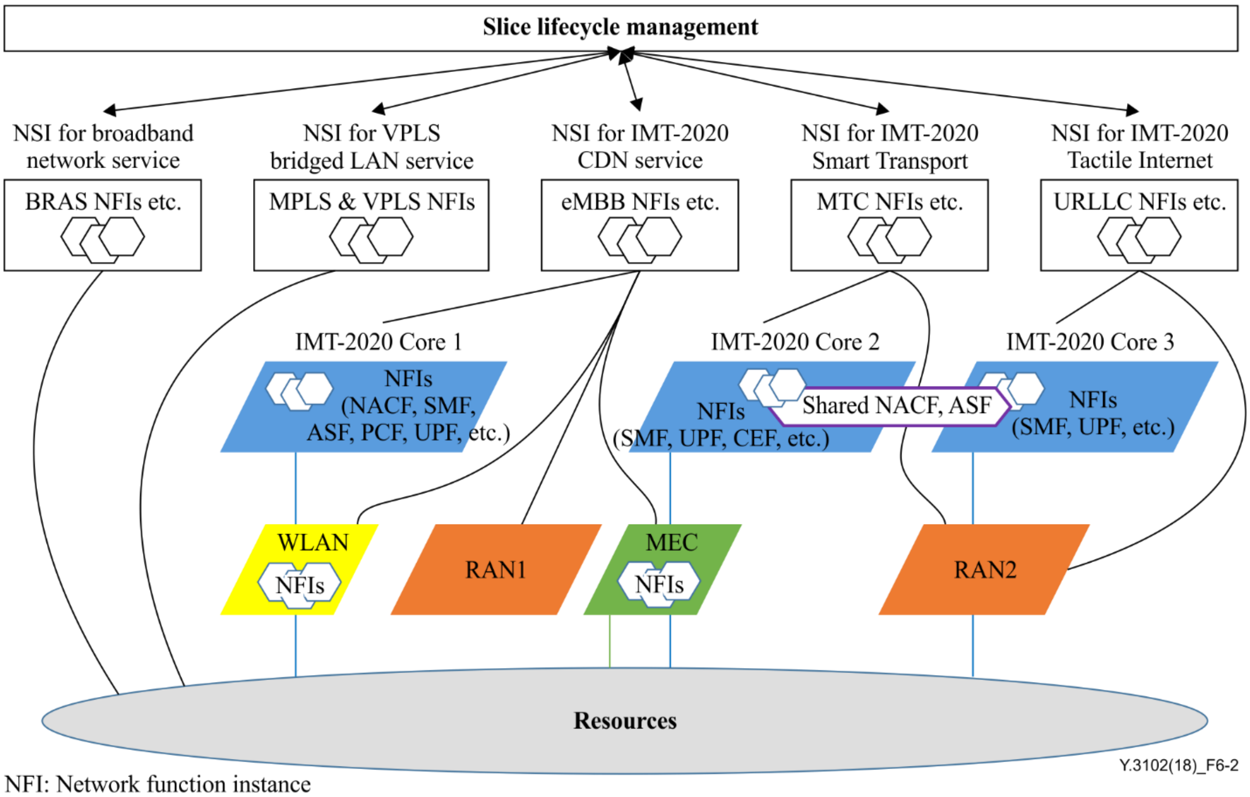
In line with what is described above, a network slice instance can support one or more application services. Also, the same application service can be supported by multiple network slice instances. As an example, in Figure 6-1, Service 4 is supported by both NSI-3 and NSI-4.

An NSI may be composed of one or multiple sub-network slice instances (sub-NSIs). Similar to an NSI, a sub-NSI is composed of a set of NFIs running over the allocated resources. However, in contrast to an NSI, a sub-NSI does not necessarily constitute a complete logical network.

A sub-NSI may be shared by two or more NSIs. In Figure 6-1, NSI-3 and NSI-4 share a sub-NSI: resources and network functions in the sub-NSI serve NSI-3 and NSI-4 according to the policy pre-defined by the network slice life-cycle management. Examples of policies include best-effort based policy, where NSI-3 and NSI-4 compete for the required resources and network functions, priority-based policy and pre-configuration of the isolated resources and network functions serving each NSI.

Some NFIs may be shared across multiple (sub-)NSIs. For example, the mobility management function or authentication function instance may be shared by two NSIs to serve them with common user context information.

In order to illustrate how the concept of network slicing can be implemented in the IMT-2020 network, Figure 6-2 provides an example of IMT-2020 network deployment from a network slicing perspective. Details provided in Figure 6-2 are out of scope of this Recommendation.


Slice lifecycle management
NSI for broadband network service
BRAS NFIs etc.
NSI for VPLS bridged LAN service
MPLS & VPLS NFIs
NSI for IMT-2020 CDN service
eMBB NFIs etc.
NSI for IMT-2020 Smart Transport
MTC NFIs etc.
NSI for IMT-2020 Tactile Internet
URLLC NFIs etc.
IMT-2020 Core 1
NFIs (NACF, SMF, ASF, PCF, UPF, etc.)
IMT-2020 Core 2
NFIs (SMF, UPF, CEF, etc.)
Shared NACF, ASF
IMT-2020 Core 3
NFIs (SMF, UPF, etc.)
WLAN
NFIs
RAN1
MEC
NFIs
RAN2
Resources
Y.3102(18)_F6-2

NFI: Network function instance
NSI: Network slice instance

Figure 6-2 – An example of the IMT-2020 network from network slicing perspective

7 Design considerations for the IMT-2020 network architecture

In line with the key features described in clause 6 and the requirements identified in [ITU-T Y.3101], the following clauses constitute design considerations for the IMT-2020 network architecture.

7.1 Support of network slicing

The IMT-2020 network is required to be flexible to support the extreme variety of requirements in terms of application services. Therefore, the IMT-2020 network is a network where multiple logical network instances, tailored to different customer specific requirements, can be created by using network slicing. The IMT-2020 network architecture is required to support multiple network slices and to allow a single user equipment (UE) to be attached to multiple network slices.

When a UE registers with the IMT-2020 network, the UE is required to provide information for the selection of the required network slice(s) which the UE wishes to establish one or more sessions on. The selection of the network slice for the UE is triggered by the network access control function through its interaction with the network slice selection function. Details about network slice selection are provided in clause 8.

7.2 Support of network capability exposure

Network slices are composed of network functions. The IMT-2020 network architecture is required to support network capability exposure in order to enable 3rd parties to use the capabilities provided by network slices as well as network functions.

7.3 Common interface to support access network agnostic common core network

As described in clause 6.2, the IMT-2020 network architecture is required to provide a core network which can be commonly used by different access networks. For this, the common core network (CN) is required to be designed with minimum access network (AN) dependency. This requires AN-CN functional separation and a common signalling interface, e.g., non-access stratum (NAS) [b-3GPP TS 24.501], between ANs and CN.

NOTE – For ANs which do not natively support a common signalling interface, an interworking function (IWF) needs to be provided at the AN-CN interface so that network functions deployed in the CN can still use a common signalling interface.

7.4 Separation of control plane and user plane

The IMT-2020 network architecture is required to be scalable and distributed, with network functions in the user plane (UP) and control plane (CP) which can be flexibly deployed as required. The separation of CP and UP allows scalability and independent evolution of both planes as well as flexible network function deployments (e.g., centralized versus distributed deployment of UP network functions).

7.5 Efficient support of different mobility requirements

Mobility requirements for user devices may largely differ depending on device and application types. While handover is a required basic feature of most mobile devices, there are still a lot of user devices, e.g., smart meters and customer premises equipment (CPE), which do not require mobility. The mobility management in the IMT-2020 network architecture is required to support diverse mobility requirements.

7.6 Support of low latency requirements

Ultra-low latency communications-based services will be essential services to be provided by the IMT-2020 network. Several factors such as network structure, access signalling delay and data transport delay contribute to the end-to-end service latency.

The IMT-2020 network architecture design is required to support low latency requirements. In the IMT-2020 network, flexible deployment of network functions can help reduce the end-to-end service latency.

7.7 Leveraging existing techniques

The IMT-2020 network architecture design is required to leverage existing techniques such as network function virtualization (NFV) [b-ETSI GS NFV 002] and software defined networking (SDN) [b-ITU-T Y.3300].

SDN can be leveraged to enable separation of CP and UP functions as well as to enhance flexibility and programmability of the IMT-2020 network.

NFV is expected to play a significant role in making the IMT-2020 network more flexible by realizing network components in software. It can help to reduce of the total cost of ownership as well as to increase efficiency, simplicity and flexibility for service offering.

8 Framework of the IMT-2020 network

The IMT-2020 network architecture is expected to be based on distributed network functions as described in clause 6. The framework of the IMT-2020 network including high-level description of network functions and basic network service framework is provided in this clause.

Figure 8-1 illustrates the framework of the IMT-2020 network from a functional point of view.

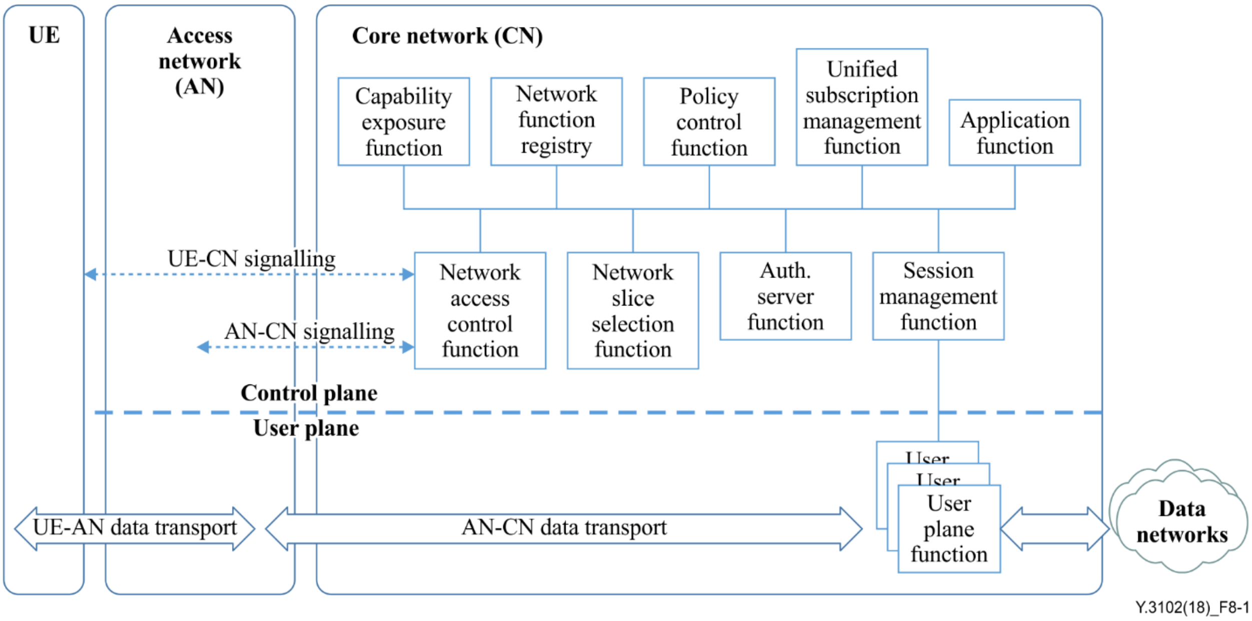


Figure 8-1 – Framework of the IMT-2020 network

8.1 High-level description of IMT-2020 network functions

This Recommendation identifies the common core network functions required to develop a basic IMT-2020 network service framework applicable to most of the application services to be supported by the IMT-2020 network.

Access network functions and service specific core network functions vary depending on the application services to be supported and, consequently, network services to be provided. Therefore, the IMT-2020 network architecture design is required not to be dependent on particular services. Service specific access and core network functions may be needed in addition to the common core network functions and basic network service framework described in this Recommendation.

NOTE – Service specific functions can be provided based on the targeted individual application services and are out of scope of this Recommendation.

The following clauses provide the high-level description of the common core network functions required for a basic IMT-2020 network service framework.

8.1.1 Network access control function (NACF)

The NACF functionalities include registration management, connection management and session management function (SMF) selection.

- Registration management

  When a UE accesses the network, NACF provides functionalities to register and de-register the UE with the network and it establishes the user context in the network. In the registration procedure, NACF performs, but is not limited to, network slice instance selection, UE authentication, authorization of network access and network services, network access policy control.

- Connection management

When a registered UE requests network services to the network, NACF provides functionalities to establish and release signalling connections between UE and core network. This includes mobility management functionalities.

– SMF selection

When a session establishment request message is received from UE, NACF performs discovery and selection of the SMF that is the most appropriate to manage the session.

When network slicing is used and a NACF instance, which has received a registration request through a signalling message, cannot serve an appropriate network slice for the UE's request, NACF instance re-allocation is required. Rerouting of the signalling message to the target NACF instance is required during the registration procedure to re-allocate the serving NACF instance including the transfer of the UE context.

Depending on the deployment scenarios, the NACF functionalities in a network slice may be performed in distributed multiple NACF instances in order to minimize the signalling delays. In this case, local NACF instances distributed at the network edge can perform the mobility management functionalities for the (intra-RAT and inter-RAT) handovers. The serving NACF instance notifies UE location to SMF. If user plane function (UPF) re-allocation is required to support mobility, SMF selects a new UPF and performs inter-UPF mobility management. NACF re-allocation between local NACF instances can be performed if necessary.

8.1.2 Session management function (SMF)

This function provides functionalities to setup the IP or non-IP protocol data unit (PDU) connectivity (i.e., PDU session) for a UE as well as to control the user plane for that connectivity (e.g., selection/re-selection of user plane network functions and user path, enforcement of policies including QoS policy and charging policy). SMF gets policy information related to session establishment from the policy control function (PCF).

SMF also provides IP address management functionalities for allocation and release of the UE's IP address.

8.1.3 Policy control function (PCF)

This function provides functionalities for the control and management of policy rules including rules for QoS enforcement, charging and traffic routing. PCF enables end-to-end QoS enforcement with QoS parameters (e.g., maximum bit rate, guaranteed bit rate and priority level) at the appropriate granularity (e.g., per UE, per flow and per PDU session).

8.1.4 User plane function (UPF)

This function provides functionalities for traffic routing and forwarding, PDU session tunnel management and QoS enforcement. The PDU session tunnels are used between AN and UPF(s) as well as between different UPFs as user plane data transport for PDU sessions.

NOTE – A UPF instance can act as an anchor point for intra-/inter-RAT mobility when UPF instance re-allocation is required.

UPF also provides optional functionalities including packet inspection and collection of UP traffic for lawful intercept.

In order to accommodate the diversity of network scenarios, UPF may also provide interworking functionalities among different network segments, e.g., interworking between IP-based core network and non-IP based access network.

8.1.5 Capability exposure function (CEF)

This function provides functionalities for network functions and network slices to expose their capabilities as a service to 3rd parties. In order to expose the capabilities, CEF stores the capability information and provides it upon capability discovery request.

8.1.6 Network function registry function (NFR)

This function provides functionalities to assist the discovery and selection of required network functions. Each network function instance registers itself when instantiated and updates its status (i.e., activation/de-activation) so that NFR can maintain information of the available network function instances.

Multiple instances may be discovered by NFR per discovery request from network functions (for example, NACF uses NFR to select appropriate SMF, ASF and PCF). In such cases, NFR responds to the requesting network function with a list of discovered network functions, network function capabilities and optionally additional selection rules. The requesting network function selects an instance from the list and updates NFR to reflect its selection.

When the discovery of network function instances in different network slices is required, NFR instances in different network slices interact with each other. A typical example is the case of discovery of network functions (e.g., user plane function) in visited public land mobile network (VPLMN) when a UE roams.

In general, each network slice instance has its own NFR, at least logically. In certain cases, e.g., if the network slice instances are in the same administrative domain, a single NFR instance can be shared by multiple network slice instances as shown in Figures 6-1 and 6-2.

8.1.7 Unified subscription management function (USM)

This function stores and manages, in a unified way, UE context and subscription information including, but not limited to, information on UE's registration and mobility management, information on network functions which serve the UE, information on session management for PDU session establishment. USM also provides authentication information of UE to ASF.

8.1.8 Network slice selection function (NSSF)

This function provides functionalities to select appropriate network slice instances for a UE. When a UE requests registration with the network, NACF sends a network slice selection request to NSSF with preferred network slice selection information. The NSSF responds with a message including the list of appropriate network slice instances for the UE.

8.1.9 Authentication server function (ASF)

This function performs authentication between UE and the network. NACF initiates the UE authentication by invoking ASF. Based on the UE authentication information obtained from USM, ASF selects an authentication method and performs UE authentication procedures [b-3GPP TS 33.501].

8.1.10 Application function (AF)

This function provides session related information to PCF so that SMF can finally use this information for session management.

NOTE – AF interacts with application services that require dynamic policy control. AF extracts session related information (e.g., QoS requirements) from application signalling and provides it to PCF in support of its rule generation.

8.2 Basic IMT-2020 network service framework

This clause illustrates the basic IMT-2020 network service framework, i.e., how network services are provided by network functions as described in clause 8.1.

This Recommendation addresses the following basic network services: registration management, connection management, session management, user plane management and handover management.

8.2.1 Registration management (RM)

RM is used to register or deregister a UE with the IMT-2020 network and to establish the user context in the network. Two RM states are identified for UE and NACF to reflect the UE registration status with the IMT-2020 network:

– DEREGISTERED, when a UE is not registered with the IMT-2020 network.

– REGISTERED, when a UE is registered with the IMT-2020 network.

Before registration, a UE selects the IMT-2020 access network to be attached. The network selection procedure is out of scope of this Recommendation.

A UE can attach to the IMT-2020 common core network simultaneously over different types of access network such as IMT-2020 RAN, WiFi and fixed wireline access network. RM states for the attached access networks are independent of each other. RM maintains a common Temporary Identifier across multiple ANs to associate the different access network-specific RM contexts and provides a unified registration procedure for such case.

The common Temporary Identifier is assigned upon the first successful registration of the UE over an AN and is valid through the following registrations over other ANs. It is globally unique for the IMT-2020 network and is stored both in the UE and in NACF as UE context. For the subsequent registration requests to the network, the UE provides the IMT-2020 common core network with the Temporary Identifier it has received in the first successful registration. This enables access networks to select a NACF that maintains the UE context created at the previous registration(s).

User authentication and access authorization are initiated by NACF and are performed based on user subscription profiles in USM in order to verify the identity of the requesting UE. Authentication information is stored in the UE context, together with the globally unique Temporary Identifier, as a result of the registration over an AN. This authentication information is used for the subsequent registrations over other ANs.

A single UE can be served simultaneously by multiple network slice instances and a single NACF instance may be shared by the different network slice instances.

The selection of a set of network slice instances for the UE is triggered by the first NACF instance but this may lead to NACF instance relocation. For example, when a NACF instance is not proper to serve the UE's requirements related to a network slice, the NACF instance reroutes the UE registration request message to the appropriate NACF instance.

Upon de-registration request from either UE or network, NACF deletes the UE context and subscription information and notifies the access network and UPFs via the corresponding SMF. The UPFs terminate the PDU sessions and release the resources allocated to the de-registered UE.

Figure 8-2 illustrates the RM framework for registration request.

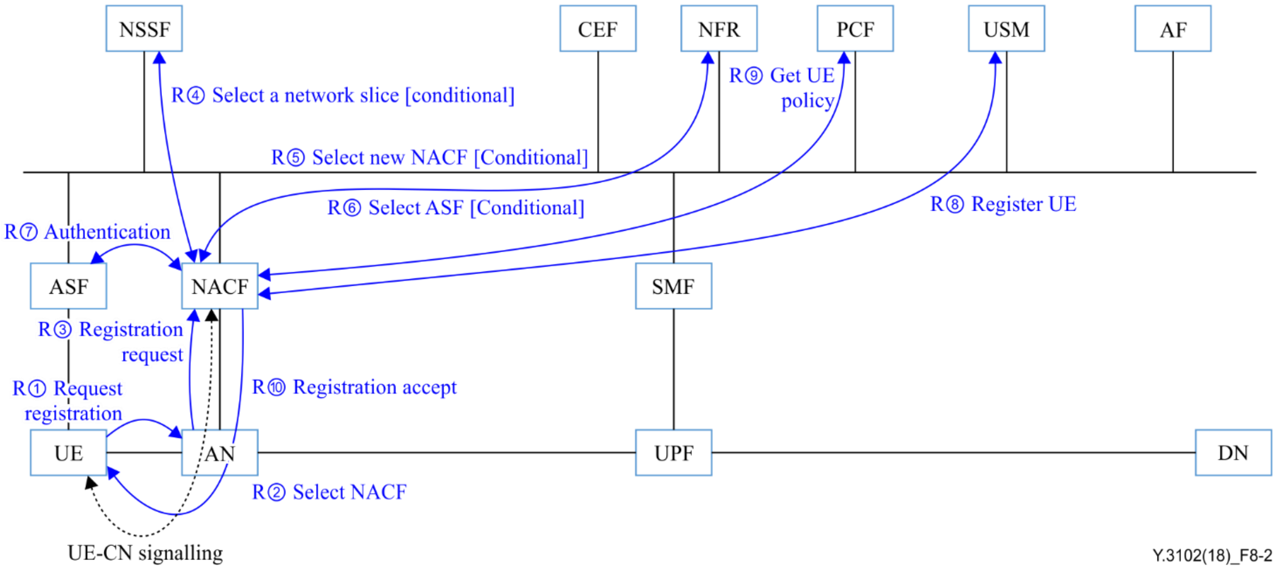


Figure 8-2 – IMT-2020 RM framework for registration request

To register with the network, as shown in Figure 8-2, UE sends a registration request message through an AN. The AN relays this message to the pre-configured NACF. If the NACF cannot serve the UE's requirements, it performs re-allocation of serving network slice instance and NACF instance with, respectively, NSSF and NFR. After the serving NACF authenticates the UE with the proper ASF, it registers the UE to USM and gets policy information for the UE from PCF. Then the serving NACF responds to the requesting UE with a registration acceptance message.

8.2.2 Connection management (CM)

CM is used to establish and release signalling connection between UE and NACF.

The signalling connection is used to enable signalling exchange between UE and core network. It uses the signalling connection between AN and NACF.

Two CM states are identified to reflect the status of the UE signalling connectivity with NACF:

- IDLE, when a UE is in REGISTERED RM state and it has no signalling connection established with NACF.
- CONNECTED, when a UE has a signalling connection with NACF.

When a UE in IDLE state needs to transmit a signalling message to NACF or to SMF via NACF, the UE sends a service request signalling message to establish a signalling connection with NACF. Upon receiving the service request signalling message, NACF performs authentication and authorization of the UE for the requested services and performs the required security procedures. Through the established secure signalling connection, the UE and the network may exchange signalling messages including session management and user plane management messages.

A single UE can be connected simultaneously to multiple access networks with a separate interface for each connection. The CM states of the different connections are independent of each other.

The release procedure of a signalling connection can be initiated by the AN or NACF. The UE considers the signalling connection released if it detects the release of the AN signalling connection. NACF considers the signalling connection released if it detects the deletion of the signalling connection context.

Figure 8-3 illustrates the CM framework for service request.

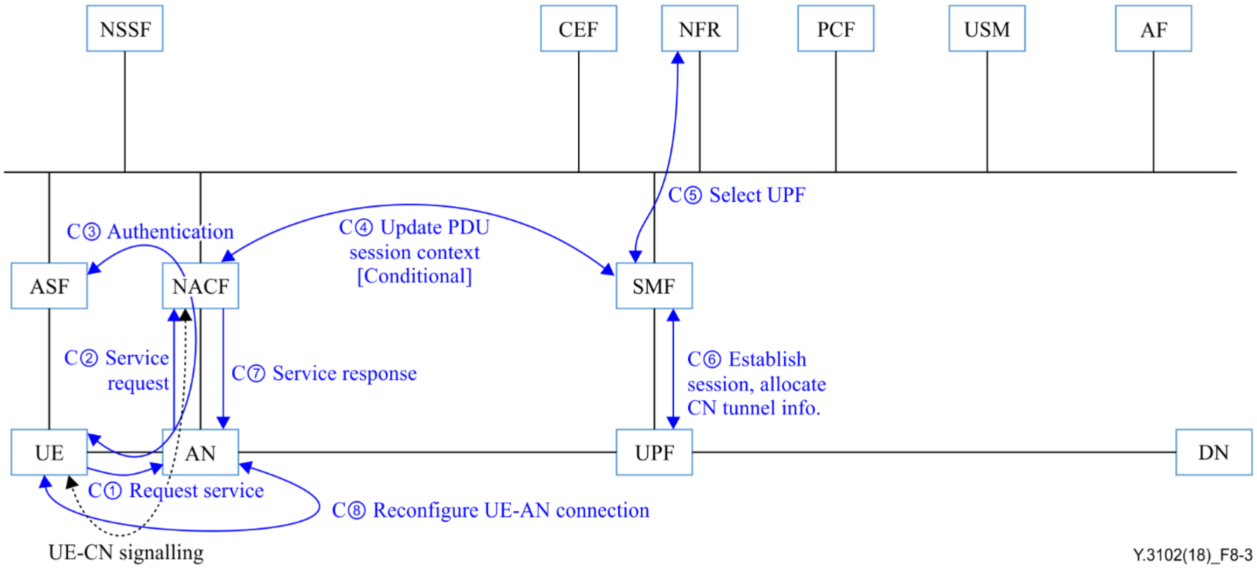


Figure 8-3 – IMT-2020 CM framework for service request

In Figure 8-3, the UE sends a service request signalling message to the serving NACF via AN. After NACF has authenticated the UE's requested service, it establishes a secure signalling connection with the UE. NACF lets SMF select the proper UPF(s) for the service request or update the existing PDU session context if necessary. SMF establishes a session for the service request and allocates a PDU session tunnel for the user traffic between AN and UPF(s) as well as between UPFs. SMF sends a service response signalling message to the requesting UE via NACF, including the IP address allocated to the UE. With the allocated PDU session tunnel information, AN reconfigures the UE-AN connection for the PDU session.

8.2.3 Session management (SM)

SM manages PDU sessions including control of PDU session tunnel establishment, modification, and release.

The IMT-2020 network is required to provide PDU connectivity service, i.e., a service that enables exchange of PDUs between UEs and data networks (DNs). The PDU connectivity service is supported via PDU sessions that are established upon session request from UEs. Each PDU session supports a single PDU type as requested by the UE at the establishment of the PDU session.

The following details of session management address the IP type of PDU sessions. Details of PDU session management for PDU types other than the IP type are not in the scope of this Recommendation.

PDU session tunnels are required between ANs and UPFs as well as between different UPFs. SM enables the establishment, modification and release of PDU session tunnels. A single PDU session can carry multiple IP flows. The types of IP flows which can be handled by IP flow PDU sessions (i.e., PDU sessions constituted by IP flows) are guaranteed bit rate (GBR) and non-GBR.

NOTE 1 – GPRS Tunnelling Protocol (GTP) [b-3GPP TS 29.274] and generic routing encapsulation (GRE) [b-IETF RFC 2784] may be considered as PDU session tunnelling technologies.

NOTE 2 – An IP flow is a user traffic stream of packets between the UE and a data network (DN) in the user plane. Multiple IP flows can belong to a single PDU session. Each IP flow is identified in general by 5-tuples of the IP header, i.e., source and destination IP addresses, source and destination ports and protocol.

SMF controls the establishment, modification and release of IP flow PDU sessions. SM messages are exchanged between SMF and UE by NACF signalling. SMF controls UPFs for the management of IP flow PDU sessions including IP flow QoS. The following procedures apply to IP flow PDU session management:

– IP flow PDU session establishment

  - After the UE has secured the signalling connection with NACF, the UE sends a PDU Session Establishment Request message to NACF. NACF forwards the message to SMF.
  - Upon PDU Session Establishment Request, SMF selects a proper UPF and allocates an IP address to the UE.
  - SMF controls UPF and, via NACF, AN to establish PDU session tunnels and UE-AN data transport tunnel.

– IP flow PDU session release

  - Explicit: The UE can request the release of an IP flow PDU session explicitly to SMF. SMF releases the session, deletes all the flows belonging to the session and requests the deletion of the flows to UPF and AN. UPF and AN delete the corresponding resources.
  - Implicit: SMF or AN can trigger the PDU session release. For example, if there is no traffic through an IP flow within a given period, UPF notifies it to SMF. SMF deletes the flow and requests the deletion of the flow to UPF and AN. UPF and AN delete the corresponding resources. If there are no more IP flows in the PDU session, SMF releases the PDU session.

– IP flow PDU session modification

  - A PDU session modification may be initiated in order to change the path and QoS of an IP flow, e.g., to cope with the status changes in access networks or for load balancing.
  - SMF requests UPF to modify the IP flow PDU session.
  - According to the response message received from UPF, SMF sends a PDU Session Modification Request message to AN via NACF.

Figure 8-4 illustrates the SM framework for PDU session establishment.

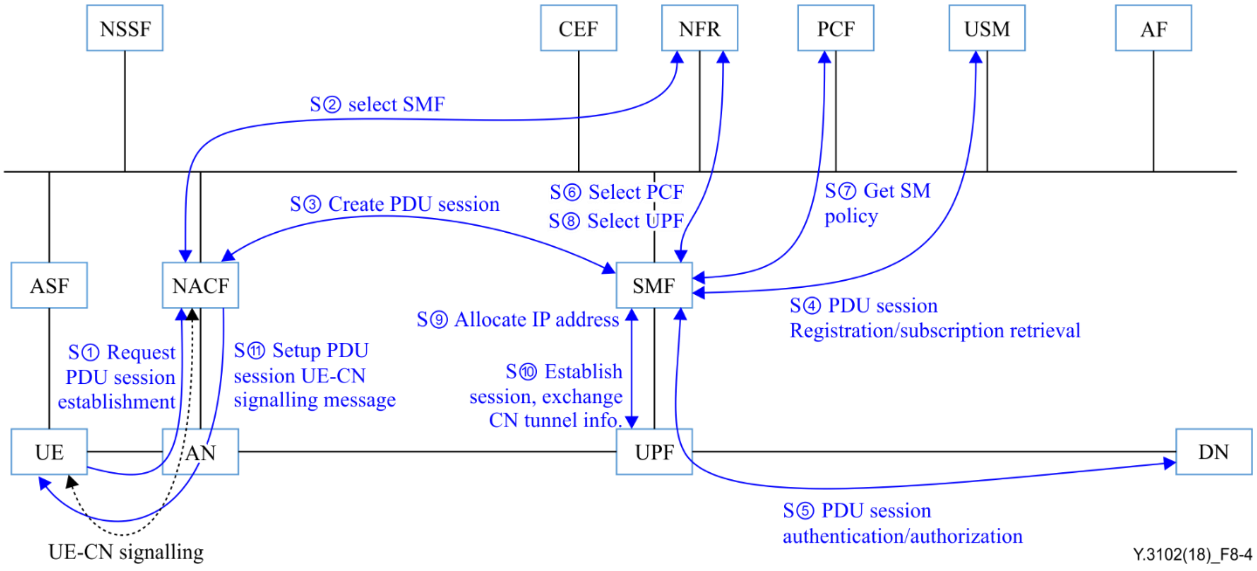

NSSF
CEF
NFR
PCF
USM
AF
S② select SMF
S③ Create PDU session
S⑥ Select PCF
S⑧ Select UPF
S⑦ Get SM policy
ASF
NACF
SMF
S⑨ Allocate IP address
S④ PDU session Registration/subscription retrieval
S① Request PDU session establishment
S⑪ Setup PDU session UE-CN signalling message
S⑩ Establish session, exchange CN tunnel info.
UE
AN
UPF
DN
S⑤ PDU session authentication/authorization
UE-CN signalling
Y.3102(18)_F8-4

Figure 8-4 – IMT-2020 SM framework for PDU session establishment

In Figure 8-4, the UE sends a signalling message to NACF to establish a PDU session. The serving NACF selects the most appropriate SMF and lets it create a PDU session. After retrieving PDU session information from USM, the serving SMF performs authentication and authorization with the data network (DN). Then SMF gets policy information for the requested PDU session and selects the most appropriate UPF. Finally, SMF informs the requesting UE about the session establishment via the serving NACF.

8.2.4 User plane management (UPM)

UPM is used to forward user traffic, including user traffic rerouting between UPFs due to the serving UPF relocation and to enforce QoS policies.

PDU session tunnels managed by UPM are used between ANs and UPFs as well as between different UPFs.

UPFs enforce per IP flow QoS based on QoS policies given by SMF.

8.2.5 Handover management (HM)

Mobility management is used to handle all aspects related to UE mobility. Mobility management aspects include, but are not limited to, UE reachability management and handover management. This Recommendation addresses handover management as a key aspect.

HM provides unified procedures according to the access agnostic common core network principle.

Handover procedure triggering includes, but is not limited to, the case of a UE moving from the serving AN to the target AN and the case of a serving AN which cannot serve a UE anymore, e.g., due to changes in radio conditions or load balancing.

In order to maintain session and service continuity during handover, NACF initiates the switching of the CM signalling connection between AN and NACF and triggers SM to re-establish the PDU session tunnels.

The serving NACF instance and UPF instances may be relocated depending on the specific handover situation. For UPF instance relocation, the serving SMF instance selects target UPF instance(s) to provide the optimal path.

Bibliography

[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.3300] Recommendation ITU-T Y.3300 (2014), *Framework of SDN (Software-Defined Networking).*

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.*

[b-3GPP TS 23.228] 3GPP TS 23.228 (2017), *IP Multimedia Subsystem (IMS), Stage 2 (Release 15).*

[b-3GPP TS 24.501] 3GPP TS 24.501 (2018), *Non-Access-Stratum (NAS) protocol for 5G system, Stage 3 (Release 15).*

[b-3GPP TS 29.274] 3GPP TS 29.274 (2017), *Evolved General Packet Radio Service (GPRS), Tunnelling Protocol for Control plane (GTPv2-C), Stage 3 (Release 15).*

[b-3GPP TS 33.501] 3GPP TS 33.501 (2018), *Security architecture and procedures for 5G system (Release 15).*

[b-ETSI GS NFV 002] ETSI GS NFV 002 (2013), *Network Functions Virtualisation (NFV), Architectural Framework.*

[b-IETF RFC 2784] IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE).*

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