International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3114

(02/2022)

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

Future networks

Future networks including IMT-2020: requirements and functional architecture of lightweight core for dedicated networks

Recommendation ITU-T Y.3114

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
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3114

Future networks including IMT-2020: requirements and functional architecture of lightweight core for dedicated networks

Summary

In the context of future networks including IMT-2020, dedicated networks are networks designed for application domains with common requirements. Lightweight core is a core network designed for dedicated networks, which builds on the integration of IMT-2020 core network functions.

Recommendation ITU-T Y.3114 specifies requirements, functional architecture, reference points and procedures for lightweight cores for dedicated networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3114	2022-02-13	13	11.1002/1000/14853

Keywords

Application domain, architecture, dedicated network, IMT-2020, lightweight core, network functions, reference points, requirements

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3114

Future networks including IMT-2020: requirements and functional architecture of lightweight core for dedicated networks

1 Scope

In the context of future networks including IMT-2020, dedicated networks are networks designed for application domains with common requirements. Lightweight core is a core network designed for dedicated networks, which builds on the integration of IMT-2020 core network functions.

The following topics related to lightweight core are addressed in this Recommendation:

- Overview;
- Requirements;
- Functional architecture;
- Reference points;
- Procedures.

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 M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

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

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

[ITU-T Y.3104] Recommendation ITU-T Y.3104 (2018), *Architecture of the IMT-2020 network.*

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

[ITU-T Y.3131] Recommendation ITU-T Y.3131 (2019), *Functional architecture for supporting fixed mobile convergence in IMT-2020 networks*.

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

[ITU-T Y.3172] Recommendation ITU-T Y.3172 (2019), *Architectural framework for machine learning in future networks including IMT-2020.*

[ITU-T Y.3200] Recommendation ITU-T Y.3200 (2022), *Fixed, mobile and satellite convergence – Requirements for IMT-2020 network and beyond*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application domain [ITU-T Y.4100]: An area of knowledge or activity applied for one specific economic, commercial, social or administrative scope.

NOTE – Transport application domain, health application domain and government application domain are examples of application domains.

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

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

3.1.4 fixed, mobile and satellite convergence [ITU-T Y.3200]: The capabilities that provide services and applications to end users regardless of the fixed, mobile or satellite access technologies being used and independently of the users' location.

3.1.5 fixed mobile convergence [ITU-T Y.3100]: In the context of IMT-2020, the capabilities that provide services and applications to end users regardless of the fixed or mobile access technologies being used and independently of the users' location.

3.1.6 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].

3.1.7 machine learning (ML) [ITU-T Y.3172]: Processes that enable computational systems to understand data and gain knowledge from it without necessarily being explicitly programmed.

3.1.8 machine learning overlay [ITU-T Y.3172]: A loosely coupled deployment model of machine learning functionalities whose integration and management with network functions are standardised.

NOTE – A machine learning overlay aims to minimise interdependencies between machine learning functionalities and network functions using standard interfaces, allowing for the parallel evolution of functionalities of the two.

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

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

3.1.11 third party (3rd party) [ITU-T Y.3100]: In the context of IMT-2020, with respect to a given network operator and network end-users, an entity which consumes network capabilities and/or provides applications and/or services.

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 dedicated network: A network designed for application domains with common requirements.

3.2.2 lightweight core: A core network of a dedicated network, which builds on the integration of IMT-2020 core network functions.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

Ack	Acknowledgement
AF	Application Function
AI	Artificial Intelligence
AN	Access Network
AR	Augmented Reality
ASF	Authentication Server Function
CEF	Capability Exposure Function
CM	Connection Management
CN	Core Network
CUF	Centralized User Function
DN	Data Network
E2E	End-to-End
EUF	Edge User Function
FCAPS	Fault, Configuration, Accounting, Performance, Security
FMC	Fixed Mobile Convergence
FMSC	Fixed, Mobile and Satellite Convergence
FQDN	Fully Qualified Domain Name
GBR	Guaranteed Bit Rate
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ML	Machine Learning
NACF	Network Access Control Function
NFR	Network Function Registry function
NIF	Network Intelligence Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDU	Protocol Data Unit
QoS	Quality of Service
RP	Reference Point
RRC	Radio Resource Control
SM	Session Management
SMF	Session Management Function
TCP	Transmission Control Protocol
UCF	Unified Control Function
UDF	Unified Data Function

UE User Equipment

UHD Ultra High Definition

UP User Plane

UPF User Plane Function

URL Uniform Resource Locator

USM Unified Subscription Management function

VR Virtual Reality

5 Conventions

In this Recommendation:

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

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview

With the deployment of IMT-2020 networks, services and applications related to, but not limited to, the following examples of application domains increasingly need to be supported:

- Smart city, with applications related to municipal administration, environmental protection, city transportation, emergency management.
- Industry, with applications related to power grid, industrial internet, smart manufacturing.
- Education, with applications related to remote education, virtual education, campus security.
- Transport, with applications related to vehicular networking, automatic driving.
- Healthcare, with applications related to remote healthcare, interactive medical diagnosis, remote surgery operation.
- Agriculture, with applications related to farming, livestock location tracking, real-time weather warning.
- Finance, with applications related to immersive customer service, intelligent assets management, financial network security.
- Media, with applications related to augmented reality (AR), virtual reality (VR), ultra high definition (UHD) live broadcasting, interactive live programme.

With regards to networks designed to meet the requirements of application domains, some are adopting the IMT-2020 network architecture and network functions as specified in [ITU-T Y.3102] and [ITU-T Y.3104], while others may use dedicated network architectures based on customized IMT-2020 network functions.

The "lightweight core" is a core network of a dedicated network, which builds on the integration of IMT-2020 core network functions. The internal details of the resulting network functions of the lightweight core, such as internal functionalities, internal interfaces, internal protocols and internal

procedures, are hidden from one another. In addition, with proper customization of the lightweight core network functions (e.g. activation or de-activation of some of their internal functionalities), the complexity of the lightweight core can be reduced, its performance can be optimized and the requirements of application domains can be supported. These characteristics make the lightweight core architecture a core network architecture adapted to application domains in the context of future networks including IMT-2020.

The use of the lightweight core is especially suited to, but not limited to, the following dedicated network deployment scenarios:

- A dedicated network with limited computing, storage and networking resources, which makes it hard to deploy the complete set of functions of the IMT-2020 core network [ITU-T Y.3104];
- A dedicated network with limited technical capabilities, e.g. without the support of network slicing capabilities and/or edge computing capabilities, which makes it unnecessary to deploy the complete set of functions of the IMT-2020 core network [ITU-T Y.3104];
- A dedicated network requiring extensive customization of functionalities, interfaces, protocols and procedures, which does not fully conform to the requirements and design principles of the IMT-2020 core network [ITU-T Y.3104];
- A dedicated network requiring secure isolation from the public network and other dedicated networks, which is not required to be supported in the IMT-2020 core network [ITU-T Y.3104];
- A dedicated network requiring artificial intelligence (AI) / machine learning (ML) related capabilities, which are not required as basic capabilities of the IMT-2020 core network [ITU-T Y.3104];
- A dedicated network aiming to support a small number of users, which is suitable to deploy a lightweight version of the IMT-2020 core network [ITU-T Y.3104];
- A dedicated network for service and application scenarios requiring fast deployment (e.g. emergency communications), which is suitable to deploy a lightweight version of the IMT-2020 core network [ITU-T Y.3104].

It is expected that the lightweight core support the evolving requirements of services and applications of application domains. Depending on the deployment environment, the lightweight core may support different categories of quality of service (QoS), including best-effort QoS and guaranteed bit rate (GBR) QoS.

7 Requirements for lightweight core

7.1 General requirements for lightweight core

The general requirements for lightweight core are as follows:

- It is required for lightweight core to support the services and applications supported by the IMT-2020 network, as specified in [ITU-T Y.3101].
- It is required for lightweight core to be compatible with user equipment (UEs) and access networks (ANs) supported by the IMT-2020 network.
- It is required for lightweight core to support interworking with IMT-2020 networks.
- It is recommended for lightweight core to reduce the complexity of the core network in terms of number of network functions and number of interfaces.
- It is recommended for lightweight core to be designed based on the integration of the IMT-2020 core network functions.

7.2 Service requirements for lightweight core

The service requirements supported by lightweight core are as follows:

- It is required for lightweight core to support the service requirements specified in [ITU-T Y.3101].
- It is recommended for lightweight core to support customized services and applications.

NOTE – The term 'customized services and applications' refers to the customization of service characteristics. Taking voice service as an example, the calling party number displayed to the callee could be customized from the E.164 [b-ITU-T E.164] number to a short number.

- It is required for lightweight core to support best-effort QoS.
- It is recommended for lightweight core to support GBR QoS.
- It is recommended for lightweight core to support service continuity among different ANs.
- It is recommended for lightweight core to support traffic routeing across different ANs.

7.3 Network capability requirements for lightweight core

The network capability requirements for lightweight core are as follows:

- It is required for lightweight core to support the network capability requirements specified in [ITU-T Y.3102] and [ITU-T Y.3104].
- It is required for lightweight core to support the customization of network functions based on the requirements of services and applications, including with respect to computing, storage, and networking resources.
- It is recommended for lightweight core to support fixed mobile convergence (FMC) [b-ITU-T Y.3131], and fixed, mobile and satellite convergence (FMSC) [b-ITU-T Y.3200].
- It is recommended for lightweight core to enable the use of AI/ML functionalities [ITU-T Y.3172].

NOTE – The enabled AI/ML functionalities can be internal and/or external to the lightweight core. These functionalities are provided in both cases via an ML overlay [ITU-T Y.3172].

8 Functional architecture of lightweight core

8.1 Architecture reference model

Figure 8-1 depicts the architecture reference model of lightweight core.

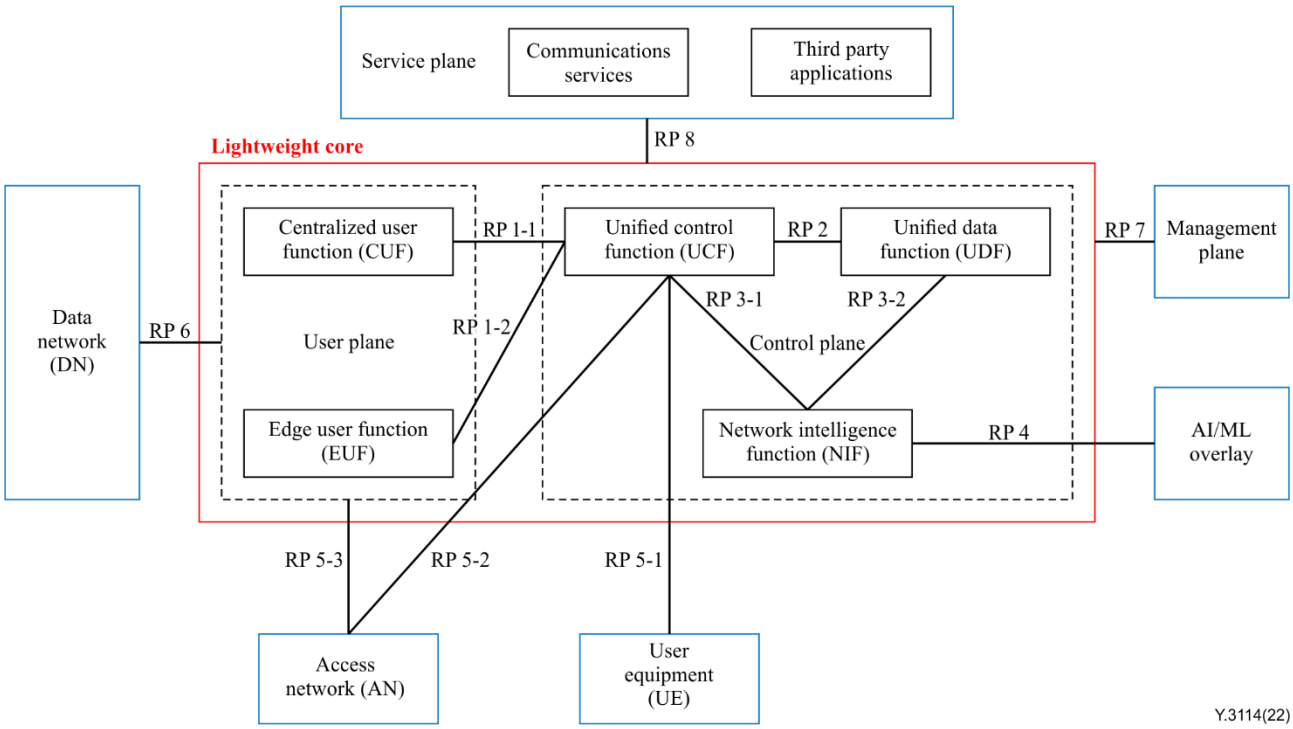

Figure 8-1 – Architecture reference model of lightweight core

8.2 Lightweight core functions

Lightweight core is a core network consisting of control plane and user plane network functions, respectively, unified control function (UCF), unified data function (UDF) and network intelligence function (NIF) as control plane network functions, and centralized user function (CUF) and edge user function (EUF) as user plane network functions.

NOTE – The detailed design of functionalities, interfaces, protocols and procedures internal to the lightweight core network functions are out of the scope of this Recommendation.

Lightweight core interacts with UE, AN, data network (DN), service plane, management plane, and AI/ML overlay functionalities.

8.2.1 Control plane network functions

8.2.1.1 Unified control function (UCF)

The UCF network function provides the control functionalities of lightweight core. The UCF supports the functionalities of the following IMT-2020 network functions [ITU-T Y.3102]: network access control function (NACF), session management function (SMF), policy control function (PCF), capability exposure function (CEF), network function registry function (NFR), network slice selection function (NSSF) and application function (AF). The functionalities of the UCF are customized on the basis of the IMT-2020 network functions specified in [ITU-T Y.3102], to meet the requirements of application domains. UCF may provide service invoking interfaces and capability exposure interfaces to communications services and third party applications, respectively.

8.2.1.2 Unified data function (UDF)

The UDF network function provides the user data functionalities of the lightweight core. The UDF supports the functionalities of the following IMT-2020 network functions [ITU-T Y.3102]: unified subscription management function (USM) and authentication server function (ASF). The functionalities of the UDF are customized on the basis of the IMT-2020 network functions specified in [ITU-T Y.3102], to meet the requirements of application domains. Data under the responsibility of the UDF include user subscription data, policy data, network status data and capability exposure data.

8.2.1.3 Network intelligence function (NIF)

The NIF network function is an optional network function to enable the use of AI/ML related functionalities internal to the lightweight core control plane. When supported, the NIF interacts with UCF and UDF to assist in the aspects of routing selection, traffic scheduling, data processing, data mining, network optimization, resource orchestration, etc. The NIF takes the role of ML overlay [ITU-T Y.3172] internal to the lightweight core. The NIF may also use AI/ML related functionalities provided externally to the lightweight core as an ML overlay.

NOTE – The lightweight core control plane network functions are usually deployed in a centralized location.

8.2.2 User plane network functions

8.2.2.1 Centralized user function (CUF)

The CUF network function provides the user plane functionalities for non-edge capabilities of lightweight core. The CUF includes functionalities for traffic routeing and forwarding, traffic filtering, protocol data unit (PDU) session tunnel management, QoS enforcement and service identification. The CUF functionalities are customized on the basis of the IMT-2020 user plane function (UPF) specified in [ITU-T Y.3102], to meet the requirements of application domains.

NOTE – The CUF is typically deployed in a centralized location.

8.2.2.2 Edge user function (EUF)

The EUF network function provides the user plane functionalities for edge capabilities of lightweight core. The EUF includes functionalities for traffic routeing and forwarding, traffic filtering, PDU session tunnel management, QoS enforcement, service identification, local traffic off-load, and local fully qualified domain name (FQDN)/uniform resource locator (URL) resolution. The EUF functionalities are customized on the basis of the IMT-2020 user plane function (UPF) specified in [ITU-T Y.3102], to meet the requirements of application domains.

NOTE 1 – The EUF is typically deployed in an edge location.

NOTE 2 – CUF and EUF could be integrated in case of lightweight core deployment for application domains requiring the support of both non-edge and edge capabilities.

8.3 Functions external to lightweight core

8.3.1 AI/ML overlay

The AI/ML overlay plays the same role as the ML overlay specified in [ITU-T Y.3172].

8.3.2 Access network (AN)

The AN includes fixed access network, mobile access network and satellite access network.

8.3.3 User equipment (UE)

The UE includes, but is not limited to, mobile phone, wearable device, customer premise equipment and satellite terminal.

8.3.4 Data network (DN)

The DN plays the same role as the DN specified in [ITU-T Y.3104].

8.3.5 Management plane

The management plane provides the functionalities for the management of the lightweight core according to the management functional areas listed in [ITU-T M.3010], i.e. performance management, fault management, configuration management, accounting management and security management, also known as fault, configuration, accounting, performance, security (FCAPS) functional areas. These functionalities are expected to include the management of the lightweight core functions described in clause 8.2, including, but not limited to, network connectivity management, management of user information, capability management and orchestration, and resource management and orchestration.

8.3.6 Service plane

The service plane supports communications services and third party applications. Communications services may use service invoking interfaces of UCF, while third party applications may use capability exposure interfaces of UCF.

9 Reference points of lightweight core

As shown in Figure 8-1, lightweight core has five internal reference points (RPs) and seven external reference points as follows.

- RP 1-1: The reference point exists between UCF and CUF. RP 1-1 is expected to adopt a protocol stack based on Hypertext Transfer Protocol (HTTP) [b-IETF RFC 7540] / Transmission Control Protocol (TCP) / Internet Protocol (IP). Service based interfaces [b-3GPP TS 23.501] can optionally be used.
- RP 1-2: The reference point exists between UCF and EUF. RP 1-2 is expected to adopt a protocol stack based on HTTP [b-IETF RFC 7540] / TCP / IP. Service based interfaces [b-3GPP TS 23.501] can optionally be used.
- RP 2: The reference point exists between UCF and UDF. RP 2 is expected to adopt a protocol stack based on HTTP [b-IETF RFC 7540] / TCP / IP. Service based interfaces [b-3GPP TS 23.501] can optionally be used.
- RP 3-1: The reference point exists between UCF and NIF. RP 3-1 is expected to adopt a protocol stack based on HTTP [b-IETF RFC 7540] / TCP / IP. Service based interfaces [b-3GPP TS 23.501] can optionally be used.
- RP 3-2: The reference point exists between UDF and NIF. RP 3-2 is expected to adopt a protocol stack based on HTTP [b-IETF RFC 7540] / TCP / IP. Service based interfaces [b-3GPP TS 23.501] can optionally be used.
- RP 4: The reference point exists between NIF and AI/ML overlay. RP 4 corresponds to the data handling reference points in [ITU-T Y.3172]. RP 4 is recommended to adopt a protocol stack based on HTTP [b-IETF RFC 7540] / TCP / IP.
- RP 5-1: The reference point exists between the UE and UCF. RP 5-1 corresponds to the reference point RP-tn as defined in [ITU-T Y.3104]. The details of this reference point are out of the scope of this Recommendation.
- RP 5-2: The reference point exists between the AN and UCF. RP 5-2 corresponds to the reference point RP-an as defined in [ITU-T Y.3104]. The details of this reference point are out of the scope of this Recommendation.

- RP 5-3: The reference point exists between the AN and user plane network functions of lightweight core (including CUF and EUF). RP 5-3 corresponds to the reference point RP-au as defined in [ITU-T Y.3104]. The details of this reference point are out of the scope of this Recommendation.
- RP 6: The reference point exists between user plane network functions of lightweight core (including CUF and EUF) and DN. RP 6 corresponds to the reference point RP-ud as defined in [ITU-T Y.3104]. The details of this reference point are out of the scope of this Recommendation.
- RP 7: The reference point exists between lightweight core and the management plane, including, but not limited to, network connectivity management interfaces, management interfaces of user information, capability management and orchestration interfaces, and resource management and orchestration interfaces. The details of this reference point are out of the scope of this Recommendation.
- RP 8: The reference point exists between lightweight core and the service plane, including service invoking interfaces and capability exposure interfaces. RP 8 is recommended to adopt a protocol stack based on HTTP [b-IETF RFC 7540] / TCP / IP. The details of this reference point are out of the scope of this Recommendation.

10 Procedures of lightweight core

Based on the architecture reference model specified in clause 8 and the reference points described in clause 9, this clause specifies the procedures of lightweight core to provide:

– Each of the basic network services defined in [ITU-T Y.3104], that is, registration management, connection management, session management and handover;

– Capability exposure defined in [ITU-T Y.3108];

– Network slicing defined in [ITU-T Y.3153].

10.1 Registration management procedure

The registration management procedure of lightweight core conforms to the registration management procedure of the IMT-2020 network specified in [ITU-T Y.3104], except that the functionalities of the NACF, SMF, PCF, NFR, NSSF and AF are integrated in the UCF, the functionalities of the USM and ASF are integrated in the UDF, and the functionalities of the UPF are integrated in the CUF.

Figure 10-1 depicts the general registration management procedure of lightweight core.

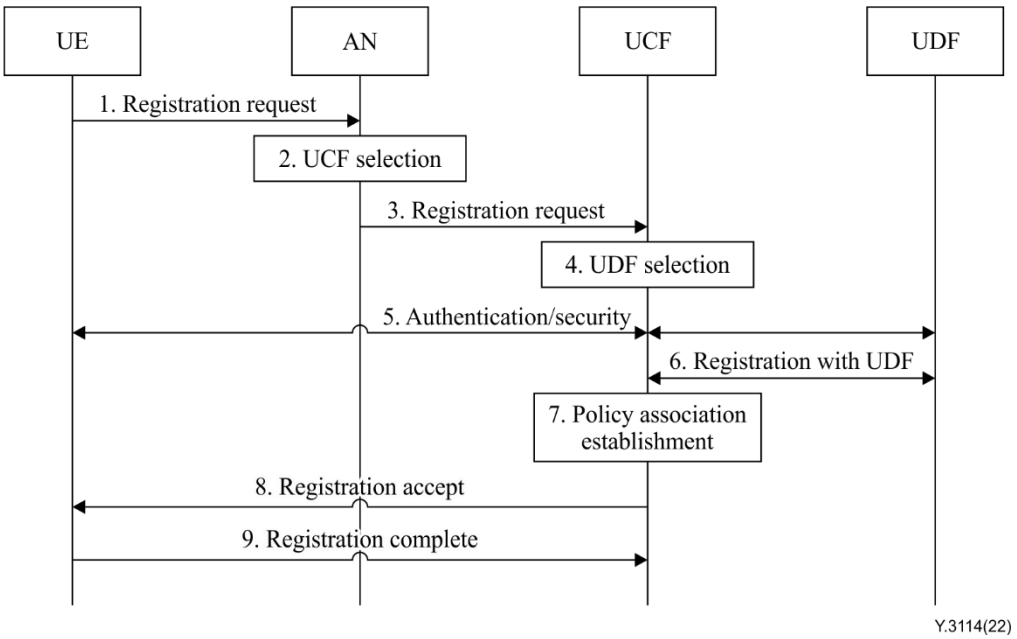

Figure 10-1 – General registration management procedure of lightweight core

1) Registration Request message (UE to AN)

The UE sends the Registration Request AN message to an AN, including network slice instance selection preference information and the NACF instance identifier, if available from a previous registration procedure. The UE can attach to the lightweight core simultaneously over different types of AN. A UCF selected for the first successful registration of the UE over an AN can be used for subsequent registrations over other ANs.

2) UCF selection

If the Registration Request AN message received from UE does not indicate a valid NACF instance identifier, the AN selects a UCF based on the requested network slice instance selection preference information, location of the UCF, network operator policy, load balancing, etc. When the UE-provided NACF instance identifier in the Registration Request AN message is valid, the AN selects the UCF that maintains the UE context created on the previous registration(s).

3) Registration Request message (AN to UCF)

The AN sends the Registration Request message to the selected UCF.

4) UDF selection

The UCF selects a UDF to initiate UE authentication. The UCF utilizes the functionality of NFR for the selection.

5) Authentication of the UE

The UDF executes authentication of the UE. The UDF utilizes the functionality of USM to obtain the UE authentication information; then it selects an authentication method and performs UE authentication procedures. After successful authentication, the UDF returns the results to the UCF. The UCF initiates UE to core network (CN) signalling security function setup procedures. Upon completion of the signalling security function setup, the UCF provides the security context to the AN, which enables the AN to use the security context of the signalling security function setup in order to protect the messages exchanged with the UE. The AN stores the security context and acknowledges the UCF.

6) Registration with UDF

The UCF registers with the UDF and subscribes to the event notification service in order to be notified when the UDF deregisters the UCF in the following cases: if the UCF has

changed since the last registration procedure; if the UE-provided subscription identifier, which is permanent and globally unique in the IMT-2020 network, does not refer to a valid context in the UCF; and if the UE is registered over a non-IMT-2020 AN and initiates another registration procedure on an IMT-2020 AN. The UCF provides the AN type of the UE to the UDF. The UDF stores the associated AN type together with the serving UCF. The UCF creates a mobility management context for the UE after obtaining the mobility subscription data from the UDF.

7) Policy association establishment

The UCF performs policy association of the UE with the functionality of policy control.

8) Registration Accept message (UCF to UE)

The UCF sends a Registration Accept message to the UE indicating that the registration request has been accepted. If a globally unique temporary identifier is allocated by the UCF, it can be commonly used in both an IMT-2020 AN and a non-IMT-2020 AN. The identifier is included in the Registration Accept message.

9) Registration Complete message (UE to UCF)

If a new globally unique temporary identifier is assigned, the UE sends a Registration Complete acknowledgement (Ack) message to the UCF.

10.2 Connection management procedure

The connection management procedure of lightweight core conforms to the connection management procedure of the IMT-2020 network specified in [ITU-T Y.3104], except that the functionalities of the NACF, SMF, PCF, NFR, NSSF and AF are integrated in the UCF, the functionalities of the USM and ASF are integrated in the UDF, and the functionalities of the UPF are integrated in the CUF.

Figure 10-2 depicts the general connection management procedure of lightweight core.

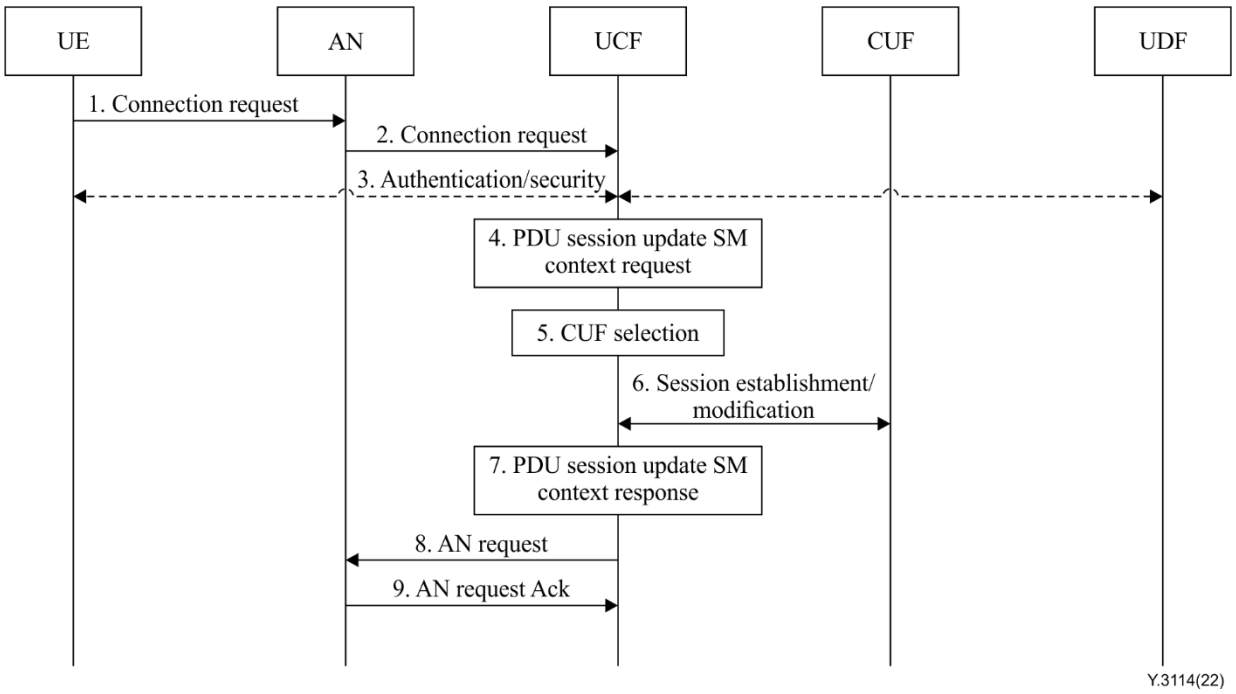

Figure 10-2 – General connection management procedure of lightweight core

1) Connection Request message (UE to AN)

The UE sends a Connection Request message towards UCF encapsulated in an AN message requesting the establishment of a radio resource control (RRC) connection to the AN. If the

Connection Request message is triggered for uplink user data by the UE in the connection management (CM) CONNECTED state, the UE identifies the PDU session(s) for which the user plane (UP) connections are to be activated.

2) Connection Request message (AN to UCF)

The AN encapsulates the Connection Request message received from the UE in the message and sends it to the UCF. If the UE is in the CM IDLE state, the AN selects a proper UCF according to the UE identity information which includes the set of NACF identifiers.

3) Authentication and security

If the Connection Request is not integrity protected or the integrity protection verification has failed, the UCF initiates the authentication and security procedure with the UDF. After a successful authentication and security procedure, a secure signalling connection between the UE and the UCF is established. If the UE in a CM IDLE state triggered the Connection Request only to establish a signalling connection, after its successful establishment, the UE and the network can exchange messages for session management (SM), etc.

4) PDU Session Update SM context Request

If the Connection Request was not sent only for the establishment of a signalling connection, and if the UE provides a list of PDU sessions to be activated in the Connection Request message, the UCF associates with the PDU sessions to update their SM context, e.g., establishment of UP resources for the PDU session(s). The PDU Session Update SM context Request message contains PDU session identifier(s), UE location information, access type, etc.

5) CUF selection

The UCF performs the following actions based on the UE location information: it accepts activation of the UP connection of PDU session(s) and continues using the current CUF; or it accepts the activation of the UP connection of PDU session(s) and selects a new CUF; or it rejects the activation of the UP connection of a PDU session and triggers the re-establishment of the PDU session after the connection request procedure.

6) Session establishment or modification

If the UCF selects a new CUF in step 5, in order to relocate the CUF, the UCF establishes a session with the new CUF and modifies the session with the old CUF. The new CUF, acting as terminating point in CN, provides new tunnel CN interface information to the UCF. The old CUF forwards buffered downlink data to the new CUF and releases the allocated resources for the PDU session.

7) PDU Session Update SM context response

For the activated PDU session in step 5, the UCF generates the corresponding SM information that is encapsulated in a message. The SM information contains the information that the UCF will provide to the AN, e.g., PDU session identifier, QoS profile and tunnel CN interface information.

8) AN Request message (UCF to AN)

The UCF sends AN Request message to the AN. The message includes SM information and connection request acceptance-related information, e.g., the result of requested PDU session(s) activation. If the result of PDU session(s) activation includes failures, the cause of the failures is also provided.

9) AN Request Ack message (AN to UCF)

The AN Request Ack message may include SM information, e.g., AN tunnel information. The AN may respond to SM information with separate AN Request Ack messages (e.g., tunnel setup response) if the UCF sends separate AN messages in step 8.

10.3 Session management procedure

The session management procedure of lightweight core conforms to the session management procedure of the IMT-2020 network specified in [ITU-T Y.3104], except that the functionalities of the NACF, SMF, PCF, NFR, NSSF and AF are integrated in the UCF, the functionalities of the USM and ASF are integrated in the UDF, and the functionalities of the UPF are integrated in the CUF.

Figure 10-3 depicts the general SM procedure of lightweight core.

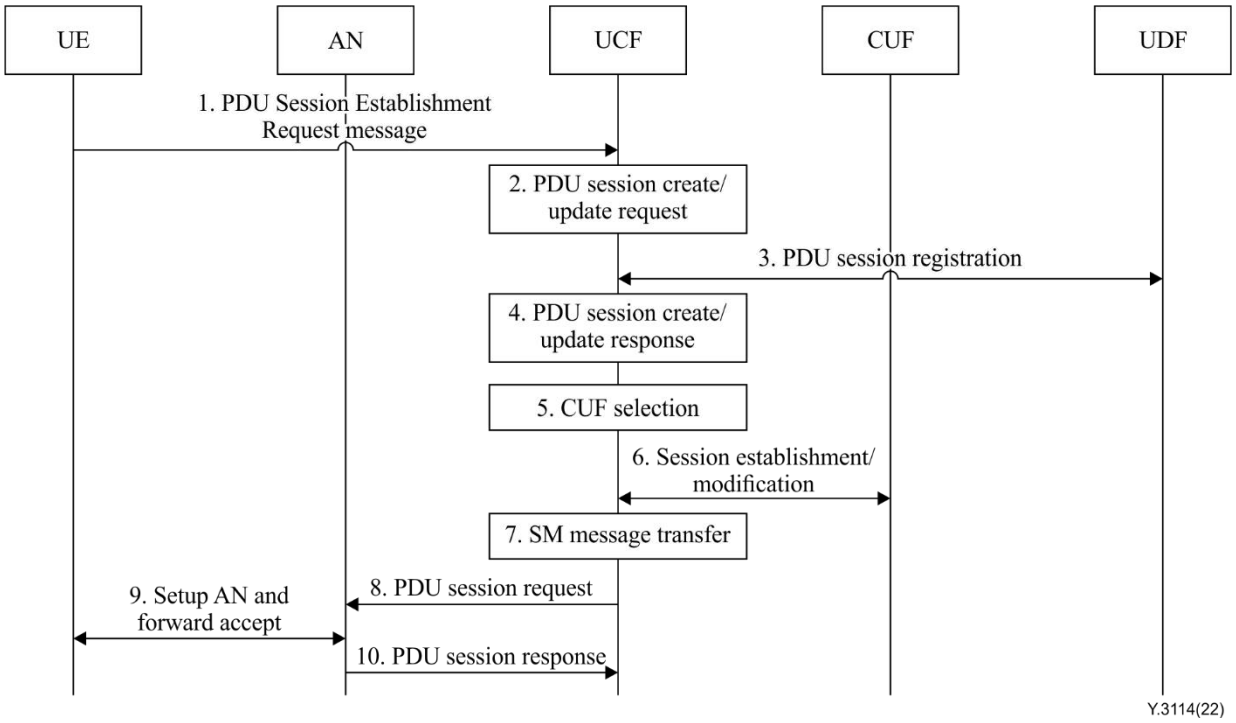

Figure 10-3 – General session management procedure of lightweight core

1) PDU Session Establishment Request message (UE to UCF)

   In order to establish a new PDU session, the UE generates a new PDU session identifier and sends a message containing a PDU Session Establishment Request to the UCF. The message includes the PDU session identifier, request type and PDU session type. The request type indicates "initial request" if the PDU session establishment is a request to establish a new PDU session, or indicates "existing PDU session" if the request is for an existing PDU session switching between different IMT-2020 ANs. The AN encapsulates the message sent by the UE in a message and sends it, together with user location information and access type information, to the UCF.

2) PDU Session Create/Update Request

   The UCF performs a PDU Session Create Request or PDU Session Update Request as an internal procedure.

3) Registration with UDF for the PDU session

   If the UCF has not yet registered for a PDU session identifier, the UCF registers with the UDF for it. If the request type in the PDU Session Establishment Request message is "existing PDU session" for switching between different IMT-2020 ANs, the UCF identifies the existing PDU session based on the given PDU session identifier. In this case, the UCF does not create a new SM context, but instead updates the SM context. The UCF checks the validity of the request, such as whether the request is compliant with the user subscription

and with local policies. If the request is determined to be invalid, the UCF does not accept establishment of the PDU session.

4) PDU session create/update response

The UCF performs a PDU session create response or PDU session update response as an internal procedure.

5) CUF selection

If the request type in the PDU session establishment request is "initial request", the UCF selects CUF(s) as needed. For IP type PDU sessions, the UCF allocates an IP address (prefix) for the PDU session. If the request type is "existing PDU session", the UCF maintains the same IP address (prefix) that has already been allocated to the UE.

6) Session establishment or modification

If the request type is "initial request", the UCF initiates the session establishment procedure with the selected CUF, otherwise it initiates the session modification procedure. If more than one CUF is selected for the PDU session, the UCF initiates the procedure with each CUF of the PDU session. If the request type is "existing PDU session" and the UCF creates a tunnel, this step is skipped. Otherwise, this step is performed to obtain the tunnel CN interface information from the CUF. The UCF sends a session establishment/modification request message to the CUF. If the tunnel CN interface information is allocated by the UCF, it is provided to the CUF in this step. The CUF responds to the UCF by sending a session establishment/modification response message. If the tunnel CN interface information is allocated by the CUF, it is provided to the UCF in this step.

7) SM message transfer

The UCF performs SM message transfer as an internal procedure.

8) PDU Session Request message (UCF to AN)

The UCF sends to the AN a PDU Session Request message, which contains a PDU session identifier and PDU Session Establishment Accept targeted to the UE and SM information.

9) AN setup and forwarding PDU session establishment accept

The AN allocates an AN tunnel for the PDU session. The AN may also initiate AN specific signalling exchange with the UE, related to the information received from the UCF. If the setup of necessary AN resources and AN tunnel allocation is successful, the AN forwards the PDU session identifier and PDU Session Establishment Accept message provided in step 8 to the UE.

10) PDU Session Response message (AN to UCF)

The AN sends to the UCF a PDU Session Response message, which includes SM information, etc. The SM information contains an AN tunnel address corresponding to the PDU session.

10.4 Handover procedure

The handover procedure of lightweight core conforms to the handover procedure of the IMT-2020 network specified in [ITU-T Y.3104], except that the functionalities of the NACF, SMF, PCF, NFR, NSSF and AF are integrated in the UCF, the functionalities of the USM and ASF are integrated in the UDF, and the functionalities of the UPF are integrated in the CUF.

Figure 10-4 depicts the general handover procedure of lightweight core.

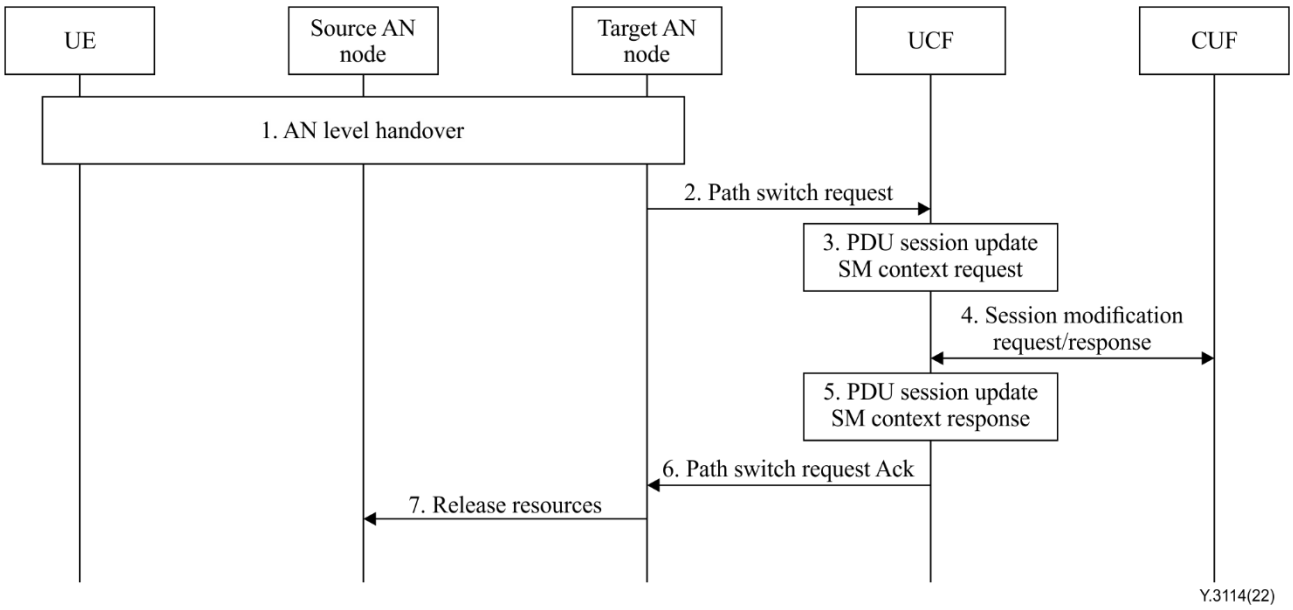

Figure 10-4 – General handover procedure of lightweight core

1) AN level handover

The UE, source AN node and target AN node perform AN level handover.

2) Path Switch Request message (Target AN node to UCF)

The target AN node sends a Path Switch Request message to the UCF to indicate that the UE has moved to a new AN node. The message provides the list of PDU sessions to be switched. If none of the QoS flows of a PDU session are accepted by the target AN node or if the target AN node cannot set up the required UP resources for some PDU sessions, the message is required to include the list of rejected PDU sessions. For the PDU sessions to be switched to the target AN node, the message also includes the accepted QoS flows.

3) PDU Session Update SM context Request

The UCF performs PDU Session Update SM context Request as an internal procedure.

4) Session Modification Request message (UCF to CUF) and Response message (CUF to UCF)

For PDU sessions that are modified by the target AN node, the UCF sends a Session Modification Request message to the CUF. After the requested PDU sessions are modified by the CUF, the CUF returns a Session Modification Response message to the UCF.

5) PDU Session Update SM context Response

The UCF performs PDU Session Update SM context Response as an internal procedure.

6) Path Switch Request Ack message (UCF to Target AN node)

The UCF aggregates received CN interface information about the tunnel, and sends it in a Path Switch Request Ack message to the target AN node. Any information about PDU sessions that have failed to be switched is also included in the message.

7) Release resources message (Target AN node to Source AN node)

The target AN node confirms the success of the handover by sending a Release Resources message to the source AN node.

10.5 Capability exposure procedure

The capability exposure procedure of lightweight core conforms to the capability exposure procedure of the IMT-2020 network specified in [ITU-T Y.3108], except that the functionalities of the NACF, SMF, PCF, CEF, NFR, NSSF and AF are integrated in the UCF, the functionalities of

the USM and ASF are integrated in the UDF, and the functionalities of the UPF are integrated in the CUF.

Figure 10-5 depicts the general capability exposure procedure of lightweight core.

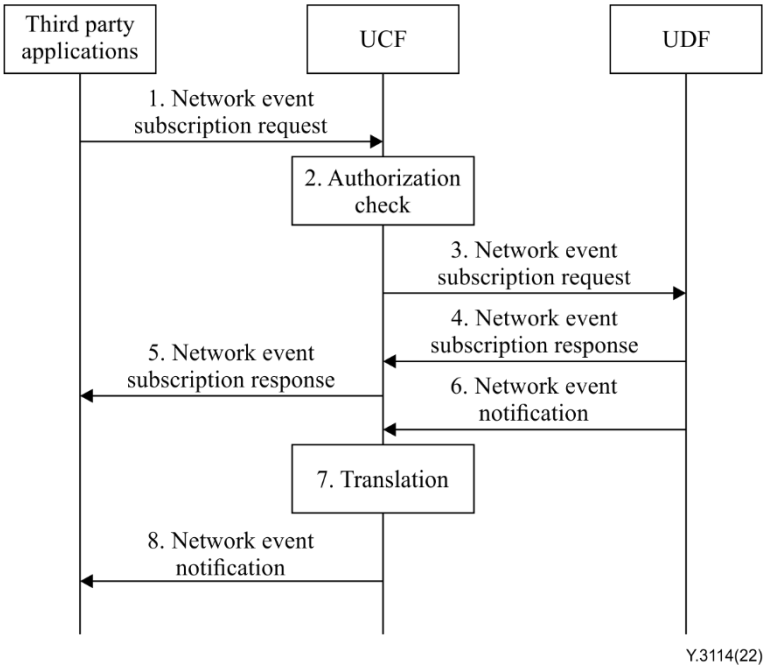

Figure 10-5 – General capability exposure procedure of lightweight core

1) The third party application subscribes to the network event by sending a network event subscription request to the UCF, specifying the target event(s), which may include loss of UE network connectivity, UE roaming status or communication failure.
2) The UCF checks whether the third party is authorized for the request. If not, the procedure proceeds to step 5.
3) The UCF subscribes the target event(s) to the UDF by sending a network event subscription request.
4) The UDF registers and maintains the association of the target monitoring event and the UCF to be notified; and the NF acknowledges the subscription by sending a network event subscription response to the UCF.
5) The UCF registers and maintains the association of the target monitoring event and the target third party to be notified; and the UCF acknowledges the subscription by sending a network event subscription response to the third party. If authorization fails, the UCF responds indicating the authorization failure and the procedure ends at this step.
6) When the UDF detects that a target monitoring event occurred, the UDF notifies it to the target UCF by sending a network event notification.
7) The UCF translates the internal network information by masking it from the external use.
8) The UCF notifies the monitoring event to the target third party by sending a network event notification.

10.6 Network slicing procedure

The network slicing procedure of lightweight core conforms to the network slicing procedure of the IMT-2020 network specified in [ITU-T Y.3153], except that the functionalities of the NACF, SMF, PCF, CEF, NFR, NSSF and AF are integrated in the UCF, the functionalities of the USM and ASF are integrated in the UDF, and the functionalities of the UPF are integrated in the CUF.

Figure 10-6 depicts the general network slicing procedure of lightweight core.

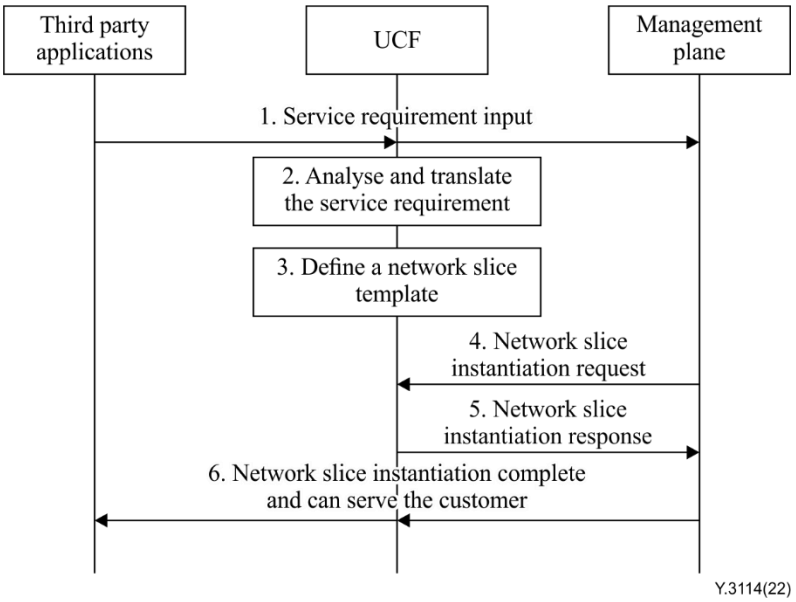

Figure 10-6 – General network slicing procedure of lightweight core

1) A third party application's service requirement is provided as an input to the UCF and sent to the management plane.

2) The management plane analyses the service requirement and translates it into a network requirement. During the translation, the management plane also decides if an existing network slice instance can support the new requirement. If it cannot, the management plane has to decide what kinds of network slice instances and how many network slice instances can support the new service requirement.

3) The UCF defines a network slice template which contains:

   – Detailed specifications of resources for a network slice that can be implemented by the UCF;

   – Service-level configuration.

   There is a network function repository in the management plane. The repository stores the whole network slice templates. The management plane looks for the existing end-to-end (E2E) network slice template which can fulfil the service requirement. When there is no appropriate E2E network slice template, the management plane searches sub network slice templates which can partly meet the received service requirement. Then it generates the whole new E2E network slice template by using the sub network slice templates, and stores the new E2E network slice template in the repository.

   The template may also contain attribute information of a network slice such as a network slice identifier, deployment information and management information. The management plane generates the deployment configuration information and maintenance management configuration information.

4) and 5) The UCF instantiates the network slice instance based on the network slice template in step 3 according to requests from the management plane. After resource allocation and instantiation are finished, the management plane also sends a network configuration request to the UCF to configure sub network slice instances.

6) The E2E network slice instance is instantiated to serve a specific third party application.

11 Security considerations

The security and privacy considerations of the lightweight core include the following aspects:

- Control plane security, which includes the security considerations on the UCF, UDF and NIF. The secure operations of control functionalities, user data functionalities, and AI/ML related functionalities are to be addressed.

NOTE 1 – For example, the functionality of network access control is provided within the UCF. It is expected to ensure the secure operation of this functionality within the UCF, with signalling analysis and status analysis of the UCF.

- UP security, which includes the security considerations on the CUF and EUF. The secure operations of non-edge and edge UP functionalities are to be addressed.

NOTE 2 – For example, the functionality of traffic routeing and forwarding is provided within the CUF and/or EUF. It is expected to ensure the secure operation of this functionality within the CUF and/or EUF, with signalling analysis and status analysis of the CUF and/or EUF.

- User privacy, which includes the privacy considerations on the UCF, UDF, NIF, CUF and EUF network functions, which could store, cache and process privacy sensitive user and network data. The transmission of privacy sensitive data among network functions and the exposure of privacy sensitive data to service plane are subject to authentication, authorization and privacy management.

In addition, the security and privacy considerations of lightweight core should be aligned with the requirements specified in [ITU-T Y.3101] and [b-ITU-T Y.2701].

Bibliography

[b-ITU-T E.164] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

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

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

[b-ITU-T Y.3174] Recommendation ITU-T Y.3174 (2020), *Framework for data handling to enable machine learning in future networks including IMT-2020*.

[b-ITU-T Y.3176] Recommendation ITU-T Y.3176 (2020), *Machine learning marketplace integration in future networks including IMT-2020*.

[b-ITU-T Y.3179] Recommendation ITU-T Y.3179 (2021), *Architectural framework for machine learning model serving in future networks including IMT-2020*.

[b-ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

[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 23.501] 3GPP TS 23.501 (2020), *System architecture for the 5G System (5GS); Stage 2 (Release 16)*.

[b-3GPP TS 23.502] 3GPP TS 23.502 (2021), *Procedures for the 5G System (5GS); Stage 2 (Release 16)*.

[b-IETF RFC 7540] IETF RFC 7540 (2020), *Hypertext Transfer Protocol Version 2 (HTTP/2)*.

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, 2022