ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3325 (01/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Future networks

Framework for high-level AI-based management communicating with external management systems

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.3325

Framework for high-level AI-based management communicating with external management systems

Summary

Recommendation ITU-T Y.3325 describes the requirements for a reference model of such interactions including interface and metadata. After the IMT-2020 technology and network virtualization technology spread, the appearance of emerging services such as multimedia services (high resolution, AR, VR, etc.) and IoT is expected. Since huge amount of traffic of these new coming services will be incurred to the network, the importance of network flexibility and stability will increase. Network operators intend to improve network operations such as provisioning, resource control, failure detection and recovery, and so on. Automatic network management supported by recent AI technologies called AI-based networks will play an essential role in such an era.

On the other hand, a service provider needs to manage service dynamically based on service and network status for better quality of service (QoS). In order for service providers to use the information managed by AI-based networks effectively, a common interface between a system of service providers over AI-based networks and AI-based networks is required.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3325	2023-01-13	13	11.1002/1000/15240

Keywords

AI-based network, application programming interface, metadata, reference model, 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.3325

Framework for high-level AI-based management communicating with external management systems

1 Scope

This Recommendation describes a reference model of capability exposure (communication exchange) and a high-level communication model between the AI-based network slice management and orchestration (ANSM) system of network providers and the service and application management system of service providers in future networks including the IMT-2020 network and beyond. The concerned operations consist of network resource configuration of network slice, network slice performance notification, network slice failure notification, network slice security notification, and network slice accounting notification.

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

[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.3156] Recommendation ITU-T Y.3156 (2020), *Framework of network slicing with AI-assisted analysis in IMT-2020 networks*.

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

[ITU-T Y.3177] Recommendation ITU-T Y.3177 (2021), *Architecture framework for artificial intelligence-based network automation for resource and fault management in future networks including IMT-2020*.

[ITU-T Y.3178] Recommendation ITU-T Y.3178 (2021), *Functional framework of artificial intelligence-based network service provisioning in future networks including IMT-2020*.

[ITU-T Y.3324] Recommendation ITU-T Y.3324 (2018), *Requirements and architectural framework for autonomic management and control of IMT-2020 networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 IMT-2020 [b-ITU-T Y.3100]: (Based on [b-ITU-R M.2083-0]) 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.

3.1.2 management [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at fulfilment, assurance, billing of services, network functions, and resources in both physical and virtual infrastructure including compute, storage and network resources.

3.1.3 network function [b-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.

3.1.4 network slice [b-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).

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

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

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

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

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

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

3.1.9 service instance [b-ITU-T Y.3100]: An instance of a service that is realized within a network slice.

NOTE 1 – A service may be represented by one or more service instances.

NOTE 2 – A service instance may be provided by the network slice operator or a third party [ITU-T Y.3153].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ANSM AI-based Network Slice Management and orchestration

API Application Programming Interface

eMBB enhanced Mobile Broadband

mMTC massive Machine Type Communication

MEC Multi-access Edge Computing

SLA Service Level Agreement

URLLC Ultra-Reliable and Low Latency Communications

5 Conventions

The following conventions are used in this Recommendation:

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

– 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 keyword "functions" is defined as a collection of functionalities.

6 Overview of reference model of AI-based network slice orchestration and management

6.1 Introduction

After the IMT-2020 technology and network virtualization technology spread, it is expected that a large number of new services such as multimedia services (high resolution, AR, VR, etc.) and IoT will be developed and used in the form of network slice instances over future networks including the IMT-2020 network. The amount of network traffic for those services will also remarkably increase. To satisfy the above requirements, network operations such as service provisioning, network resource control, failure detection and recovery become more complex. Automatic network slice management and orchestration supported by recent artificial intelligence (AI) technologies will play an essential role in such an era, and several use cases have already been collected [b-ITU-T Y.Sup55] and the architectural framework has been standardized in [ITU-T Y.3172], [ITU-T Y.3324] and [ITU-T Y.3153]. In addition, network service provisioning and network automation for resource adaptation and failure recovery by using AI technologies for such future networks are being standardized in [ITU-T Y.3156], [ITU-T Y.3177] and [ITU-T Y.3178]. In this Recommendation, automatic network slice management and orchestration supported by AI technologies is called an AI-based network slice management and orchestration (ANSM).

On the other hand, service providers that provide the above new services over the network slice will have to develop communication functionalities for dynamic resource management and robust failure

management for offering the services. Network slicing enables an operator to create logically partitioned networks customized to provide optimized solutions for different market scenarios which demand diverse requirements in terms of service characteristics, required functionalities, performance and isolation levels [ITU-T Y.3111].

While real-time network information over the network slice is essential for service management, predicted network information has great potential in improving the performance and practicality of service management. In order to realise an effective and robust service management without a huge investment, it is important to establish communication for exchanging real-time and predicted network information between an AI-based network slice management and orchestration in network operators, and a service and application management system of service providers.

In case the network slice customer (e.g., service provider) uses its external management system via interfaces exposed at the reference points Se and Ie defined in [ITU-T Y.3111] for communication (see Figure 6-1), the functionality and a reference model of these interfaces between AI-based network slice management and orchestration and a slice customer's management environment has to also be standardized.

In this figure, a network slice customer is equivalent to a service provider and other functional entities shows the functions of network providers in the IMT-2020.

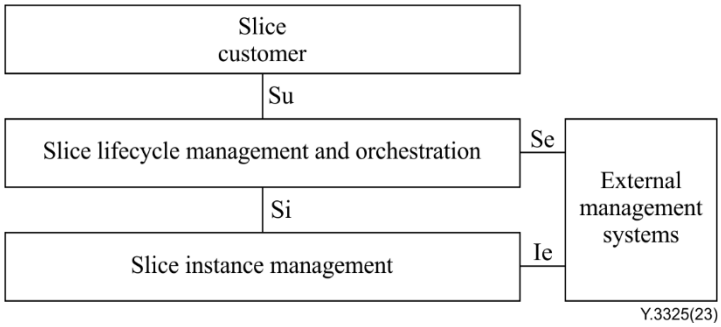

Figure 6-1 – Interfaces between external management systems in a slice customer

NOTE – A capability exposure function can be used for the Se interface [ITU-T Y.3153].

The functional architecture of network slice management and orchestration shall provide a complete set of network functions required to support customer services over different network domains. The functional architecture consists of four functional entities: network slice customer, external management system, network slice management and orchestration and network slice instance management including resource management. Once the slice management and orchestration accept a network slice requirement from a customer, then the slice management and orchestration instantiates, modifies, or releases a network slice instance. The responsibilities of slice instance management are to manage the lifecycle of the required network functions and their needed virtualized resources respectively.

6.2 Architectural scope

This Recommendation focuses on a reference model between a service and an application management of a service provider management system and an AI-based network slice management and orchestration of the network operator management system. Figure 6-2 shows the architectural scope of this Recommendation for an AI-based network slice management and orchestration system operated by a network operator. AI-based network slice management and orchestration platform interacts with the service management platform of network slice customers. Service management provides service instances with the support of AI-based network slice management and orchestration in order to realise effective dynamic management and robust failure management on network slices.

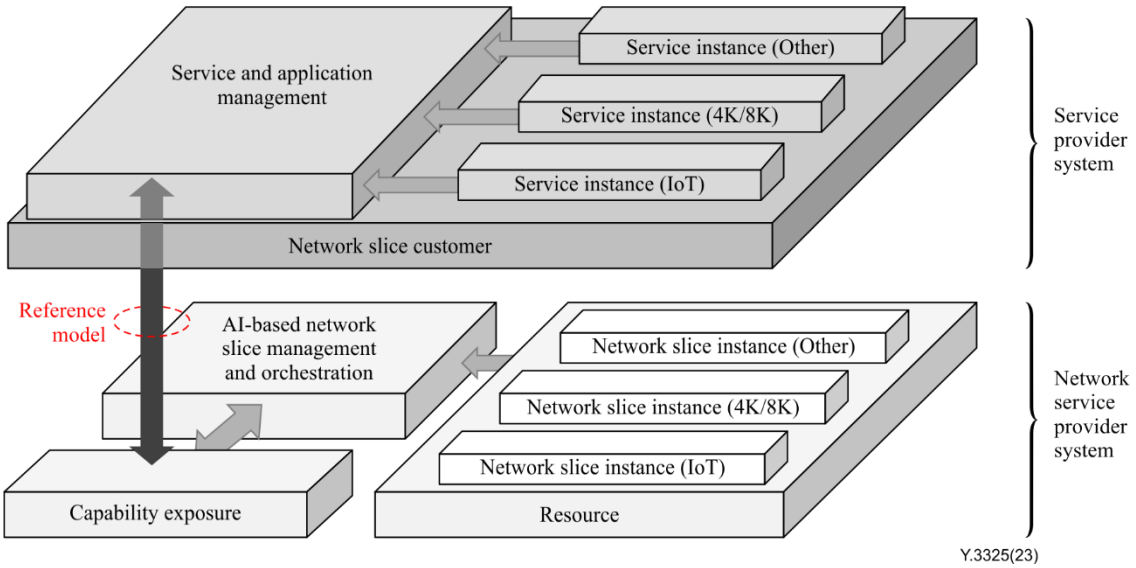

Figure 6-2 – Architectural scope of this Recommendation

7 Functional requirements for capability exposure between network slice customer and capability exposure

7.1 General requirements

In order to realise effective dynamic management and robust failure management over a network slice, the AI-based network slice management and orchestration simplify (in comparison to non AI-based management solutions) the management operations that are to be performed by the service providers that are using the external management system. The interface between network slice customer and capability exposure is requested to satisfy the following additional requirements:

[REQ-GR1]: The interface is required to have the capability for exchanging configuration information for capacity planning of the network slice.

[REQ-GR2]: The interface is required to have the capability for sending to the network slice customer the network slice instance KPIs (e.g., QoS), such as assigned and used bandwidth, packets delay and packet error ratio.

NOTE – The information includes the current and the predicted values.

[REQ-GR3]: The interface is required to have the capability for exchanging information about predicted and/or current failures of the network slice instances.

[REQ-GR4]: The interface is recommended to provide access (e.g., using the publish/subscribe mechanism) to selected network slice instance management data and management capabilities that includes the ability for creation and configuration of a new network function instance within a network slice instance.

[REQ-GR5]: The interface is recommended to provide training data that is used to improve AI capabilities in AI-based network slice management and orchestration from the network service customers.

8 A reference model between network slice customer and slice lifecycle management and orchestration

Figure 8-1 shows a high-level reference model between a network slice customer and slice lifecycle management and orchestration. The interfaces of this reference model consist of functions of network slice customer and functions of slice lifecycle management and orchestration.

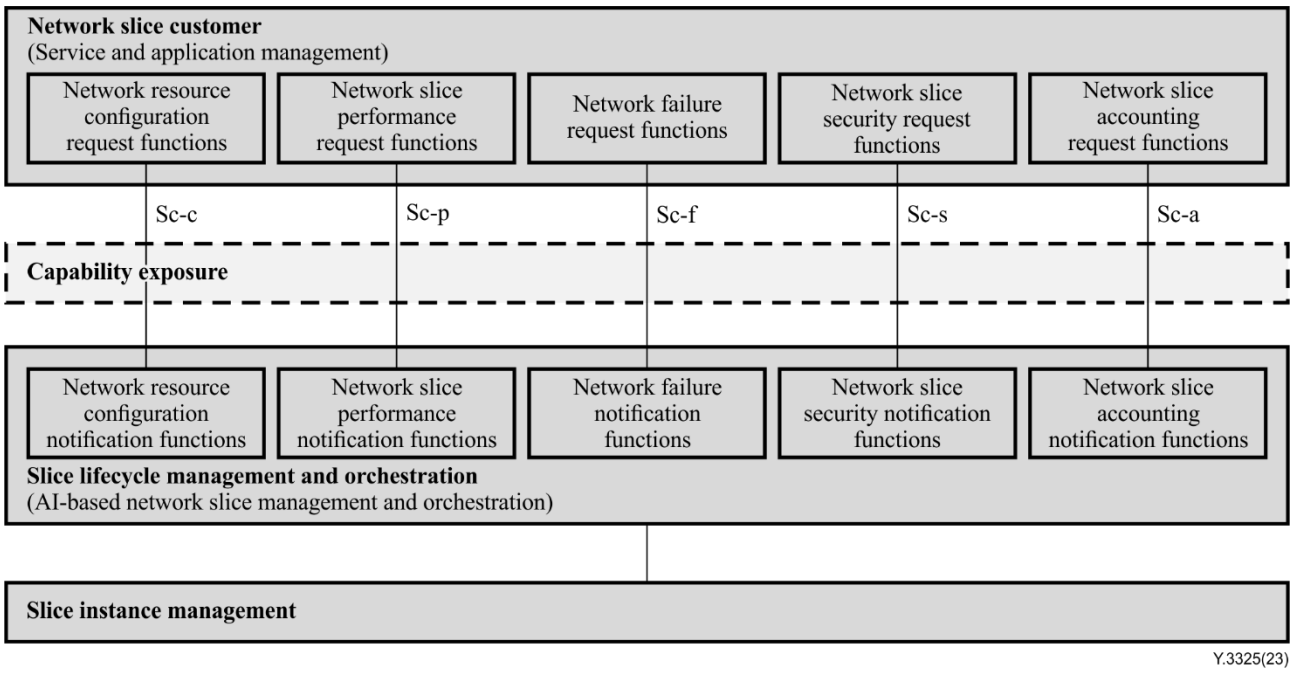

Figure 8-1 – A reference model between network slice customer and capability exposure

8.1 Functions of the network slice customer

New functions in the network slice customer consist of network configuration request functions, network slice performance request functions, network failure request functions, network slice security request functions and network slice accounting request functions. The metadata communicated by these functions is described in clause 10.

– **Network configuration request functions**

These functions are used to design the phase of the network and transport the request of the assignment of the network resources such as (R)AN, core, and transport networks to provide the services. Service providers use these functions to request the network resource assignment and receive the results of the request from AI-based network slice management and orchestration.

– **Network slice performance request functions**

These functions are used to communicate the KPI of the network used for services such as 4K/8K video streaming, IoT and other services. The request of KPI relevant specifications (e.g., KPI type (effective speed, delay, max bandwidth and so on) and timing of report) are specified by service providers, and the results of the assignment of network capability are returned by the AI-assisted network slice management and orchestration.

– **Network failure request functions**

These functions are used to communicate network failure information. Network failure functions in network slice customers receive the network failures information such as the location of the network failure, and type of failure from AI-based network slice management and orchestration. The service provider can use this information to inform their end users on the degrade of the service or provide alternative services. The information can be used to request the usage of alternative resources, and AI-based network slice management and orchestration may predict the network failure in advance.

– **Network slice security request functions**

These functions are used to communicate network security information. Network slice security functions in network slice customers receive the network security information such as data encryption methods, and protection methods against unauthorized access. The network service provider can use

this information to show the security options and to specify a user preferred security option to slice lifecycle management and orchestration.

– **Network slice accounting request functions**

These functions are used to communicate the network slice accounting information. Network slice accounting request functions in network slice customers receive the network slice accounting information such as the user network contract information (service level agreement – SLA), the data flow volume, its tariff, and the record of the payment of the specified network slice instance user. The service provider can use this information to inform their end users on the degradation of the service or provide alternative services. The AI can be used for the prediction of the cost of the network slice usage based on the overall resource consumption and propose network slicing calendaring.

8.2 Functions of slice runtime management and orchestration

Functions in slice lifecycle management and orchestration consist of network resource configuration notification functions, network slice performance notification functions, network failure notification functions, network slice security notification functions, and network slice accounting notification functions. The metadata communicated by these functions is described in clause 9.

– **Network configuration notification functions**

These functions assign the requested network resources for the service provider and return the results of the assignment. In this assignment, AI-based network slice management and orchestration can use the AI technologies in [ITU-T Y.3178].

– **Network slice performance notification functions**

These functions collect the network KPIs from the measurement points of the network and return them to the requested service provider. AI-based network slice management and orchestration may use AI technologies to predict future performance information.

– **Network failure notification functions**

These functions notify not only the network failure information but also recovery information to the service providers. AI-based network slice management and orchestration may use AI technologies in [ITU-T Y.3177] to find the failure points and create the recovery information.

– **Network slice security notification functions**

These functions notify the network slice security information. AI-based network slice management and orchestration may use AI technologies in [ITU-T Y.3177] to find the threat of recent and future unauthorized access and to protect data from security infringement.

– **Network slice accounting notification functions**

These functions periodically collect information concerning network slice accounting and may also send information about the future slice cost, till its planned termination. Such predictions use AI-based network slice management and orchestration. The functions are not applicable in the case where the flat rate model has been used.

8.3 Interfaces between new functions, Sc-c, Sc-p, Sc-f, Sc-s and Sc-a

– **Sc-c**

Sc-c is used to transport network configuration requests and responses between network configuration request functions and network resource configuration notification functions. The network configuration request is analysed, and the required resources will be assigned to the network slice by AI-based network slice management and orchestration.

– **Sc-p**

Sc-p is used to transport performance information requests and responses between network slice performance request functions and network slice performance notification functions. The response may include the prediction of the performance information in the near future. The prediction is provided by AI-based network slice management and orchestration.

– **Sc-f**

Sc-f is used to transport network failure information requests and responses between network failure request functions and network failure notification functions. The response may include failure prediction in the near future. The prediction is provided by AI-based network slice management and orchestration.

– **Sc-s**

Sc-s is used to transport security data including alarms regarding security attacks, breaches, or other security-related slice malfunctions such as slice isolation issues between network slice security request functions and network slice security notification functions.

– **Sc-a**

Sc-a is used to transport accounting information to the network slice customer between network slice accounting request functions and network slice accounting notification functions. The transferred information can include billing-related statistics that can be further used for charging or verification and adjustment of the billing policies.

9 Procedures

This clause describes general procedures to provide each of the application programming interfaces (APIs) specified in clause 8, including network configuration request functions, network slice performance request functions, network failure request functions, network slice security request functions and network slice accounting request functions.

9.1 API network configuration request procedure

This procedure is used to design the phase of the network and transport the request of the assignment of the network resources such as (R)AN, core, and transport networks to provide the services. Service providers use this function to request the network resource assignment and receive the results of the request from AI-based network slice management and orchestration. Figure 9-1 depicts the detailed procedure.

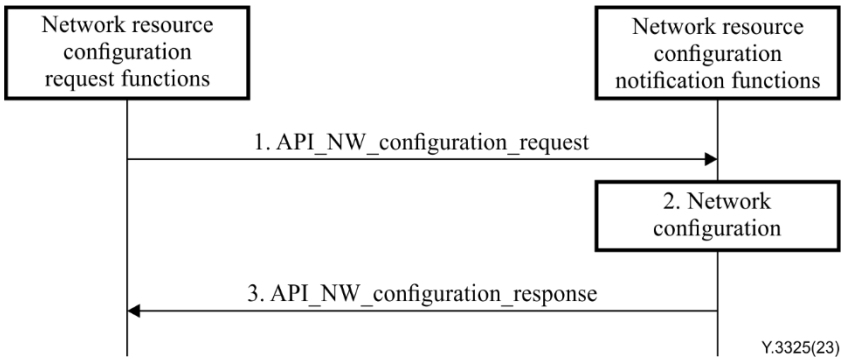

Figure 9-1 – API network resource configuration procedure

1) Network resource configuration request functions in the service provider, sends a network configuration request to the network resource configuration notification functions in the network service provider.

2) Network service provider checks whether this request can be feasible or not. If feasible, the requested network configuration is executed by AI-based network slice management and orchestration.

3) Network service provider returns the results of the check in the above 2) and the results of the network configuration if it was feasible.

9.2 API network slice performance notification procedure

This procedure is used to communicate the KPI of the network used in services such as 4K/8K video streaming, IoT and other services. Figure 9-2 depicts the detailed procedure.

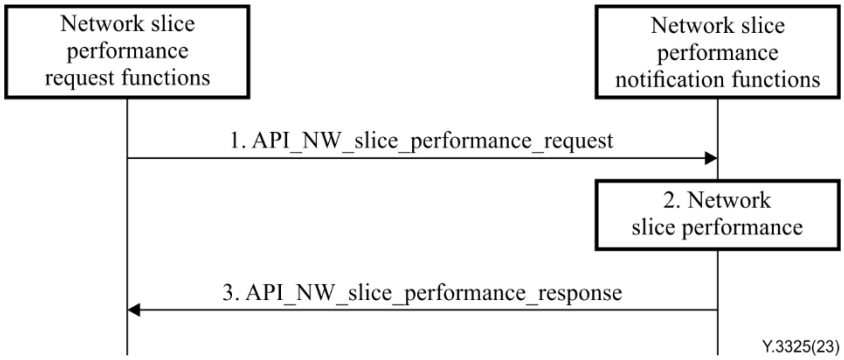

Figure 9-2 – API network slice performance notification procedure

1) Network slice performance request functions in the service provider, sends the network service KPIs and its target network to the network slice performance notification functions in the network service provider.

2) Network service provider checks whether this request can be feasible or not. If feasible, AI-based network slice management and orchestration configures the network to provide the specified network service KPIs in the target network.

3) Network service provider returns the results of the check in the above 2) and the results of the network configuration if it was feasible.

9.3 API network failure notification procedure

This procedure is used to communicate the network failure information. Network failure request functions in service provider receives the network failure information such as the location of the network failure, and the type of failure from AI-based network slice management and orchestration. The service provider can use this information to inform their end users on the degrade of the service or provide alternative services. The information can be used to request the usage of alternative resources, and AI-based network slice management and orchestration may predict the network failure in advance. Figure 9-3 depicts the detailed procedure.

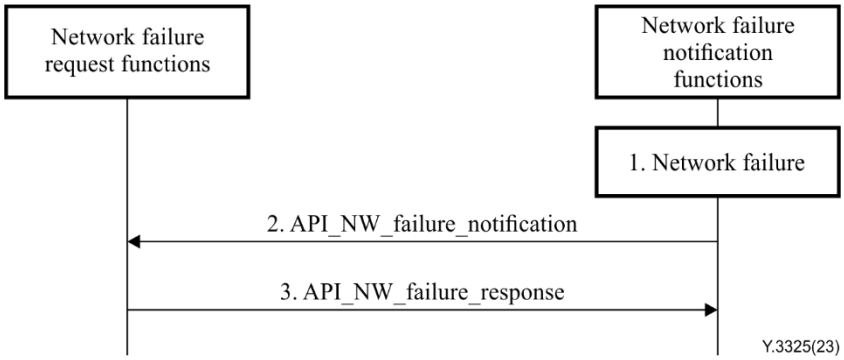

Figure 9-3 – API network failure notification procedure

1) Network failure notification functions in the network service provider, notices the network failure in the network and collects information about this network failure. The gathered information includes the location of the network failure and the type of failure from AI-based network slice management and orchestration. AI-based network slice management and orchestration can use this procedure to provide the prediction of the network failure in advance.

2) Network failure notification functions in the network service provider, sends the collected network failure information to the network failure request functions in the service provider.

3) Network failure request functions in the service provider informs the influence of this network failure to their end users. This information can be used to request the usage of an alternative resource to the network provider services.

9.4 API network slice security notification procedure

This procedure is used to communicate network security information. Network slice security request functions in a network slice customer, receives the network security information such as the data encryption methods, and protection methods against unauthorized access. Figure 9-4 depicts the detailed procedure.

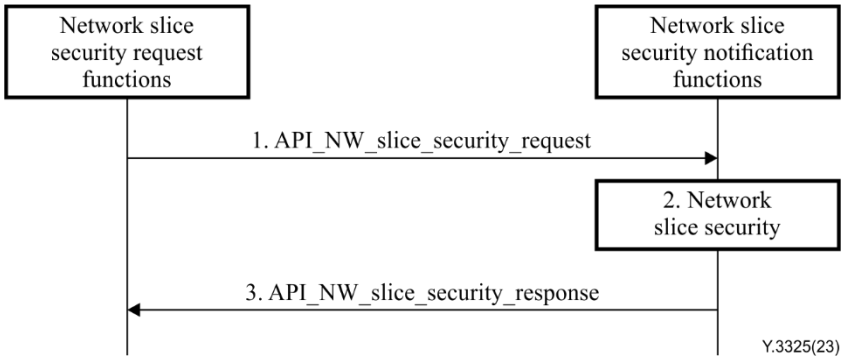

Figure 9-4 – API network slice security notification procedure

1) Network slice security request functions in the service provider, sends a network slice security request to the network slice security notification functions in the network service provider. This request may include network security information such as data encryption methods and protection methods against unauthorized access.

2) Network service provider checks whether this request can be feasible or not. If feasible, AI-based network slice management and orchestration in the network provider use this information to show security options and to specify a user's preferred security option to the specified network.

3) Network service provider returns the security options of the specified network or the results of the network security configuration.

9.5 API network slice accounting notification procedure

This procedure is used to communicate the network slice accounting information. Figure 9-5 depicts the detailed procedure.

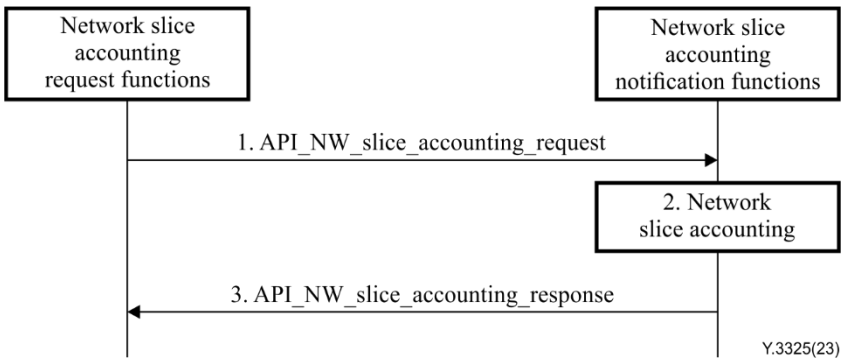

Figure 9-5 – API network slice accounting notification procedure

1) Network slice accounting request functions in the service provider, sends a network slice accounting request to the network slice accounting notification functions in the network service provider. This request may include the user network contract information, the data flow size, its tariff, and the record of the payment of the specified service instance user.
2) Network service provider checks whether this request can be feasible or not. If feasible, AI-based network slice management and orchestration in the network provider collects or predicts this information.
3) Network service provider returns the current or predicted accounting information of the specified network.

10 Metadata in the reference model

This clause introduces metadata exchanged via capability exposure.

NOTE – In Table 10-5, "Prediction" shows the data produced by AI in a network service provider. It means AI-based network slice management and orchestration predicts future network failure and notifies it to the service provider by the API and the metadata specified in this Recommendation. Only this metadata specifies AI explicitly. The other results of AI-based network slice management and orchestration are shown in the metadata implicitly.

10.1 Network configuration request data

This metadata enables network configuration request related functions in both the service provider and network service provider. The procedures using this metadata are described in subclause 9-1. Table 10-1 describes the detailed information of API_NW_configuration_request.

Table 10-1 – API_NW_configuration_request

Information element	Status	Data type	Cardinality	Code value	Description
SST	M	string	1	Enhanced mobile broadband (eMBB) Massive machine type communication (mMTC) Ultra-reliable and low latency communications (URLLC)	Specifies an attribute of the network slice that is requested by the network slice customer to the capability exposure.

Table 10-1 – API_NW_configuration_request

Information element	Status	Data type	Cardinality	Code value	Description
Slice specification	M	string	1...N	N/A	Specifies a detailed specification of the network slice. It includes bandwidth, delay and packet loss rate that are guaranteed by AI-based network slice management and orchestration.

Table 10-2 describes the detailed information of API_NW_configuration_response.

Table 10-2 – API_NW_configuration_response

Information element	Status	Data type	Cardinality	Code value	Description
Slice ID	M	num	1	N/A	Specifies the identification of a network slice. It is assigned by AI-based network slice management and orchestration and is provided to the network slice customers. It is used in subsequent data exchange.
Network slice virtual resources	M	string	1...N	N/A	Specifies the available virtual resources allocated to the slice such as connectivity resources, computing or memory.
Network slice topology	M	string	1...N	N/A	Specifies the topology of the network slice. It includes information on network slice instances, network functions instances and their connectivity. It is sent from the capability exposure to the network slice customer.

10.2 Network slice performance request data

This metadata enables network slice performance request related functions in both the service provider and network service provider. The procedures using this metadata are described in clause 9-2.

Table 10-3 describes the detailed information of API_NW_slice_performance_request.

Table 10-3 – API_NW_slice_performance_request

Information element	Status	Data type	Cardinality	Code value	Description
Slice ID	M	num	1	N/A	Specifies the identification of a network slice.
Link ID	M	string	1...N	N/A	Specifies the identification of the communication links.

Table 10-4 describes the detailed information of API_NW_slice_performance_response.

Table 10-4 – API_NW_slice_performance_response

Information element	Status	Data type	Cardinality	Code value	Description
Assigned bandwidth	M	num	1	N/A	Specifies a network bandwidth assigned by AI-based network slice management and orchestration.
Used bandwidth	M	num	1...N	N/A	Specifies a network bandwidth used over a network slice. It includes current value and/or predicted value.
Delay	M	num	1...N	N/A	Specifies a network delay over a network slice. It includes current value and/or predicted value.
Packet error ratio	M	num	1...N	N/A	Specifies the packet error ratio over network slice. It includes current value and/or predicted value.
Reliability	O	num	1...N	N/A	Specifies the probability of a successful data transmission under given requirements (e.g., delay, bandwidth).
Accessibility	O	num	1...N	N/A	Specifies the number of customers connected to the network slice and the subscriber registration success/ failure rate.
Mobility	O	num	1...N	N/A	Specifies a number of successful/ failed mobility operations.
Virtual resources utilization	O	num	1...N	N/A	Specifies the utilization of virtual resources allocated to the network slice such connectivity, computing or memory resources.

10.3 Network failure data

This metadata enables network failure related functions in both the service provider and network service provider. The procedures using this metadata are described in clause 9-3.

Table 10-5 describes the detailed information of API_NW_failure_data_notification.

Table 10-5 – API_NW_failure_data_notification

Information element	Status	Data type	Cardinality	Code value	Description
Failure point	M	num	1...N	N/A	Specifies the slice instance or communication link at which the failure happened or will happen with the probability of its occurrence. It is sent from the capability exposure to the network slice customer.
Failure time	M	string	1...N	N/A	Specifies the time when the failure happened or will happen with the probability of its occurrence. It is sent from the capability exposure to the network slice customer.
Recovery advice	O	string	1...N	N/A	Specifies the necessary operation for failure recovery. It includes an expected recovery time. While the network provider is responsible for failure recovery in the network layer, the network provider does not usually involve in the failure recovery in the service layer. AI-based network slice management and orchestration derives necessary recovery operation in the service layer using its AI functionality. It is sent from the capability exposure to the network slice customer.
Prediction	O	string	1...N	Prediction, fact	Specifies whether the failure information is based on the fact or the prediction that AI-based network slice management and orchestration provides.

Table 10-6 describes the detailed information of API_NW_failure_data_response.

Table 10-6 – API_NW_failure_data_response

Information element	Status	Data type	Cardinality	Code value	Description
Slice ID	M	num	1	N/A	Specifies the identification of a network slice. If no slices are specified the whole slices are examined.
Link ID	M	num	1...N	N/A	Specifies the identification of a communication link. If no links are specified the whole links are examined.

Table 10-6 – API_NW_failure_data_response

Information element	Status	Data type	Cardinality	Code value	Description
Feedback information	O	String	1	N/A	Specifies the evaluation information in a network service customer. The network service customer evaluates the failure content or recovery advice provided and sends it to capability exposure as feedback. It is used to improve AI capabilities in AI-based network slice management and orchestration.

10.4 Network security data

This metadata enables network security related functions in both the service provider and network service provider. The procedures using this metadata are described in clause 9.4.

Table 10-7 describes the detailed information of API_NW_slice_security_request.

Table 10-7 – API_NW_slice_security_request

Information element	Status	Data type	Cardinality	Code value	Description
Slice ID	M	num	1	N/A	Specifies the identification of a network slice.
Observation period	M	num	1	N/A	Specifies the observation interval.

Table 10-8 describes the detailed information of API_NW_slice_security_response.

Table 10-8 – API_NW_slice_security_response

Information element	Status	Data type	Cardinality	Code value	Description
Slice ID	M	num	1	N/A	Specifies the identification of a network slice.
Security status	M	string	1…N	N/A	Provides a synthetic list of security-related events in a specified period.
Newly detected attack or anomaly (in progress) (unsolicited)	M	string	1	N/A	Proactive attack detection based on anomaly detection. A list of indicators of the attack is provided. This is an early warning, and the problem does not have to be an attack, it can also be a failure or a misconfiguration. The obtained information can be later used for AI/ML algorithms training.

Table 10-8 – API_NW_slice_security_response

Information element	Status	Data type	Cardinality	Code value	Description
Recently finished attack details	O	string	1…N	N/A	Specifies recent attack details (start time, duration, affected functions or links). It is sent from the capability exposure to the network slice customer.
Recent attack impact	O	string	1	N/A	Specifies which performance indicators suffered from the attack. It is sent from the capability exposure to the network slice customer.
Mitigation action advice	M	string	1…N	N/A	Specifies the necessary operation for attack mitigation. While the network provider is responsible for taking mitigation action (fast reaction), the slice customer may approve them or suggest other actions. The AI-based network slice management and orchestration derive necessary mitigation operations using its AI functionality, which may include adding security-related functions.
Feedback information	O	string	1	N/A	Specifies the evaluation information by a network service customer. The network service customer evaluates the attack or mitigation advice and sends it to the capability exposure as feedback. It improves AI capabilities in AI-based network slice management and orchestration.

10.5 Network accounting data

This metadata enables network slice accounting related functions in both the service provider and network service provider. The procedures using this metadata are described in clause 9.5.

Table 10-9 describes the detailed information of API_NW_slice_accounting_request.

Table 10-9 – API_NW_slice_accounting_request

Information element	Status	Data type	Cardinality	Code value	Description
Slice request ID	M	num	1	N/A	Specifies the identification of network slice requests. Slice requests may comply with the GSMA GST/NEST description (high level) and should include slice KPIs, deployment time and duration.

Table 10-9 – API_NW_slice_accounting_request

Information element	Status	Data type	Cardinality	Code value	Description
Slice deployment start time	M	num	1	N/A	Specifies slice deployment start time.
Slice deployment duration	M	num	1	N/A	Specifies slice deployment duration.

Table 10-10 describes the detailed information of API_NW_slice_accounting_response before slice deployment.

Table 10-10 – API_NW_slice_accounting_response (before slice deployment)

Information element	Status	Data type	Cardinality	Code value	Description
Slice request ID	M	num	1	N/A	Specifies the identification of network slice requests. Slice requests may comply with the GSMA GST/NEST description (high level) and should include slice KPIs, deployment time and duration.
Cost estimation	M	num	1	N/A	Specifies estimates of the cost for the slice request for given KPIs. The cost calculation considers expected resource consumption based on AI/ML techniques.
Slice calendaring cost	O	num	1…N	N/A	Provides an estimation of the cost of a slice if the slice is short-lived (duration < 24h), and it can benefit from the time-of-day resource consumption curve. A list of slice deployment start times with related costs is provided for such slices.

Table 10-11 describes the detailed information of API_NW_slice_accounting_response during slice runtime.

Table 10-11 – API_NW_slice_accounting_response (during slice runtime)

Information element	Status	Data type	Cardinality	Code value	Description
Slice ID	M	num	1	N/A	Specifies the identification of a network slice.
Slice actual cost	M	num	1	N/A	The accumulative cost is based on the resource consumption.
Feedback information	M	num	1	N/A	Based on resource consumption it provides an estimation of the cost for the whole slice duration.

11 Security consideration

This Recommendation describes the reference model and metadata for exchanging information between network slice customers and the capability exposure. The contents of this Recommendation are closely related to network management and orchestration. Therefore, the security considerations of IMT-2020 network management and orchestration [ITU-T Y.3111] can be applied.

Appendix I

Example use cases

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

IMT-2020 systems have been developed to realize three usage scenarios, namely enhanced mobile broadband (eMBB), ultra-reliable and low latency communications (URLLC) and massive machine type communication (mMTC). To support these distinct scenarios, the traditional "one fits all" approach is not suitable from both technical and economic aspects, and network slicing is a promising approach in which logical networks are created according to specific requirements. Beyond the IMT-2020 era, AI-based network slice management or AI-based network slice management (e.g., intelligent network slice provisioning and prompt failure detection/recovery, etc.) will be realized.

This appendix presents two use cases regarding a reference model between AI-based network slice management and orchestration (ANSM) and network slice customers.

I.1 Ultra high definition on-demand video services

In IMT-2020 systems, various ultra-high definition on-demand video services will be provided. The user equipment (UE) will not access the original content server provided by the content provider, but the cache server provided by service providers, called the CDN providers. We assume that there will be several paths to access several cache servers on the Internet from the IMT-2020 network shown in Figure I.1-1.

In this figure, network (A) will connect cache server Cache-A on the Internet and network (B) will connect cache server Cache-B to the Internet.

When ANSM notices the network failure symptoms or the network failure itself, it will try to fix them by the technology in [ITU-T Y.3156], [ITU-T Y.3177] and [ITU-T Y.3178]. However, if the whole resource will be run out in some local network area, it may cause a network failure locally.

If the new communication method between a service provider and network service provider will be provided the service provider will notice the depletion of the under-layer network resource through this interface. In this use case, by using this kind of network failure information, the service provider will change cache servers that the UE will access. It means to avoid the failed network path and avoid long time service down including video image corruption [b-AINW-2021].

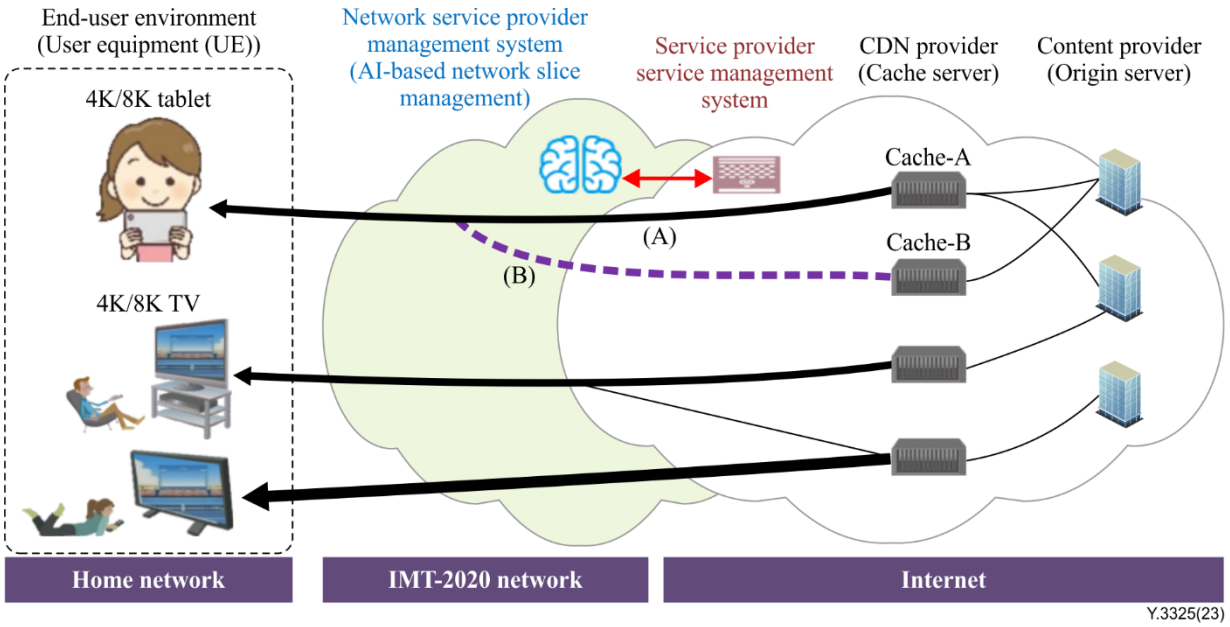

Figure I.1-1 – System configuration for ultra-high definition on-demand video services

Figure I.1-2 shows that a network error happens in network (A). It causes video image corruption in 4K/8K tablet in this figure. Figure I.1-3 shows the recovered network by communicating network failure information between the network service provider management system and the service provider management system and changing cache server Cache-A to Cache-B by the service provider management system. It keeps video streaming service in 4K/8K tablet in this figure.

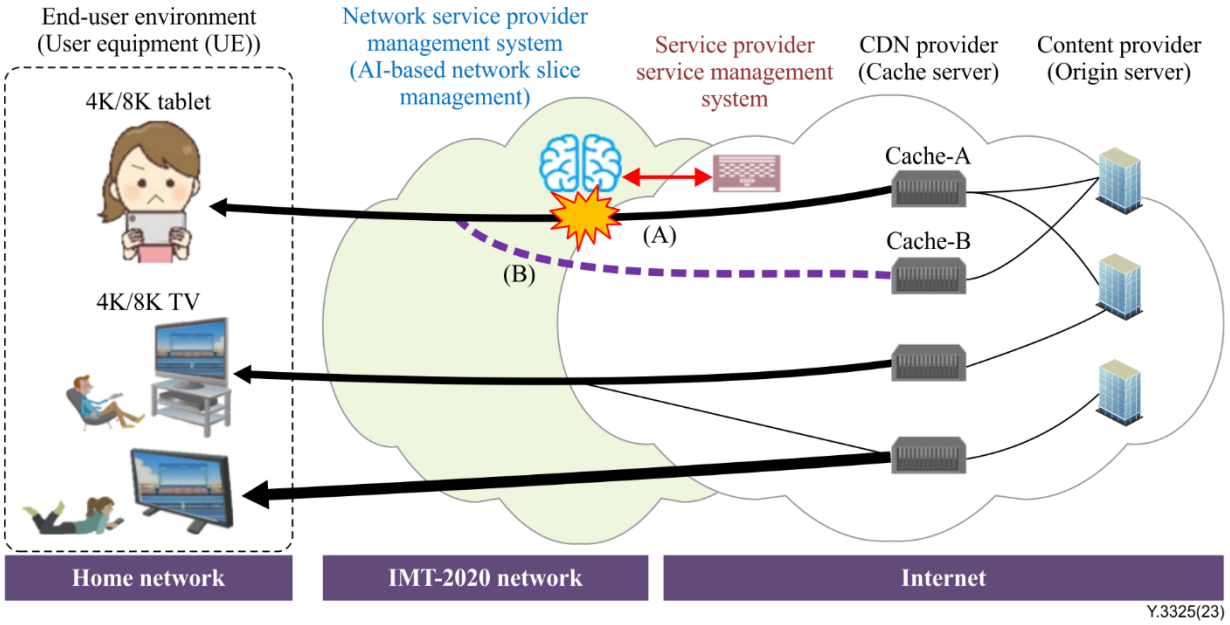

Figure I.1-2 – Network error happens around network (A)

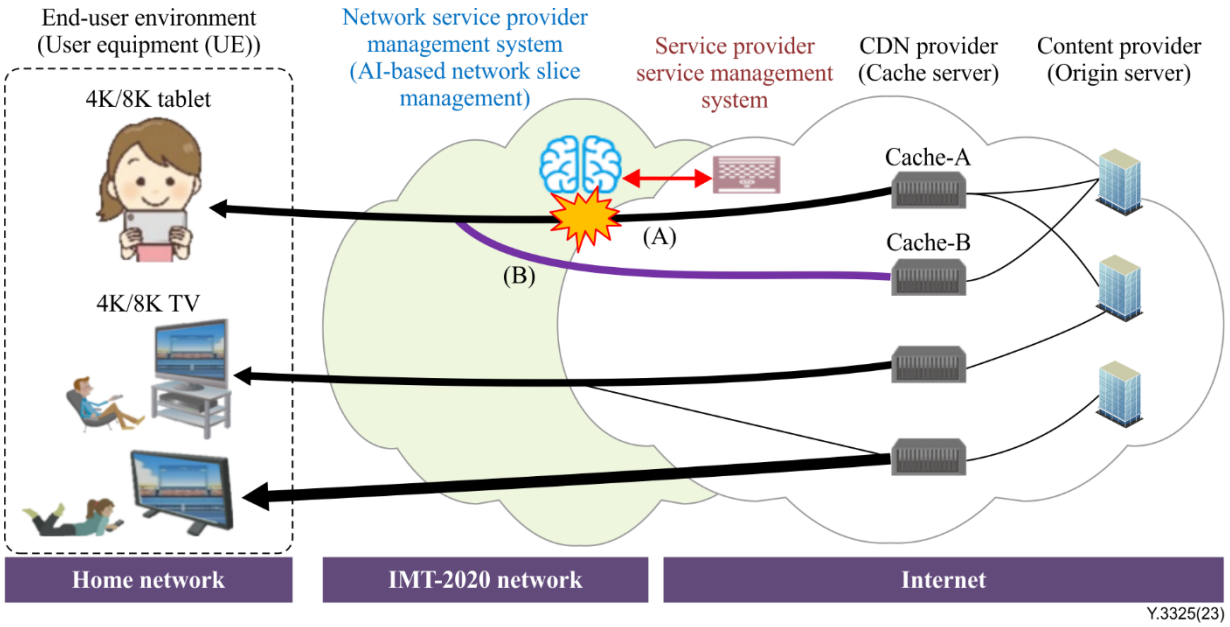

Figure I.1-3 – Network error recovery by changing network from network (A) to (B)

I.2 Low latency IoT services

In IMT-2020 systems, various IoT services will be realised and some of these services will impose low latency requirements on the systems. To support the latency sensitive services, much attention has been paid to multi-access edge computing (MEC) systems in which server functionalities (called MEC hosts) are allocated at the edge side of the network (Figure I.2-1). After service requests from user equipment are routed to the local MEC hosts (a. in Figure I.2-1), the MEC hosts perform necessary processing (b.) and return the processing outputs to the user equipment and/or other equipment/hosts (c.). In this way, the MEC system contributes to a significant reduction in the response time. To improve scalability and flexibility, some MEC hosts which have high performance ability, can be allocated in a central network. Regarding service provisioning of the MEC systems, services providers (i.e., network slice customers) request the network slice creation to the ANSM through capability exposure as "URLLC mode". Then the service providers embed the processing instances (called applications) required for the services on the MEC hosts.

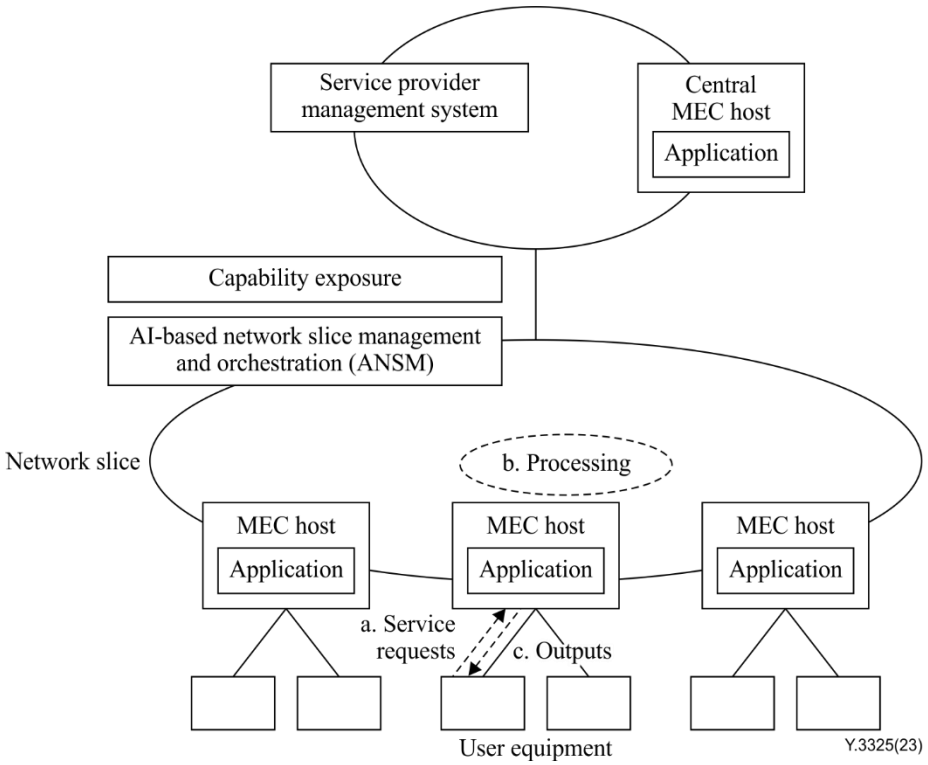

Figure I.2-1 – System configuration for low latency IoT services

One of the technical issues in the MEC system is congestion because the computing resources of the MEC hosts located at the network edge are limited. When a large number of service requests are concentrated at a certain MEC host (imagine that many AR/VR users gather at a stadium), the server cannot satisfy the required service quality. To handle such a congested condition, it is a reasonable solution to distribute some part of the necessary processing into the surrounding MEC hosts or maybe into the central MEC hosts. The distribution should be done with consideration of the service quality.

To select suitable MEC hosts during the distribution process, network delay in the network slice and processing delay on the MEC hosts are essential information. While the service providers obtain the network delay from the ANSM through the capability exposure, the processing delay is obtained from the application on the MEC host (Figure I.2-2). Using the information, the service providers estimate end-to-end delay for each user and select suitable MEC hosts. After the services providers send the results of the MEC host selection to the ANSM through the capability exposure, the ANSM assigns some users to neighbouring MEC hosts and/or central MEC hosts. Moreover, if the ANSM supports the forecasting of network conditions, information on predicted network delay improves the performance of the MEC host selection.

Some works of literature discuss detailed mechanisms of the MEC host selection. It is out of the scope of this Recommendation.

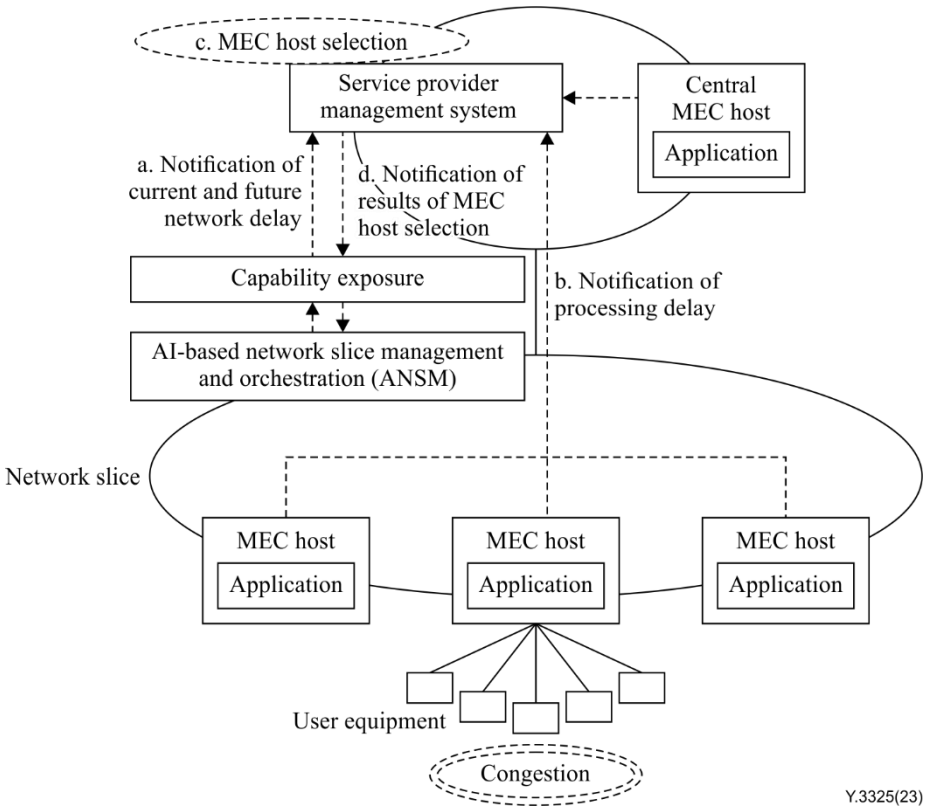

Figure I.2-2 – Example data linkage for low latency IoT services

Appendix II

Future capability exposure functions

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

The following data should be considered to implement the extended functions where network slice customers use AI functions in AI-based networks explicitly. Further study is needed.

– **AI model training data**: specifies training data that is used to improve AI capabilities in AI-based network slice management and orchestration. It is provided by network slice customers. The result of the training can be reflected in the response from capability exposure to network slice customers.

– **Feedback information**: specifies evaluation information in network service customers. The network service customer evaluates the network slice topology assigned and sends it to capability exposure as feedback. It is used to improve AI capabilities in AI-based network slice management and orchestration.

Bibliography

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

[b-ITU-T Y.Sup55] Supplement 55 (2019), *ITU-T Y.3170-series – Machine learning in future networks including IMT-2020: use cases*.

[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-ITU-R M.2083-0] Recommendation ITU-R M.2083-0 (2015), *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

[b-AINW-2021] Yamamoto, H., Kondo, N., Joh, T., Warabino, T., Suzuki, Y., Mori, G., and Jibiki, M. (2021), *Design and implementation of a reference model between services and AI-assisted network.*
<https://ieeexplore.ieee.org/document/9415274/authors#authors>

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, 2023