ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3159 (10/2023)

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

Future networks

Framework for classifying network slice levels in future networks including IMT-2020

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
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	Y.1000-Y.1999
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	Y.2000-Y.2999
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	Y.4000-Y.4999
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.3159

Framework for classifying network slice levels in future networks including IMT-2020

Summary

The objective of Recommendation ITU-T Y.3159 is to specify a framework for classifying network slice levels in future networks, including IMT-2020. This framework is guidance for network slice deployment and management. A method for classifying network slice levels of future networks, including IMT-2020, is introduced.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3159	2023-10-23	13	11.1002/1000/15237

Keywords

Framework, IMT-2020, isolation, network slice level.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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.3159

Framework for classifying network slice levels in future networks including IMT-2020

1 Scope

This Recommendation specifies a framework for classifying network slice levels in future networks, including IMT-2020. This framework is guidance for network slice deployment and management. This Recommendation also introduces a method for classifying network slice levels of future networks, including IMT-2020.

2 References

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

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

[ITU-T Y.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.*

[3GPP TS 23.501] 3GPP TS 23.501 V18.0.0 (2022), *System architecture for the 5G System (5GS); Stage 2 (Release 18).*

[3GPP TS 28.530] 3GPP TS 28.530 V17.3.0 (2022), *Management and orchestration; Concepts, use cases and requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application domain [b-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 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].

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

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

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

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

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

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

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

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

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

3.1.6 service level agreement (SLA) [b-ITU-T Y.3106]: A formal agreement between two or more entities reached after a negotiating activity with the scope to assess service characteristics, responsibilities and priorities of every part. A SLA may include statements about performance, billing, service delivery but also legal and economic issues.

NOTE – Definition based on [b-ITU-T E.860].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
ASF	Authentication Server Function
CEF	Capability Exposure Function
CN	Core Network
E2E	End-to-End
eMBB	enhanced Mobile Broadband
FlexE	Flexible Ethernet
FlexO	Flexible Optical transport network
IMT-2020	International Mobile Telecommunication 2020
IoT	Internet of Things
KPI	Key Performance Indicator
MPLS	Multi-Protocol Label Switching
MTN	Metro Transport Network
NE	Network Equipment
NF	Network Function
NR	New Radio
NRF	Network Function Registry Function
NSSF	Network Slice Selection Function

OAM	Operation, Administration and Management
OTN	Optical Transport Network
PCF	Policy Control Function
QoS	Quality of Service
RAN	Radio Access Network
RB	Radio Bear
SLA	Service Level Agreement
SMF	Session Management Function
S-NSSAI	Single- Network Slice Selection Assistance Information
UE	User Equipment
UPF	User Plane Function
USM	Unified Subscription Management Function
VPN	Virtual Private Network

5 Conventions

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

6 Overview of framework for classifying network slice levels

6.1 Principle for classifying network slice levels

Unlike a traditional network that works in "one pipe and best effort" mode, the IMT-2020 network in combination with network slicing aims to provide various end-to-end logical private networks that run on a shared infrastructure and a shared network to cater for the specific requirements of vertical industries. As defined in [3GPP TS 23.501], network slices may differ for supported features and network function optimizations, in which case such network slices may have e.g., different S-NSSAIs with different slice/service types. The operator can deploy multiple network slices delivering exactly the same features but for different groups of users, e.g., as they deliver a different committed service and/or because they are dedicated to a customer, in which case such network slices may have e.g., different S-NSSAIs with the same slice/service type but different slice differentiators. Based on analytics of performance indicators, flexible functions, network requirements and OAM modes, users who uses network slice as a service can be the communication service provider or the communication service customer defined in [3GPP TS 28.530]. Here, for IMT-2020 networks these can fall into two types:

- Public network users:

The services for public network users that traditional networks provide are all retained in an IMT-2020 network with a consistent or even better user experience.

- Application domain users:

  Application domain users can be divided into general application domain users and special application domain users.

  – General application domain users have general requirements for service isolation and quality, and may call for a differentiation in customization, in terms such as connection management.

– Special application domain users who have specific requirements (for example, high isolation or high service quality assurance) demand extremely high security, such as power grids, government and armies.

In accordance with public network users and application domain users, the network architecture forms public networks and application domain networks, where public networks and application domain networks share core network hardware, transport resources and radio resources, as shown in Figure 1. This sharing mechanism gives full play to a network scale effect. IoT numbers and public network numbers are used to separate user equipment (UE) on different networks, and network equipment (NE), resources and base stations can be exclusively used by different networks, enabling flexible architecture and configuration modes.

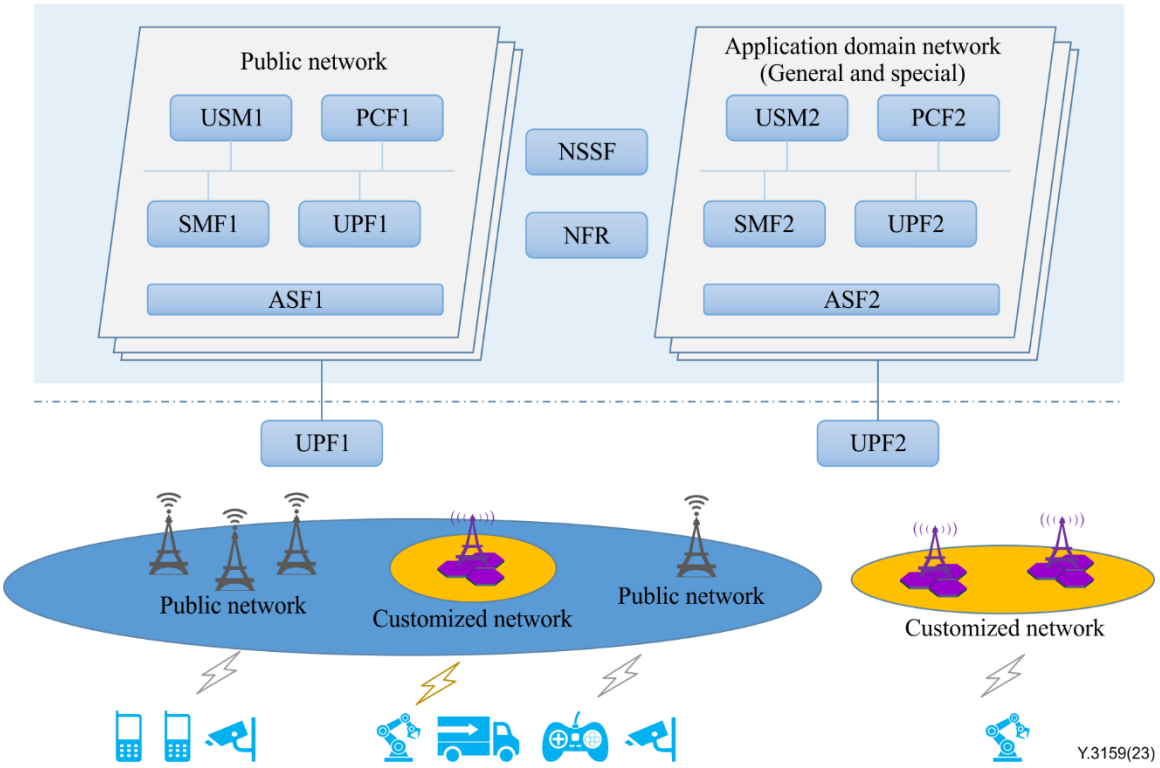

Figure 1 – Architecture of public networks and application domain networks

To meet these IMT-2020 network slicing requirements and those concerning isolation, deployment, and operation, two relatively independent IMT-2020 networks slices are available: public network slices and application domain network slices. This Recommendation defines multilevel slices with varying capabilities to meet the corresponding requirements of users.

Network functions interact with each other to provide the IMT-2020 network services specified in [ITU-T Y.3102]. Interaction procedures between network functions in order to provide network services are specified in clause 7 of [ITU-T Y.3104].

6.2 Classification of network slice levels

This clause provides the overall classification of network slice levels. Depending on the existing network capabilities, the radio access network (RAN), transport network, core network, security and operation capabilities are holistically considered for different slice levels to match the most possible network deployment policies. A total of five slice capability levels are provided to meet the two types of IMT-2020 network slicing requirements, as shown in Table 1.

Table 1 – The classification of network slice level

Network slice level	Title	Type	Definition	Customized resources	Service experience		
				Isolation	Security	Exposure of network management and orchestration capabilities	Customized service
L0	Public network	General	Based on IMT-2020 public network infrastructure, no special requirements	Fully shared	Basic safety	None	Default
L1		High-quality users	Based on IMT-2020 public network infrastructure, superimposed customization requirements	Fully shared	Encryption	None	Differentiation
L2	General application domain	General	Based on IMT-2020 application domain network infrastructure, providing value-added services.	Fully shared	Boundary isolation	Visible	Differentiation
L3		High-quality users	Based on the IMT-2020 application domain network infrastructure, it provides exclusive resources and advanced services.	Partially exclusive	Boundary isolation + Encryption	Manageable	Differentiation
L4	Special application domain	Special application domain users	Based on the construction of IMT-2020 application domain private network facilities, it provides exclusive resources and reliability services for all resources.	Completely independent	Advanced security	Manageable	Differentiation

– Slice level:

Five slice levels, including L0 to L4, are defined.

– Network type:

  Two network types, including public network and application domain network.

– Level classification:

  Public networks have two levels: general and high-quality users. Application domain networks have three levels: general, high-quality users and special.

– Slice level definition:

  It defines each slice level.

– Resource customization:

  Three options are available, including fully shared, partially exclusive and completely independent. At initial construction, public networks and application domain networks are separated, delivering original isolation. Resource customization refers to the degree of resource isolation among the RAN, transport network and core network.

– Service experience:

  – Security:

    Five options are available, including basic security, enhanced Mobile Broadband (eMBB) enhanced security, service feature security, high-level service feature security and high-level security.

– Exposure of network management and orchestration capabilities:

  Three options are available, including no need for exposure, application domain visualization for exposure information and application domain manageability for exposure information.

– Customized service:

  Except for general users on public networks that have no special requirements, L1 to L4 require different assurance capabilities, which are to be tailored to specific scenarios and requirements.

In addition to the aforementioned basic network capabilities (network resources, isolation, exposure, security and customized services), different vertical industries have their own customization requirements. Network slicing needs to provide customization capabilities, which can be found as the attributes of network slices/services in [b-GSMA NG.116], such as support for non-IP transmission, clock synchronization, and high-speed device processing, and such capabilities can be added to each of the capability levels.

7 Methods for classifying network slice levels

This clause provides detailed solutions to the aforementioned five capability levels in terms of RAN, transport network, core network and management system in the preceding dimensions.

7.1 Network slicing isolation capability

7.1.1 RAN slice isolation solution

Table 2 provides the classification of a RAN slice level. The RAN slice isolation solution aims to isolate and guarantee resources for network slices on RAN. Slice-specific QoS assurance, air interface dynamic radio bear (RB) resource sharing, and static RB resource reservation are available, differentiating in service latency, reliability and isolation requirements.

NOTE – The specific technology of RAN is out of scope of this Recommendation.

Table 2 – Suggestions on RAN slice levels

Network slice level	Title	Type	RAN slice capability	Application domain
L0	Public network	General	Capability 1: RB resource sharing and QoS-specific slice	Enterprise broadband
L1		High-quality users		
L2	General application domain	General		
L3		High-quality users	Capability 2: partially reserved RB resources and dynamically shared slices Or Capability 3: resource-exclusive slice	For Capability 2: Basic service assurance is required. Example services include smart grid inspection and media live broadcast. For Capability 3: Strong requirements are put on service isolation and bandwidth. Examples include power grid distribution automation, government and public security private networks.
L4	Special application domain	Special application domain users		

7.1.2 Transport network slice isolation solution

Table 3 provides the classification of a TN slice level. The isolation on transport networks between RANs and core networks (CNs) can be hard isolation or soft isolation, depending on latency, slice security and reliability requirements. The isolation technology can be:

i) physical isolation: metro transport network (MTN) interface isolation adapting Flex Ethernet (FlexE) [b-ITU-T G.8310] [b-ITU-T G.8312], optical transport network (OTN) isolation including Flex OTN (FlexO) in ITU-T G.709 series [b-ITU-T G.709]; or

ii) soft isolation: multi-protocol label switching (MPLS) in ITU-T G.8100 series [b-ITU-T G.8110]/VPN+QoS [b-ITU-T Y.1311.1] isolation.

Table 3 – Suggestions on TN slice levels

Slice level	Title	Type	TN slice capability	Application domain
L0	Public network	General	Softwarized sharing	Internet access and OTT video
L1		High-quality users	Softwarized sharing +physical isolation (tunnel isolation, Gbit/s-level services)	Cloud gaming, home cloud VR, and application domain applications such as mobile rescue, drones and mobile surveillance

Table 3 – Suggestions on TN slice levels

Slice level	Title	Type	TN slice capability	Application domain
L2	General application domain	General	soft isolation +physical isolation (physical isolation, tunnel isolation, Gbit/s-level services)	Power grid, manufacturing, healthcare, mining, port and IoV
L3		High-quality users	Partial physical isolation	Government and enterprise private line, meter reading and collection, video surveillance and live broadcast
L4	Special application domain	Special application domain users	E2E physical isolation	Private lines for government, finance, securities and power grid customers

7.1.3 Core network slice isolation solution

Table 4 provides the classification of CN slice levels. The core network slice isolation solution helps isolate core network slice resources from the networking and guarantees the customized services. The resource view mainly includes the hardware resource layer, virtual resource layer and network function (NF) layer allocated for slice isolation.

– Hardware resource layer: This mainly refers to a variety of servers, which can support both "shared" and "dedicated" isolation modes.

– Virtual resource layer: The communication functions are carried on the general hardware through virtual machines, containers and other virtualization technologies, which can realize rapid development, deployment and flexible scaling up of new business. The virtual resource layer can also support both "shared" and "dedicated" isolation modes.

– NF layer: The network function/virtual network function layer of the core network can support the on-demand isolation mode at different levels to ensure the independence of different slices.

Table 4 – Suggestions on CN slice levels

Slice level	Title	Type	CN slice capability	Application domain
L0	Public network	General	NF layer, virtual resource layer and hardware resource layer shared	Internet access and OTT video
L1		High-quality users	NF layer, virtual resource layer and hardware resource layer shared or partially shared	Cloud gaming, home cloud VR, and application domain applications such as mobile rescue, drones and mobile surveillance
L2	General application domain	General	NF layer, virtual resource layer and hardware resource layer shared or partially shared	Power grid, manufacturing, healthcare, mining, port and IoV

Table 4 – Suggestions on CN slice levels

Slice level	Title	Type	CN slice capability	Application domain
L3		High-quality users	NF layer, virtual resource layer and hardware resource layer shared or partially shared	Government and enterprise private line, meter reading and collection, video surveillance and live broadcast
L4	Special application domain	Special application domain users	NF layer, virtual resource layer and hardware resource layer isolation	Private lines for government, finance, securities and power grid customers

7.2 Security capabilities of IMT-2020 network slices

To support end-to-end (E2E) security protection for different services, flexible security architecture is required to provide multilevel slice security assurance. When vertical application domain users have specific security requirements, they can request customized network slices with different security protection levels from carriers. Differentiated security capabilities include security management capabilities, security capabilities of network protocols and network device resource security capabilities.

NOTE – The specific technology of security capabilities of IMT-2020 network slices is out of scope of this Recommendation.

7.3 Exposure of network management and orchestration capabilities

Table 5 provides the classification of orchestration and management levels for exposure. As defined in [b-ITU-T Y.3108], in terms of interaction with CEF, the network management and orchestration capabilities [ITU-T Y.3110] expose a set of management data required by the customer and authorized by the network operator. For example, network operation status and current network performance can be exposed to third parties through CEF within an operator's policy.

The exposure of network management and orchestration capabilities for network slices can be divided into several scenarios based on the operator's policy.

Table 5 – Suggestions on orchestration and management levels for exposure

Slice level	Title	Type	Degree of capability openness	Visible for exposure information	Manageable for exposure information
L0	Public network	General	None	None	Managed by operator.
L1		High-quality users	None	None	Managed by operator.
L2	General application domain	General	User portal (KPI visualization)	Users can view slice status, UE information, bills and obtain SLA reports through the network slice provider's portal.	Managed by operator.

Table 5 – Suggestions on orchestration and management levels for exposure

Slice level	Title	Type	Degree of capability openness	Visible for exposure information	Manageable for exposure information
L3		High-quality users	User P portal (KPI visualization + self-service business)	Users can view slice status, UE information, bills and obtain SLA reports through the network slice provider's portal.	It can be implemented through a self-service portal: 1) Business subscription, modification and termination, etc. 2) UE lifecycle management, such as UE account opening and cancellation, shutdown and recovery, etc. 3) Simple failure diagnosis, such as real-time diagnosis, diagnosis based on historical information correlation (non-real-time diagnosis), location services, etc.
L4	Special application domain	Special application domain users	Open API capabilities (KPI visualization + self-service business)	Users implement slice business monitoring using APP through open API.	Users implement slice business management using APP through open API.

8 Security considerations

This Recommendation defines methods for classifying network slice levels, including a slice isolation solution for RAN, transport and core networks, security capabilities and OAM modes. Thus, it is assumed that security considerations in general are based on the security of IMT 2020 network management and orchestration [ITU-T Y.3111].

Bibliography

[b-ITU-T E.860] Recommendation ITU-T E.860 (2002), *Framework of a service level agreement*.

[b-ITU-T G.709] Recommendation ITU-T G.709/Y.1331 (2020), *Interfaces for the optical transport network*.

[b-ITU-T G.8110] Recommendation ITU-T G.8110/Y.1370 (2005), *MPLS layer network architecture*.

[b-ITU-T G.8310] Recommendation ITU-T G.8310 (2020), *Architecture of the metro transport network*.

[b-ITU-T G.8312] Recommendation ITU-T G.8312 (2020), *Interfaces for metro transport networks*.

[b-ITU-T Y.1311.1] Recommendation ITU-T Y.1311.1 (2001), *Network-based IP VPN over MPLS architecture*.

[b-ITU-T Y.3106] Recommendation ITU-T Y.3106 (2019), *Quality of service functional requirements for the IMT-2020 network*.

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

[b-ITU-T Y.3111] Recommendation ITU-T Y.3111 (2019), *IMT-2020 network management and orchestration framework.*

[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-GSMA NG.116] GSMA NG.116 v3.0 (2020), *Generic Network Slice Template*.

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

Published in Switzerland
Geneva, 2024