International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3107

(08/2019)

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

Future networks

Functional architecture for QoS assurance management in the IMT-2020 network

Recommendation ITU-T Y.3107

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3107

Functional architecture for QoS assurance management in the IMT-2020 network

Summary

Recommendation ITU-T Y.3107 aims to specify the functional architecture for quality of service (QoS) assurance management in the International Mobile Telecommunications (IMT) 2020 network.

This Recommendation first describes the functional architecture for QoS assurance management under the IMT-2020 network management and orchestration framework. It then specifies reference points between QoS functional entities and the IMT-2020 network management and orchestration plane.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3107	2019-08-13	13	11.1002/1000/13986

Keywords

IMT-2020 network, functional architecture, QoS assurance management

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Functional architecture for QoS assurance management in the IMT-2020 network	5
	6.1 Functional architecture for QoS assurance management	5
	6.2 Functional entities for QoS assurance management	7
7	Reference points	9
	7.1 Reference point Si	9
	7.2 Reference point Se	11
	7.3 Reference point Is	13
	7.4 Reference point Ic	15
	7.5 Reference point Id	17
8	QoS assurance management procedure	19
9	Security considerations	21
Bibliography		22

Recommendation ITU-T Y.3107

Functional architecture for QoS assurance management in the IMT-2020 network

1 Scope

This Recommendation specifies functional architecture for quality of service (QoS) assurance management in the IMT-2020 network. The scope of this Recommendation is as follows:

– Functional architecture for QoS assurance management in the IMT-2020 network;

– Reference points between QoS assurance management functional entities and the IMT-2020 network management and orchestration plane;

– QoS assurance management procedure.

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

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

[ITU-T P.10] Recommendation ITU-T P.10/G.100 (2017), *Vocabulary for performance, quality of service and quality of experience*.

[ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

[ITU-T X.1211] Recommendation ITU-T X.1211 (2014), *Techniques for preventing web-based attacks*.

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

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

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

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

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

[ITU-T Y.3170] Recommendation ITU-T Y.3170 (2018), *Requirements for machine learning-based quality of service assurance for the IMT-2020 network.*

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

[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*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 anomaly [ITU-T X.1211]: A pattern in the data that does not conform to the expected behaviour.

3.1.2 assurance [b-ITU-T X.1500]: The degree of confidence that the process or deliverable meets defined characteristics or objectives.

3.1.3 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.

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

3.1.5 IMT-2020 [ITU-T Y.3100]: (Based on [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.

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

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

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

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

3.1.7 network slice instance [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.

3.1.8 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.

3.1.9 quality of experience [ITU-T P.10]: The overall acceptability of an application or service, as perceived subjectively by the end-user.

NOTE – Quality of experience includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.).

3.1.10 quality of service [ITU-T Q.1743]: The collective effect of service performances, which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as:

– service operability performance;

– service accessibility performance;

– service retainability performance;

– service integrity performance; and

– other factors specific to each service.

3.1.11 service level agreement (SLA) [ITU-T E.860]: 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.

3.1.12 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.

NOTE 1 – An example of 3rd party, a virtual network operator (VNO) may use capabilities exposed by a network operator, e.g., to manage specific network slices. Another example of 3rd party, a service and/or application provider (e.g., an over the top (OTT) player) may provide applications and/or services to enhance the network capabilities.

NOTE 2 – Network end-users are not regarded as 3rd parties.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AN	Access Network
ASPM	Application and Service Plane Management
ASPM-S	Application and Service Plane Management Support
ASP-S	Application and Service Plane Support
BSS	Business Support System
CN	Core Network
CPM	Control Plane Management
CPM-S	Control Plane Management Support
CP-S	Control Plane Support
DPM	Data Plane Management
DPM-S	Data Plane Management Support
DP-S	Data Plane Support
DSCP	Differentiated Service Code Point
E2E	End-to-End
EMES	External Management Entity Support
ERM	External Relationship Management

IASP	IMT-2020 Applications and Service Plane
ICP	IMT-2020 Control Plane
IDP	IMT-2020 Data Plane
IMT	International Mobile Telecommunications
KPI	Key Performance Indicator
MANO	Management and Orchestration
OSS	Operational Support System
OTT	Over The Top
PQ	Priority Queuing
QCI	QoS Class Indicator
QoE	Quality of Experience
QoS	Quality of Service
SCM	Slice Charging Management
SCPO	Slice Capacity Planning and Optimization
SDN	Software-defined Networking
SFM	Slice Fault Management
SI	Slice Instance
SLM	Slice Life-cycle Management
SLMCCS	Slice Lifecycle Customer Care Support
SP	Slice Provisioning
SRMA	Slice Resource Monitoring and Analysis
SRR	Slice Resource Repository
SSM	Slice Security Management
WRED	Weighted Random Early Detection
WRR	Weighted Round-Robin

5 Conventions

This Recommendation uses the following conventions:

The term "is required to" indicates 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 the specification.

6 Functional architecture for QoS assurance management in the IMT-2020 network

6.1 Functional architecture for QoS assurance management

The quality of service (QoS) functional requirements for the IMT-2020 network are specified in [ITU-T Y.3106]. Assurance is defined in [b-ITU-T X.1500] as the degree of confidence that the process or deliverable meets defined characteristics or objectives. The functional architectures for QoS assurance management in this Recommendation are based on the high-level architecture of IMT-2020 network slice management and orchestration provided in [ITU-T Y.3110], [ITU-T Y.3111] and [ITU-T Y.3324]. Figure 1 illustrates the functional architecture for QoS assurance management in IMT-2020 network slice life cycle management. Figure 2 illustrates the functional architecture for QoS assurance management in IMT-2020 network slice instance management.

Network slicing enables the 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 functionality, performance and isolation issues. The orchestration functionalities are specified in the functional elements: slice capacity planning and optimization (SCPO), slice provisioning (SP), and inter-slice orchestration. Management functionalities are specified in the functional elements: slice fault/security/charging management, slice resource monitoring and analytics and resource repository.

The slice capacity planning and optimization functional element is responsible for the planning of necessary resources for the requested slice provisioning and optimizing usage of resources for creating and maintaining slices. During the slice capacity planning, the IMT-2020 QoS planning is involved. The IMT-2020 network QoS planning provides an estimate of the network coverage, capacity and resources requirements. This requires knowledge of real traffic estimates and network topology for each analysed area, utilisation of accurate models for signal and user data transmissions, and implementation of the actual network element characteristics, functionalities and parameters. During the slice optimization, the IMT-2020 QoS optimization is involved. The IMT-2020 network QoS optimisation can be seen as a process to improve the overall network quality, users' quality of experience (QoE) [ITU-T P.10] and to ensure that the network resources are efficiently utilised.

The slice provisioning functional element is responsible for provisioning requested slices by the customers. During the slice provisioning, the IMT-2020 QoS provisioning is also involved. The IMT-2020 network QoS provisioning includes: translation of service-centric service level agreement (SLA) [ITU-T E.860] to resource-facing network slice descriptions, unified and end to end (E2E) QoS controlling, QoS interworking and mapping, efficient E2E QoS provisioning, etc.

The slice resource monitoring and analytics functional element is responsible for collecting the status and events of the provisioned slice resources and analysing them for the purpose of fault, quality, and security management. During the slice resource monitoring and analytics, the IMT-2020 QoS monitoring and analytics is also involved. This includes IMT-2020 QoS monitoring [b-3GPP TS 22.261], measurements, analysis of measurement results, modelling and training [ITU-T Y.3170], anomaly [ITU-T X.1211] detection, anomaly prediction and updates of the network slice parameters.

The QoS policy repository functional element provides capabilities to store the network-wide QoS policy information in a distributed manner.

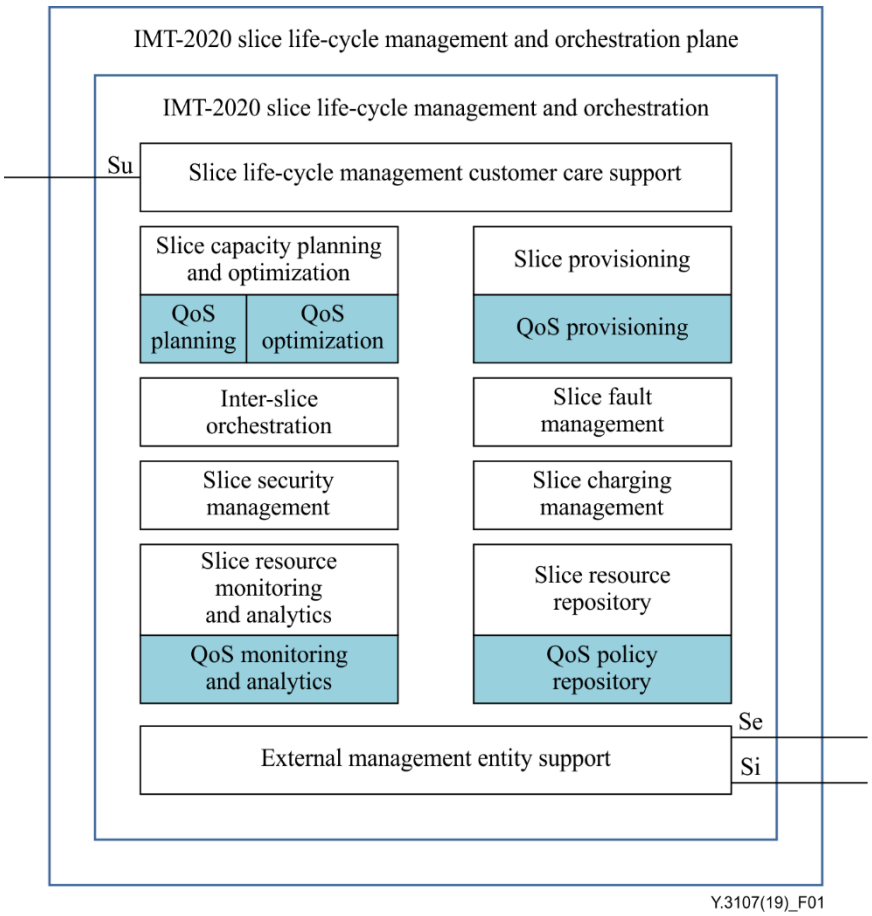

Figure 1 – Functional architecture for QoS assurance management in IMT-2020 network slice life-cycle management

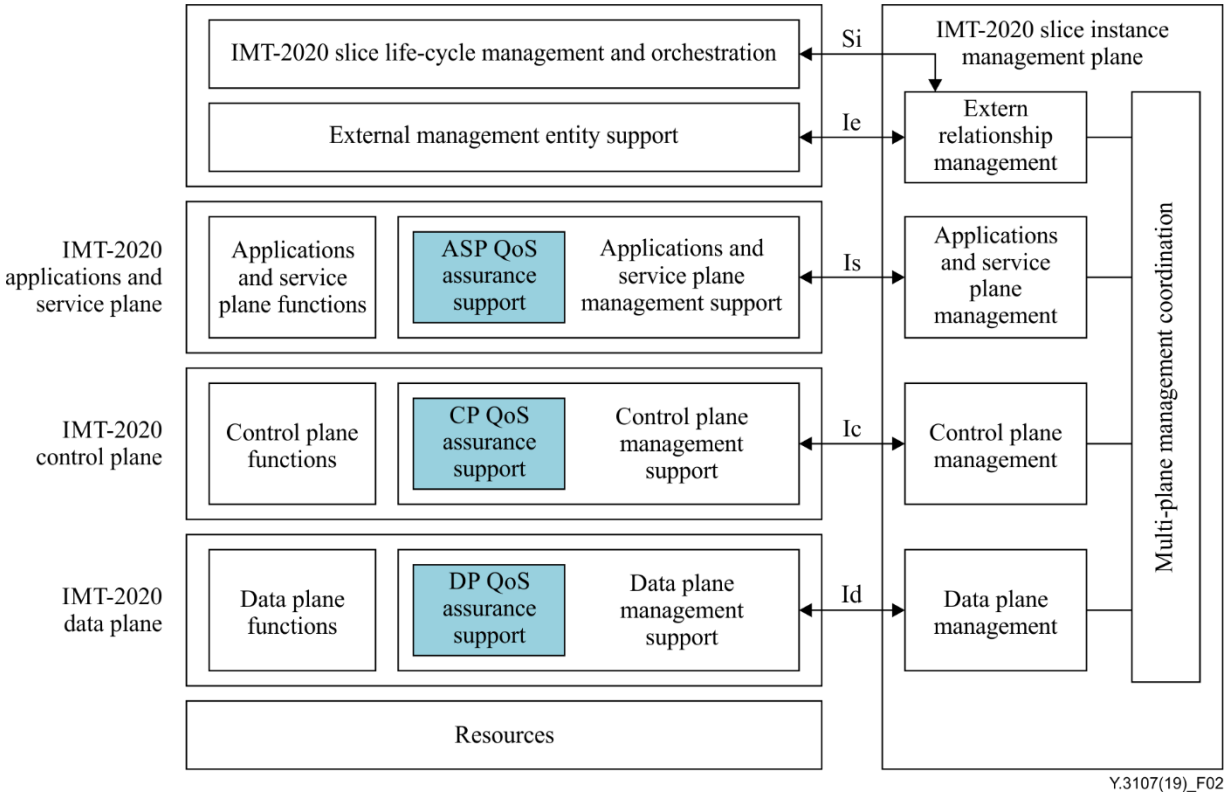

Figure 2 – Functional architecture for QoS assurance management in IMT-2020 network slice instance management

6.2 Functional entities for QoS assurance management

The QoS assurance management functional entities are illustrated in Figure 3. The IMT-2020 applications and service plane QoS assurance support functional entities include: SLA support, QoS policy and QoS capabilities exposure to third party [ITU-T Y.3100]. The control plane [ITU-T Y.2011] QoS assurance support functional entities include: QoS data analysis, QoS planning and optimization, QoS provisioning. The data plane [ITU-T Y.2011] QoS assurance support functional entities include: QoS policy enforcement, QoS data collection and QoS mapping.

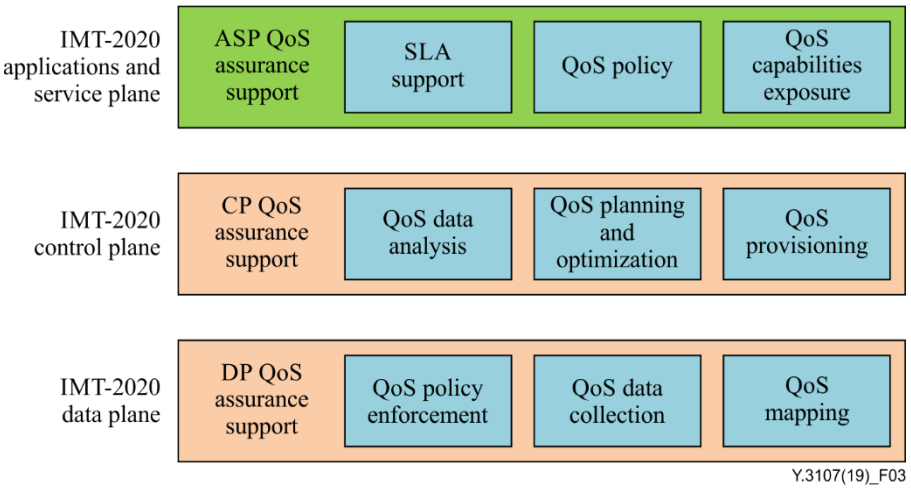

Figure 3 – QoS functional entities

6.2.1 Applications and service plane QoS assurance support functional entity

The applications and service plane QoS assurance support functional entity includes the following functions:

1) Service level agreement (SLA) support

SLA is 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. SLA may include statements about performance, billing, service delivery but also legal and economic issues [ITU-T E.860]. The SLA is from the user and service point of view. The QoS policy is from the network point of view. The SLA support receive the SLAs from the network users and translate them to QoS policies.

2) QoS policy support

In general, SLAs are used to establish QoS parameters for QoS enforcement functions. Each SLA consists of a set of objectives that are used to derive network level policies, which are in turn translated into QoS primitives (e.g., forwarding rules, queue configurations, packet dropping rate, and traffic shaping policies). The QoS mapping policies for QoS interworking between access network (AN) and core network (CN) is also included in QoS policy functional entity.

The QoS policy support distributes the translated QoS policies to the control plane and data plane for QoS enforcement.

3) QoS capabilities exposure

IMT-2020 networks are expected to bring some new and enhanced capabilities. The opening of IMT-2020 network capabilities exposure will bring new business opportunities to operators, vendors and third parties e.g., enterprises or over the top (OTT) players. Except for the network slicing capabilities exposure, the IMT-2020 QoS capabilities exposure is also one of the network capabilities which can open the QoS capabilities for third parties.

All QoS functions and capabilities can be accessed through service-oriented interfaces which include service registration, service discovery, service request and service deregistration.

6.2.2 Control plane QoS assurance support functional entity

The control plane QoS assurance support functional entity includes the following functions:

1) QoS data analysis

The QoS data analysis receives QoS related information data and construct QoS model for QoS assurance. For example, it can construct correlations model between QoS information data and QoS anomalies and the correlations between QoS data and user QoE using machine learning methods [ITU-T Y.3170].

QoS data analysis can detect QoS related anomalies and predict QoS anomaly when current QoS related information data is input into the model with high confidence.

2) QoS planning and optimization

The IMT-2020 network QoS planning receives the knowledge of real traffic estimates and network topology for each analysed area, utilisation of accurate models for signal and user data transmissions, and implementation of the actual network element characteristics, functionalities and parameters. Then, QoS planning provides an estimate of the network coverage, capacity and resources requirements.

The IMT-2020 network QoS optimisation can update the QoS planning results to improve the overall network quality, user's QoE and to ensure that the network resources are efficiently utilized.

The estimation and optimization results are embedded in the network slice planning and optimization.

3) QoS provisioning

The IMT-2020 QoS provisioning translates QoS policies to resource-facing network slice descriptions to enforce unified and E2E QoS controlling, QoS interworking and mapping, efficient E2E QoS provisioning.

6.2.3 Data plane QoS assurance support functional entity

The data plane QoS assurance support functional entity includes the following functions:

1) QoS policy enforcement

The QoS enforcement is mainly focusing on queue management. An important goal of queue management is to minimize the steady-state queue size while not under-utilizing link as well as avoiding the lock-out phenomenon where a single connection or flow monopolizes the queue space. The detailed QoS enforcement functions include packet marking, congestion avoidance, queue shaping, and queue scheduling with a finer level of QoS granularities (per-UE, per-flow). Schemes for queue management differ mainly in the criteria for dropping packets and what packets should be dropped. The use of multiple queues introduces further variation in the schemes, for example, in the way packets are distributed among the queues. It can utilize weighted random early detection (WRED) queue management algorithm, priority queuing (PQ), and weighted round-robin (WRR) queue scheduling algorithms.

2) QoS monitoring and data collection

The IMT-2020 networks are very complicated and are composed of many different network domains such as front haul, backhaul, and core networks. IMT-2020 QoS analysis is data driven. QoS monitoring solution should cover the entire network environment. This complexity is typically solved by distributed domain QoS monitoring.

The QoS monitoring and data collection function entity monitors and collects static information data of IMT-2020 physical or virtual resources, network slice, configuration, fault, performance, security and key performance indicators (KPIs). The QoS monitoring and data collection function entity also monitors and collects dynamic information data of IMT-2020 configuration, fault, performance and security events. The QoS monitoring and data collection functional entity sends these information to the QoS data analysis functional entity for further processing.

3) IMT-2020 QoS mapping

IMT-2020 QoS mapping is used to support proper QoS interworking between networks that packets traverse different network domains (e.g., mapping access network QoS class indicator (QCI) to core network differentiated service code point (DSCP)). QCI value is associated with three attributes: priority, packet delay budget and packet error loss. QCI values are used for selecting scheduling weights, queue thresholds, link-layer configuration which can be translated and mapped into other network domain.

7 Reference points

Based on the reference points specified in [ITU-T Y.3111] and [ITU-T Y.3324], the reference points in this Recommendation are described in this clause.

NOTE – [ITU-T M.3010] specifies management reference points among various management functional entities such as x, q, g, m, and f depending on the context that they are used. Two of them are applicable in this Recommendation: x and q. x is for an inter-operators system and q is for intra-operator system purposes. Although SG13 uses different naming conventions for reference points, Si and Se reference points may serve in the context of x or q and Is, Ic and Id reference points in the context of q.

7.1 Reference point Si

The Si reference point is required to enable request/response information needed for IMT-2020 network slice instance life-cycle management to be exchanged between the external management entity support functional element (EMES) in the management and orchestration plane of the IMT-2020 network slice life-cycle management (SLM) and the external relationship management functional component (ERM) in the management plane of a network slice instance (SI).

This reference point is extended to support QoS assurance management in the overall network slice life cycle. The extension is described in this clause.

The Si reference point may operate as an intra-domain and/or inter-domain reference point.

7.1.1 Functional requirements

7.1.1.1 Slice instance life-cycle management functional requirements

The Si reference point provides the ability to make requests/responses between the EMES in the SLM and ERM in SI for:

– network slice provisioning;
– network slice instance monitoring;
– network slice instance fault management;
– network slice instance charging management;
– network slice instance security management;
– inter-network slice instance orchestration;
– autonomic network slice life-cycle instance management;
– QoS related network slice life-cycle instance management;

– a status report of network slice provisioning, network slice instance performance, fault, charging and security events.

7.1.1.2 Slice instance life-cycle management session processing functional requirements

To assure the reliability and performance of slice instance life-cycle management session operations across the Si reference point, the following capabilities are required:

– **Overload control**: The Si reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the EMES and ERM.

– **Synchronization and audit**: The Si reference point is required to support the capability on synchronization and audit of the network slice instance life-cycle management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Si reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

7.1.2 Information exchange requirements

This clause provides brief descriptions of the information exchange requirements for the Si reference point:

– **Request-response transactions**: The reference point is required to allow EMES to request a transaction to be performed by the ERM and get a response (that can be correlated with the request) in return and also vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: EMES and ERM.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting network slice instance life-cycle management functions.

– **Security**: The Si is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: an EMES is required to be able to communicate with multiple ERMs; 2) many-to-one mode: multiple ERM instances are required to be able to make requests to a given EMES.

7.1.3 Information components

The information components exchanged across the Si reference point are categorized in Table 7-1 as follows:

Table 7-1 – Information components for reference point Si

Information component	Description
Connection ID	Identifies a transport connection or path. A unique value for Connection ID is set by ERM in SI. Two types supported are IPv4 & IPv6 transport connection IDs.
Authentication Information	Authenticates the peers (i.e., EMES and ERM)
Reason Code	Specifies the reason associated with a particular connection ID or service ID.

Table 7-1 – Information components for reference point Si

Information component	Description
Identity Identification	Specifies unique identification. It adopts only International Alphabet No. 5 string format defined in the [ITU-T T.50]. Generally, it is a static IP address of EMES/ERM. When the ERCM/ERM adopts dynamic IP address, identity identification object can use domain name system (DNS) domain name.
Keep-Alive Timer	Specifies the maximum time interval over which an Si protocol transport channel message is recommended in order to be sent or received.
Data Consistency Information	Verifies the consistency of the Se protocol message.
SLM Service ID	Identifies an SLM service and a unique value should be set for each service by ERCM.
Service Profile	Describes a service profile generated by ERCM for a service request.
Connection Profile	Describes a connection that can be set up or has already been set up by ERM.
EventNotify	Allows ERM send notification to ERCM for event that may need ERCM take appropriate action.
Service Attribute Object	Describes the attributes associated with the service profile. It is a sub-object of the Service Profile Object.
Constraint Object	Describe the constraint imposed by a service. It is a sub-object of the Service Profile Object.
Connection Attribute Object	Describes the attributes associated with the transport connection. It is a sub-object of the Connection Profile Object.
Autonomic Management Profile	Describes overall network slice life-cycle autonomic management monitoring and provisioning policies.
Autonomic Management Attribute Object	Describes the attributes associated with overall network slice life-cycle autonomic management monitoring and provisioning policies.
QoS Assurance Management Profile	Describes overall network slice life-cycle QoS management monitoring and provisioning policies.
QoS Assurance Management Attribute Object	Describes the attributes associated with overall network slice life-cycle QoS management monitoring and provisioning policies.

7.2 Reference point Se

The Se reference point is required to enable request/response information needed for an IMT-2020 network slice instance communicating with external management entities to be exchanged between the external management entity support functional element (EMES) in the management and orchestration plane of the IMT-2020 network slice life-cycle management (SLM) and external management entities: management and orchestration (MANO), operation support system (OSS), business support system (BSS), etc.

This reference point is extended to support QoS assurance management in the overall network slice life cycle in relationship with external management entities. The extension is described in this clause.

The Se reference point may operate as an inter-domain reference point.

7.2.1 Functional requirements

7.2.1.1 Communication of a slice life-cycle management and orchestration plane with external management entities functional requirements

The Se reference point provides the ability to make requests/responses between the EMES in the SLM and external management entities for:

– network slice management interworking and orchestration including autonomic management and QoS assurance management capabilities;

– a status report of interworking and orchestration requests including autonomic management capabilities and QoS assurance management actions.

7.2.1.2 Communication of a slice life-cycle management and orchestration plane with external management entities session processing functional requirements

To assure the reliability and performance of communication of a slice life-cycle management and orchestration plane with external management entities session operations across Se reference point, the following capabilities are required:

– **Overload control**: The Se reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the EMES and external management entities.

– **Synchronization and audit**: The Se reference point is required to support the capability on synchronization and audit of the communication of a slice instance with the external management entities session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Se reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

7.2.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Se reference point.

– **Request-response transactions**: The reference point is required to allow the EMES to request a transaction to be performed by the external management entity and get a response (that can be correlated with the request) in return and vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: EMES and external management entities.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting communication of a slice instance with external management entities functions.

– **Security**: The Se is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: an EMES is required to be able to communicate with multiple external management entities; 2) many-to-one mode: multiple EMES are required to be able to make requests to a given external management entity.

7.2.3 Information components

The information components exchanged across the Se reference point are categorized in Table 7-2 as follows:

Table 7-2 – Information components for reference point Se

Information component	Description
User Identifier	A unique identifier for different instances of the IMT-2020 slice life-cycle management and orchestration plane within the same administrative domain of a single requester.
Authentication Information	Authenticates the peers (i.e., IMT-2020 slice life-cycle management and orchestration plane and external management system).
Management Interworking Profile Identifier	A unique management interworking profile identifier required for an exchange of management information between EMES and external management entity.
Management Interworking Profile	Describes management interworking profile information required for an exchange of management information including autonomic management information between EMES and external management entity.
EventNotify	Allows IMT-2020 management plane to send notification to the external management entities for an event that may need external management entities to take appropriate actions.

7.3 Reference point Is

The Is reference point is required to enable request/response information needed for an IMT-2020 network slice application and service plane management to be exchanged between the application and service plane support (ASP-S) of the application and service plane management (ASPM) in the SI and application and service plane management support (ASPM-S) of the IMT-2020 applications and service plane (IASP) in the SI.

This reference point is extended to support QoS assurance management of the network slice instance application and service plane. The extension is described in this clause.

The Is reference point may operate as an intra-domain and/or inter-domain reference point.

7.3.1 Functional requirements

7.3.1.1 Network slice application and service plane management functional requirements

The Is reference point provides the ability to make requests/responses between the ASP-S in the ASPM and the ASPM-S in the IASP for:

– network slice application and service plane management including autonomic management capabilities and QoS assurance management capabilities;

– a status report of slice application and service plane management actions including autonomic management and QoS assurance management actions.

7.3.1.2 Network slice application and service plane management session processing functional requirements

To assure the reliability and performance of network slice application and service plane management session operations across the Is reference point, the following capabilities are required:

– **Overload control**: The Is reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the ASP-S in the ASPM and the ASPM-S in the IASP.

– **Synchronization and audit**: The Is reference point is required to support the on synchronization and audit of the network slice application and service plane management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Is reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

7.3.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Is reference point.

– **Request-response transactions**: The reference point is required to allow the ASP-S in the ASPM to request a transaction to be performed by the ASPM-S in the IASP and get a response (that can be correlated with the request) in return and vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: ASP-S and ASPM-S.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of the appropriate corresponding instance when requesting network slice application and service plane management functions.

– **Security**: The Is is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: an ASP-S is required to be able to communicate with multiple ASPM-S; 2) many-to-one mode: multiple ASP-S are required to be able to make requests to a given ASPM-S in the IASP.

7.3.3 Information components

The information components exchanged across the Is reference point are categorized in Table 7-3 as follows:

Table 7-3 – Information components for reference point Is

Information component	Description
User Identifier	A unique identifier for different instances of the application and service plane management (ASPM) within the same administrative domain of a single requester.
Management Operation Request Session Identifier	An identifier for the session for which the management operation requests are sent to the application and service plane. The identifier has to be unique within the same application and service plane instance.
Globally Unique IP Address Information (Optional)	A set of IP address information used for locating the network in which the ASP-S is requesting the management operations.
Unique IP address	The IP address for identifying ASP-S.
Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID).

Table 7-3 – Information components for reference point Is

Information component	Description
Management Operation Requester Identifier	An identifier for the requester (i.e., the owner of ASP-S in ASPM) of application and service plane management service. It is unique over the requesters sending requests for the ASPM.
Management Operation Request Priority (Optional)	The indication of the importance of a management operation request. It can be used for processing simultaneous requests by application and service plane management based on the priority level.
ASP Autonomic Management Operation Profile	Describes the policies related to autonomic management monitoring and provisioning of network slice instance application and service plane.
ASP Autonomic Management Operation Attribute Object	Describes attributes associated with the policies of the autonomic management monitoring and provisioning of the network slice instance application and service plane.
ASP QoS Assurance Management Operation Profile	Describes the policies related to QoS assurance management monitoring and provisioning of network slice instance application and service plane.
ASP QoS Assurance Management Operation Attribute Object	Describes attributes associated with the policies of the QoS assurance management monitoring and provisioning of the network slice instance application and service plane.
Management Operation Request Result	Indication of the result for a management operation request (includes both synchronous and scheduled request result).
EventNotify	Allows application and service plane to send notifications to ASP-S for events that may need to take appropriate action for requested management operations.

7.4 Reference point Ic

The Ic reference point is required to enable request/response information needed for an IMT-2020 network slice control plane management to be exchanged between the control plane support (CP-S) of control plane management (CPM) in the SI and control plane management support (CPM-S) of the IMT-2020 control plane (ICP) in the SI.

This reference point is extended to support QoS assurance management of the network slice instance control plane. The extension is described in this clause.

The Ic reference point may operate as an intra-domain and/or inter-domain reference point.

7.4.1 Functional requirements

7.4.1.1 Network slice control plane management functional requirements

The Ic reference point provides the ability to make requests/responses between the CP-S in the CPM and the control plane management support (CPM-S) in the ICP for:

– network slice control plane management including autonomic management and QoS assurance management capabilities;

– a status report of slice control plane management actions including autonomic management and QoS assurance management actions.

7.4.1.2 Network slice control plane management session processing functional requirements

To assure the reliability and performance of network slice control plane management session operations across the Ic reference point, the following capabilities are required:

– **Overload control**: The Ic reference point is required to support the on overload control for preventing the overflow of information messages exchanged between the CP-S and the CPM-S in the ICP.

– **Synchronization and audit**: The Is reference point is required to support the capability on synchronization and audit of the network slice control plane management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Ic reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

7.4.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Ic reference point.

– **Request-response transactions**: The reference point is required to allow the CP-S to request a transaction to be performed by the CPM-S in the ICP and get a response (that can be correlated with the request) in return and vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: CP-S and CPM-S.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting network slice control plane management functions.

– **Security**: The Ic is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: a CP-S is required to be able to communicate with multiple CPM-S in the ICP; 2) many-to-one mode: multiple CP-S are required to be able to make requests to a given CPM-S in the ICP.

7.4.3 Information components

The information components exchanged across the Ic reference point are categorized in Table 7-4 as follows:

Table 7-4 – Information components for reference point Ic

Information component	Description
User Identifier	A unique identifier for different instances of the control plane management (CPM) within the same administrative domain of a single requester.
Management Operation Request Session Identifier	An identifier for the session for which the management operation requests are sent to the control plane. The identifier has to be unique within the same control plane instance.

Table 7-4 – Information components for reference point Ic

Information component	Description
Globally Unique IP Address Information (Optional)	A set of IP address information used for locating the network in which the CP-S is requesting the management operations.
Unique IP address	The IP address for identifying CP-S.
Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID)
Management Operation Requester Identifier	An identifier for the requester (i.e., the owner of CP-S in CPM) of control plane management service. It is unique over the requesters sending requests for the CPM.
Management Operation Request Priority (Optional)	The indication of the importance of a management operation request. It can be used for processing simultaneous requests by control plane management based on the priority level.
CP Autonomic Management Operation Profile	Describes the policies related to autonomic management monitoring and provisioning of network slice instance control plane.
CP Autonomic Management Operation Attribute Object	Describes attributes associated with the policies of the autonomic management monitoring and provisioning of the network slice instance control plane.
CP QoS assurance Operation Profile	Describes the policies related to QoS assurance management monitoring and provisioning of network slice instance control plane.
CP QoS assurance Management Operation Attribute Object	Describes attributes associated with the policies of the QoS assurance management monitoring and provisioning of the network slice instance control plane.
Management Operation Request Result	Indication of the result for a management operation request (includes both synchronous and scheduled request result)
EventNotify	Allows control plane to send notifications to the CP-S for events that may need to take appropriate action for requested management operations.

7.5 Reference point Id

The Id reference point is required to enable request/response information needed for an IMT-2020 network slice physical and virtual data plane management to be exchanged between the data plane support (DP-S) of the data plane management (DPM) in the SI and data plane management support (DPM-S) of the IMT-2020 data plane (IDP) in the SI.

This reference point is extended to support QoS assurance management of the network slice instance physical and virtual data planes. The extension is described in this clause.

The Id reference point may operate as an intra-domain and/or inter-domain reference point.

7.5.1 Functional requirements

7.5.1.1 Network slice data plane management functional requirements

The Id reference point provides the ability to make requests/responses between the DP-S in the DPM and the DPM-S for a status report of slice data plane management actions including autonomic management actions.

7.5.1.2 Network slice data plane management session processing functional requirements

To assure the reliability and performance of network slice data plane management session operations across the Id reference point, the following capabilities are required:

– **Overload control**: The Id reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the DP-S and DPM-S of the IDP in the SI.

– **Synchronization and audit**: The Id reference point is required to support the capability on synchronization and audit of the network slice data plane management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Id reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

7.5.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Id reference point.

– **Request-response transactions**: The reference point is required to allow the DP-S to request a transaction to be performed by the DPM-S in the IDP and get a response (that can be correlated with the request) in return and also vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: DP-S and DPM-S.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting network slice data plane management functions.

– **Security**: The Id is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: a DP-S is required to be able to communicate with multiple DPM-S in the IDP; 2) many-to-one mode: multiple DP-S are required to be able to make requests to a given DPM-S in the IDP.

7.5.3 Information components

The information components exchanged across the Id reference point are categorized in Table 7-5 as follows:

Table 7-5 – Information components for reference point Id

Information component	Description
User Identifier	A unique identifier for different instances of the data plane management (DPM) within the same administrative domain of a single requester.
Management Operation Request Session Identifier	An identifier for the session for which the management operation requests are sent to the data plane. The identifier has to be unique within the same data plane instance.
Globally Unique IP Address Information (Optional)	A set of IP address information used for locating the network in which the DP-S is requesting the management operations.

Table 7-5 – Information components for reference point Id

Information component	Description
Unique IP address	The IP address for identifying DP-S.
Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID)
Management Operation Requester Identifier	An identifier for the requester (i.e., the owner of DP-S in DPM) of data plane management service. It is unique over the requesters sending requests for the DPM.
Management Operation Request Priority (Optional)	The indication of the importance of a management operation request. It can be used for processing simultaneous requests by data plane management based on the priority level.
DP Autonomic Management Operation Profile	Describes the policies related to autonomic management monitoring and provisioning of network slice instance data plane.
DP Autonomic Management Operation Attribute Object	Describes attributes associated with the policies of the autonomic management monitoring and provisioning of the network slice instance data plane.
Management Operation Request Result	Indication of the result for a management operation request (includes both synchronous and scheduled request result)
DP QoS assurance Management Operation Profile	Describes the policies related to QoS assurance management monitoring and provisioning of network slice instance data plane.
DP QoS assurance Management Operation Attribute Object	Describes attributes associated with the policies of the QoS assurance management monitoring and provisioning of the network slice instance data plane.
EventNotify	Allows data plane to send notifications to DP-S for events that may need to take appropriate action for requested management operations.

8 QoS assurance management procedure

During the lifecycle of services and associated network slice instances [ITU-T Y.3111], the QoS lifecycle management is also involved. This clause describes a QoS assurance management lifecycle procedure in IMT-2020 network which is illustrated in Figure 4.

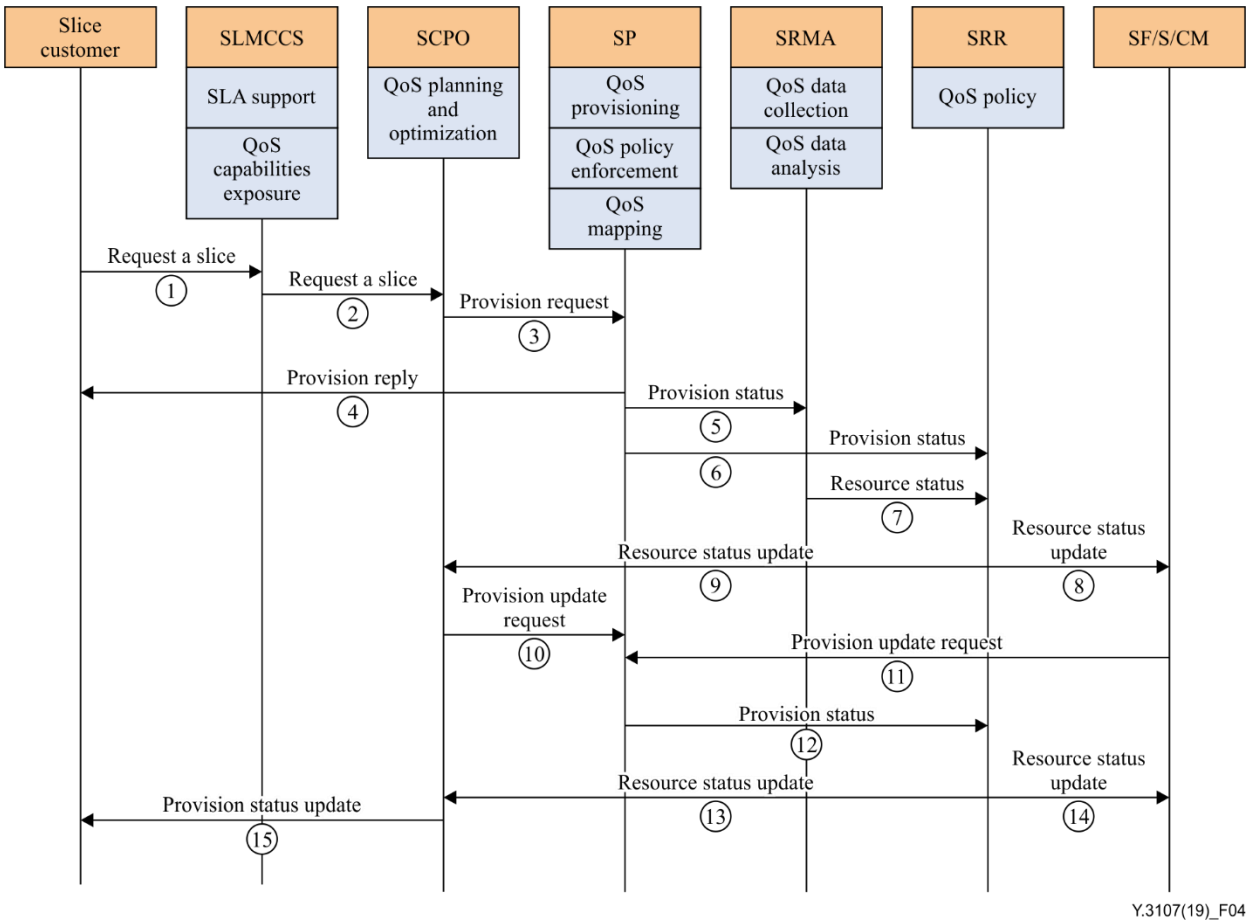

Figure 4 – Procedure for QoS assurance management

1) The IMT-2020 customer requests a slice to be provisioned with its specified service requirements from slice lifecycle management – customer care support (SLMCCS). The QoS capabilities exposure can open the QoS capabilities for third parties. The QoS SLA support provide QoS information for the template of slice provision which include: statements about performance, billing, service delivery.

2) IMT-2020 SLMCCS functional element receives the customer's request and carries it to the slice capacity planning and optimization (SCPO) functional element.

3) After decision of QoS planning and optimization, SCPO then determines an optimal slice plan based on the available resources which matches the customer's request. Once the provisioning policy is determined, SCPO requests provisioning to slice provisioning (SP) functional element.

4) SP then performs the requested slice provisioning task. It involves various sub-tasks including QoS related aspects: QoS provisioning, QoS policy enforcement and QoS mapping, etc. If the provisioning functionality including QoS provisioning functionality is fully supported by the SLM functional component, all the tasks are performed internally. If not, SP then interacts with external slice provisioning related functional entities such as MANO orchestrator, software-defined networking (SDN) controller, etc. When SP interacts with external management entities, it uses external management entity support (EMES) functional element. Upon completion of the provisioning process, SP sends a provision reply message to the customer via SLMCCS.

5) At the same time, it sends a provision status slice resource monitoring and analytics functional element to initiate the collection and monitoring of the provisioned resources.

6) It also sends the status update to slice resource repository (SRR) to store the provisioned resource information.

7) Slice resource monitoring and analysis (SRMA) performs collection, monitoring, and analysis tasks of the provisioned slice resources. The QoS related data is also collected. Data and information collected and analysed are then stored in SRR for further processing by other functional elements.

8) The QoS policy information is also stored in SRR. When SRR receives any resource status updates, it stores them in the repository and, at the same time, it emits notification to all functional elements that are listening to the status updates. In this case, it sends its update notification to slice fault management (SFM), slice security management (SSM), slice charging management (SCM), and 9) SCPO.

10) When SCPO receives the notification, it updates available resource status and determines if re-optimization is needed upon status updates. 11) Also SF/S/C/PM receive the notification, they perform fault, security and charging management of the provisioned slices and their resources and determine if any control or re-provisioning actions are required. If so, they send a request to SP for provisioning update processes.

12) SP, upon receiving the provisioning update requests, performs re-provisioning tasks for the provisioned slices. When re-provisioning tasks are done, SP generates provision status to SRR and SRR further conveys the notification to 13) SF/S/CM, SCPO and 14) IMT-2020 slice customer for resource status updates.

15) SCPO sends provision status update to the customer.

9 Security considerations

The QoS functional entities for the IMT-2020 network are subject to security and privacy measures. Sensitive QoS information should be protected in high priority in order to avoid leaking and unauthorized access. Security and privacy concerns should be aligned with the requirements specified in [b-ITU-T Q.1762], [ITU-T Y.3101] and [b-ITU-T Y.2701].

Bibliography

[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-T Q.1762] Recommendation ITU-T Q.1762/Y.2802 (2007), *Fixed-mobile convergence general requirements*.

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

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

[b-3GPP TS 22.261] 3GPP TS 22.261(2018), 3rd Generation Partnership Project, *Service requirements for the 5G system, Stage 1,(Release 16).*

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, 2019