International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3111

(09/2017)

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

Future networks

IMT-2020 network management and orchestration framework

Recommendation ITU-T Y.3111

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.3111

IMT-2020 network management and orchestration framework

Summary

The objective of Recommendation ITU-T Y.3111 is to provide network management and orchestration architecture and functional components for design, deployment and operation to implement IMT-2020 network covering fixed and mobile networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3111	2017-09-13	13	11.1002/1000/13351

Keywords

IMT-2020 network management and orchestration, IMT-2020 network management and orchestration high-level/functional architecture, IMT-2020 network management and orchestration reference points, network slice lifecycle management and orchestration, network slice instance 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

Recommendation ITU-T Y.3111

IMT-2020 network management and orchestration framework

1 Scope

This Recommendation provides an overview of IMT-2020 network management and orchestration. It also specifies the high-level architecture of IMT-2020 network management and orchestration, the slice life-cycle management and orchestration functional architecture, and an IMT-2020 network management and orchestration procedure and implementation scenarios. The architectures and capabilities defined in this Recommendation are based on the requirements specified in the [ITU-T Y.3110].

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.3001] Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals*.

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

[ITU-R M.2083-0] Recommendation 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 functional component [b-ITU-T Y.3502]: A functional building block needed to engage in an activity, backed by an implementation.

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

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

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

3.1.4 orchestration [b-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 infrastructure by optimization criteria.

3.1.5 software-defined networking [b-ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and mange network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

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

NOTE 1 – A network slice enables the operator to create networks customized to provide flexible solutions for different market scenarios, which have diverse requirements, with respect to the functionality, performance and resource separation.

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).

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

NOTE 1 – A network slice instance is composed of a set of managed run-time network functions, and physical/logical/virtual resources to run these network functions, forming a complete instantiated logical network to meet certain network characteristics required by the service instance(s).

NOTE 2 – A network slice instance may also be shared across multiple service instances provided by the network operator. A network slice instance may be composed of none, one or more sub-network slice instances which may be shared with another network slice instance.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 domain: (Based on the definition given in [b-ITU-T Y.110]) A collection of physical or functional entities which are owned and operated by a player and can include entities from more than one role. The extent of a domain is defined by a useful context and one player can have more than one domain.

3.2.2 IMT-2020: (Based on the definition given in [ITU-R M.2083-0]) Systems, system components and related aspects that support to provide far more enhanced capabilities than those described in [b-ITU-R M.1645]

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Program Interface
A&SP-CM	Applications and Service Plane Charging Management
A&SP-FM	Applications and Service Plane Fault Management
A&SPM	Applications and Service Plane Management
A&SP-MMCS	Applications and Service Plane Multi-Plane Management Coordination Support
A&SP-QM	Applications and Service Plane Quality Management
A&SP-RD	Applications and Service Plane Resource Discovery
A&SP-RMA	Applications and Service Plane Resource Monitoring and Analytics
A&SP-RR	Applications and Service Plane Resource Repository
A&SP-S	Applications and Service Plane Support
A&SP-SM	Applications and Service Plane Security Management
BSS	Business Support System

CP	Control Plane
CP-CM	Control Plane Configuration Management
CP-FM	Control Plane Fault Management
CPM	Control Plane Management
CP-MMCS	Control Plane Multi-plane Management Coordination Support
CP-PM	Control Plane Performance Management
CP-PoM	Control Plane Policy Management
CP-RD	Control Plane Resource Discovery
CP-RMA	Control Plane Resource Monitoring and Analytics
CP-RR	Control Plane Resource Repository
CP-S	Control Plane Support
CP-SM	Control Plane Security Management
DoS	Denial of Service
DP	Data Plane
DP-CM	Data Plane Charging Management
DP-DB	Data Plane Discovery and Bootstrapping
DP-FM	Data Plane Fault Management
DPRM	Data Plane Resource Management
DP-MA	Data Plane Monitoring and Analytics
DP-MMCS	Data Plane Multi-Plane Management Coordination Support
DP-PM	Data Plane Performance Management
DPRR	Data Plane Resource Repository
EIPM	External IMT-2020 Policy Management
eMBB	Enhanced Mobile BroadBand
EMIS	External Management Interworking Support
ERM	External Relationship Management
ERM-MMCS	External Relationship Management Multi-plane Management Coordination Support
IPSC	Inter-Plane Service Coordination
IMT	International Mobile Telecommunications system
ISO	Inter Slice Orchestration
KPI	Key Performance Indicator
LTE	Long Term Evolution
MANO	Management and Orchestration
MIA	Management Information Abstraction

MMFC	Multi-plane Management Function Coordination
MMCS	Multi-plane Management Coordination Support
MMC	Multi-plane Management Coordination network equipment
NFV	Network Function Virtualization
NMS	Network Management System
OAM	Operations and Management
OSS	Operations Support System
PDA	Physical Data Abstraction
PDPR-SM	Physical Data Plane and Resource Security Management
RREM	Request/Reply with External Management
SCM	Slice Charging Management
SCPO	Slice Capacity Planning and Optimization
SDN	Software-defined Network
SFM	Slice Fault Management
SI	Slice Instance
SLM	Slice Lifecycle Management
SLM-CCS	Slice Lifecycle Management – Customer Care Support
SLMS	Slice Lifecycle Management Support
SP	Slice Provisioning
SRMA	Slice Resource Monitoring and Analytics
SRR	Slice Resource Repository
SSM	Slice Security Management
VDAVIM	Virtual Data Abstraction Virtualized Infrastructure Manager
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
VPC	Virtual Physical Correlation
VPR-MO	Virtual/Physical Resource Management Orchestration
WAN	Wide Area Network

5 Conventions

None.

6 Overview of IMT-2020 network management and orchestration

Since the current network architecture may not be appropriate to support various IMT-2020 network requirements, enhancement of the network architecture has been studied. Among the enhanced capabilities including distributed function deployment, network slicing, and resource allocation, IMT-2020 also requires a study on new aspects of network management and orchestration (MANO) whose results are described in this Recommendation.

6.1 Motivation

Based on the understanding of the new trends of networking technology as mentioned above, the following gap analysis items are identified [b-ITU-T Gap Analysis]

- Multiple network management protocols in different network domains make it difficult to support unified network operations over multiple network domains. A unified network management should be considered to ensure compatibility and flexibility for the operation and management of an IMT-2020 network.
- Operations and management (OAM) protocols are not standardized in some parts of IMT networks such as the front haul network. Standard OAM protocols should be studied for fault management and performance management between network equipment that may be commonly used across the IMT-2020 network.
- There are two aspects to consider for network management and orchestration for the network softwarization. The first aspect is how to manage and orchestrate the softwarized network components. The second is how to softwarize network management and orchestration functionality.
- Network slice lifecycle management and orchestration.

This Recommendation specifies a network management and orchestration framework for IMT-2020 in a systematic approach including the aforementioned gap analysis items.

As defined in clause 3, management is the processes aiming at fulfilment, assurance, and billing of services, network functions, and resources in both physical and virtual infrastructure including compute, storage, and network resources. The overall coordination and adaptation for configuration and event reporting are achieved between network functions and network management systems. The network management systems include the collection and feedback of performance measurement information and fault and anomalous events. Network function lifecycle management is included as a part of network function instance management. Network management system is authorized to exercise control over and/or collect management information from another system. It is tightly connected with the existing business support system/operations support system (BSS/OSS) such that the most efficient and effective way to access, control, deploy, schedule and bind legacy resources is chosen for the purpose of integrated management of IMT-2020 and legacy networks.

As defined in clause 3, orchestration is the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructure by optimization criteria. Orchestration results in automation with control network systems. Orchestration is the key function in management and orchestration plane. Orchestration coordinates the management of network service life cycle, network function lifecycle and network function infrastructure resources to ensure optimized allocation of the necessary resources and connectivity.

Based on the analysis in Appendix I and corresponding definitions above, both management and orchestration capabilities are specified in a logically integrated way in the following functional architectures.

7 IMT-2020 network management and orchestration high-level architecture

IMT-2020 network shall provide network services with diverse requirements, by using network functions instantiated as appropriate. IMT-2020 infrastructure will provide the required infrastructure resources to instantiate the network functions. Network operators can provision and operate many different network slices according to their business strategies.

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 functional architecture of IMT-2020 network shall provide a complete set of network functions required to support all IMT-2020 services. A network slice is comprised of only the necessary network functions. They are collected from a complete set of network functions in the IMT-2020 network functional architecture, and orchestrated for the particular service and purpose.

The general framework of IMT-2020 can be represented by two separate architecture levels, i.e., 'slice orchestration and management' level and 'network slice instances' level as shown in Figure 1. Functions for creating and managing network slice instances and the functions instantiated in the network slice instance are illustrated in the respective architectural level.

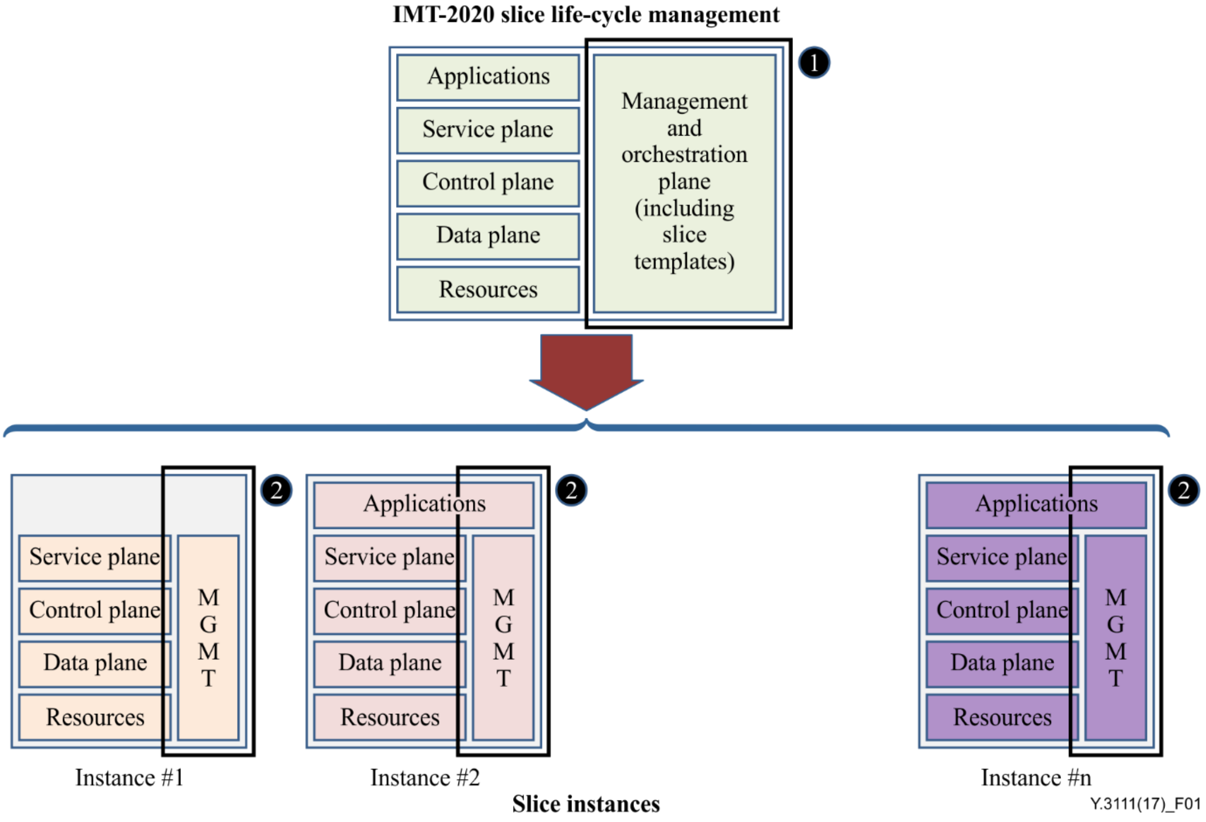

Figure 1 – Conceptual IMT-2020 network framework from the network slicing perspective

As the conceptual framework of IMT-2020 consists of two levels, the management and orchestration architecture is also required to deal with two levels: management and orchestration in IMT-2020 network slice life-cycle management (Instance 1) and management in each network slice instances (Instance 2). This Recommendation specifies management and orchestration architecture and capabilities of slice lifecycle in clause 8. It also specifies management architecture and capabilities of slice instances in clause 9.

The conceptual framework only describes the relationship between slice lifecycle management and slice instance functional entities. For a clear understanding of management and orchestration capabilities in IMT-2020, it is useful to describe the relationships with additional associated functional components such as a slice customer and an external management system.

Figure 2 illustrates such relationship among a slice customer, slice lifecycle management and orchestration and slice instance management functional components, and external management system with reference points.

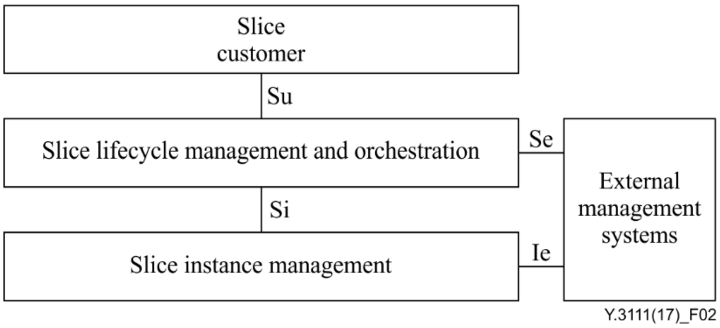
Slice customer
Su
Slice lifecycle management and orchestration
Se
External management systems
Si
Slice instance management
Ie
Y.3111(17)_F02

Figure 2 – Slice lifecycle management and orchestration functional relationship

Functional components specified in clauses 8 and 9 are decomposed into functional elements that represent a logical functionality provided by the functional component, independent of any implementation.

8 IMT-2020 network slice lifecycle management and orchestration plane functional architecture

This clause describes detailed management functionality in the slice lifecycle management (SLM) functional component. Figure 3 shows its functional elements.

As described in clause 6, orchestration and management functionalities are defined in an integrated manner in the IMT-2020 slice lifecycle management functional component. Orchestration functionality are specified in the functional elements: slice capacity planning and optimization, 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. They work together to achieve the slice lifecycle management objectives. Detailed interactions among functional elements are defined in clause 11, IMT-2020 slice lifecycle management procedure.

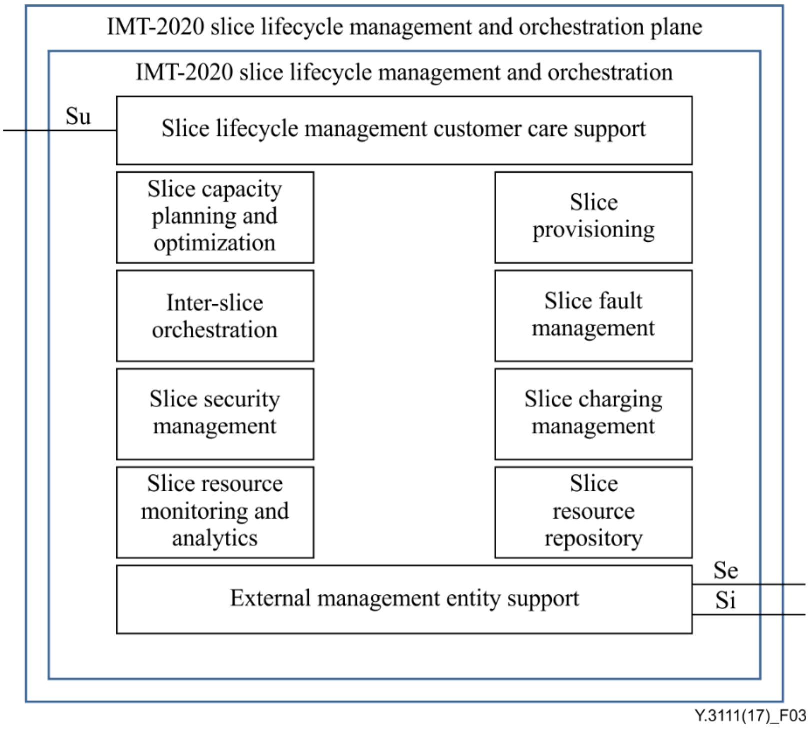
IMT-2020 slice lifecycle management and orchestration plane
IMT-2020 slice lifecycle management and orchestration
Su
Slice lifecycle management customer care support
Slice capacity planning and optimization
Slice provisioning
Inter-slice orchestration
Slice fault management
Slice security management
Slice charging management
Slice resource monitoring and analytics
Slice resource repository
External management entity support
Se
Si
Y.3111(17)_F03

Figure 3 – Slice lifecycle management and orchestration functional component

IMT-2020 slice lifecycle management customer care support

The IMT-2020 slice lifecycle management customer care support (SLM-CCS) functional element provides a standard interface to the slice lifecycle management functionality to its customers and applications. It supports requesting and receiving management operations and associated information in SLM.

The request from slice customer to create a slice includes the specific catalogue of service requirements on network slice, e.g., service type (eMBB, mIoT, URLLC, etc.), slice priority, slice sharing option.

NOTE 1 – Slice priority is used to indicate that a network slice with higher priority has the preference to obtain resources under circumstances of limited resources.

NOTE 2 – The slice sharing option is used to indicate whether a network slice can be shared with other customers.

Slice capacity planning and optimization

The slice capacity planning and optimization (SCPO) 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. It provides capabilities as follows:

- making planning decisions based on a slice catalog, available resources discovered by the slice resource monitoring and analytics functional element and customers' requests, slice sharing option and availability of existing or activated network slice instance;
- finding optimal available resource matches against a customer's request;
- monitoring and ensuring the quality of the provisioned slices and take the necessary actions (including re-provisioning or modification – e.g., scaling up/down – of the existing slice resource) if resource re-optimization is needed.

Slice provisioning

The slice provisioning (SP) functional element is responsible for provisioning requested slices by the customers and provides capabilities for:

- provisioning the requested slices by the customers;
- mapping and translating customer's high-level slice provisioning profile into technology-aware slice provisioning policies;
- managing provisioning policy lifecycle.

NOTE – Slice provisioning can involve interactions with the MANO network function virtualization (NFV) orchestrator, other NFV management systems, and/or software-defined network (SDN) controllers depending on the administration boundaries of the underlying slice resources. If the SP functional element provides full provisioning capabilities, the slice provisioning can be done internally by itself. If interactions with external provisioning functional entities are needed, it can be done through IMT-2020MPS functional element which is the interface to the external IMT-2020 management systems.

Inter-slice orchestration

The inter-slice orchestration (ISO) functional element is responsible for the orchestration of inter-slice matters and provides capabilities for:

- orchestrating multiple slices provisioning;
- resolving inter-slice quality, fault, anomaly, and charging issues.

Slice fault management

The slice fault management (SFM) functional element is responsible for the fault management of the provisioned slices and provides capabilities for:

- detecting anomalous events which cause failure of the provisioned slice resources;
- analysing a root cause of the failure of the provisioned slice resources;
- generating failure resolving policies and interact with SCPO functional element for the actual healing actions.

Slice security management

The slice security management (SSM) functional element is responsible for the security management of the provisioned slices and provides capabilities for:

- providing authentication and authorization capabilities of the provisioned slices;
- detecting and avoiding anomalous attacks of the provisioned slices.

Slice charging management

The slice charging management (SCM) functional element is responsible for the accounting management of the provisioned slices resource usage and provides capabilities for metering and reporting slice resource usage data for charging. Resource usage data can be metered per slice or per end-user/customer.

Slice resource monitoring and analytics

The slice resource monitoring and analytics (SRMA) functional element is responsible for collecting the status and events of the provisioned slice resources and analyzing them for the purpose of fault, quality, and security management and provides capabilities for:

- monitoring the activities, status, anomalous events of the application resources in the provisioned slices;
- analysing the monitored data and providing reports on the behaviour of the resources, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., resource usage data);
- storing and retrieving monitored data and analysis reports as logging records in the slice resource repository.

Slice resource repository

The slice resource repository (SRR) functional element is responsible for:

- storing the management information discovered by the SFM, SSM, SCM, and SRMA;
- storing the slice catalog, and slice related information from customer requests;
- managing the lifecycle of the information in the repository.

It provides capabilities for:

- storing and providing application program interfaces (APIs) to query the information in the repository;
- managing the lifecycle of the information in the repository (e.g., creation by storing, modification, deletion, etc.).

External management entity support

The external management entity support (EMES) functional element provides an interface to the external management system including IMT-2020 multi-plane management functional component for requesting and receiving management operations and associated information for slice management specific to a particular slice instance and to the external IMT-2020 management systems for provisioning and providing capabilities for:

- requesting and receiving slice instance specific operational status;

- requesting and receiving slice instance specific performance, fault, security related statistics and events;
- requesting and receiving slice provisioning requests and responses to/from the external IMT-2020 management systems.

9 IMT-2020 network slice instance management functional architecture

This clause specifies the network slice instance management functional architecture and components. Figure 4 shows a general network slice instance management plane functional architecture and relationship, interfaces with slice lifecycle management and orchestration functional component and external management systems.

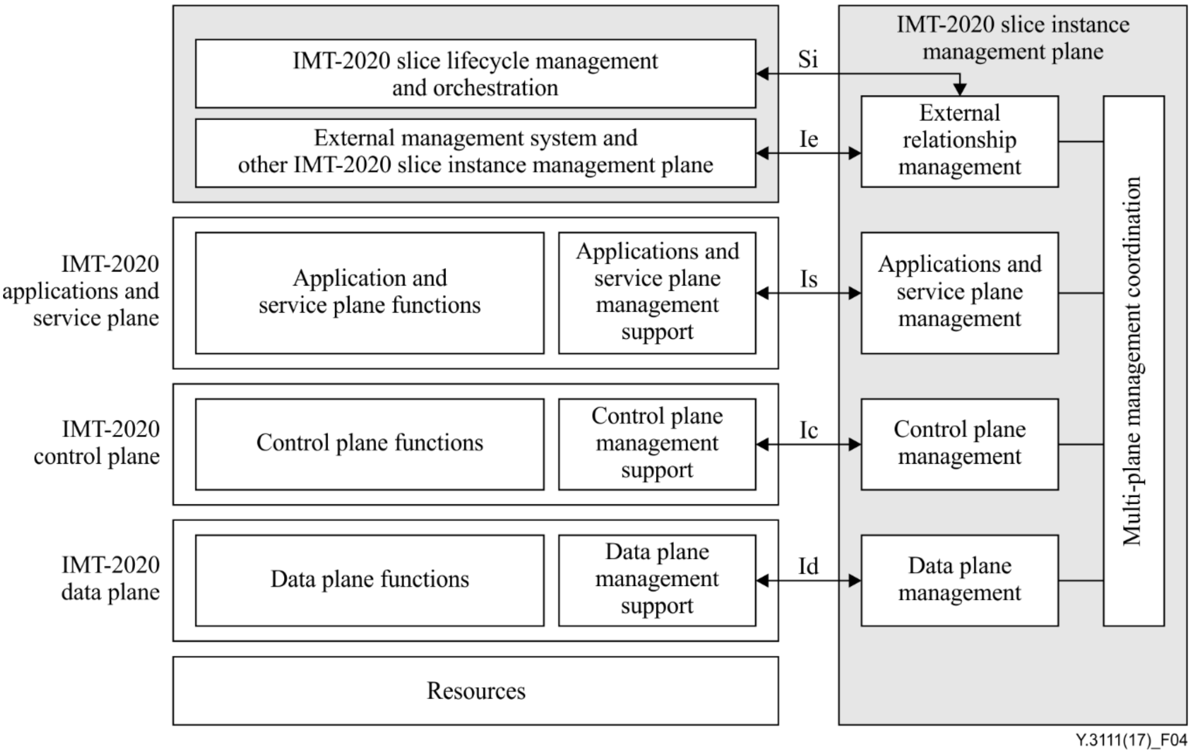
IMT-2020 slice lifecycle management and orchestration
External management system and other IMT-2020 slice instance management plane
IMT-2020 applications and service plane
Application and service plane functions
Applications and service plane management support
IMT-2020 control plane
Control plane functions
Control plane management support
IMT-2020 data plane
Data plane functions
Data plane management support
Resources
Si
Ie
Is
Ic
Id
IMT-2020 slice instance management plane
External relationship management
Applications and service plane management
Control plane management
Data plane management
Multi-plane management coordination
Y.3111(17)_F04

Figure 4 – IMT-2020 network slice instance management functional architecture

The remaining part of this clause specifies the details of each management functional components.

9.1 Applications and service plane management functional component

The applications and service plane management (A&SPM) monitors end-to-end network service assurance such as bandwidth, latency, etc., to meet the customer service requirements. It also manages applications healthiness if applications are supported in a slice instance. A&SPM provides services and assures network performance to customers. It also performs billing management based on the accounting and charging information provided by the data plane (DP) and the control plane (CP). Overall, customer key performance indicator (KPI) is established and managed through service management.

The following clause describes detailed management functionality in the application and service plane management (A&SPM) functional component. Figure 5 shows its functional elements.

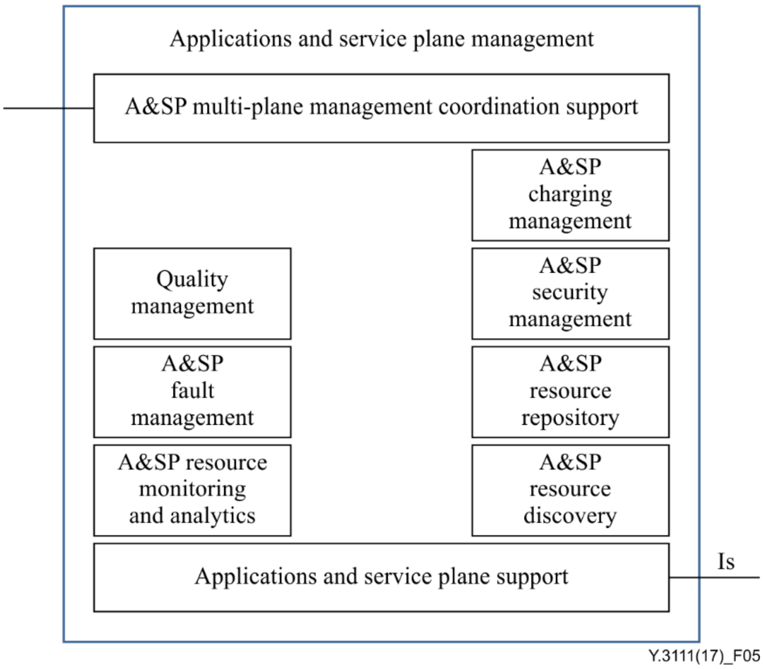
Applications and service plane management
A&SP multi-plane management coordination support
A&SP charging management
Quality management
A&SP security management
A&SP fault management
A&SP resource repository
A&SP resource monitoring and analytics
A&SP resource discovery
Applications and service plane support
Is
Y.3111(17)_F05

Figure 5 – Application and service plane management functional component

Applications and service plane support

The IMT-2020 applications and service plane support (A&SP-S) functional element provides a standard interface to the A&SP management support for requesting and receiving management operations and associated information in A&SP.

Applications and service plane resource discovery

The applications and service plane resource discovery (A&SP-RD) functional element is responsible for discovering applications and service plane managed resources in the A&SP and provides capabilities for discovering applications and service managed resources in the A&SP of the managed IMT-2020 networks. The discovered resources are stored in the A&SP resource repository.

Applications and service plane resource monitoring and analytics

The applications and service plane resource monitoring and analytics (A&SP-RMA) functional element is responsible for collecting the status and events of A&SP managed resources and analyzing them for the purpose of fault, quality, and security management and provides capabilities for:

- monitoring the activities, status, anomalous events of the applications and service plane managed resources of the underlying IMT-2020 networks;
- analysing the monitored data and providing reports on the behaviour of the resources, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., resource usage data);
- storing and retrieving monitored data and analysis reports as logging records in the A&SP resource repository.

Applications and service plane resource repository

The applications and service plane resource repository (A&SP-RR) functional element is responsible for storing the management information discovered by the A&SP resource discovery and managing the lifecycle of the management information in the repository and provides capabilities for:

- storing and providing APIs for querying the management information discovered by the A&SP resource discovery;

- storing and providing APIs for querying the management information generated by the A&SP resource monitoring and analytics;
- lifecycle management of the management information in the repository (e.g., creation by storing, modification, deletion, etc.)

Applications and service plane fault management

The application and service plane fault management (A&SP-FM) functional element is responsible for fault management of the A&SP and provides capabilities for:

- detecting anomalous events which cause failure of the A&SP resources;
- analysing a root cause of the failure of the A&SP resources;
- generating failure resolving policies and interact with control and provisioning functional components for the actual healing actions.

Applications and service plane quality management

The applications and service plane quality management (A&SP-QM) functional element is responsible for ensuring the performance of the A&SP managed resources and provides capabilities for:

- monitoring and ensuring the quality of the A&SP applications and service managed resources based on the given KPIs.

Applications and service plane security management

The applications and service plane security management (A&SP-SM) functional element is responsible for security management of A&SP and provides capabilities for

- providing authentication and authorization capabilities of A&SP;
- detecting and avoiding anomalous attacks of A&SP.

Applications and service plane charging management

The applications and service plane charging management functional element is responsible for the accounting management of A&SP and provides capabilities for metering and reporting applications and service managed resource usage data for charging. Resource usage data can be metered per application/service or per end-user/customer.

Applications and service plane multi-plane management coordination support

The application and service plane multi-plane management coordination support (A&SP-MMCS) functional element provides an internal interface to the multi-plane management coordination support functional element in the MPMC for requesting and receiving management operations and associated information for multi-plane management coordination specific to applications management.

9.2 Applications and service plane management support functional component

The applications and service plane management support (A&SP-MS) functional component provides management support of functional components of the applications and service plane (A&SP) and – if delegated by the multi-plane management functional component (MPM) – the management of the applications and service plane functions and resources based on the policies provided by the MPM. The A&SP-MS functional component also keeps track of the overall state of allocated and available resources in the A&SP to meet the objective of the slice instance healthiness. If applications are not supported in the slice instance, the management support of applications is out of the scope of this functional component.

9.3 Control plane management functional component

This following clause describes detailed management functionality in the control plane management (CPM) functional component. Figure 6 shows its functional elements.

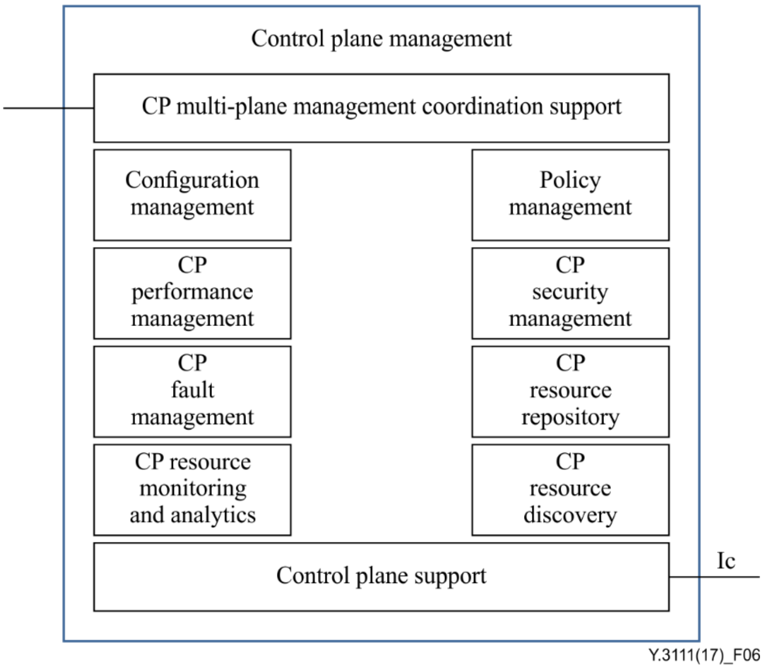

Figure 6 – Control layer management functional components

Control plane support

The control plane support (CP-S) functional element provides a standard interface to the CP management support for requesting and receiving management operations and associated information in CP.

Control plane resource discovery

The control plane resource discovery (CP-RD) functional element is responsible for discovering the control plane managed resources and provides capabilities for:

- discovering the control plane managed resources in the managed IMT-2020 networks. The discovered resources are stored in the CP-resource repository.

Control plane resource repository

The control plane resource repository (CP-RR) functional element is responsible for storing the managed resource discovered by the CP-RD functional element and managing their lifecycle in the repository and provides capabilities for:

- storing and providing APIs for querying the managed resources discovered by the CP-RD functional element;
- storing and providing APIs for querying the managed resources generated by the CP-RMA functional element;
- lifecycle management of the managed resources in the repository (e.g., creation by storing, modification, deletion, etc.).

Control plane resource monitoring and analytics

The control plane resource monitoring and analytics (CP-RMA) functional element is responsible for collecting the status and events of CP managed resources and analysing them for the purpose of performance, fault, and security management and provides capabilities for:

- monitoring the activities, status, anomalous events of the CP managed resources of the underlying IMT-2020 networks;
- analysing the monitored data and providing reports on the behavior of the managed resources, which can take the form of alerts for behavior which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., resource usage data);
- storing and retrieving monitored data and analysis reports such as logging records in the CP resource repository.

Control plane configuration management

The control plane configuration management (CP-CM) functional element is responsible for configuration management of the CP and provides capabilities for:

- provisioning CP managed resources;
- scaling in/out of CP managed resources based on the demand and availability.

Control plane fault management

The control plane fault management (CP-FM) functional element is responsible for the fault management of the CP and provides capabilities for:

- detecting anomalous events which cause failure of the CP managed resources;
- analysing a root cause of the failure of the CP managed resources;
- generating failure resolving policies and interact with control and provisioning functional components for the actual healing actions.

Control plane performance management

The control plane performance management (CP-PM) functional element is responsible for ensuring performance of the CP managed resources and provides capabilities for monitoring and ensuring performance of the CP managed resources based on the given KPIs.

Control plane security management

The control plane security management (CP-SM) functional element is an optional functional element. It is responsible for the security management of CP and provides capabilities for:

- providing authentication and authorization capabilities of CP;
- detecting and avoiding anomalous attacks against CP;
- providing APIs for querying the management information discovered by the CP-RD;
- providing APIs for querying the management information generated by the CP-RMA.

Control plane policy management

The control plane policy management (CP-PoM) functional component provides capabilities to define, store and retrieve policies that apply to CP functions. Policies can include business, technical, security, privacy and certification policies that apply to CP functions and their usage by IMT-2020 applications.

Some policies can be general and apply to a CP function irrespective of the IMT-2020 application concerned. Other policies can be specific to a particular IMT-2020 application.

Control plane multi-plane management coordination support

The control plane multi-plane management coordination support (CP-MMCS) functional element provides an internal interface to the multi-plane coordination support functional element in the MPMC functional component for requesting and receiving management operations and associated information for multi-layer coordination specific to control plane management.

9.4 Control plane management support functional component

The control plane management support (CP-MS) functional component provides management support of functional components of the control plane and – if delegated by the multi-plane management functional component (MPM) – the management of control plane functions and resources based on the policies provided by the MPM. The CP-MS functional component also keeps track of the overall state of allocated and available resources in the CP to meet the objective of the slice instance healthiness.

9.5 Data plane management functional component

The data plane management (DPM) functional component manages physical and virtual data plane functions and associated resources including compute, storage, and configuration information. It provides complete visibility into the physical state of the data plane and its resource at any given time. Handling many devices is achieved providing both device-centered perspective and network-wide perspective. Connectivity is established over the data plane and resource through its management. All device accesses pass through data plane management such that access and catalogue real-time status information about physical and virtual data plane functions and resource is available at all times. The state of every physical and virtual data plane functions and resource connection is reported whether or not it is connected, how much bandwidth it can carry and the type with corresponding mapping and alarming. It manages the entire physical layer, mapping routes, issuing work orders, reserving available ports, reporting on flow/path information and other physical and virtual data plane functions.

DPM also supports instantiation of a virtual data function and validation. Validation and authorization of a virtual data function are handled in response to a network service request. Virtual resource is managed across operator's domain including distribution, reservation, and allocation for network service instances. It also collects usage information of virtual resources and feeds back the information for update.

This clause describes detailed management functionality in the DPM functional component. Figure 7 shows its functional elements.

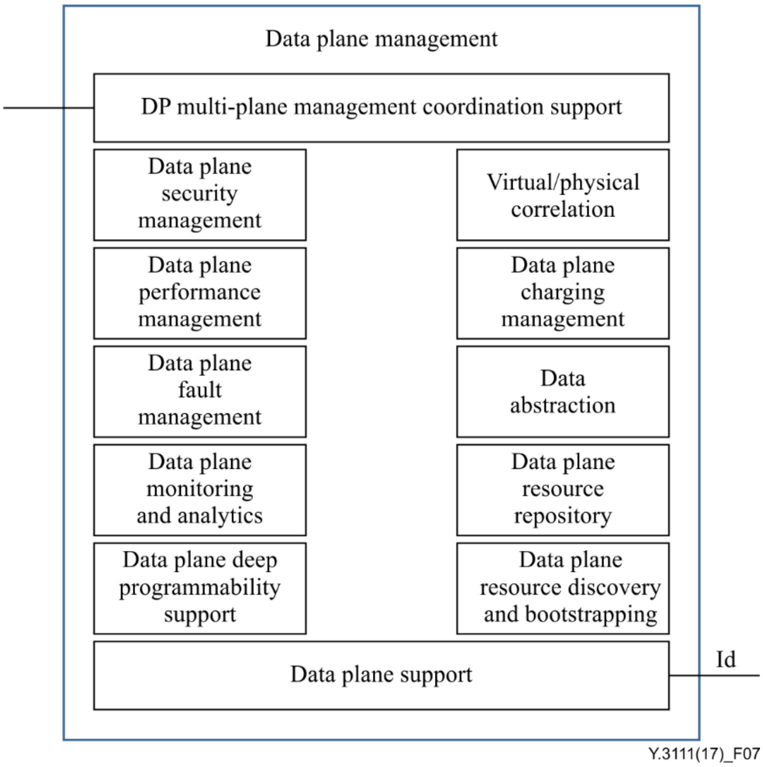
Data plane management
DP multi-plane management coordination support
Data plane security management
Virtual/physical correlation
Data plane performance management
Data plane charging management
Data plane fault management
Data abstraction
Data plane monitoring and analytics
Data plane resource repository
Data plane deep programmability support
Data plane resource discovery and bootstrapping
Data plane support
Id
Y.3111(17)_F07

Figure 7 – Data plane management functional components

Data plane support

The data plane support (DP-S) functional element provides a standard interface to the DP management support in the DP for requesting and receiving management operations and associated information in the DP.

Data plane resource discovery and bootstrapping

The data plane discovery and bootstrapping (DP-DB) functional element is responsible for discovering and bootstrapping DP functions and managed resources and provides capabilities for:

- discovering technology specific physical and virtual data plane functions and managed resources. The discovered resources are stored in the DP resource repository. Note that CP is responsible for abstract DP managed resource discovery which is common across any underlying heterogeneous technology specific DP;
- bootstrapping of physical and virtual data plane functions to make them ready for operation based on the bootstrapping policies.

Data plane resource repository

The data plane resource repository (DPR-R) functional element is responsible for storing the DP functions and managed resource discovered by the DPR-DB and managing the lifecycle of the stored management information in the repository and provides capabilities for:

- storing and providing APIs for querying the DP functions and managed resources discovered by the DPR-DB;
- storing and providing APIs for querying the management information generated by the DPR-MA;
- lifecycle management of the management information in the repository (e.g., creation by storing, modification, deletion, etc.).

Physical data abstraction

The physical data abstraction (PDA) functional element is responsible for generating abstractions of technology specific physical managed resources into technology independent common information and provides capabilities for:

- converting device dependent managed resource data into independent abstracted information;
- storing abstracted information in DPR-R and providing APIs to other functional components which need abstraction information.

Virtual data abstraction

The virtual data abstraction (VDA) is responsible for generating abstractions of technology specific virtual resources into technology independent common information and provides capabilities for:

- converting device dependent resource data into independent abstracted information;
- storing abstracted information in DP-R and providing APIs to other functional components which need abstraction information.

Virtual/physical correlation

The virtual/physical correlation (VPC) functional element is responsible for correlating the relationship between virtual and physical managed resources in DP-R and provides the following capabilities for:

- identifying correlation information among virtual and physical managed resources in the underlying IMT-2020 networks for efficient provisioning, performance monitoring and fault detection and root-cause analysis;
- identifying correlation information between virtual and physical flows for charging purpose;
- storing correlation information in a DPR-R and providing programming interfaces to other functional components which need correlation information.

Data plane monitoring and analytics

The data plane monitoring and analytics (DP-MA) functional element is responsible for collecting the status and events of DP functions and managed resources and analysing them for the purpose of FCAPS and provides capabilities for:

- monitoring the activities, status, anomalous events of the physical and virtual DP functions and managed resources in the IMT-2020 networks;
- analysing the monitored data and providing reports on the behavior of the DP functions and managed resources, which can take the form of alerts for behavior which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., resource usage data);
- storing and retrieving monitored data and analysis reports as logging records in the DPR-R functional element.

Data plane fault management

The data plane fault management (DP-FM) functional element is responsible for the fault management of the DP and provides capabilities for:

- detecting anomalous events which cause failure of the DP;
- analysing a root cause of the failure including the correlated event among DP;
- generating failure resolving policies and interact with control and provisioning functional components for the actual healing actions.

Data plane performance management

The data plane performance management (DP-PM) functional element is responsible for ensuring the performance of the DP including energy-aware data plane & resource management and provides capabilities for:

- monitoring and ensuring the performance of the physical and virtual data plane functions and managed resources based on the given KPIs;
- estimating the total energy consumption costs of DP (physical and virtual nodes and links) with the monitored DKP status information;
- calculating energy efficient optimal DP mapping based on the current estimated total energy consumption costs and the requested KPI.

Data plane security management

The data plane security management (DP-SM) functional element is an optional functional element responsible for the security management of the DP and provides authentication and authorization capabilities and detecting and avoiding anomalous attacks of physical data plane & resources.

Data plane charging management

The data plane charging management (DP-CM) functional element is responsible for accounting and charging management of DP and provides capabilities for:

- metering and reporting DP manged resource usage data for charging. It can be metered per flow or aggregated flows of physical links.

Data plane multi-plane management coordination support

The data plane multi-plane management coordination support (PDPR-MMCS) functional element provides an internal interface to the multi-plane coordination support functional element in the MPMC functional component for requesting and receiving management operations and associated information for multi-layer coordination specific to resource layer management.

9.6 Date plane management support functional component

The data plane management support (DP-MS) functional component provides management support of functional components of the data plane (DP) and – if delegated by the multi-plane management functional component (MPM) – the management of data plane functions and resources based on the policies provided by the MPM. The DP-MS functional component also keeps track of the overall state of allocated and available resources in the DP to meet the objective of the slice instance healthiness.

9.7 Multi-plane management coordination functional component

The multi-plane management coordination functional component (MPMC) manages automated arrangement, coordination, and management of both physical and virtual networks, control service, and application managed resources. Physical and virtual network resources are coordinated in a manner best suited to match the network constraints specified by other management plane components. Dynamic resource selection is determined based on the current physical and virtual network management status information. It ensures optimized allocation of the necessary managed resources and the connectivity for the best suited service information from service management. Based on managed resource availability and load, it coordinates related managed resources to assure the network management direction. Therefore, it plays the key role in management plane for IMT-2020.

This clause describes detailed management functionality in the slice lifecycle management support (MMC-SLMS) functional component. Figure 8 shows its functional elements.

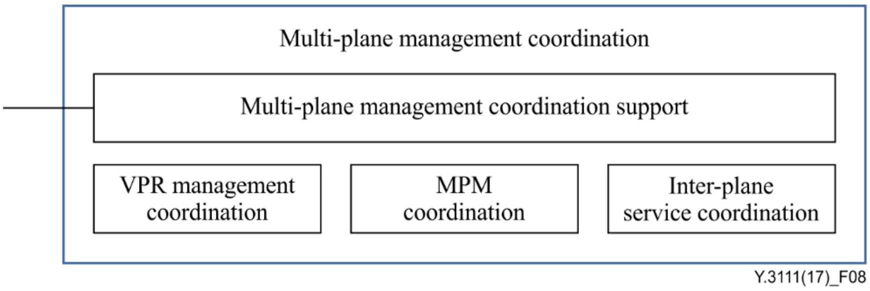
Multi-plane management coordination
Multi-plane management coordination support
VPR management coordination
MPM coordination
Inter-plane service coordination
Y.3111(17)_F08

Figure 8 – Functional elements of multi-plane management orchestration

Multi-plane management coordination support

The multi-plane management coordination support (MMCS) functional element provides an internal interface to the multi-plane coordination support functional element in the A&SPM, CPM, DPM functional components for requesting and receiving management operations and associated information for multi-plane coordination.

Virtual/physical resource management coordination

The virtual/physical resource management coordination (VPR-MC) functional element provides coordination in terms of monitoring, analysis, configuration, and inter-plane slice instance resource optimization of the virtual and physical managed resources that reside in A&SP, CP, and DP.

Multi-plane management functions coordination

The multi-plane management functions coordination (MMFC) functional element provides the functionality for supporting the lifecycle management of IMT-2020 application/network services across the entire IMT-2020 operator's domain (e.g., multiple IMT-2020 access and core networks, data centres interconnected by a wide area network (WAN) transport network, etc.).

Inter-plane service coordination

The inter-plane service coordination (IPSC) functional element provides the coordination of multi-plane managed resource management. It coordinates management operations among AS&P, CP, and DP, especially relationship among virtualized and physical resource across multi-plane scope. Some examples include: coordination for a multi-plane virtual to physical resource fault correlation, coordination for scale-in and scale-out of the control element (e.g., controller instances) depending on the traffic demand changes in the underlying data plane.

9.8 External relationship management functional component

This clause describes detailed management functionality in the external relationship management (ERM) functional component. Figure 9 shows its functional elements.

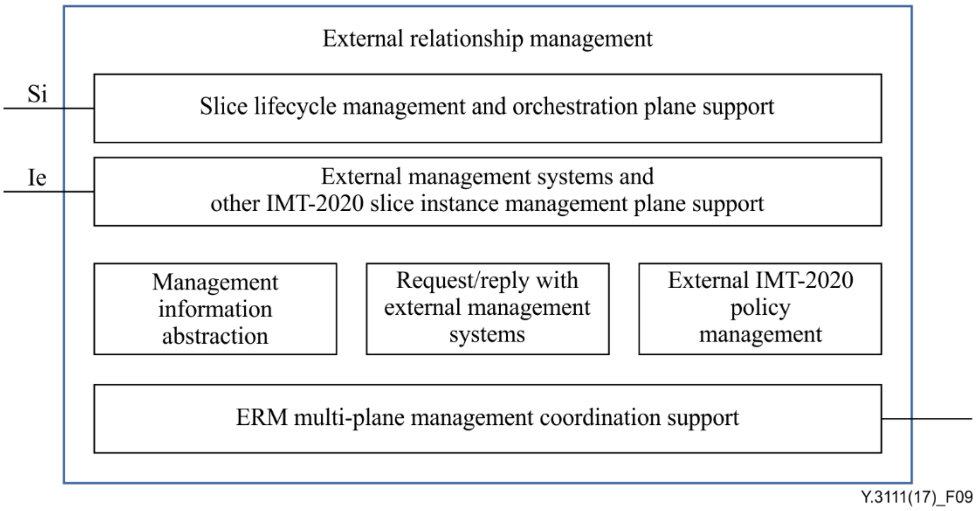
External relationship management
Si
Slice lifecycle management and orchestration plane support
Ie
External management systems and other IMT-2020 slice instance management plane support
Management information abstraction
Request/reply with external management systems
External IMT-2020 policy management
ERM multi-plane management coordination support
Y.3111(17)_F09

Figure 9 – External relationship management functional components

The external relationship management functional component provides management functionality to interwork with external management entities. External management entities can be a slice lifecycle management and orchestration plane, IMT-2020 SIMP in other IMT-2020 domain, 2G/3G/LTE OSS/BSS, MANO, cloud management entities, or other management functionality which can be defined in the future. The ERM plays the role of representative interface of IMT-2020 management toward the external management entities. Its main functionality includes abstraction of IMT-2020 management information for the exchange and request/reply of management operations with external management entities. It can be used for external IMT-2020 policy management, data analytics, charging, etc.

Slice lifecycle management and orchestration plane support

The slice lifecycle management and orchestration plane support (SLMOPS) functional element provides a standard interface to a SLMOP for requesting and receiving management operations and associated information. It communicates with SLMOP to receive requests from SLM on specific management requests and respond with the results of the requested management operation. Examples of such operations are the current slice instance managed resource status, performance statistics, any fault or security related events, etc.

External management systems and other IMT-2020 slice instance management plane support

The external management systems and other IMT-2020 slice instance management plane support (EMS-SIMPS) functional element provides a standard interface to an external management systems or an IMT-2020-SIMP in other IMT-2020 domain for requesting and receiving management operations and associated information.

Management information abstraction

The management information abstraction (MIA) functional element provides for the abstraction of IMT-2020 management information for the exchange with external management entities or IMT-2020-SIMP in other IMT-2020 domains for inter-domain management information hiding purpose.

Request/Reply with external management

The request/reply with external management (RREM) functional element provides functionality associated with request/reply management operations with external management entities.

The external IMT-2020 policy management (EIPM) functional element provides external IMT-2020 policy exchanges involved between IMT-2020-SIMP and external management systems, data analytics, and charging.

ERM multi-plane management coordination support

The ERM multi-plane management coordination support (ERM-MMOSMMCS) functional element provides an internal interface to the multi-plane coordination support functional element in the multi-plane management coordination functional component for the purpose of inter-domain orchestration between IMT-2020-SIMP and external management systems and/or IMT-2020-SIMP in other IMT-2020 domains.

10 Reference points

NOTE – By default, all information components in an information flow defined in clause 9 are to be considered "mandatory" unless they are explicitly identified as being "optional".

10.1 Reference point Su

The Su reference point is required to enable slice instance provisioning request/response information needed for IMT-2020 network slice lifecycle management customer care to be exchanged between customer(s) and the external relationship management functional element in the management plane of the IMT-2020 network slice instance (SI).

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

10.1.1 Functional requirements

10.1.1.1 Slice lifecycle management customer care functional requirements

The Su reference point provides the ability to make requests/responses between the customer and SLM-CS in SLM for:

- network slice creation;
- a status report of slice creation.

10.1.1.2 Slice lifecycle management customer care session processing functional requirements

To assure the reliability and performance of slice lifecycle management customer care session operations across Su reference point, the following capabilities are required:

Overload control: The Su reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between the customer and SLM-CS.

Synchronization and audit: The Su reference point is required to provide the capability to support the synchronization and audit of the slice lifecycle management customer care session status in support of the recovery and operational information statistics and auditing.

Session state maintenance: The Su reference point is required to be able to maintain the session state using either soft-state or hard-state approaches.

10.1.2 Information exchange requirements

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

Request-response transactions: The reference point is required to allow the customer to request a transaction to be performed by the SLM-CS and to 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 planes.

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

Capabilities: Each plane is required to be able to determine the capabilities of the appropriate corresponding instance when requesting slice lifecycle management customer care functions.

Security: The Su is required to support the authentication between two planes so that requests from unauthenticated sources will not be performed and as such each plane 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 customer is required to be able to communicate with multiple SLM-CSs; 2) many-to-one mode: multiple customer instances are required to be able to make requests to a given SLM-CS.

10.1.3 Information components

The information components exchanged across the Su reference point are categorized in Table 1.

Table 1 – Information components for reference point Su

Information component	Description
User identifier	A unique identifier for different instances of the customers within the same administrative domain of a single requestor.
Slice instance provisioning session identifier	An identifier for the session for which the slice instance provisioning requests are sent to the SLM-CS. The identifier has to be unique within the same Customer instance.
Globally unique IP address information (Optional)	A set of IP address information used for locating the client network in which the client is requesting the slice instance provisioning.
– Unique IP address	The IP address for identifying the application.
– Address realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID).
Slice instance provisioning requestor identifier	An identifier for the requestor (i.e., the owner of customer) of slice instance provisioning service. It is unique over the requestors sending requests for the slice instance.
Slice instance provisioning request priority (Optional)	The indication of the importance of a slice instance provisioning request. It can be used for processing simultaneous requests by SLM-CS based on the priority level.
Reservation holding time (Optional)	The value of time interval for which the slice instance is provisioned.
Slice instance provisioning request result	Indication of the result for a slice instance provisioning request (includes both synchronous and scheduled request result).
EventNotify	Allows SRCM-FE to send notification to the user plane for an event that may need the user plane to take the appropriate action for the requested resource reservation.
Catalogue of service requirement	It identifies the detailed service requirement to requested network slice, including but not limited to: service scenario (e.g., eMBB, mIoT, URLLC); network capability requirement (e.g., high mobility support, non-IP transport support); capacity requirement (maximum connections); bandwidth requirement (e.g., users experience rate); slice priority; slice sharing option.

10.2 Reference point Si

The Si reference point is required to enable request/response information needed for IMT-2020 network slice instance lifecycle 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 lifecycle management (SLM) and the external relationship management functional component (ERM) in the management plane of SI.

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

10.2.1 Functional requirements

10.2.1.1 Slice instance lifecycle management functional requirements

The Si reference point provides the ability to make requests/responses between EMES in 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;
- a status report of slice provisioning, performance, fault, charging, and security events.

10.2.1.2 Slice instance lifecycle management session processing functional requirements

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

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

Synchronization and audit: The Si reference point is required to provide the capability to support the synchronization and audit of the slice instance lifecycle management session status in support of recovery and operational information statistics and auditing.

Session state maintenance: The Si reference point is required to be able to maintain the session state using either soft-state or hard-state approaches.

10.2.2 Information exchange requirements

This clause provides a brief description 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 planes.

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

Capabilities: Each plane is required to be able to determine the capabilities of the appropriate corresponding instance when requesting slice instance lifecycle management functions.

Security: The Se is required to support the authentication between two planes such that requests from unauthenticated sources will not be performed and such that each plane 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.

10.2.3 Information components

The information components exchanged across the Se reference point are categorized in Table 2.

Table 2 – 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.
Identity identification	Specifies unique identification. It adopts only the International Alphabet No. 5 string format defined in the [b-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 a 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 a 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 to send notification to the ERCM for an event that may need the ERCM to take the 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.

10.3 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 external management entity support functional element (EMES) in the management and orchestration plane of the IMT-2020 network slice lifecycle management (SLM) and external management entities (MANO, OSS/BSS, etc.).

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

10.3.1 Functional requirements

10.3.1.1 Communication of a slice lifecycle management and orchestration plane with external management entities functional requirements

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

- network slice management interworking and orchestration;
- a status report of interworking and orchestration requests.

10.3.1.2 Communication of a slice lifecycle management and orchestration plane with external management entities session processing functional requirements

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

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

Synchronization and audit: The Se reference point is required to provide the capability to support synchronization and audit of the communication of a slice instance with 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 be able to maintain the session state using either soft-state or hard-state approaches.

10.3.2 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 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 also vice versa.

Notifications: The reference point is required to support the notification of asynchronous events between two planes.

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

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

Security: The Ie is required to support the authentication between two planes such that requests from unauthenticated sources will not be performed and such that each plane can verify the source of the 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 EMESs are required to be able to make requests to a given external management entity.

10.3.3 Information components

The information components exchanged across the Se reference point are categorized in Table 3:

Table 3 – Information components for reference point Se

Information component	Description
User identifier	A unique identifier for different instances of the IMT-2020 slice lifecycle management and orchestration plane within the same administrative domain of a single requestor.
Authentication information	Authenticates the peers (i.e., IMT-2020 slice lifecycle 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 the management interworking profile information required for an exchange of management information between EMES and the external management entity.
EventNotify	Allows IMT-20202 management plane to send notification to the external management entities for an event that may need the external management entities to take the appropriate actions.

10.4 Reference point Ie

The Ie 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 ERM in SI and external management entities (MANO, OSS/BSS, etc.).

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

10.4.1 Functional requirements

10.4.1.1 Communication of a slice instance with external management entities functional requirements

The Ie reference point provides the ability to make requests/responses between EMIS in ERM and external management entities for:

- network slice management interworking and orchestration;
- a status report of interworking and orchestration requests.

10.4.1.2 Communication of a slice instance with external management entities session processing functional requirements

To assure the reliability and performance of communication of a slice instance with external management entities session operations across Ie reference point, the following capabilities are required:

Overload control: The Ie reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between EMIS and external management entities.

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

Session state maintenance: The Ie reference point is required to be able to maintain the session state using either soft-state or hard-state approaches.

10.4.2 Information exchange requirements

This sub-clause provides a brief description of the information exchange requirements for the Ie reference point.

Request-response transactions: The reference point is required to allow EMIS to request a transaction to be performed by the external management entity and to 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 planes.

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

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

Security: The Ie is required to support the authentication between two planes so that requests from unauthenticated sources will not be performed and as such each plane 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 EMIS is required to be able to communicate with multiple external management entities; 2) many-to-one mode: multiple EMISs are required to be able to make requests to a given external management entity.

10.4.3 Information components

The information components exchanged across the Ie reference point are categorized in Table 4:

Table 4 – Information components for reference point Ie

Information Component	Description
User identifier	A unique identifier for different instances of the IMT-2020 management plane within the same administrative domain of a single requestor.
Authentication information	Authenticates the peers (i.e., IMT-2020 management plane and external management system).
Management interworking profile identifier	A unique management interworking profile identifier required for an exchange of management information between EMIS and external management entity.
Management interworking profile	Describes management interworking profile information required for an exchange of management information between EMIS and external management entity.
EventNotify	Allows IMT-20202 management plane to send notification to the external management entities for an event that may need the external management entities to take the appropriate actions.

10.5 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 ASP-S of application and service plane management (ASPM) in SI and application and service plane (ASP) in SI.

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

10.5.1 Functional requirements

10.5.1.1 Network slice application and service plane management functional requirements

The Is reference point provides the ability to make requests/responses between ASP-S in ASPM and management support, softwarization and orchestration (MSO) in ASP for:

- network slice application and service plane management;
- a status report of slice application and service plane management actions.

10.5.1.2 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 Is reference point, the following capabilities are required:

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

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

Session state maintenance: The Is reference point is required to be able to maintain the session state using either soft-state or hard-state approaches.

10.5.2 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 ASP-S to request a transaction to be performed by MSO in ASP 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 planes.

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

Capabilities: Each plane 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 planes so that requests from unauthenticated sources will not be performed and as such each plane 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 ASP-S is required to be able to communicate with multiple MSOs; 2) many-to-one mode: multiple ASP-Ss are required to be able to make requests to a given MSO in ASP.

10.5.3 Information components

The information components exchanged across the Is reference point are categorized in Table 5.

Table 5 – 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 requestor
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)
Management operation requestor identifier	An identifier for the requestor (i.e., the owner of ASP-S in ASPM) of application and service plane management service. It is unique over the requestors 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.
Management operation request result	Indication of the result for a management operation request (includes both synchronous and scheduled request result).
EventNotify	Allows the application and service plane to send notifications to ASP-S for an event that may need to take the appropriate action for the requested management operations.

10.6 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 CP-S of control plane management (CPM) in SI and control plane (CP) in SI.

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

10.6.1 Functional requirements

10.6.1.1 Network slice control plane management functional requirements

The Ic reference point provides the ability to make requests/responses between CP-S in CPM and management support, softwarization and orchestration (MSO) in CP for:

- network slice control plane management;
- a status report of slice control plane management actions.

10.6.1.2 Network slice control plane management session processing functional requirements

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

Overload control: The Ic reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between CP-S and MSO in CP.

Synchronization and audit: The Is reference point is required to provide the capability to support 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 be able to maintain the session state using either soft-state or hard-state approaches.

10.6.2 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 CP-S to request a transaction to be performed by MSO in CP 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 planes.

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

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

Security: The Ic is required to support the authentication between two planes so that requests from unauthenticated sources will not be performed and as such each plane 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 MSOs in CP; 2) many-to-one mode: multiple CP-Ss are required to be able to make requests to a given MSO in CP.

10.6.3 Information components

The information components exchanged across the Ic reference point are categorized in Table 6.

Table 6 – 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 requestor.
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.
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 requestor identifier	An identifier for the requestor (i.e., the owner of CP-S in CPM) of control plane management service. It is unique over the requestors sending requests for the CPM.

Table 6 – Information components for reference point Ic

Information component	Description
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.
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 CP-S for an event that may need to take the appropriate action for the requested management operations.

10.7 Reference point Id

The Ic 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 PDPR-S/VDPR-S of virtual/physical data plane and resource management (VPDPRM) in SI and data plane (DP) in SI.

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

10.7.1 Functional requirements

10.7.1.1 Network slice data plane management functional requirements

The Id reference point provides the ability to make requests/responses between PDPR-S/VDPR-S in VPDPRM and management support and softwarization (MS) a status report of slice data plane management actions.

10.7.1.2 Network slice data plane management session processing functional requirements

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

Overload control: The Id reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between PDPR-S/VDPR-S and MS of DP in SI.

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

Session state maintenance: The Id reference point is required to be able to maintain the session state using either soft-state or hard-state approaches.

10.7.2 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 PDPR-S/VDPR-S to request a transaction to be performed by MS in DP and to 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 planes.

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

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

Security: The Id is required to support the authentication between two planes so that requests from unauthenticated sources will not be performed and as such each plane 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 PDRF-S/VDPR-S is required to be able to communicate with multiple MSs in DP; 2) many-to-one mode: multiple PDRF-S/VDPR-Ss are required to be able to make requests to a given MS in DP.

10.7.3 Information components

The information components exchanged across the Id reference point are categorized in Table 7:

Table 7 – 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 requestor.
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.
– 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 requestor identifier	An identifier for the requestor (i.e., the owner of DP-S in DPM) of data plane management service. It is unique over the requestors 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.
Management operation request result	Indication of the result for a management operation request (includes both synchronous and scheduled request result).
EventNotify	Allows data plane to send notifications to the DP-S for an event that may need to take the appropriate action for the requested management operations.

11 IMT-2020 network slice lifecycle management and orchestration procedure

This clause describes a slice lifecycle management and orchestration procedure which is illustrated in Figure 10.

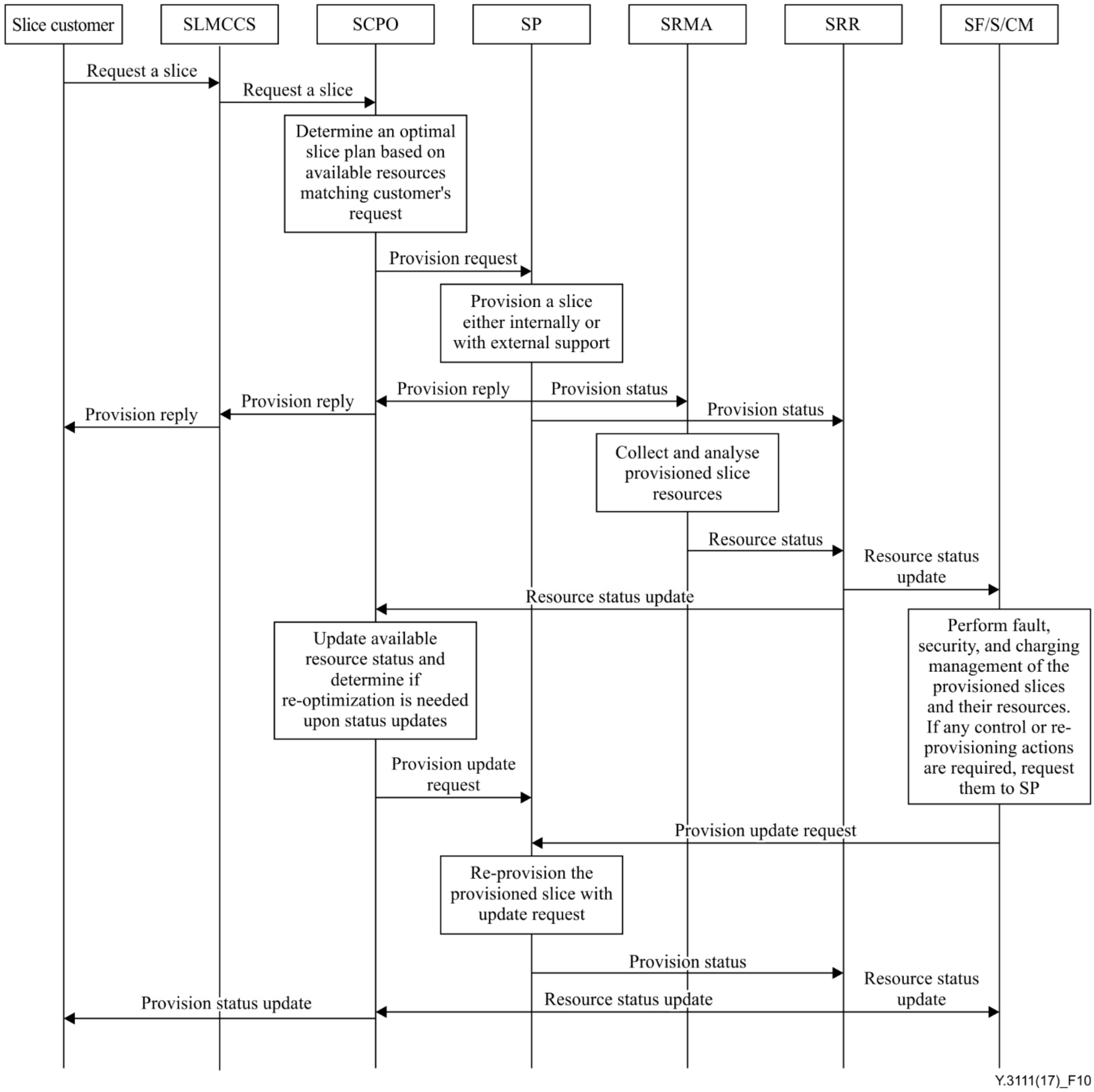
Slice customer
SLMCCS
SCPO
SP
SRMA
SRR
SF/S/CM
Request a slice
Request a slice
Determine an optimal slice plan based on available resources matching customer's request
Provision request
Provision a slice either internally or with external support
Provision reply
Provision status
Provision reply
Provision reply
Provision status
Collect and analyse provisioned slice resources
Resource status
Resource status update
Resource status update
Update available resource status and determine if re-optimization is needed upon status updates
Perform fault, security, and charging management of the provisioned slices and their resources. If any control or re-provisioning actions are required, request them to SP
Provision update request
Provision update request
Re-provision the provisioned slice with update request
Provision status
Resource status update
Provision status update
Resource status update
Y.3111(17)_F10

Figure 10 – Slice lifecycle management procedure

- The IMT-2020 customer requests a slice to be provisioned with its specified service requirements. The template for the slice provision is provided by the IMT-2020 service provider as a form of service requirement catalogue through its service portal, which includes, but is not limited to, service scenario (e.g., eMBB, mIoT, URLLC); network capability requirement (e.g., high mobility support, non-IP transport support); capacity requirement (maximum connections); bandwidth requirement (e.g., users experience rate); slice priority; slice sharing option.
- IMT-2020 slice lifecycle customer care support (SLMCCS) functional element receives the customer's request and carries it to the slice capacity planning and optimization functional element (SCPO). SCPO then determines an optimal slice plan based on the available resources which matches the customer's request. The detailed optimization algorithms based on resource is out of the scope of this Recommendation. If a customer prefers to request the shared network instance and there is the available instantiated network slice instance(s) meeting the customer's service requirement, an existing network slice instance will be provisioned by, e.g., configuring subscription information and scaling out the capacity. If a

customer prefers to request a dedicated network slice instance or there is no available network slice instance that meets the customer's service requirement, a new network slice instance will be provisioned.

- Once the provisioning policy is determined, SCPO requests provisioning to slice provisioning (SP) functional element. SP then performs the requested slice provisioning task. It involves various sub-tasks. If the 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, 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. 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. It also sends the status update to slice resource repository (SRR) to store the provisioned resource information.
- SRMA performs collection, monitoring, and analysis tasks of the provisioned slice resources. Data and information collected and analysed are then stored in SRR for further processing by other functional elements.
- 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 SCPO.
- When SCPO receives the notification, it updates available resource status and determines if re-optimization is needed upon status updates. Also SF/S/CM 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.
- 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 SF/S/CM, SCPO and IMT-2020 slice customer for resource status updates.

12 Security consideration

This clause describes security threats and potential attacks and defines security requirements for IMT-2020 network management and orchestration. The security requirements are based on [b-ITU-T Y.2701].

The type of generic threats and their applicability to IMT-2020 network management and orchestration are as follows:

Destruction of information: This threat refers to the deletion of information pertaining to IMT-2020 network management and orchestration operations, such as transaction state information, resource usage information, accounting information, topology information, or policy rules. An example of a potential consequence is that, if the information about the existence (or availability) of a particular resource has been destroyed, the resource effectively becomes unavailable.

Corruption or modification of information: This threat has three aspects:

1) Corruption of the recorded resource information (or policy rules) so that such data are rendered meaningless or unusable.

2) Undetected modification of the recorded resource information or policy rules so that such data appear to be meaningful. This can result in theft of service, degradation of service, loss of service, or fraudulent accounting, or any combination of the above.

3) Corruption or modification of a signalling message, with the same results as the above.

Theft, removal, or loss of information: This threat refers to the theft or loss of recorded resource information. It may result in 1) violation of a subscriber's privacy (in the case of theft of subscriber information), 2) theft of service and 3) degradation, interruption, and, ultimately, unavailability of service (in case of the loss of information).

Disclosure of information: This can take place because of the interception of the signalling messages or because of granting access to an illegitimate user. The consequence is the same as in the case of theft, removal, or loss of information.

Interruption of services: This threat is typically realized through a denial of service (DoS) attack. Such attacks can make the IMT-2020 network management and orchestration partially or totally unavailable.

The major security requirements for IMT-2020 network management and orchestration are:

1) To take into account the above security threats and supporting measures to counter relevant attacks.

2) To protect signalling exchange in support of resource requests and responses.

3) To protect the information contained in all IMT-2020 network management and orchestration functional components involved in this exchange.

4) To ensure the availability and overall expected performance of the IMT-2020 network management and orchestration functional components.

5) To prevent illegitimate access to IMT-2020 network management and orchestration functional components.

Appendix I

Further considerations on management and orchestration for IMT-2020

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

I.1 Clarification of management and orchestration for IMT-2020

It is essential to clarify the difference between management and orchestration for IMT-2020. A network architecture view of IMT-2020 combined network management and orchestration in a single plane.

In order to clarify the difference between orchestration and management, the implementation scenarios shown in Figures I.1 to I.3 are taken into account.

1) Orchestration and management will exist independently, with close collaborating relationship.

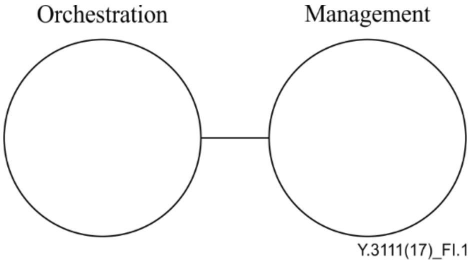

Figure I.1 – Independent orchestration and management

2) Among orchestration and management, one of them will include the other.

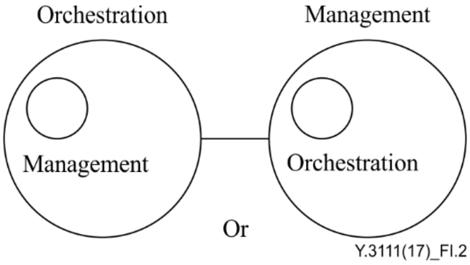

Figure I.2 – Management/orchestration includes the other

But, it might be reasonable to see the current status as an intersection type of relationship between them.

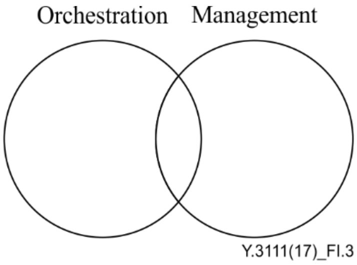

Figure I.3 – Orchestration and management with an intersection

Table I.1 shows particular contents to differentiate between the functions of orchestration and management.

Table I.1 – Difference between OCH and NMS

	Orchestration	Management
Monitoring purpose	Availability	Healthiness
Action purpose	Provisioning	Maintaining
Representative actions	Control/Configuration Create/Destroy/Move	Monitor/Alarm for event Detection/Isolation/Resolve for fault
Target resources	Dissimilar devices	Similar devices

Bibliography

[b-ITU-T Gap Analysis] Technical Report ITU-T Report on Standards Gap Analysis (2015), *Report on standards gap analysis*

[b-ITU-T T.50] Recommendation ITU-T T.50 (1992), *International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) – Information technology – 7-bit coded character set for information interchange*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-ITU-T Y.110] Recommendation ITU-T Y.101 (1998), *Global Information Infrastructure principles and framework architecture*.

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

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

[b-ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[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*.

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, 2017