International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3105

(12/2018)

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

Future networks

Requirements of capability exposure in the IMT-2020 network

Recommendation ITU-T Y.3105

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

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

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

Recommendation ITU-T Y.3105

Requirements of capability exposure in the IMT-2020 network

Summary

Recommendation ITU-T Y.3105 identifies requirements of capability exposure in the International Mobile Telecommunication 2020 (IMT-2020) network.

In particular, it first provides an overview and general aspects of capability exposure in the IMT-2020 network, and then identifies requirements for the following key network capabilities: network slicing management, edge computing (EC), network data analytics (NWDA), fixed and mobile convergence (FMC), and quality of service (QoS) capabilities.

The exposure of the IMT-2020 network capabilities will bring new opportunities to network operators, vendors and third parties. Relevant capability exposure scenarios in the IMT-2020 network are provided in an appendix.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3105	2018-12-14	13	11.1002/1000/13809

Keywords

5G, capability exposure, edge computing, fixed mobile convergence, IMT-2020, network data analytics, network slicing, parameters, requirements, QoS.

---

* 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

Recommendation ITU-T Y.3105

Requirements of capability exposure in the IMT-2020 network

1 Scope

This Recommendation identifies requirements of capability exposure in the International Mobile Telecommunication 2020 (IMT-2020) network.

In particular, it first provides an overview and general aspects of capability exposure in the IMT-2020 network, and then identifies requirements for the following key network capabilities: network slicing management, edge computing (EC), network data analytics (NWDA), fixed and mobile convergence (FMC) and quality of service (QoS) capabilities.

Relevant capability exposure scenarios in the IMT-2020 network are provided in Appendix I.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 IMT-2020 [b-ITU-T Y.3100]: Systems, system components, and related technologies that support to provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

NOTE – [b-ITU-R M.1645] defines the framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000 for the radio access network.

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

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

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

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

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

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

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

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

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

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

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

3.1.6 protocol data unit session [b-ITU-T Y.3100]: In the context of IMT-2020, an association between a user equipment (UE) and a data network that provides a protocol data unit (PDU) connectivity service.

NOTE – The type of the association includes IP type, non-IP type and Ethernet type.

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

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

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

3.1.8 user plane [b-ITU-T Y.2011]: A synonym for user plane.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AGV Automated Guided Vehicle

AN Access Network

API Application Programming Interface

DC Data Centre

EC Edge Computing

eMBB enhanced Mobile Broadband

FMC Fixed and Mobile Convergence

IMT-2020 International Mobile Telecommunication 2020

IoT Internet of Things

IP Internet Protocol

MM Mobility Management

NWDA Network Data Analytics

NSI Network Slice Instance

O&M Operation and Maintenance

OTT Over The Top

PCF Policy Control Function

PDU Protocol Data Unit

QoS Quality of Service

SLA Service-Level Agreement

SM Session Management

UE User Equipment

URLLC Ultra-Reliable and Low Latency Communications

VNO Virtual Network Operator

VoLTE Voice over Long-Term Evolution

VR Virtual Reality

WLAN Wireless Local Area Network

5 Conventions

In this Recommendation:

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

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

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

6 Overview of capability exposure in the IMT-2020 network

The IMT-2020 network is expected to bring some new and enhanced capabilities.

The exposure of the IMT-2020 network capabilities will bring new opportunities to network operators, vendors and third parties.

The IMT-2020 network is required to support the exposure of network capabilities accessible by third parties [ITU-T Y.3101]. The exposure of network capabilities is enabled by the exposure of network information and control function customization.

Key network capabilities that are expected to be exposed include, but are not limited to:

– network slicing management;
– edge computing (EC);
– network data analytics (NWDA);
– fixed and mobile convergence (FMC);

– quality of service (QoS).

7 Requirements of capability exposure in the IMT-2020 network

7.1 General aspects of capability exposure

7.1.1 Description

The IMT-2020 network provides various control functions, such as mobility management (MM), session management (SM), QoS control and charging, by using relevant information maintained within the IMT-2020 network operator domain. Such control and information in the IMT-2020 network may help third party applications and services to fine tune their operations, as the third party applications or services expected to be supported by the IMT-2020 are more and more diverse in terms of functional and performance requirements. For example, a third party service may track user location by exploiting the UE location exposed by the IMT-2020 network or it may change the expected transport QoS depending on usage patterns by customizing QoS control parameters of the traffic within the IMT-2020 network.

Capability exposure can consist of either exposing network information to third parties or customizing control functions on third party request.

The third parties are assumed to be properly authenticated and authorized to access the capability exposure functions of the IMT-2020 network.

Additionally, the use of application programming interfaces (APIs) by third parties is subject to network operator policies.

7.1.1.1 Exposing network information to third parties

The network information of the IMT-2020 network that can be exposed to third parties includes, but is not limited to, UE location, UE connectivity status, UE reachability and network status. This information can be provided to third parties via appropriate APIs.

NOTE – While the IMT-2020 network may manage a dedicated repository for the storage of the information to be exposed, this lies outside the scope of this Recommendation.

A third party can subscribe to specific events (e.g., loss of network connectivity of UE) so that, when some network information changes in the IMT-2020 network, the subscribed third party is notified by the IMT-2020 network.

7.1.1.2 Control functions customization on third party request

The control functions of the IMT-2020 network that can be customized by third parties include, but are not limited to, MM, SM and QoS control. The customization of the control functions can be done by third parties via provisioning of the relevant configuration parameters of the control functions (e.g., UE mobility patterns, communication characteristics and QoS parameters).

7.1.2 Requirements

The following are requirements applied to the IMT-2020 network concerning the exposure of capabilities:

The IMT-2020 network is required to support authentication and authorization of third parties that want to access the IMT-2020 network capability exposure functions.

The IMT-2020 network is required to provide APIs that allow authorized third parties to query and retrieve the exposed network information.

The IMT-2020 network is required to provide APIs that allow authorized third parties to subscribe to, and be notified of, a specific event concerning changes in exposed network information.

The IMT-2020 network is required to provide APIs that allow authorized third parties to provision exposed configuration parameters for customization of control functions.

7.2 Network slice management

7.2.1 Description

The flexibility and customization offered by network slicing can be reflected in the possibility of accommodating third party applications. In addition to the network functions provided by network operators, third party application deployment on network slice instances (NSIs) can also be envisaged in order to meet the requirements from tenants. Such third party applications could be provided directly from tenants or from non-tenant parties.

The deployment of third party applications may enable the support of services having third party specific requirements, such as the ultra-low latency requirement of ultra-reliable and low latency communications (URLLC) services.

The deployment of third party applications may also enable third party substitution of network functions, such as customized authentication and MM functionalities, which are designed especially to support third party own services. Other than control plane-related network functions, customized user plane network functions can also be deployed within the network slice.

7.2.1.1 Support of authorized third parties to create, modify and delete network slices

Network slicing is used in IMT-2020 networks to improve network flexibility to accommodate diverse service scenarios.

The IMT-2020 network allows a third party to create, modify and delete a network slice. Network operators can specify which network capabilities can be included in a network slice to support a given set of services.

For example, an Internet of things (IoT) service provider will require a dedicated network slice that supports IoT services and the network operator can create an IoT network slice according to the requirements of the IoT service provider, including capabilities, e.g., SM, MM for stationary UE, charging function without online charging or additional services like a short message service. On the other hand, an enhanced mobile broadband (eMBB) provider will require a network slice supporting eMBB services and the network operator can create an eMBB network slice including capabilities, e.g., SM, MM for UE with high mobility, online charging or additional services like voice over long-term evolution (VoLTE). One scenario related to network slice creation is provided in clause I.1.

Meanwhile, after a third party is assigned a network slice, it may further want to deploy new capabilities or upgrade the existing capabilities, e.g., update the network slice capacity.

The third party may also want to delete a network slice when it no longer needs to use it.

7.2.1.2 Support of authorized third parties to monitor the network slice state

After network operator creation of a customized network slice for a third party, it is necessary to have monitoring capabilities in the network slice management system in order for the third party to monitor the current state of the network slice.

For example, as the network operator may charge the third party for the network slice in use, it is important to allow the third party to monitor the state of the network slice in order to ensure that the third party obtains the network slice service provided, and charged, by the network operator.

7.2.1.3 Support of authorized third parties to adjust the network slice capacity

Based on third party service requirements, the IMT-2020 network allows the third party to create a network slice. However, this may be not enough for a third party. For example, after third party creation of a customized network slice, the third party may plan its business development (e.g., based

on user traffic variation), and predict the trend of traffic load of the network slice. So, it is essential to allow the third party to perform elastic scaling of the network slice capacity in order to ensure the required service quality, e.g., scale out in advance to face huge growths of traffic.

Furthermore, assuming the network operator charges the third party for the network slice in use, refund policies may be enabled so that the third party can be refunded if it uses less resources because of scale in operations. The third party can define a scale in/scale out plan to improve resource utilization and the capability of network slice capacity adjustment exposed to the third party can then be beneficial to improve network resource utilization and save operating costs of both the network operator and third party.

7.2.2 Requirements

The following requirements apply to the IMT-2020 network concerning the exposure of the network slice management capability:

The IMT-2020 network is required to provide APIs that allow authorized third parties to create, modify and delete specific network slices.

The IMT-2020 network is required to provide APIs that allow authorized third parties to monitor the state of specific network slices.

The IMT-2020 network is required to provide APIs that allow authorized third parties to specify and update the capabilities supported by specific network slices.

The IMT-2020 network is required to provide APIs that allow authorized third parties to adapt the capacity (elastic scaling of the capacity) of specific network slices.

7.3 Edge computing

7.3.1 Description

EC capability allows the deployment of application servers close to the location of UE, enabling applications to run on the network edge. Due to the proximity of UE, the latency for the delivery of such applications can be reduced.

Such applications can expose information that can be used, in addition to latency reduction, to optimize the network and services, and support personalized and contextualized services.

IoT applications and enterprise applications can generally benefit greatly from EC capability, as this allows service delivery in close proximity to terminal devices for those applications.

7.3.1.1 Support of traffic offloading policy based on third party request

When third party applications are deployed on the network edge, not all data traffic from/to third party applications should always be routed to the network edge: some data traffic can be routed to the network edge or to a remote application server.

For example, the video content of a video website is stored in a local application server while its webpage content is stored in a remote application server. The video website can notify the IMT-2020 network about which type of data traffic is routed to the local server via network operator-provided APIs. The IMT-2020 network can then implement the traffic offloading policy based on third party request.

7.3.1.2 Access control for an application in the network edge

A trend in enterprise networks is movement towards a true mobile office coupled with cloud-based business tools integrated with mobile devices.

Enterprises place some of their applications on a local application server on the network edge. Access control is obviously necessary also for these enterprise applications. The IMT-2020 network is

required to be able to control whether UE can access third party applications on a local server on the network edge.

7.3.1.3 Monitoring of the state of applications hosted on the network edge

To facilitate management by third parties of their own applications, it is key that the IMT-2020 network provide a monitoring capability that third parties can utilize to collect the real-time operational state of their applications on the network edge of the network operator.

For example, monitoring the latency of data traffic delivery between UE and applications can allow third parties to verify how well application service-level agreements (SLAs) are met. Also, when a third party application is overloaded and its performance degrades, the third party should take proper action (e.g., to request the network operator to allocate more resources to the application on the network edge, such as instantiation of more application instances).

The monitoring capability may include, but is not limited to, the following aspects:

1) monitoring of the performance of third party application, e.g., the latency of data traffic delivery between UE and the application;
2) monitoring of the load of the application, e.g., the utilization of resources;
3) monitoring UE-related information, e.g., the number of pieces of UE accessing the third party application.

One scenario related to the EC capability exposure is provided in clause I.2.

7.3.2 Requirements

The following requirements apply to the IMT-2020 network concerning the exposure of EC capability:

The IMT-2020 network is required to provide APIs that allow authorized third parties to divert data traffic to/from UE to the network edge of the network operator close to the UE location.

The IMT-2020 network is required to provide APIs that allow authorized third parties to control UE access to applications on the network edge of the network operator.

The IMT-2020 network is required to provide APIs that allow authorized third parties to monitor the real-time operational state of applications on the network edge of the network operator.

7.4 Network data analytics

7.4.1 Description

Network operators have traditionally collected information about their network through network probes, operation and maintenance (O&M) tools and other proprietary means. More and more of such collected information is being mined in real time to ascertain network health, as well as to predict network status.

An NWDA capability can be introduced to collect network conditions in real time and to extract network characteristics or status through analysis of the collected network data. The output of the NWDA analysis can be used as an input to IMT-2020 core network functions, such as the policy control function (PCF), which can then create policies for provisioning of network resources, as well as for traffic steering, taking into consideration the input from NWDA.

In terms of capability exposure, third party applications may provide the NWDA capability with information to help the NWDA analysis, and may leverage the output of the NWDA analysis to improve the user experience.

7.4.1.1 Third party access to the network data analytics results

Some third party applications are sensitive to network conditions. If they know the dynamic status of the network in advance, they can adjust in order to improve the user experience.

Taking a video application as an example, a video server can control the encoding rate depending on the estimated traffic congestion on the network. If the video server knows in advance that the network will be congested for a given period of time, it can adjust the encoding rate in time to adapt to the predicted network conditions and, as a result, improve the user experience.

One scenario related to NWDA analysis results exposure is provided in clause I.3.

7.4.1.2 Third party provision of information to network data analytics for analysis

Information from third parties, such as third party business model related information and QoS requirements, can also be used as input to the NWDA analysis. Combining the information obtained from third parties with the information obtained from the network operator's network, the NWDA capability can conduct a more accurate analysis.

7.4.2 Requirements

The following requirements apply to the IMT-2020 network concerning the exposure of the NWDA capability:

The IMT-2020 network is required to provide APIs that allow authorized third parties to retrieve the analysis results of the NWDA capability.

The IMT-2020 network is required to provide APIs that allow authorized third parties to provide information to the NWDA capability.

7.5 Fixed and mobile convergence

7.5.1 Description

The IMT-2020 network is envisioned to have an access network-agnostic unified core network supporting diverse fixed and mobile access networks (ANs) [ITU-T Y.3101].

Via the support of FMC, the services provided to UE can be switched between fixed access and mobile access seamlessly, depending on defined criteria, e.g., UE preferences, the network operator's policies or UE location. Information related to UE current AN type and available AN types may be required by third party applications to decide on the services or contents to be provided.

7.5.1.1 Exposure of information related to user equipment access network type

Some third party applications can provide different services or contents based on the UE AN type.

For example, an application may provide video streaming with higher resolution when it detects the UE has switched from 3G to wireless local area network (WLAN). As another example, an application may decide to display video news and advertisement via WLAN, while displaying text or graphic news and advertisements via mobile access.

One scenario related to FMC capability exposure is provided in clause I.4.

7.5.2 Requirements

The following requirements apply to the IMT-2020 network concerning the FMC capability exposure:

The IMT-2020 network is required to provide APIs that allow authorized third parties to get information related to UE AN types.

NOTE – This information may include network performance of the AN type, assuming the IMT-2020 network supports the capability of network performance measurement of fixed and mobile ANs.

7.6 Customization of quality of service capabilities

7.6.1 Description

The IMT-2020 network is expected to enable customization by third parties of network functionalities in order to support diverse third party requirements.

Information related to network capabilities is needed by some third party applications to analyse and make a decision on the services to be provided by the network in order to get the required user experience, e.g., information related to the QoS parameterization of network capabilities.

7.6.1.1 Exposure to third party of quality of service information related to network capabilities

Some third party applications may have strict requirements in terms of network performance. In such a case, when the third party gets services from the network operator, it first analyses the QoS capabilities exposed by the IMT-2020 network and then configures, if and as needed, the most appropriate QoS parameters to ensure that the IMT-2020 network can provide the required user experience.

One scenario related to QoS parameter exposure is provided in clause I.5.

7.6.2 Requirements

The following requirements apply to the IMT-2020 network concerning QoS capability exposure:

The IMT-2020 network is required to expose QoS information related to network capabilities that is accessible to authorized third parties.

The IMT-2020 network is required to provide APIs that allow authorized third parties, based on third party application requirements, to configure the appropriate QoS parameters related to the exposed QoS information.

8 Security considerations

As specified in clause 7.1.2, when the IMT-2020 network exposes its capabilities to third parties, authentication and authorization of third parties to access the exposed network capabilities is required to be performed.

Appendix I

Scenarios of capability exposure in the IMT-2020 network

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

I.1 Network slice customization by third party

The IMT-2020 network is expected to accommodate diverse applications with diverse requirements imposed on the network, e.g., in terms of functional and performance requirements of network capabilities, e.g., charging, policy control, security and mobility. The capability exposure functions of the IMT-2020 network enable the network operator to create customized networks by means of network slicing.

The scenario in Figure I.1 illustrates how the exposure of network capabilities can be used to build network slices according to diverse application requirements.

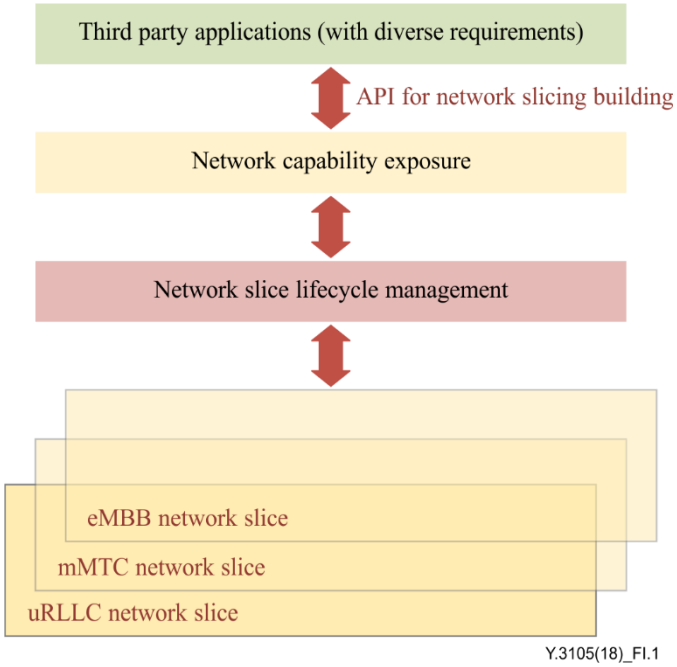

Figure I.1 – Capability exposure for network slice building

1) The third party (application) indicates the functional and performance requirements of the associated network slice by means of the network slice building API. In terms of implementation, a data template profile can be sent to the third party through the API, containing the parameters necessary to describe the functional and performance requirements.
2) The capability exposure functions transfer the network slice creation request to the network slice lifecycle management functions.
3) Based on network operator policies, the network slice lifecycle management functions authorize the functional and performance requirements and accordingly create the customized network slice for the third party (application).

I.2 Exposure of application-related information for edge computing

Mobile robots, such as automated guided vehicles (AGVs), have numerous applications in the industrial field and will play an increasingly important role in the factory of the future. The high reliability of the IMT-2020 network can ensure the stable control of AGVs. AGV vendors can deploy applications for AGV control on the EC platform of the IMT-2020 network.

In this scenario, illustrated in Figure I.2, the AGV vendor makes a business agreement with the IMT-2020 network operator and installs its AGV control application on the EC platform of the IMT-2020 network. The AGV control application running on the EC platform collects AGV-related information, e.g., movement information and application-running information, and reports such information to the server in the AGV control centre of the AGV vendor. Two methods may be used to implement information reporting:

– the AGV application on the EC platform delivers the information directly to the server located in the AGV vendor data centre (DC);

– the AGV application on the EC platform delivers the information to the server located in the central DC of the network operator and the information is then conveyed to the server in the AGV vendor DC.

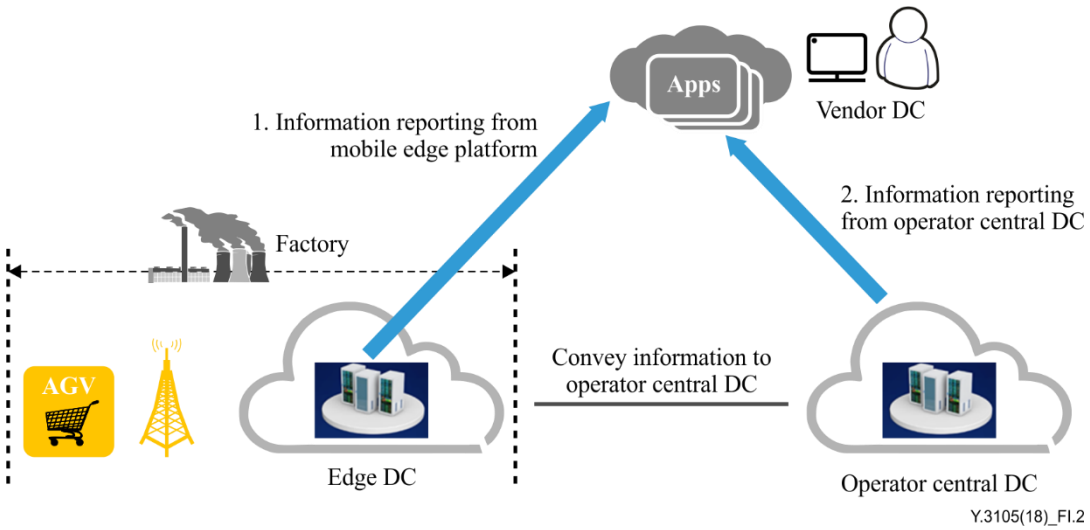

Figure I.2 – Capability exposure for third party application information reporting in mobile edge computing

I.3 Exposure of network performance predicted by network data analytics

During autonomous driving, it may be helpful for vehicles to get predictable network performance (e.g., latency, reliability) of upcoming IMT-2020 ANs.

The network performance of the upcoming IMT2020 AN predicted by the NWDA capability may consider different factors, e.g., speed, driving direction, upcoming location of the vehicles and network performance-related information (load based on time and spatial information). As shown in Figure I.3, predictable network performance of the upcoming IMT-2020 AN can be provided by the NWDA capability to the vehicle application and the vehicle application can make changes based on predicted network performance, e.g., changing driving mode from autonomous to manual.

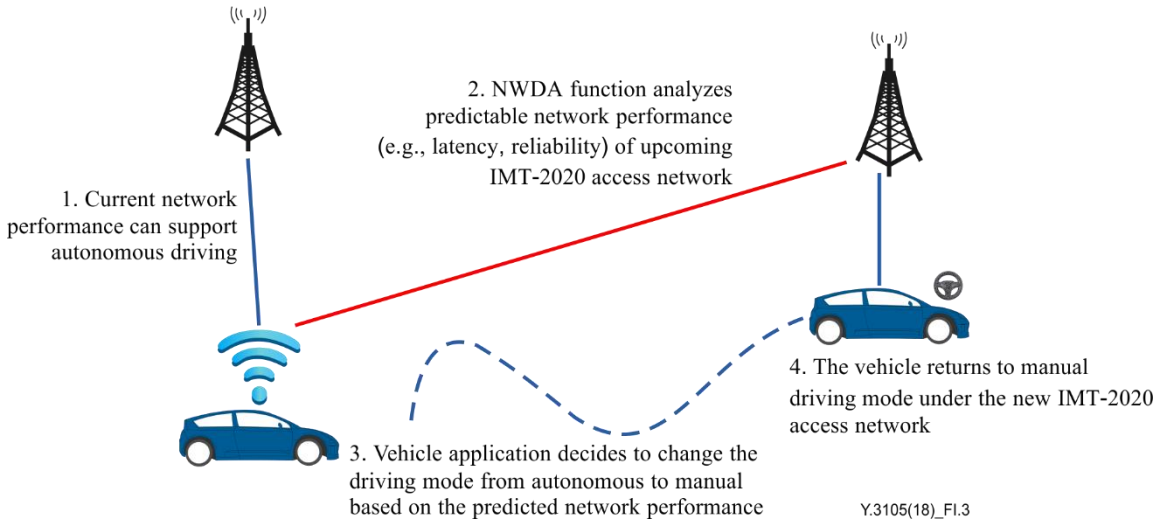

Figure I.3 – Capability exposure (predictive network performance) for third party application in network data analytics

I.4 Exposure of access network type and network performances for fixed and mobile convergence

In this scenario, the traffic is carried via the most suitable AN among all those available. The unified management for fixed and mobile ANs provides network performance measurement so that IMT-2020 applications can leverage the AN with the best network performance.

Each application has its own performance requirements in terms of the IMT-2020 network (e.g., bandwidth, latency). The application may actually have analytical capabilities to judge what kind of content should be provided to customers based on the current AN type and network performance.

For example, as shown in Figure I.4, a virtual reality (VR) game application is able to connect to the IMT-2020 network via both fixed and mobile ANs. When it attempts to access the IMT-2020 network, it first analyses the network performances of the different available ANs, then chooses the available AN type that has the best network performance.

It is possible that the chosen AN cannot provide a high-resolution data streaming service. Under this circumstance, the application can adjust the image quality to reduce the data rate in order to maintain service continuity.

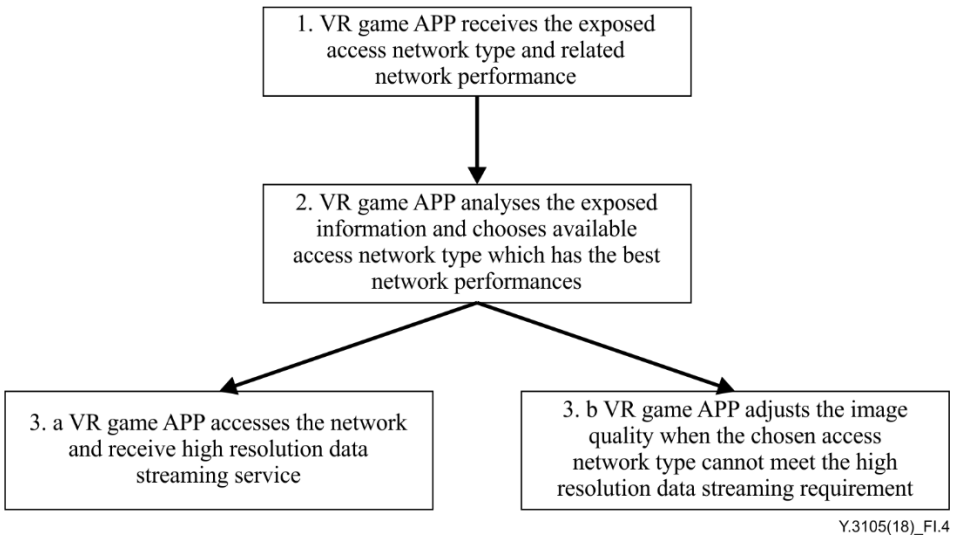

Figure I.4 – Capability exposure (access network type and network performances) for third party application in fixed and mobile convergence

I.5 Quality of service parameters configuration by third parties

The IMT-2020 network may offer end-to-end services to third party customers according to their specific performance requirements.

In order to be able to customize the QoS of end-to-end services, as shown in Figure I.5, a third party accesses QoS parameters whose configurability is allowed to authenticated and authorized third parties.

Based on service requirements, the third party requests the appropriate QoS parameter configuration from the network via APIs. The network may, or may not, accept to implement the requested configuration.

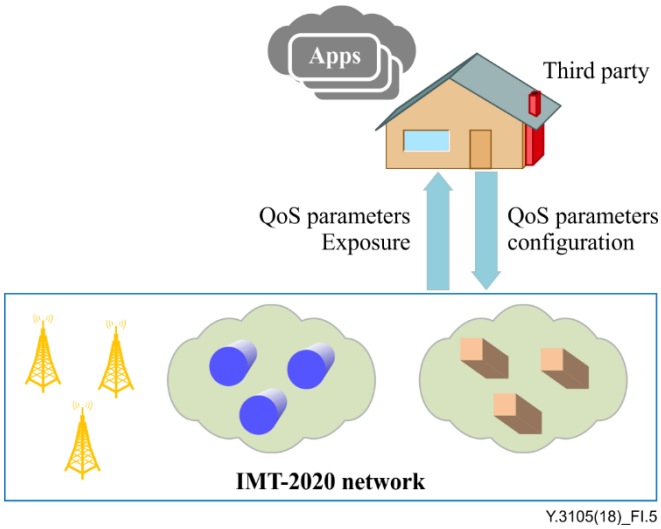

Figure I.5 – Capability exposure (quality of service parameters) for quality of service customization by third party

Bibliography

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*

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

[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, 2019