International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3158

(09/2022)

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

Future networks

Local shunting for multi-access edge computing in IMT-2020 networks

Recommendation ITU-T Y.3158

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3158

Local shunting for multi-access edge computing in IMT-2020 networks

Summary

Recommendation ITU-T Y.3158 describes the relationship between international mobile telecommunication 2020 (IMT-2020) networks and a multi-access edge computing (MEC) system, and specifies an architecture for transmitting traffic flows at the edge of IMT-2020 networks. Recommendation ITU-T Y.3158 specifies the requirements, architecture, functional entities, reference points and information flows for MEC in IMT-2020 networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3158	2022-09-29	13	11.1002/1000/15057

Keywords

Data network, edge service data flow, IMT-2020 networks, local data network, local shunting, MEC.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Y.3158

Local shunting for multi-access edge computing in IMT-2020 networks

1 Scope

The Recommendation specifies the requirements, architecture, functional entities, reference points and information flows of local shunting for multi-access edge computing (MEC) in International Mobile Telecommunication 2020 (IMT-2020) networks.

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.3104] Recommendation ITU-T Y.3104 (2018), *Architecture of the IMT-2020 network.*

[ITU-T Y.3150] Recommendation ITU-T Y.3150 (2020), *High-level technical characteristics of network softwarization for IMT-2020.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 backhaul [ITU-T Y.3100]: A network path between base station systems and a core network.

3.1.2 functional entity [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.3 multi-access edge computing [b-ETSI GS MEC 001]: System which provides an IT service environment and cloud-computing capabilities at the edge of an access network which contains one or more type of access technology, and in close proximity to its users.

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

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

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

3.1.6 service function [b-ITU-T Y-Suppl.41]: A function, specifically representing network service function, that is responsible for specific treatment of received packets other than the normal, standard functions of an IP router (e.g., IP forwarding and routing functions) on the network path between a source host and destination host.

3.1.7 service function chain [b-ITU-T Y-Suppl.41]: A chain that defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification and/or policy.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

Ack	Acknowledgement
AF	Application Function
AN	Access Network
ASF	Authentication Server Function
CEF	Capability Exposure Function
CN	Core Network
HD	High Definition
ID	Identifier
IMT-2020	International Mobile Telecommunication 2020
IP	Internet Protocol
IT	Information Technology
MEC	Multi-access Edge Computing
NACF	Network Access Control Function
NFR	Network Function Repository
NSSF	Network Slice Selection Function
PCF	Policy Control Function
RP	Reference Point
SDN	Software-Defined Network
SFC	Service Function Chain
SMF	Session Management Function
UE	User Equipment
UPF	User Plane Function
USM	Unified Subscription Management

5 Conventions

In this Recommendation:

The phrase "is required" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformity to this Recommendation is to be claimed.

The phrase "is recommended" indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformity.

The phrase "can optionally" indicates an optional requirement that 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 or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformity with this Recommendation.

6 Overview of local shunting for multi-access edge computing in IMT-2020 networks

At present, the requirements of traffic density and the expected data rate from users of IMT-2020 networks are growing rapidly, which brings great challenges to IMT-2020 networks. Core networks (CNs) also experience a larger data traffic impact; MEC technology can effectively reduce the bandwidth requirements of network backhaul through local shunting and alleviate the pressure of data transmission for CNs. Local shunting for MEC can be realized by network softwarization technology specified in [ITU-T Y.3150]. MEC is an effective way to deploy IMT-2020 network service applications by network providers close to the users, and the users can access dynamically according to their needs. It is benefit for satisfying the users' experience with low latency and high bandwidth.

Figure 6-1 shows the relationship between IMT-2020 networks specified in [ITU-T Y.3104] and an MEC system. As one of the core technologies of IMT-2020, MEC can be deployed at the edge of IMT-2020 network and can provide services closer to the users. Network providers (e.g., operators) can use MEC to provide information technology (IT) services and computing functions needed by users, and build an environment with high performance, low latency and high bandwidth, so that the users can enjoy high-quality service experience.

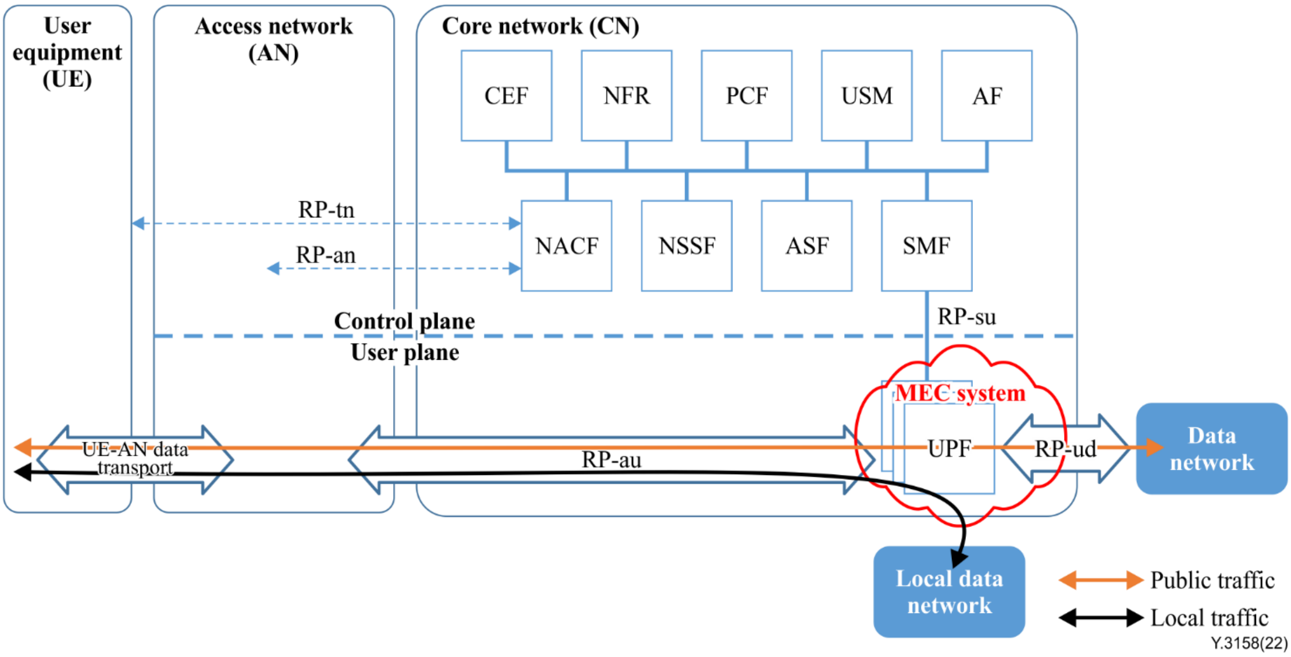
In this Recommendation, an MEC system is designed to transmit traffic flows at the edge of IMT-2020 networks. Local shunting for MEC in IMT-2020 networks can meet the network transmission requirements of local and public network services. All of these service traffic flows go through the MEC system, and are then forwarded to the public or local data network based on local shunting policies.

Figure 6-1 shows the following general roles of local shunting.

– Local traffic: the traffic flow does not need to go through the CN, and is directly diverted from an MEC system to the local data network. User equipment (UE) can directly access local data networks through the MEC system. Local shunting can reduce backhaul bandwidth consumption, service access latency and improve service experience.

– Public traffic: the traffic flow goes through a CN to the data network via an MEC system. When UE needs to access the public network, the MEC system sends the public network traffic flows directly to the CN, then forwards them to the data network.

– Typical scenario: Live high-definition (HD) video broadcasting can be a typical scenario to use the local shunting mechanism. Traditional CN solutions may cause high latency. However, the traffic flows of video broadcasting can be diverted through an MEC system to a local network, which can better satisfy user real-time demand.



AF	application function	ASF	authentication server function
CEF	capability exposure function	NACF	network access control function
NFR	network function repository	NSSF	network slice selection function
PCF	policy control function	RP	reference point
SMF	session management function	USM	unified subscription management

NOTE – For the RP suffixes, see [ITU-T Y.3104].

Figure 6-1 – Relationship between IMT-2020 networks and an MEC system

7 Requirements for local shunting for multi-access edge computing in IMT-2020 networks

7.1 General requirements

[REQ-GR1]: The IMT-2020 network is required to support traffic offloading based on UE request.

[REQ-GR2]: The IMT-2020 network is required to provide application programming interfaces that allow an MEC system authorized in an IMT-2020 network to divert data traffic from UE to the network edge close to the UE location.

[REQ-GR3]: The IMT-2020 network is required to allow an authorized MEC system to control UE access to applications on the network edge of a network operator.

[REQ-GR4]: The IMT-2020 network is required to allow an authorized MEC system to monitor relevant traffic.

[REQ-GR5]: The IMT-2020 network is required to steer local service data traffic from an MEC system to local applications or local data networks.

[REQ-GR6]: Local shunting for MEC in IMT-2020 networks is required to avoid affecting other traffic in IMT-2020 networks.

7.2 Local traffic requirement for local shunting

Traffic flow regarding the service needs to be processed locally and can be routed directly from the edge data routing module system to local traffic without going through the CN in the IMT-2020 network. The edge data routing module system is specified in clause 8.

Local shunting not only reduces the consumption of backhaul bandwidth, but also can reduce the service access latency and improve user service experience.

[REQ-LT1]: Local shunting for MEC in IMT-2020 networks is required to support control local traffic data streams.

7.3 Public traffic requirement for local shunting

In public traffic, there are two types of local shunting: 1) the edge data routing module system sends public service data to the data network by pass-through CN; 2) the edge data routing module system streams specific service data to the local network and then accesses the data network through the local network.

[REQ-PT1]: Local shunting for MEC in IMT-2020 networks is required to support access to public traffic services.

7.4 Traffic adjustment requirement for local shunting

It is necessary to adjust edge service traffic base on local shunting policies.

[REQ-TA1]: Local shunting for MEC in IMT-2020 networks is required to support adjustment for edge service traffic when a local shunting policy is changed or deleted.

7.5 Functional requirement for local shunting based on a software-defined network

Local shunting for MEC in IMT-2020 networks can be executed based on a software-defined network (SDN). SDN technology is an effective mechanism for orchestrating, controlling and managing the network resources of an MEC system. Furthermore, the management and configuration of MEC network resources are carried out by the SDN controller. The following service capabilities should be supported.

[REQ-FR1]: The SDN controller is required to create and enable edge service traffic paths and path policies for edge service data traffic.

[REQ-FR2]: The SDN controller is required to generate according to routing rules a flow table, which contains traffic flow information and a diversion strategy.

[REQ-FR3]: The diversion gateway is required to conduct local shunting according to the flow table.

[REQ-FR4]: Local shunting based on SDN is recommended to shorten the response time between UE and applications,

[REQ-FR5]: Local shunting based on SDN is recommended to ensure the continuity requirements of end-user data traffic.

[REQ-FR6]: The SDN controller can optionally create a service function chain (SFC) and perform the orchestration of the service function when receiving an MEC service request.

NOTE – An SFC for MEC local shunting is also considered in this Recommendation. An SFC is identified in [b-ITU-T Y.2242] and [b-ITU-T Y-Suppl.41]. If operator applications, edge user applications, or third party applications are deployed on the edge of an IMT-2020 network, an SFC can provide an elastic and automatic service deployment mechanism based on the conditions of multiple access networks and MEC service requirements, then end users can select personalized edge services.

8 Architecture, functional entities and reference points for local shunting for multi-access edge computing in IMT-2020 networks

8.1 Architecture

Local shunting for MEC in IMT-2020 networks includes three functional areas for: control; edge data routing module system; and edge application. See Figure 8-1.

The control functional area provides the following functions.

– Controller function: determine and update the routing rules of traffic flow regarding MEC service data traffic and the local shunting policy per UE or per flow, and orchestrate an SFC when needed.

NOTE – MEC service data traffic that is diverted via the MEC system contains two types of flow: 1) traffic for local applications or local data networks, called "local service data traffic"; 2) traffic going through a CN, called "public service data traffic".

The edge data routing module system area provides the following functions.

– Edge data routing function: routes traffic based on the rules of MEC service data traffic determined by the SDN controller function.

– Classifier function: classifies the traffic based on local shunting policies and traffic flows that can be routed to a public data network or directly to a local data network without going through the CN in the IMT-2020 network.

The edge application area provides MEC applications, e.g., live HD video broadcasting, cloud gaming. The applications can be provided by operators, edge users or third parties.

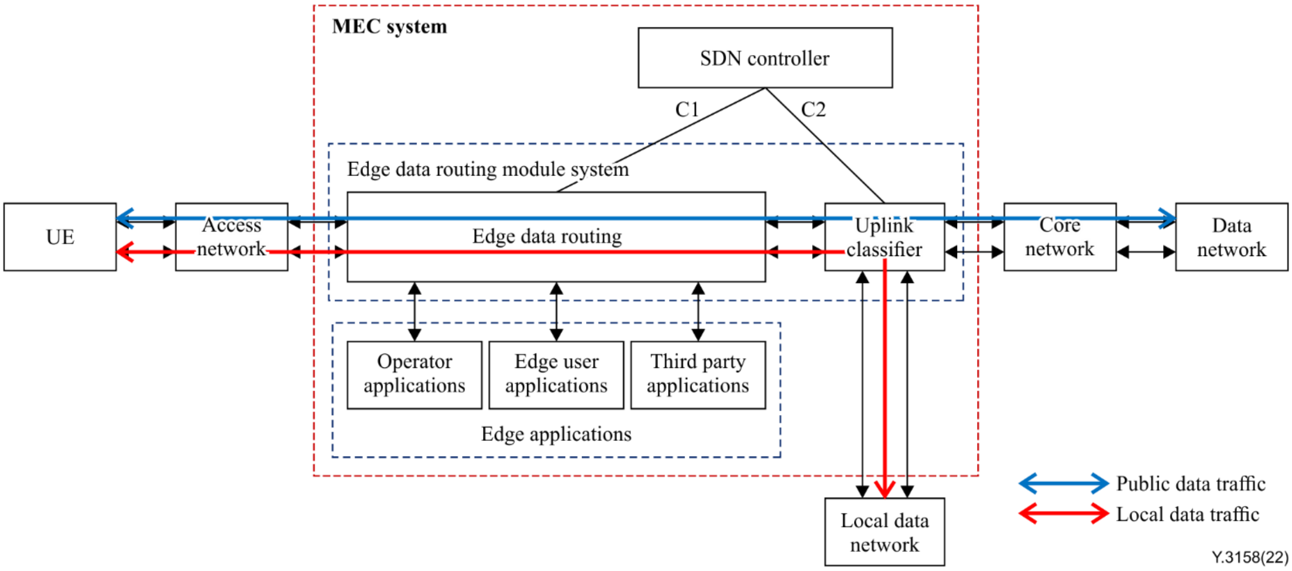


Figure 8-1 – Architecture of local shunting for MEC in IMT-2020 networks

NOTE – Flows between edge data routing and operator applications, edge user applications and third party applications are omitted in Figure 8-1.

8.2 Functional entities

8.2.1 SDN controller

The SDN controller performs the following functions:

– obtains the current status of all equipment under control, UE traffic information and other related information;

– performs local shunting for an MEC system: designs traffic flows are either local traffic or public traffic;

– creates, updates or deletes a local shunting policy and transfers it to an uplink classifier;

– monitors the routers or switches under control and monitors edge applications connected to edge data routing;

- when an SFC is needed in an MEC service, the SDN controller orchestrates service functions, including designating which service functions are included in an SFC, and determining the sequence of service functions in the SFC.

8.2.2 Uplink classifier

The uplink classifier performs the following functions:

- obtains local shunting policies from the SDN controller function;
- receives local traffic flows and applies a corresponding local shunting policy to them to steer the traffic going through the local data network.

8.3 Reference points

8.3.1 Reference point C1

A SDN controller function interacts with an edge data routing function via a reference point C1 to get information about switches under its control. The SDN controller function sends path information of a traffic flow with regard to MEC service data traffic to the edge data routing function.

8.3.2 Reference point C2

An uplink classifier interacts with the SDN controller function via a reference point C2 to receive path information of flow with regard to MEC service data traffic created by the controller function; the uplink classifier then applies the rules to the flow.

9 Information flows for local shunting for multi-access edge computing in IMT-2020 networks

This clause describes information flows for local shunting when creating a new edge service data traffic path. See Figure 9-1.

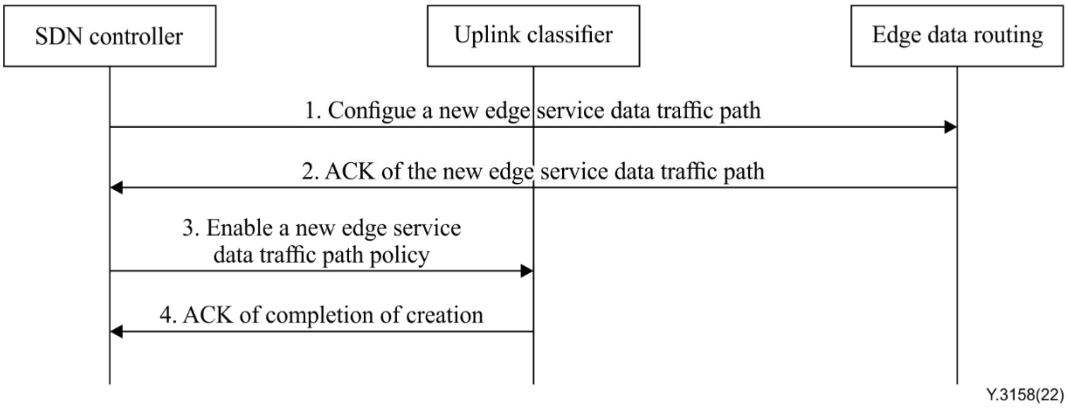

SDN controller
Uplink classifier
Edge data routing
1. Configue a new edge service data traffic path
2. ACK of the new edge service data traffic path
3. Enable a new edge service data traffic path policy
4. ACK of completion of creation
Y.3158(22)

Figure 9-1 – Creation of a new edge service data traffic path

The main steps for creating a new edge service data traffic path are as follows.

Step 1: An SDN controller creates and enables a new edge service data traffic path. The SDN controller configures the related edge data routers with the forwarding rules.

Step 2: Edge data routers reply to the SDN controller with an acknowledgement (Ack) character.

Step 3: The SDN controller creates a new edge service data traffic path policy with path rules. Attributes of rules include the application identifier (ID), edge service characteristics, the ID of the edge service data traffic path and destination information of the traffic. The SDN controller then sends the new policy for target flows to the uplink classifier.

NOTE – The policy can be composed of several path rules.

- The application ID can be derived from the UE.
- The edge service characteristics are the information that is used to identify edge services and can be pre-configured by the SDN controller. Edge services may have the characteristics like: 1) isolation from data network (e.g., the service data only transmit locally); 2) low latency (e.g., the services need synchronized information among devices and control devices remotely); 3) high bandwidth (e.g., the services need large traffic data transmission).
- The ID of the edge service data traffic path is used to apply the rules to the edge service data traffic path created by the SDN controller.
- The destination information of the traffic is used to specify service traffic flows to the local or public data network.

Step 4: The uplink classifier replies to the SDN controller with an Ack character. When traffic enters the uplink classifier, it carries information like the application ID, edge service characteristic and destination information. The uplink classifier distinguishes traffic flows for local shunting by searching and selecting the edge service data traffic path rules with the same ID carried by users, and then steers the traffic to the local or public data network.

10 Security considerations

This Recommendation is recognized as an enhancement of mobile networks based on the Internet protocol (IP). Thus, it is assumed that security considerations in general are based on the security considerations identified by [b-ITU-T Y.2701][b-ITU-T Y.3101].

The IMT-2020 network including UE, ANs and CN are subject to security and privacy measures. Sensitive information should be protected as a high priority in order to avoid leakage and unauthorized access. Specific security concerns highlighted in this Recommendation deal with MEC system authentication, as specified in clause 7.1.

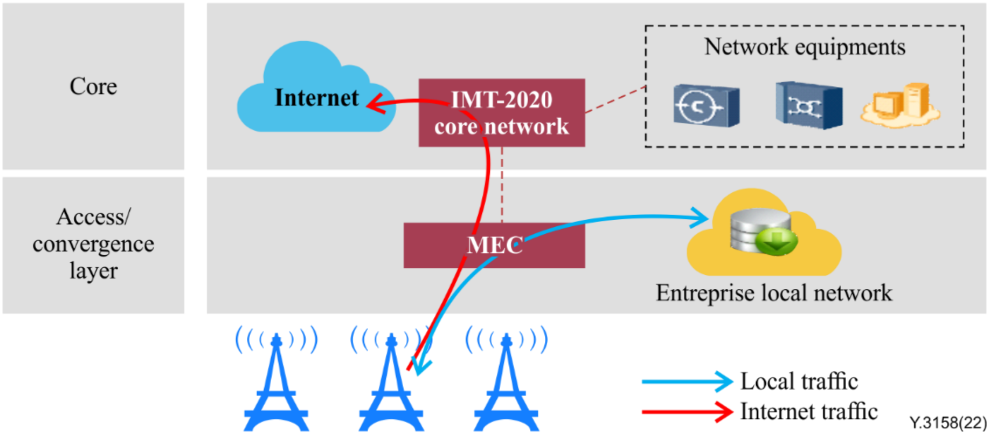
Appendix I

Local shunting for MEC development for smart port scenario based on operator network

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

See Table I.1.

Table I.1 – Local shunting for MEC development for smart port scenario based on operator network

Description	In the construction of a local data network of smart ports, traditional wireless fidelity cannot guarantee service effectiveness such as coverage, stability, security and service continuity. The construction should meet design requirements, such as the isolation between local and public data networks, and ensure the security of the local network. The following aspects should be considered: 1) internal transmission of enterprise data; 2) interconnection, remote control among devices with low latency requirements; 3) port real-time video monitoring with high bandwidth requirements
Technical points for consideration	– Deployment of applications in edge areas – Identification in a local network – Local traffic flow distribution
Figure (optional)	 Core Access/ convergence layer Internet IMT-2020 core network Network equipments MEC Entreprise local network Local traffic Internet traffic Y.3158(22)
Solution description	The MEC system identifies edge service traffic flows, the traffic flows to the enterprise local network based on the edge service data path policy
Derived requirements	The traffic flows of a local data network can be routed directly from the edge data-routing module system to the local data network without going through the core network

Bibliography

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

[b-ITU-T Y.2242] Recommendation ITU-T Y.2242 (2018), *Service function chaining in mobile networks*.

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

[b-ITU-T Y-Suppl.41] ITU-T Y-series Recommendations – Supplement 41 (2016), *ITU-T Y.2200-series – Deployment models of service function chaining*.[b-ETSI GS MEC 001] ETSI Group Specification MEC 001 V2.1.1 (2019), *Multi-access edge computing (MEC); Terminology*.

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, 2022