International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3136

(09/2020)

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

Future networks

Session management for fixed mobile convergence in IMT-2020 networks

Recommendation ITU-T Y.3136

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.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.3136

Session management for fixed mobile convergence in IMT-2020 networks

Summary

Recommendation ITU-T Y.3136 describes the scenarios, general requirements and design principles of session management (SM) for fixed mobile convergence (FMC) in IMT-2020 networks. This Recommendation also describes the functional architecture and key functions of session management for supporting FMC in IMT-2020 networks as well as provides information flows of protocol data unit (PDU) session management and traffic routing management for FMC in IMT-2020 networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3136	2020-09-29	13	11.1002/1000/14398

Keywords

IMT-2020 network, PDU session, session continuity, session management, traffic routing.

* 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.3136

Session management for fixed mobile convergence in IMT-2020 networks

1 Scope

This Recommendation aims to describe the framework of session management for fixed mobile convergence (FMC) in IMT-2020 network. Session management is a key technology to provide the PDU connectivity service via PDU sessions for FMC. This Recommendation covers the following issues, but is not limited to:

- Scenarios, requirements and design principles of session management for FMC in IMT-2020 networks,
- Functional architecture of session management for FMC in IMT-2020 networks,
- Functions of PDU session management and traffic routing management for FMC in IMT-2020 networks,
- Information flows of PDU session management and traffic routing management for FMC in 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 Q.1762] Recommendation ITU-T Q.1762/Y.2802 (2007), *Fixed-mobile convergence general requirements.*

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

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

[ITU-T Y.3102] Recommendation ITU-T Y.3102 (2018), *Framework of the IMT-2020 network.*

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

[ITU-T Y.3130] Recommendation ITU-T Y.3130 (2018), *Requirements of IMT-2020 fixed mobile convergence.*

[ITU-T Y.3131] Recommendation ITU-T Y.3131 (2019), *Functional architecture for supporting fixed mobile convergence in IMT-2020 networks.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 fixed mobile convergence [ITU-T Y.3100]: In the context of IMT-2020, the capabilities that provide services and applications to end users regardless of the fixed or mobile access technologies being used and independently of the users' location.

3.1.2 PDU session [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.

3.1.3 session continuity [ITU-T Q.1702]: The ability of the user to maintain continuity of ongoing sessions while changing between terminal devices and across various access and core networks. For example, the user of a mobile terminal may wish to switch from his mobile equipment attached to a wireless network to a laptop connected to a wire-line or Digital Subscriber Line connection. This should be supported without any session discontinuity.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AN	Access Network
ATSSS	Access Traffic Switching, Splitting and Steering
CN	Core Network
CP	Control Plane
DN	Data Network
FMC	Fixed Mobile Convergence
IP	Internet Protocol
IWF	Interworking Function
NF	Network Function
NFR	Network Function Registry function
NACF	Network Access Control Function
PCF	Policy Control Function
PDU	Protocol Data Unit
QoS	Quality of Service
SM	Session Management
SMF	Session Management Function
UE	User Equipment
UP	User Plane
UPF	User Plane Function
USM	Unified Subscription Management

5 Conventions

In this Recommendation:

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

6 Design considerations of session management for FMC in IMT-2020 networks

6.1 Session management design principles

Session management is required to manage protocol data unit (PDU) sessions including control of PDU session tunnel establishment, modification and release. In addition, session management for FMC in IMT-2020 networks is required to support traffic routing management between fixed access networks and mobile access networks. Traffic routing management includes traffic switching, splitting and steering on the network side and the user equipment side. Session management is required to support PDU session management and traffic routing management for Internet protocol (IP) type PDU session level [ITU-T Y.3102].

The application scenario of session management is shown in Figure 6-1, which illustrates the scenario of mobile broadband service via fixed and (or) mobile access. The IMT-2020 network is envisioned to have an access network agnostic architecture whose core network will be a common unified core network for new radio access technologies for IMT-2020, as well as existing fixed and wireless networks. A terminal of mobile broadband service can be globally controlled by unified core network (CN), and obtain access to data sources such as websites on the Internet via both fixed and mobile access simultaneously (which 'and' in the figure stands for) or via one of the access technologies at a given time (which ‘or’ in the figure stands for).

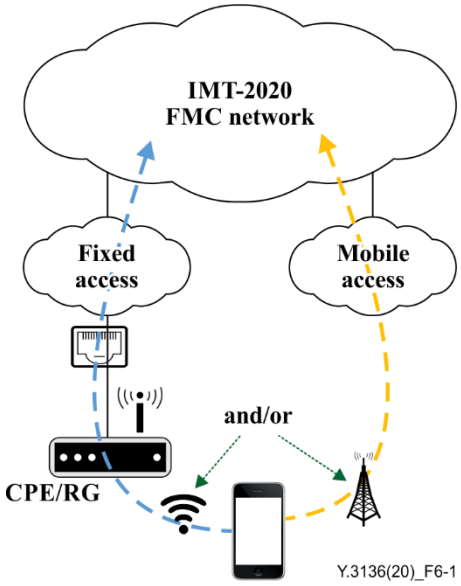

Figure 6-1 – Scenarios of session management for FMC in IMT-2020 Network [ITU-T Y.3130]

There are some points to be highlighted for this scenario. Session management for FMC in IMT-2020 networks is required:

– to serve both fixed and mobile access networks;

– to support the use of fixed or mobile access network, or simultaneous use of both, seamlessly;

– to transport traffic on one or the other access networks, or transport on both simultaneously, and traffic can be split, combined, steered according to service requirements and network conditions;
– to support unified management of subscriber's mobility and session stack.

Session management is designed with the separation of control plane (CP) and user plane (UP). This feature makes it easier to implement and deploy the session management to a variety of access networks in IMT-2020 network.

Session management is also designed by cooperating with other functionalities. The session management could be accomplished with the help of functionalities for authentication, security, call establishment and so on. For other functionalities of the CP such as authorization and charging, the interfaces are required to follow general standards.

6.2 General session management requirement

The general session management for FMC in IMT-2020 networks is required to provide PDU connectivity service including control of PDU session tunnel establishment, modification, and release. Session management is also required to provide traffic routing management including selecting the access network(s) to transport traffic (traffic steering), dividing traffic into multiple pieces which are transported through different access networks (traffic splitting), moving traffic from one access network to another (traffic switching), on both network side and user equipment side. The following details of session management for FMC in IMT-2020 networks describe the IP type of PDU sessions. Details of PDU session management for PDU types other than the IP type are outside the scope of this Recommendation.

6.3 General session management functional architecture

Session management supports different access networks and support simultaneous connections of a user equipment (UE) via multiple access technologies. For different access networks for FMC in IMT-2020 network, session management is required to enable the establishment, modification and release of PDU session tunnels, and support the management of traffic routing.

PDU session tunnels are required between access networks (ANs) and user plane functions (UPFs) as well as between different UPFs. Session management function (SMF) selects a proper UPF and allocates an IP address to the UE in the PDU session establishment. SMF releases the session, deletes all the flows belonging to the session and requests the deletion of the flows to UPF and AN when the releasing requests arrive in the PDU session release. SMF requests UPF to modify the PDU session via network access control function (NACF) in the PDU session modification.

Session management mainly consists of PDU session management and traffic routing management. Figure 6-2 shows session management related functions in IMT-2020 network architecture. Entities relevant to PDU session management include AN, NACF, SMF, interworking function (IWF), UPF, policy control function (PCF), unified subscription management (USM), network function registry function (NFR) and date network (DN). Entities relevant to traffic routing management include AN, NACF, SMF, PCF, IWF and UPF.

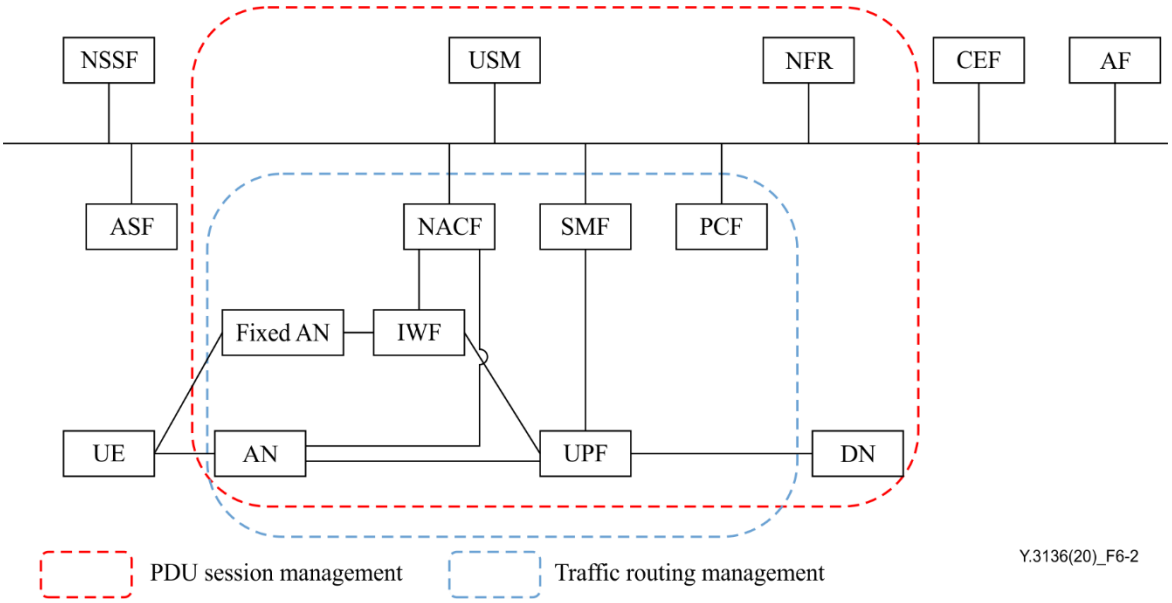

Figure 6-2 – Session management related functions in IMT-2020 network architecture [ITU-T Y.3131]

NOTE – For ANs which do not natively support a common signalling interface, an IWF needs to be provided at the AN-CN interface so that network functions deployed in the CN can still use a common signalling interface" [ITU-T Y.3102].

The IMT-2020 network is required to provide PDU connectivity service that enables exchange of PDUs between UEs and DNs. The PDU connectivity service is supported via PDU sessions that are established upon session request from UEs. The PDU session tunnels are used between AN and UPF(s) as well as between different UPFs as UP data transport for PDU sessions.

SMF controls the establishment, modification, and release of PDU sessions. SM messages are exchanged between SMF and UE via NACF. SMF controls UPFs for the management of PDU sessions. The serving SMF performs authentication and authorization with the DN. PCF provides functionalities for the control and management of policy rules including rules for traffic routing. UPF provides functionalities for traffic routing and forwarding, PDU session tunnel management.

USM stores and manages, in a unified way, UE context and subscription information including, but not limited to, information on session management for PDU session establishment. NFR provides functionalities to assist the discovery and selection of required network functions and maintains information of the available network function instances.

7 Key functions of session management for FMC in IMT-2020 networks

This clause describes the functions to support session management for FMC in IMT-2020 network. The features of PDU session management function and traffic routing management function are described in clauses 7.1 and 7.2, respectively.

7.1 Functional description for PDU session management

PDU session management function is used to provide PDU connectivity service, i.e., a service that enables exchange of PDUs between UEs and DNs. PDU sessions upon session request from UEs are required to support the PDU connectivity service. Each PDU session supports a single PDU type as requested by the UE at the establishment of the PDU session.

According to the requirements of session management for FMC, session management is required to support PDU session management, selection and control of UP function. PDU session tunnels are required between ANs and UPFs as well as between different UPFs. The UPF manages PDU

sessions including control of PDU session tunnel establishment, modification, and release. SMF controls UPFs for the management of PDU sessions. The implementation of PDU session management function requires the cooperation of NACF, SMF, UPF, PCF, and USM.

The PDU session management function includes PDU session establishment, PDU session modification and PDU session release. PDU session management procedures are based on the characteristic of FMC in IMT-2020 networks and session management in ITU-T Y.3104.

PDU session establishment procedure starts when the UE requests to establish a PDU session to NACF. SMF controls UPF and, via NACF, AN to establish PDU session tunnels and UE-AN data transport tunnel. The procedure provides tunnels that enable exchange of PDUs between UEs and DNs. PDU session modification procedure starts when the status changes in access networks or for load balancing. SMF sends the modification request to UPF. When UPF receives a response, SMF sends a request to AN to modify the PDU session. PDU session release procedure starts when the UE sends the release request to SMF or when SMF or AN trigger the PDU session release. SMF releases the session, deletes all the flows belonging to the session, and UPF and AN delete the corresponding resources. The UE can request the release of the PDU session explicitly, or the release of PDU session can be triggered by SMF or AN implicitly.

A PDU session management procedure may correspond to:

– a UE initiated PDU session management procedure,

– a UE initiated PDU session handover between mobile access network and fixed access network,

– a network triggered PDU session management procedure. In this case the network sends the device trigger message to application(s) on the UE side. The device trigger request message contains information on which application on the UE side is expected to trigger the PDU session management request. Based on that information, the application(s) on the UE side trigger the PDU session management procedure.

In session management scenarios for FMC in IMT-2020 Network, a UE may request to establish multiple PDU sessions, to the same data network or to different data networks, such as via mobile access networks and via fixed access networks at the same time. A UE with multiple established PDU sessions may be served by different SMF. A UE may request to move a PDU session between mobile accesses and fixed accesses. The SMF shall be registered and deregistered on a per PDU session granularity in the USM. The UP paths of different PDU sessions belonging to the same UE may be completely disjoint between the AN and the UPF interfacing with the same or different DN.

7.2 Functional description for traffic routing management

Traffic routing management function is used to support traffic switching, splitting, and steering between fixed access networks and mobile access networks. The function includes traffic routing management for IP type PDU session level [ITU-T Y.3102].

According to the requirements of session management for FMC, this function supports the selection of the access network(s) to transport traffic, supports to transport traffic through different access networks (such as fixed access and mobile access) by dividing traffic into multiple pieces, supports to move traffic from one access network to another, such as from mobile network to fixed network.

The traffic steering procedure selects an access network for a new data flow and transfers the traffic of this data flow over the selected access network.

The traffic switching procedure moves all traffic of an ongoing data flow from one access network to another access network in a way that maintains the continuity of the data flow. When the UE(s) move between different access networks (such as mobile network and fixed network), the traffic switching procedure will be triggered.

The traffic splitting procedure splits the traffic of a data flow across multiple access networks. When traffic splitting is applied to a data flow, some of the traffic of the data flow is transferred via one access network while some other traffic of the same data flow is transferred via another access network.

All the procedures mentioned above are applicable between mobile access networks and fixed access networks.

To provide traffic routing, the function supports multi-access PDU session, that is a type of PDU session whose traffic can be sent over mobile access, or over fixed access, or over both accesses. The UE or the UPF distributes the traffic based on access traffic switching, splitting and steering (ATSSS) rules implementing different policies. The SMF provides ATSSS forwarding rules to UPF that indicate how traffic should be routed across the PDU sessions. The ATSSS forwarding rules are derived based on the multi-access policy and charging control rules provided by PCF. When the traffic routing requests that target multiple UE(s) are sent and may target multiple PCF(s), the PCF(s) transform(s) the requests into policies that apply to PDU sessions.

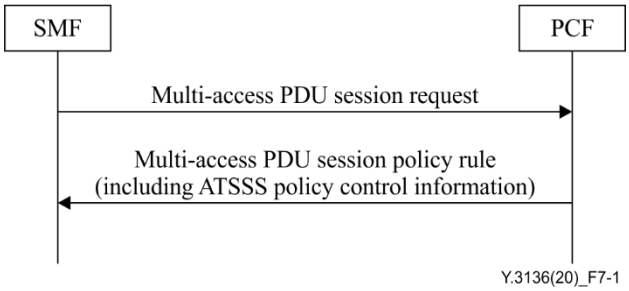

Figure 7-1 – Multi-access PDU session procedure

During the establishment of a multi-access PDU session, the PCF may take ATSSS policy decisions and create policy rules that contain ATSSS policy control information, which determines how the uplink and the downlink traffic of the multi-access PDU session should be distributed across the mobile and fixed access networks.

The PCF provides policy rules for the multi-access PDU session, i.e., policy rules that include ATSSS policy control information, as described in Figure 7-1. The SMF receives the policy rules with ATSSS policy control information and maps these rules into ATSSS rules and SMF-UPF rules. The ATSSS rules is a prioritized list of rules which are applied by the UE to enforce the ATSSS policy in the uplink direction and the SMF-UPF rules are applied by the UPF to enforce the ATSSS policy in the downlink direction.

The ATSSS rules are sent to UE with UE-CN signalling when the multi-access PDU session is created or when they are updated by the SMF, e.g., after receiving updated policy rules from the PCF. Similarly, the SMF-UPF rules are sent to UPF when the multi-access PDU session is created or when they are updated by SMF.

8 Information flows of session management for FMC in IMT-2020 networks

This clause describes detailed information flows of the PDU session management function and traffic routing management function. PDU session management procedures are based on the characteristic of FMC in IMT-2020 networks and session management in [ITU-T Y.3104].

8.1 PDU session management

The procedures of the PDU session management function include session establishment procedure, session modification procedure and session release procedure. Detailed information flows of these procedures are described in clauses 8.1.1 to 8.1.3.

8.1.1 Information flows for session establishment

PDU session tunnels are required between ANs and UPFs as well as between different UPFs. SM enables the establishment of PDU session tunnels. SMF controls the establishment of PDU sessions. SM messages are exchanged between SMF and UE by NACF signalling. SMF controls UPF and, via NACF, AN to establish PDU session tunnels and UE-AN data transport tunnel. The session establishment procedure is illustrated as Figure 8-1.

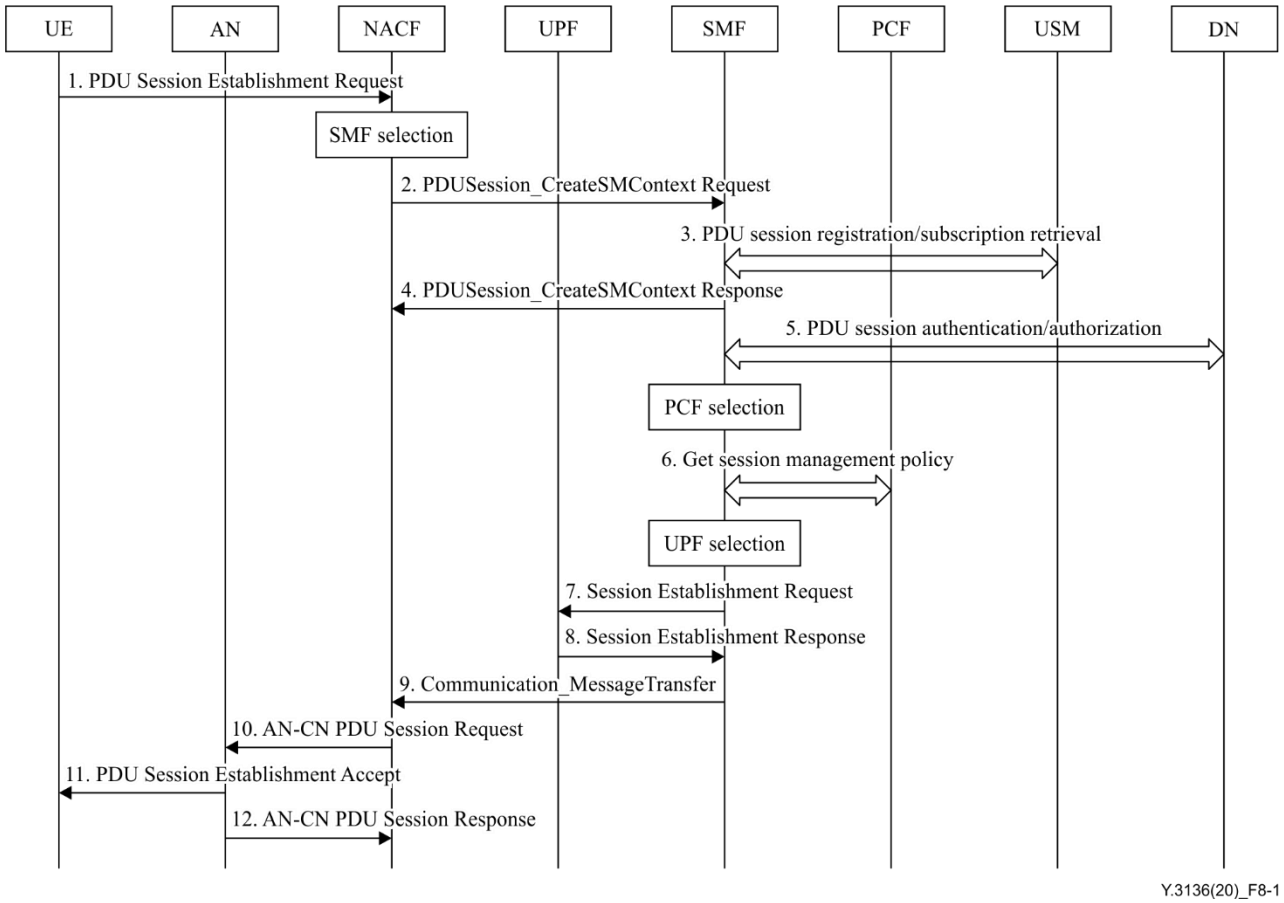

Figure 8-1 – PDU session establishment procedure

1. The UE sends a request message to the NACF. In order to establish a new PDU session, the UE generates a new PDU session ID. The UE initiates the PDU session establishment procedure by the transmission of a request message containing a PDU session establishment request. The NACF selects a most appropriate SMF.

2. The NACF sends the PDUSession_CreateSMContext Request message to the SMF.

3. The SMF retrieves PDU session information from the USM.

4. The SMF sends the PDUSession_CreateSMContext Response message to the NACF. The SMF processes the PDU session establishment request, and the SMF creates a SM context and responds to the NACF by providing a SM context identifier.

5. The serving SMF performs PDU session authentication/authorization with DN.

6. After the SMF selects an appropriate PCF via NFR, SMF gets SM policy for the PDU session via PCF.

7. Upon PDU session establishment request message, the SMF selects a proper UPF and allocates an IP address. If CN Tunnel Info is allocated by the SMF, the CN Tunnel Info is provided to the UPF in this step.

8. The UPF acknowledges by sending a session establishment response message. If CN Tunnel Info is allocated by the UPF, the CN Tunnel Info is provided to the SMF in this step.

9. The SMF sends the Communication_MessageTransfer message with PDU session and SM information to the NACF.

10. The NACF sends the AN-CN PDU session request message (PDU session ID and PDU session establishment accept targeted to the UE, the SM information received from the SMF to the AN).

11. The AN forwards the PDU session establishment accept message to the UE.

12. The AN acknowledges by sending the AN-CN PDU session response message to the NACF to setup PDU session UE-CN signalling.

8.1.2 Information flows for session modification

A PDU session modification may be initiated in order to change the path and quality of service (QoS) of an IP flow [ITU-T Y.3102], e.g., to cope with the status changes in access networks or for load balancing. The SMF requests the UPF to modify the IP type PDU session. According to the response message received from the UPF, the SMF sends a PDU session modification request message to the AN via the NACF. Figure 8-2 illustrates the PDU session modification procedure .

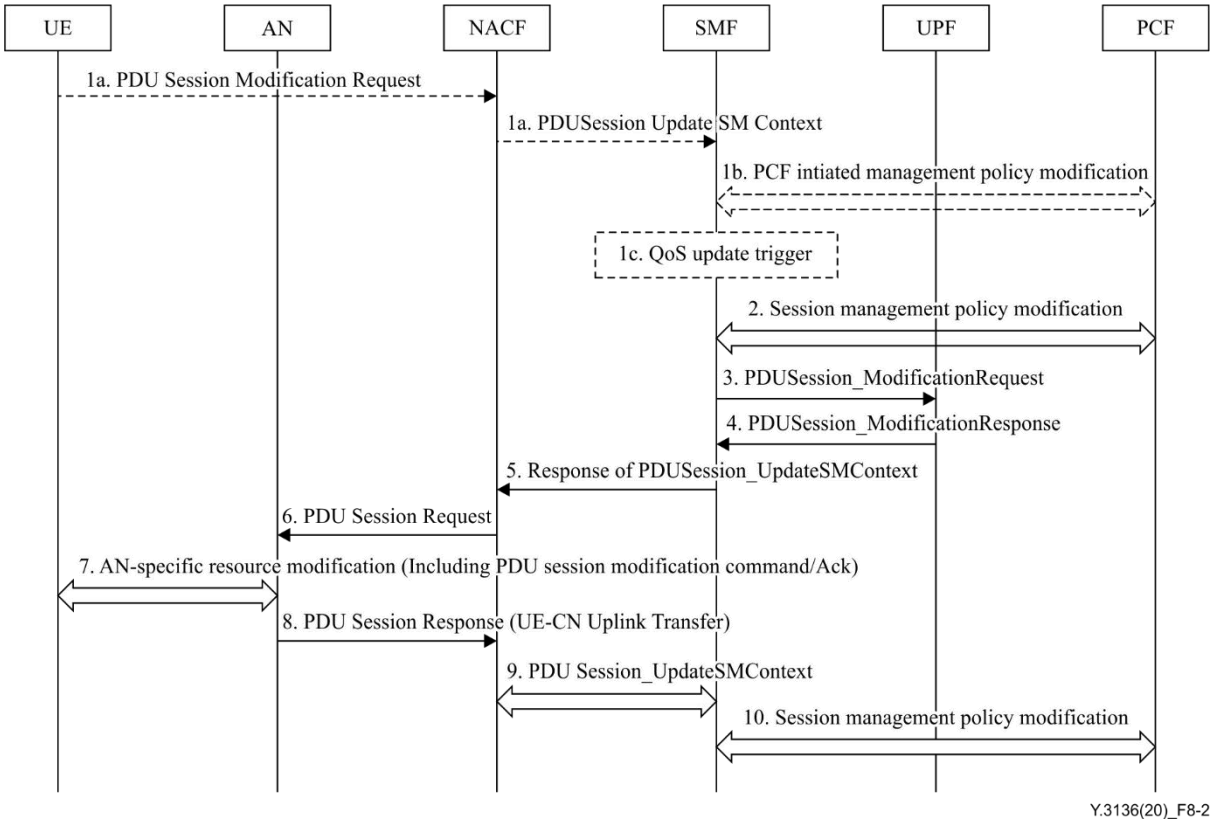

Figure 8-2 – PDU session modification procedure

1. The procedure may be triggered by the following events:

1a. The UE initiates the PDU session modification procedure by the transmission of UE-CN signalling. The signalling is forwarded by the AN to the NACF with an indication of user location information.

1b. Triggered by a policy decision or upon AF requests, the PCF performs a session management policy modification procedure to notify the SMF about the modification of policies.

1c. The SMF may decide to modify a PDU session. It may also be triggered if the SMF has marked that the status of one or more QoS flows are deleted in the CN but not yet synchronized with the UE. A QoS flow associated with the default QoS rule is required to be established for a PDU session and remains established throughout the lifetime of the PDU session.

2. The SMF may need to report some subscribed event to the PCF by performing a session management policy modification procedure. The PCF may provide new policy information to the SMF. This step may be skipped if PDU session modification procedure is triggered by step 1b or 1c, the PDU session modification requires action only at an UPF.

3. The SMF sends the PDUSession_ModificationRequest message to the UPF to modify the IP type PDU session.

4. The UPF responds to the SMF by sending the PDUSession_ModificationResponse message.

5. According to the response message received from the UPF, the SMF responds to the NACF through PDUSession_UpdateSMContext.

6. The NACF sends PDU Session Request message (SM information received from SMF, UE-CN signalling) to the AN, because the SMF sends a PDU Session Modification Request message to the AN via the NACF.

7. The AN issues AN specific signalling exchange with the UE that is related with the information received from the SMF.

8. The AN sends PDU session response message to the NACF, including that the AN forwards the UE-CN signalling to the NACF.

9. The NACF forwards the PDU Session Modification Command Ack message received from the AN to the SMF via PDUSession_UpdateSMContext Request message. The SMF replies with a PDUSession_UpdateSMContext Response message.

10. The SMF notifies the PCF with a session management policy modification message.

8.1.3 Information flows for session release

There are two types to trigger the PDU session release, explicit type and implicit type [ITU-T Y.3102]. Figure 8-3 illustrates the PDU session release procedure.

Explicit: The UE can request the release of an IP type PDU session explicitly to SMF. SMF releases the session, deletes all the flows belonging to the session and requests the deletion of the flows to UPF and AN. UPF and AN delete the corresponding resources.

Implicit: SMF or AN can trigger the PDU session release. For example, if there is no traffic through an IP flow within a given period, UPF notifies it to SMF. SMF deletes the flow and requests the deletion of the flow to UPF and AN. UPF and AN delete the corresponding resources. If there are no more IP flows in the PDU session, SMF releases the PDU session.

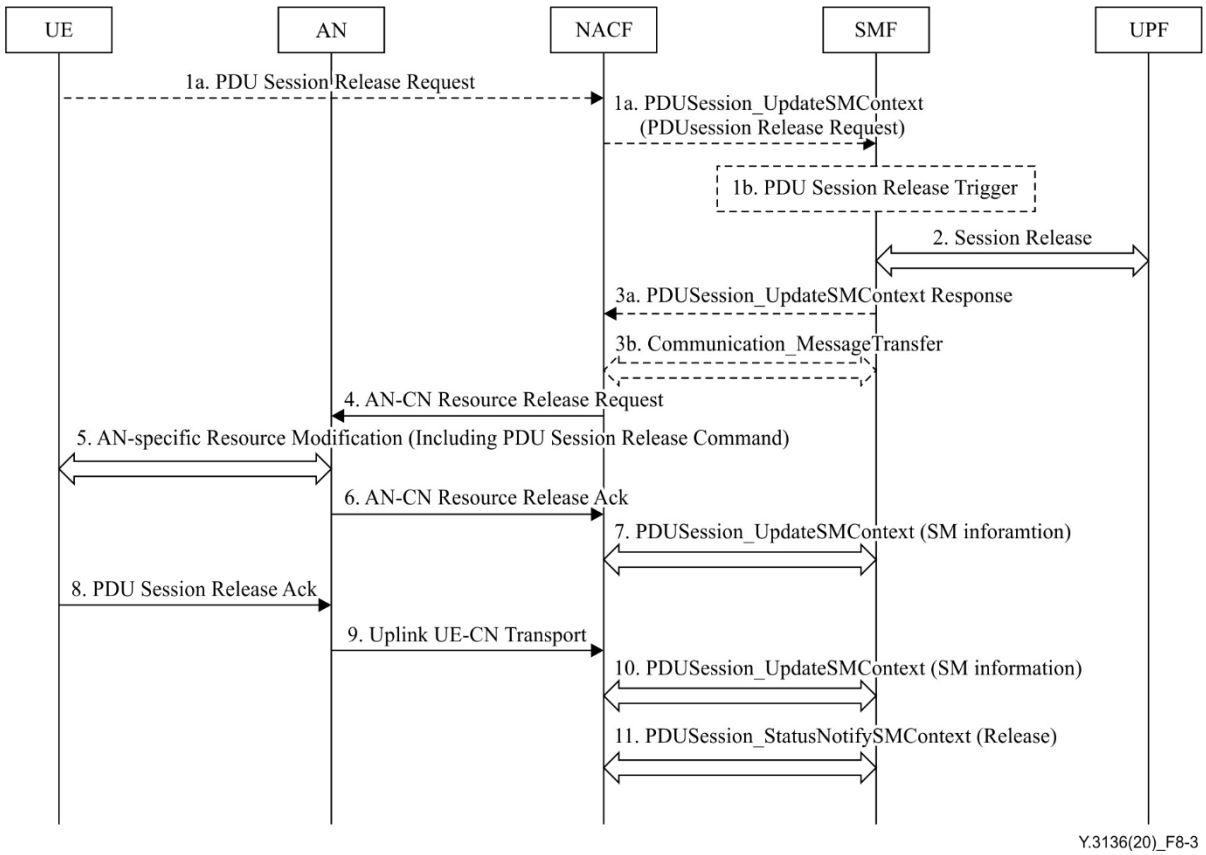

Figure 8-3 – PDU session release procedure

1. The procedure is triggered by one of the following events:

1a. The UE initiates the UE requested PDU Session Release procedure by the transmission of UE-CN signalling (PDU Session Release Request, PDU Session ID). The UE-CN signalling is forwarded by the AN to the NACF with an indication of user location information. The NACF sends the PDU Session Release Request message to the SMF together with user location information received from the AN.

1b. The SMF may decide to release a PDU session under the following scenarios:

– based on a request from the AN;

– if there is no traffic through an IP flow within a given period, the UPF notifies it to the SMF.

If the SMF receives one of the triggers in step 1a or 1b, the SMF starts PDU Session Release procedure.

2. The SMF sends a Session Release Request message (Session ID) to the UPF(s) of the PDU session. The UPF(s) shall drop any remaining packets of the PDU session and release all tunnel resource and contexts associated with the session. The UPF(s) acknowledges the session release request message by the transmission of a Session Release Response message (Session ID) to the SMF.

3a. If the PDU Session Release is initiated by the UE, the SMF creates a SM message including PDU Session Release Command message (PDU Session ID, Cause) and responds to the NACF with the PDUSession_UpdateSMContext Response message (SM Resource Release Request, SM information (PDU Session Release Command)).

3b. If the PDU session release is initiated by the SMF, the SMF invokes the Communication_MessageTransfer service operation (SM container (PDU Session Release Command), skip indicator). If the UP connection of the PDU session is active, the SMF shall also include the resource release request (PDU Session ID) in the Communication_MessageTransfer, to release the AN resources associated with the PDU session.

4. The NACF transfers the SM information (SM Resource Release Request, SM information) received from the SMF to the AN.

5. When the AN has received a SM request to release the AN resources associated with the PDU session, it issues AN specific signalling exchange(s) with the UE to release the corresponding AN resources.

6. After the AN had received a SM request to release the AN resources, the AN acknowledges the SM Resource Release Request message by sending a SM Resource Release Ack message (user location information) to the NACF.

7. The NACF invokes the PDUSession_UpdateSMContext message (SM Resource Release Ack, User Location Information) to the SMF. The SMF responds to the NACF with a PDUSession_UpdateSMContext Response message.

8. When all corresponding resources deleted, the UE acknowledges the PDU Session Release Command by sending UE-CN signalling (PDU Session ID, SM information (PDU Session Release Ack)) over the AN.

9. The AN forwards the UE-CN signalling from the UE by sending Uplink UE-CN Transport (UE-CN signalling (PDU Session ID, SM information (PDU Session Release Ack)), User Location Information) to the NACF.

10. The NACF invokes the PDUSession_UpdateSMContext message (SM information (PDU Session Release Ack), User Location Information) to the SMF. The SMF responds to the NACF with a PDUSession_UpdateSMContext Response message.

11. The SMF sends PDUSession_StatusNotify message to notify the NACF that the SM context for this PDU session is released. The NACF releases the association between the SMF ID and the PDU Session ID.

8.2 Traffic routing management

The traffic routing management describes how the ATSSS is executed based on the link quality detection and feedback. Traffic routing management function includes two procedures, downlink traffic routing management and uplink traffic routing management. In the procedures, it is assumed that UE has already established PDU sessions over mobile or fixed access network. The detailed information flow can be illustrated in the following procedures, representing the downlink and uplink procedure. For ANs which do not natively support a common signalling interface, an IWF needs to be provided at the AN-CN interface so that NFs deployed in the CN can still use a common signalling interface.

8.2.1 Downlink traffic routing management

The procedure is applied for ATSSS execution, in which the UPF implements the steering, switching, splitting operations based on the ATSSS rule and the status of the network.

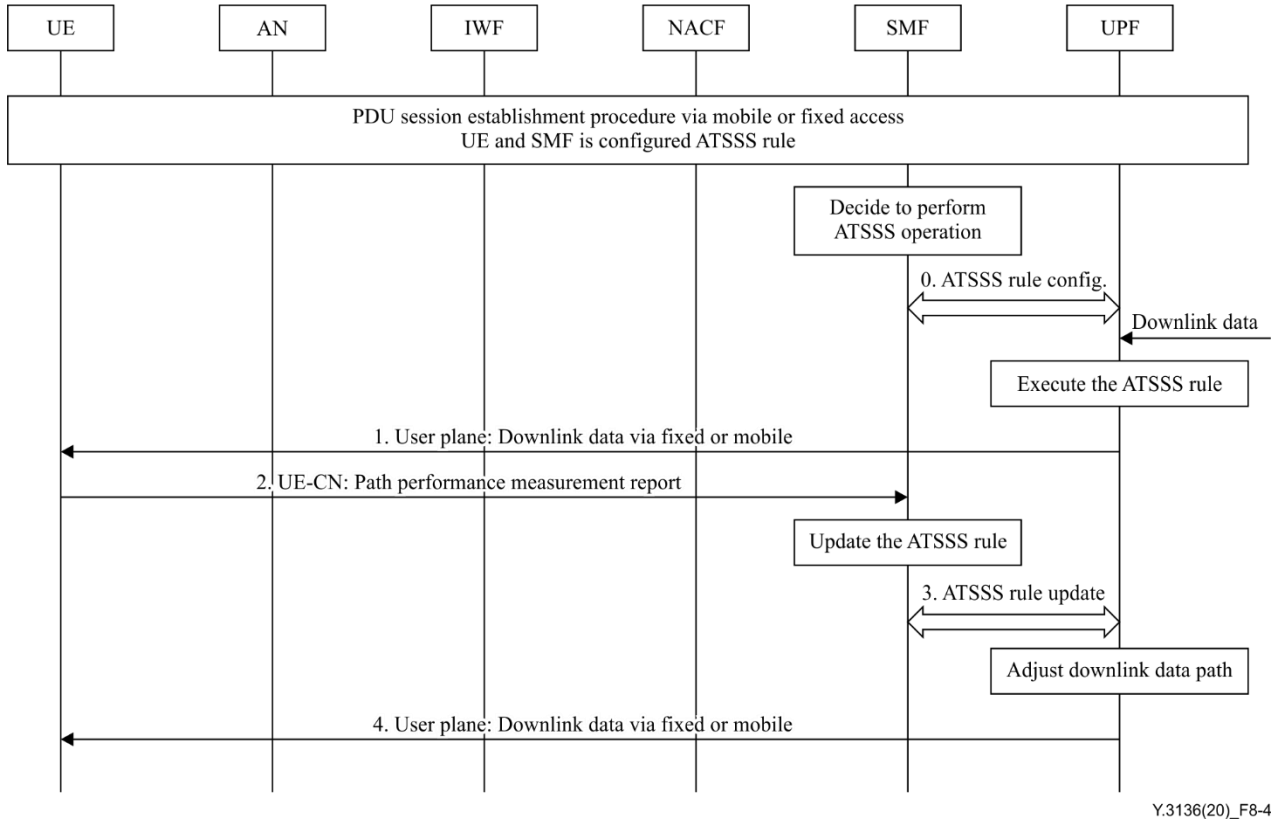

Figure 8-4 – Downlink traffic routing management procedure

The UE establishes the PDU sessions over mobile or fixed access network, and the ATSSS rule is configured at the UE and the SMF. The SMF decides to perform ATSSS operation.

0. The SMF configures the ATSSS rule and operation command to the UPF. The UPF sends the ATSSS rule configuration ACK message to the SMF.

1. When downlink data arrives, the UPF executes the ATSSS rule and determines the appropriate access path based on the ATSSS rule, to steer or split the downlink data. The UPF sends the downlink data to the UE via the selected access path.

2. The UE performs path performance measurement for each access path, e.g., the data loss rate, latency, the radio signal quality and reports the results to the SMF via UE-CN signalling based on the configured reporting condition. The SMF updates the ATSSS rule considering the UE feedback (the information of UE-CN signalling).

3. The SMF sends the updated ATSSS rule to the UPF; the UPF sends the ATSSS rule update ACK message to the SMF. The UPF implements the updated ATSSS rule and may adjust the access path for the service, e.g., switching the path from one access to another one or start/stop splitting operation for the uplink data based on the updated ATSSS rule.

4. The UPF sends the downlink data to the UE via the adjusted access path.

8.2.2 Uplink traffic routing management

The procedure is applied for ATSSS operation uplink transmission, in which the UE implements the ATSSS operation based on the ATSSS rule and the status of the network.

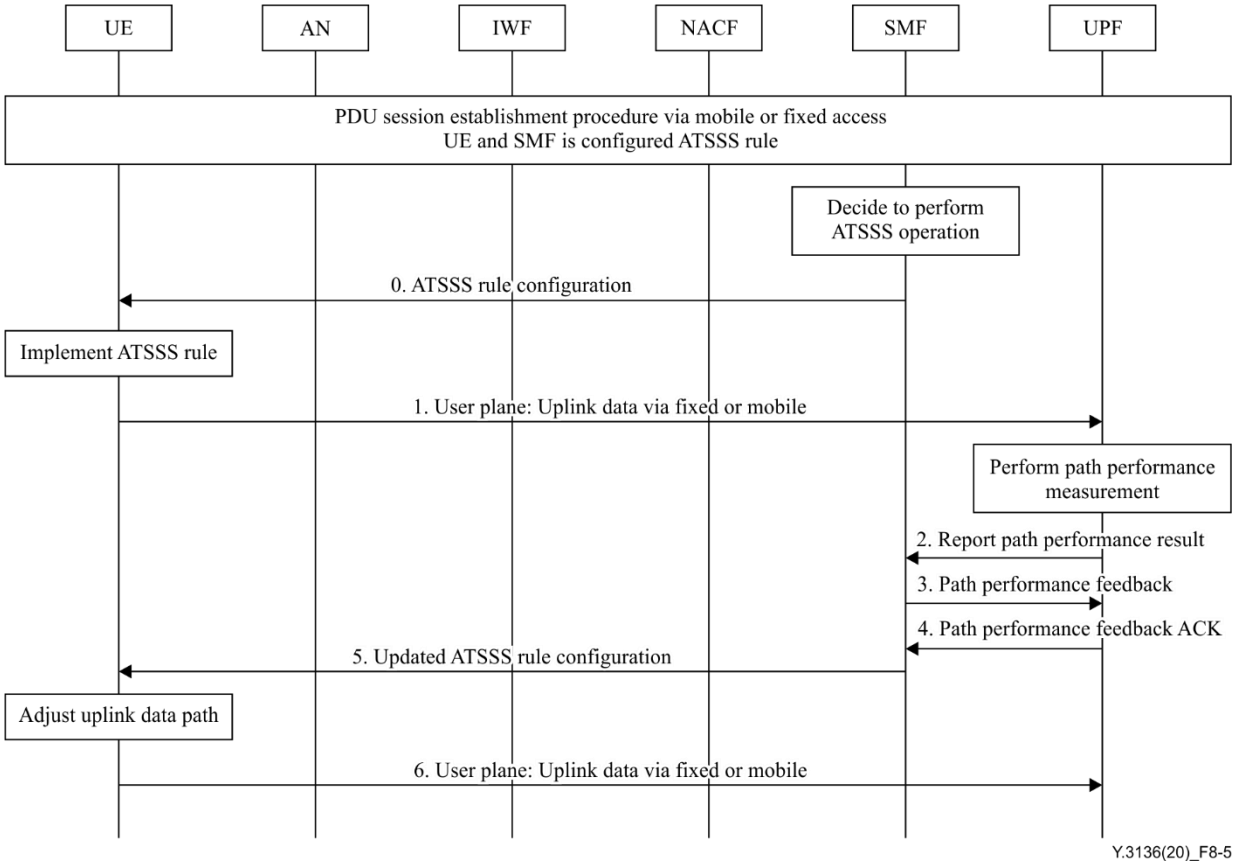

Figure 8-5 – Uplink traffic routing management procedure

The UE establishes the PDU sessions over mobile or fixed access network, and the ATSSS policy is configured at the UE and the SMF. The SMF decides to perform ATSSS operation.

0. The SMF configures the ATSSS rule and operation command to the UE.

1. The traffic flow control protocol in the UE implements ATSSS rule, and when uplink data arrives, the UE entity determines the appropriate access path based on the ATSSS rule. The UE sends the uplink data to the UPF via the selected access path.

2. The UPF performs path performance measurement, e.g., the data loss rate, latency and reports the results to the SMF based on the configured report condition.

3. The SMF sends the path performance feedback message to request the UPF feedback.

4. The UPF sends the path performance feedback ACK message to the SMF.

5. The SMF updates the ATSSS rule based on the UPF feedback and provides the updated ATSSS rule to the UE. The UE implements the updated ATSSS rule and may adjust the access path for the service, e.g., switching the path from one access to another one or start/stop splitting operation for the uplink data based on the updated ATSSS rule.

6. The UE sends the uplink data to the UPF via the adjusted access path.

9 Security considerations

The FMC in IMT-2020 network is required to be aligned with the security requirements contained in [ITU-T Q.1762] and the requirements of security and personal data protection contained in [ITU-T Y.3101], with the following additional ones:

- The FMC in IMT-2020 network is required to provide mechanisms to support data confidentiality and integrity for fixed and mobile access networks.
- The FMC in IMT-2020 network is required to provide secure storage, handling, and enforcement of policies.
- The FMC in IMT-2020 network is required to provide a security coordination function [ITU-T Y.3130] for coordinating security policies of all the individual access networks involved.

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, 2020