ETSI TS 123 527 V18.3.0 (2024-05)

TECHNICAL SPECIFICATION

5G;
5G System;
Restoration procedures
(3GPP TS 23.527 version 18.3.0 Release 18)

Reference

RTS/TSGC-0423527vi30

Keywords

5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 5
1 Scope 6
2 References 6
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 Restoration Procedures related to the N4 Interface 7
4.1 General 7
4.2 N4 Failure and Restart Detection 7
4.3 UPF Restoration Procedures 7
4.3.1 General 7
4.3.2 Restoration Procedure for PSA UPF Restart 8
4.3.3 Restoration Procedure for PSA UPF Failure without Restart 8
4.3.4 Restoration Procedure for Intermediate UPF Restart 8
4.3.5 Restoration Procedure for Intermediate UPF Failure without Restart 9
4.4 SMF Restoration Procedures 9
4.4.1 General 9
4.4.2 Restoration Procedure for SMF Restart 10
4.4.2.1 General 10
4.4.2.2 Restart of an SMF in a SMF Set 10
4.4.3 Restoration Procedure for SMF Failure without Restart 10
4.4.3.1 General 10
4.4.3.2 Failure of an SMF in a SMF set 10
4.5 N4 path failure 12
4.6 Partial failure handling over N4 12
4.6.1 General 12
4.6.2 Procedures 12
4.7 Restoration of PFCP sessions associated with a specific FQ-CISD, Group ID or SMF IP Address 14
4.7.1 General 14
4.7.2 Allocation of Group Id or FQ-CSID to a PFCP session 14
4.7.3 Restoration of PFCP sessions associated with an FQ-CSID, Group ID or SMF IP Address 14
5 Restoration Procedures related to the User Plane Interfaces N3 and N9 15
5.1 General 15
5.2 User Plane Failure Detection 15
5.2.1 Loss of GTP-U contexts 15
5.2.2 User Plane Path Failure 15
5.3 Restoration Procedures upon Loss of GTP-U contexts 16
5.3.1 General 16
5.3.2 Procedure for GTP-U Error Indication received from 5G-AN 16
5.3.2.1 Principles 16
5.3.3 Procedure for GTP-U Error Indication received from UPF 17
5.3.3.1 GTP-U Error Indication received by 5G-AN 17
5.3.3.2 GTP-U Error Indication received by another UPF 17
5.4 Restoration Procedures upon User Plane Path Failure 17
5.5 Reporting of a Peer GTP-U Entity Restart 18
6 Restoration Procedures related to Service-Based Interfaces 19
6.1 General 19
6.2 NF (NF Service) Failure and Restart Detection using the NRF 19
6.2.1 General 19

6.2.2 NF (NF Service) Failure 19
6.2.3 NF (NF Service) Restart 21
6.3 NF Service Producer Restart Detection using direct signalling between NFs 23
6.3.1 General 23
6.3.2 NF Service Producer Restart 24
6.4 NF Service Consumer Restart Detection using direct signalling between NFs 25
6.4.1 General 25
6.4.2 NF Service Consumer Restart 25
6.5 NF Service Producer Instance Reselection 27
6.5.1 General 27
6.5.2 NF Service Instance Reselection when a (Routing) Binding Indication is available 27
6.5.3 NF Service Instance Reselection when a (Routing) Binding Indication is not available 27
6.6 NF Service Consumer Instance Reselection 28
6.6.1 General 28
6.6.2 NF Service Consumer Instance Reselection when a (Routing) Binding Indication is available 28
6.6.3 NF Service Consumer Instance Reselection when a (Routing) Binding Indication is not available 29
6.7 Restoration of Profiles related to UDR 29
6.7.1 General 29
6.7.2 Procedure 31
6.8 Restoration Procedures for Home Routed PDU Sessions or PDU sessions with an I-SMF 33
6.8.1 General 33
6.8.2 V-SMF failure 33
6.8.3 H-SMF failure 34

7 Restoration Procedures related to Public Warning System (PWS) 34
7.1 General 34
7.2 PWS operation failure in NG-RAN 34
7.3 PWS operation restart in NG-RAN 34

8 Restoration Procedures for MBS 35
8.1 General 35
8.1A N4mb Failure and Restart Detection 35
8.2 Restoration procedures for MB-UPF failure with or without restart 36
8.2.1 General 36
8.2.2 Restoration Procedure for MB-UPF Restart 36
8.2.3 Restoration Procedure for MB-UPF failure without Restart 37
8.3 Restoration procedures for NG-RAN failure with or without restart 39
8.3.1 General 39
8.3.2 Broadcast MBS session restoration Procedure for NG-RAN failure with restart 39
8.3.2.1 General 39
8.3.2.2 Broadcast MBS session restoration by AMF 39
8.3.2.3 Broadcast MBS session restoration by MB-SMF 41
8.3.2.4 Selecting an alternative AMF for a Broadcast MBS Session at AMF failure 42
8.3.3 Broadcast MBS session restoration Procedure for NG-RAN failure without restart 44
8.3.4 Multicast MBS session restoration Procedure for NG-RAN failure with or without restart 45
8.4 Restoration procedures for AMF failure 48
8.4.1 Multicast MBS session (de)activation or update after an AMF failure 48
8.4.1.1 General 48
8.4.1.2 N2 MBS session request distribution with list of NG RAN Node IDs provided by MB-SMF to AMF 48

Annex A (informative): Change history 51

History 54

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document defines the restoration procedures in the 5G System.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.007: "Restoration procedures".

[3] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)".

[4] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes; Stage 3".

[5] 3GPP TS 23.502:"Procedures for the 5G System; Stage 2"

[6] 3GPP TS 29.518: "5G System; Access and Mobility Management Service; Stage 3".

[7] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[8] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[9] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[10] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[11] 3GPP TS 38.413: "NG Radio Access Network (NG-RAN); NG Application Protocol (NGAP)".

[12] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services; Stage 2".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and 3GPP TS 29.244 [4] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1] and 3GPP TS 29.244 [4].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5MBS	5G Multicast-Broadcast Services
AF/AS	Application Function / Application server
AMF	Access and Mobility Management Function
C-TEID	Common Tunnel Endpoint IDentifier
F-SEID	Fully Qualified SEID
F-TEID	Fully Qualified TEID (i.e. IP address and TEID)
PFCP	Packet Forwarding Control Protocol
GTP-U	GTP User plane
LLC SM	Low Layer Source Specific Multicast (address)
MBS	Multicast/Broadcast Service
MBSF	Multicast/Broadcast Service Function
MB-SMF	Multicast/Broadcast Session Management Function
MB-UPF	Multicast/Broadcast User Plane Function
NEF	Network Exposure Function
NG-RAN	Next Generation (5G) RAN
PSA	PDU Session Anchor
SMF	Session Management Function
TEID	Tunnel Endpoint IDentifier
UPF	User Plane Function

4 Restoration Procedures related to the N4 Interface

4.1 General

This clause specifies the procedures supported in the 5G System to detect and handle failures affecting the N4 interface.

4.2 N4 Failure and Restart Detection

Across PFCP based interfaces, an SMF and UPF shall utilize the PFCP Heartbeat Request and Heartbeat Response messages to detect a peer PFCP entity failure or restart as described in clause 19A of 3GPP TS 23.007 [2].

A PFCP function shall ignore the Recovery Timestamp received in PFCP Association Setup Request and PFCP Association Setup Response messages (see clause 6.2.6 of 3GPP TS 29.244 [4]).

4.3 UPF Restoration Procedures

4.3.1 General

When a UPF fails, all its Session contexts and PFCP associations affected by the failure become invalid and may be deleted.

4.3.2 Restoration Procedure for PSA UPF Restart

If F-TEID and/or UE IP address allocation is performed in the UPF, the UPF shall ensure that previously used F-TEID values and/or UE IP addresses are not immediately reused after a UPF restart, in order to avoid inconsistent F-TEID and/or UE IP address allocation throughout the network and to enable the restoration of PFCP sessions affected by the failure. How this is ensured is implementation specific.

The UPF shall not send GTP-U Error indication message for a configurable period after an UPF restart when the UPF receives a G-PDU not matching any PDRs.

During or immediately after an UPF Restart, the UPF shall place a local UPF Recovery Time Stamp value in all Heartbeat Request/Response messages.

Immediately after the re-establishment of a PFCP association between the SMF and the UPF, the SMF may start restoring PFCP sessions in the UPF.

The SMF should prioritize the PFCP sessions to restore based on operator's policy.

The SMF should control the load induced on the UPF when performing the PFCP restoration procedures, the way it is done is implementation specific.

When re-establishing a PFCP session and if F-TEID allocation and/or UE IP address is performed in the PSA UPF by network configuration, the SMF shall include a restoration indication in the PFCP Session Establishment Request message to indicate to the UPF it is for a restoration of an existing PFCP session and the UPF shall accept SMF allocated F-TEID and/or UE IP address if possible. If the UPF cannot accept the requested F-TEID and/or UE IP address because the IP address is no longer available at the UPF, the UPF shall reject the PFCP Session Establishment Request with the cause "PFCP session restoration failure due to requested resource not available".

NOTE: The cause "PFCP session restoration failure due to requested resource not available" corresponds to scenarios where the requested address is no longer available at the UPF, i.e. it cannot be assigned to any PFCP session, due to e.g. the address having been decommissioned by OAM from the UPF or e.g. the address being no longer operational due to a partial hardware failure at the UPF. This cause is not to be used for scenarios where the requested address would be available at the UPF but would have been re-assigned to a different PFCP session, which is a scenario that is not expected to happen based on the requirements specified above.

4.3.3 Restoration Procedure for PSA UPF Failure without Restart

Procedures for PSA UPF failure without restart are implementation specific.

4.3.4 Restoration Procedure for Intermediate UPF Restart

The SMF will receive the UPF recovery time stamps in PFCP heartbeat requests/responses.

After an Intermediate UPF restart, the PFCP association between the SMF(s) and the Intermediate UPF has to be re-established.

The restoration of the PFCP sessions may start immediately after the PFCP association setup procedure:

- if the restoration is supported in the SMF on a proactive basis, the SMF may start re-establishing PFCP sessions matching any PDRs.
- as defined in clause 4.3.2, the SMF should prioritize the PFCP sessions restoration.
- if the restoration is supported in the SMF on a reactive basis:
  - the SMF shall establish an PFCP session with a wildcarded PDR to instruct the Intermediate UPF to forward G-PDU packets which are not matching any other PDRs to the SMF (to a F-TEID uniquely assigned in the SMF for this PFCP-u tunnel);
  - upon receipt of G-PDUs from this PFCP-u tunnel, the SMF shall then check if it has an active session for each received G-PDU packet:

- if so, the SMF shall perform the PFCP Session establishment procedures to re-establish the corresponding PFCP sessions in the Intermediate UPF;
- otherwise the SMF shall generate a GTP-U Error Indication with a destination address set to the source IP address of the received G-PDU, and send it to the Intermediate UPF. The Intermediate UPF shall forward this GTP-U Error Indication transparently. The SMF shall delete the G-PDU after the check for active sessions.

NOTE 1: The UPF can filter the G-PDU packets with same target F-TEID and send only one such G-PDU to the Intermediate SMF.

When re-establishing a PFCP session and if F-TEID allocation is performed in the Intermediate UPF by network configuration, the SMF shall include a restoration indication in the PFCP Session Establishment Request message to indicate to the UPF it is for a restoration of an existing PFCP session and the UPF shall accept SMF allocated F-TEID if possible. If the UPF cannot accept the requested F-TEID because the IP address is no longer available at the UPF, the UPF shall reject the PFCP Session Establishment Request with the cause "PFCP session restoration failure due to requested resource not available".

The Intermediate UPF shall not send any Error indication messages for an operator configurable period after an Intermediate UPF restart when the Intermediate UPF receives G-PDU not matching any PDRs.

NOTE 2: If restoration on a reactive basis is used, the period needs to be longer than the time required by the SMF to detect the UPF restart, to establish the PFCP association and provision the wildcarded PDR. Otherwise, the period needs to be longer than the time required by the SMF to restore all the PFCP sessions on a proactive basis.

NOTE 3: The cause "PFCP session restoration failure due to requested resource not available" corresponds to scenarios where the requested address is no longer available at the UPF, i.e. it cannot be assigned to any PFCP session, due to e.g. the address having been decommissioned by OAM from the UPF or e.g. the address being no longer operational due to a partial hardware failure at the UPF. This cause is not to be used for scenarios where the requested address would be available at the UPF but would have been re-assigned to a different PFCP session, which is a scenario that is not expected to happen based on the requirements specified above.

4.3.5 Restoration Procedure for Intermediate UPF Failure without Restart

Procedures for Intermediate UPF failure without restart are implementation specific.

4.4 SMF Restoration Procedures

4.4.1 General

When a SMF fails, all its PDU session contexts and PFCP associations affected by the failure may become invalid and may be deleted.

When the SMF that fails is deployed as part of an SMF set, the PDU session contexts that were served by that SMF are maintained by the SMF set. The MPAS and SSET procedures specified for SMF set in clause 5.22 of 3GPP TS 29.244 [4] enable the restarted SMF to continue serving its own PFCP sessions, or other SMFs of an SMF set to take over seamlessly the PFCP sessions that were served by the SMF that fails.

If F-TEID allocation is performed in the SMF, the SMF should ensure as far as possible that previously used F-TEID values are not immediately reused after a SMF restart, in order to avoid inconsistent TEID allocation throughout the network.

NOTE: This is to ensure that F-TEIDs are not reused until earlier PDU sessions using them are released.

4.4.2 Restoration Procedure for SMF Restart

4.4.2.1 General

During or immediately after a SMF Restart, the SMF shall place local SMF-C Recovery Time Stamp value in all Heartbeat Request/Response messages.

The UPF will receive the SMF recovery time stamps in PFCP heartbeat requests/responses.

When a UPF detects that a peer PFCP entity in the SMF has restarted (as specified in clause 4.2), the UPF shall delete all session contexts affected by the PFCP entity restart that it may have stored. When the UPF receives a GTP-U PDU not matching any PDRs, it shall discard the GTP-U PDU and return a GTP error indication to the originating node (e.g. other UPF, gNB or N3IWF).

4.4.2.2 Restart of an SMF in a SMF Set

During or immediately after the restart of an SMF in an SMF set, using the MPAS or SSET procedure specified for SMF set in clause 5.22 of 3GPP TS 29.244 [4], the SMF shall not modify the local SMF Recovery Time Stamp value in its Heartbeat Request/Response messages.

Accordingly, the UPF does not detect that the peer PFCP entity in the SMF has restarted and will not delete the session contexts that were served by the restarted PFCP entity in the SMF.

When re-establishing its PFCP association with the UPF, the restarted SMF shall set the PFCP Session Retention Information IE to request the UPF to retain all its existing PFCP sessions if a PFCP association was already established in the UPF for the same Node ID (see clause 6.2.6.2.1 of 3GPP TS 29.244 [4]). Accordingly, the UPF shall retain all PFCP sessions that were established with the existing PFCP association and which have not been moved to other SMFs of the SMF set, if a PFCP association was already established at the UPF for the same Node ID.

NOTE: Depending on how fast the SMF restarts, the UPF can have moved some PFCP sessions to different SMF(s) of the SMF set as described in clause 4.4.3.2, e.g. if the UPF detected that the SMF was not responsive for some time.

4.4.3 Restoration Procedure for SMF Failure without Restart

4.4.3.1 General

When a UPF detects that a peer PFCP entity in the SMF is not reachable for a preconfigured time, and the MPAS or SSET procedure specified for SMF set in clause 5.22 of 3GPP TS 29.244 [4]) are not used, the UPF shall delete all the session contexts affected by the peer PFCP entity failure that it may have stored.

4.4.3.2 Failure of an SMF in a SMF set

When the MPAS or SSET procedure specified for SMF set in clause 5.22 of 3GPP TS 29.244 [4]) is used, when the UPF detects that a peer PFCP entity in an SMF is not responsive for a preconfigured time, or upon being instructed by SMF(s) of the SMF set to move PFCP sessions, the UPF shall move the PFCP sessions that were served by the failed PFCP entity to another PFCP entity in the same SMF or another SMF, as specified in clause 5.22 of 3GPP TS 29.244 [4] and clause 4.7.3.

Figure 4.4.3.2-1 depicts an example call flow for a failure (without restart) of an SMF in an SMF set using the MPAS or SSET feature.

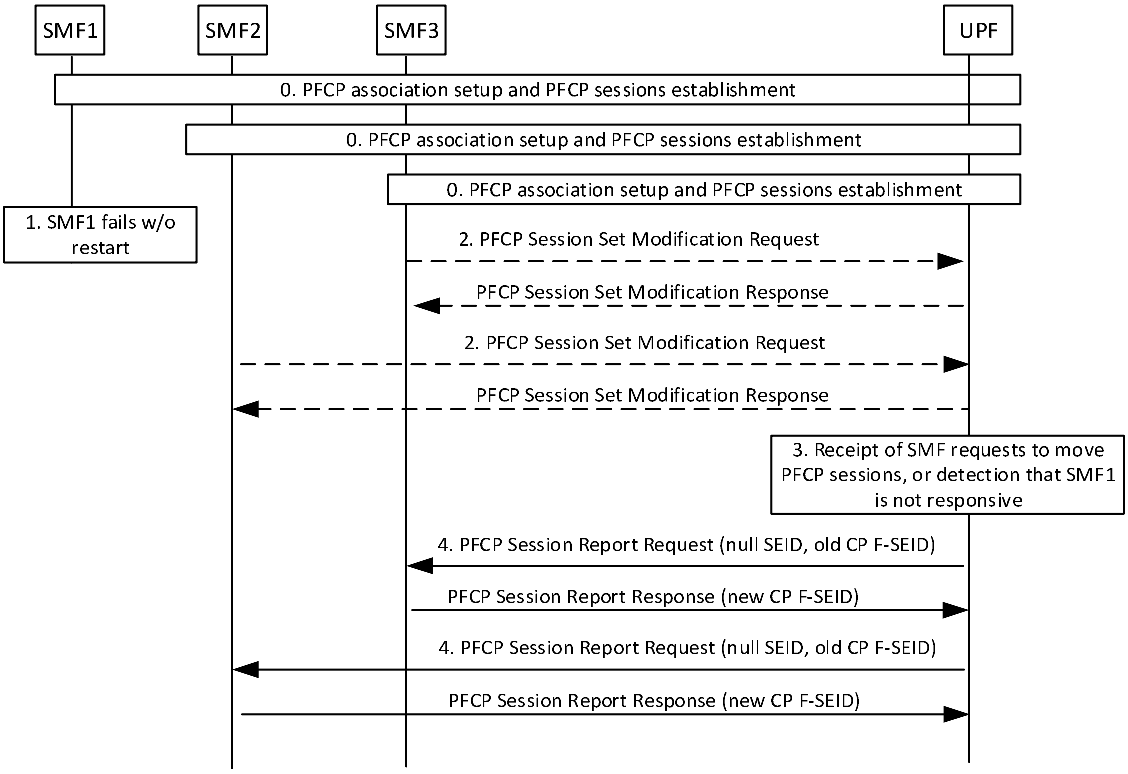
SMF1
SMF2
SMF3
UPF
0. PFCP association setup and PFCP sessions establishment
0. PFCP association setup and PFCP sessions establishment
0. PFCP association setup and PFCP sessions establishment
1. SMF1 fails w/o restart
2. PFCP Session Set Modification Request
PFCP Session Set Modification Response
2. PFCP Session Set Modification Request
PFCP Session Set Modification Response
3. Receipt of SMF requests to move PFCP sessions, or detection that SMF1 is not responsive
4. PFCP Session Report Request (null SEID, old CP F-SEID)
PFCP Session Report Response (new CP F-SEID)
4. PFCP Session Report Request (null SEID, old CP F-SEID)
PFCP Session Report Response (new CP F-SEID)

Figure 4.4.3.2-1: Failure (without restart) of an SMF in an SMF set using the MPAS or SSET feature

0. When using the MPAS feature, the SMFs of the SMF set establish PFCP associations with the UPF, including the SMF Set ID IE set to an FQDN representing the SMF Set and optionally Alternative SMF IP Address IE(s) of alternative PFCP entities in the same SMF or different SMFs of the SMF set.

   When using the SSET feature, one SMF of the SMF set establishes one PFCP association with the UPF for the SMF set, optionally including Alternative SMF IP Address IE(s) of alternative PFCP entities in the same SMF or different SMFs of the SMF set. In this case, the UPF considers that the SMF1, SMF2 and SMF3 represent different PFCP entities.

   The SMFs of the SMF set establish PFCP sessions in the UPF, optionally providing a FQ-CSID and/or a Group ID as described in clause 4.7.2.

1. The SMF1 fails without restart.

2. The SMFs of the SMF set may request the UPF to move group(s) of PFCP sessions, each identified by a FQ-CSID, Group ID or CP IP Address, to alternative SMF(s) of the SMF set.

3. Upon being instructed by the SMFs to move PFCP sessions, or upon detecting that the SMF1 is not responsive, the UPF sends subsequent PFCP Session Report Request messages to the alternative SMFs of the SMF set, as specified in clause 5.22 of 3GPP TS 29.244 [4] and clause 4.7.3. The UPF sets the SEID field to zero in the PFCP header of the PFCP Session Report Request and includes the old CP F-SEID that was assigned by the previous SMF in the request.

   Upon receiving such requests, the SMF takes over the control of the PFCP sessions from the previous SMF and sends PFCP Session Report Response messages including, for each PFCP session, the CP F-SEID IE with the IPv4 or IPv6 address of the new PFCP entity and the same or a modified SEID, and optionally including the N4-u F-TEID that the UPF shall use for sending data towards the new entity.

   Alternatively (not depicted in the figure), the SMF may redirect a PFCP Session Report Request to a different SMF of the same SMF set, either by rejecting the request with the cause "Redirection Requested" and with the IP address of the new entity to contact, or by forwarding the request to another PFCP entity pertaining to the same

SMF or another SMF in the SMF set. In the former case, the UPF resends a PFCP Session Report Request to the new PFCP entity to contact. In the latter case, the new PFCP entity sends a PFCP Session Report Response including the CP F-SEID IE with the IPv4 or IPv6 address of the new PFCP entity and the same or a modified SEID, and optionally including the N4-u F-TEID that the UPF shall use for sending data towards the new entity.

When a UPF detects that none of the SMF of the SMF set is responsive for a preconfigured time, the UPF shall delete all the session contexts established by any SMF of the SMF set that it may have stored.

4.5 N4 path failure

If the N4 path to the UPF is down, the SMF should handle this as an UPF Failure without Restart, see clause 4.3.3.

If the N4 path to the SMF is down, the UPF should handle this as a SMF Failure without Restart, see clause 4.4.3.

4.6 Partial failure handling over N4

4.6.1 General

The SMF and UPF may support the partial failure handling feature over N4. If so, they shall support the requirements specified in this clause.

This feature enables to clean up PFCP sessions optimally in the peer PFCP node (i.e. SMF or UPF), when a hardware or software failure affects a significant number of PFCP sessions. When it is not possible to recover the affected PFCP sessions, it is useful to inform the peer PFCP node about the affected PFCP sessions using an identifier that represents a large set of PFCP sessions, rather than doing so per PFCP session.

A Connection Set Identifier (CSID) shall identify a set of PFCP sessions within a PFCP node that may belong to an arbitrary number of UEs. A CSID is an opaque parameter local to a PFCP node. Each PFCP node that supports the feature shall maintain a local mapping of CSID to its internal resources. When one or more of these resources fail, the corresponding one or more fully qualified CSIDs shall be signalled to the peer PFCP nodes.

The fully qualified CSID (FQ-CSID) is the combination of the PFCP node identity and the CSID assigned by the PFCP node which together globally identifies a set of PFCP sessions.

The node identifier shall be globally unique across all 3GPP EPS and 5GS networks. Its format is defined in 3GPP TS 29.244 [4].

4.6.2 Procedures

The SMF and the UPF may each assign one FQ-CSID to a PFCP session during the PFCP session establishment, by signalling the SMF FQ-CSID in the PFCP Session Establishment Request or the UPF FQ-CSID in the PFCP Session Establishment Response, as shown in Figure 4.6.2-1.

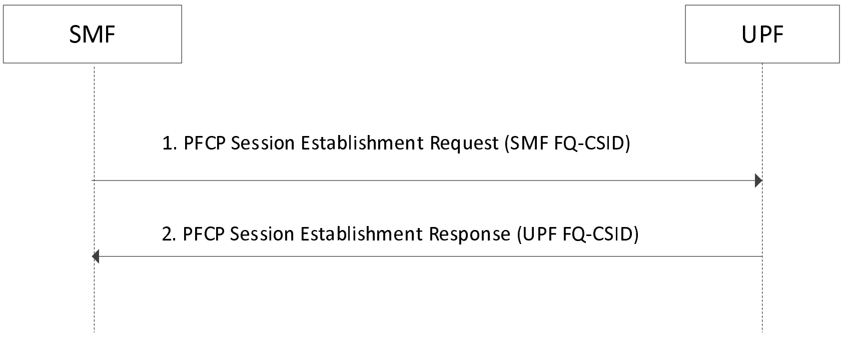
SMF
UPF
1. PFCP Session Establishment Request (SMF FQ-CSID)
2. PFCP Session Establishment Response (UPF FQ-CSID)

Figure 4.6.2-1 : PFCP Session Establishment procedure with FQ-CSID

The SMF and the UPF shall assign only one FQ-CSID for a given PFCP session and each FQ-CSID shall have exactly one CSID within the FQ-CSID. The peer PFCP node shall store the received FQ-CSID for the related PFCP session.

The receipt of a FQ-CSID also implicitly indicates that the peer FFCP node supports the feature.

The SMF and the UPF may update the FQ-CSID associated to a PFCP session during a PFCP session modification procedure, by signalling the SMF FQ-CSID in the PFCP Session Modification Request or the UPF FQ-CSID in the PFCP Session Modification Response, as shown in Figure 4.6.2-2.

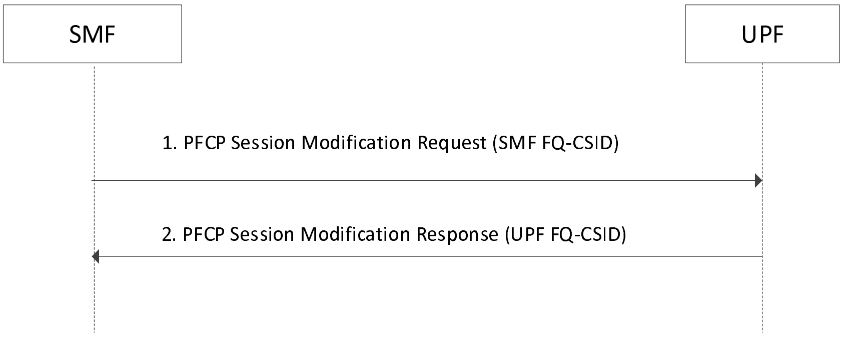
SMF
UPF
1. PFCP Session Modification Request (SMF FQ-CSID)
2. PFCP Session Modification Response (UPF FQ-CSID)

Figure 4.6.2-2: PFCP Session Modification procedure with change of FQ-CSID

An SMF that detects then that it has undergone a partial failure shall send a PFCP Session Set Deletion Request, including all its CSIDs corresponding to the component(s) that failed, to the UPF, if the UPF is known to support the feature, as shown in Figure 4.6.2-3.

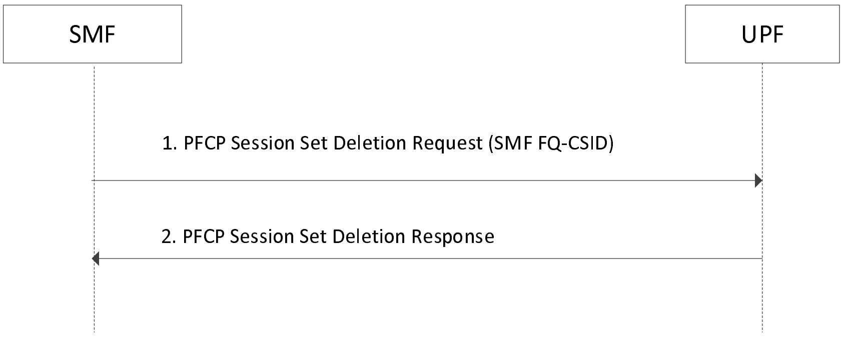
SMF
UPF
1. PFCP Session Set Deletion Request (SMF FQ-CSID)
2. PFCP Session Set Deletion Response

Figure 4.6.2-3: SMF initiated PFCP Session Set Deletion procedure

Likewise, an UPF that detects then that it has undergone a partial failure shall send a PFCP Session Set Deletion Request, including all its CSIDs corresponding to the component(s) that failed, to the SMF, if the SMF is known to support the feature, as shown in Figure 4.6.2-4.

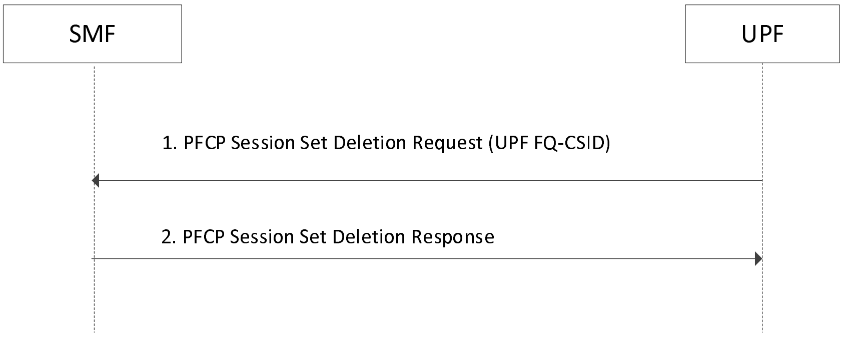
SMF
UPF
1. PFCP Session Set Deletion Request (UPF FQ-CSID)
2. PFCP Session Set Deletion Response

Figure 4.6.2-4: UPF initiated PFCP Session Set Deletion procedure

Upon receiving a PFCP Session Set Deletion Request reporting a partial failure for one or more FQ-CSID(s), the SMF or UPF shall find the PFCP sessions matching the FQ-CSID(s) and then proceed with the restoration procedures specified in clause 4 for an SMF or UPF failure.

4.7 Restoration of PFCP sessions associated with a specific FQ-CISD, Group ID or SMF IP Address

4.7.1 General

To reduce signalling latency and achieve a better load balancing among SMFs in a SMF Set when it is deployed, an SMF in a SMF Set and a UPF may support the procedures specified in this clause. These procedures enable an SMF from the same set to request UPF to move PFCP sessions associated with certain FQ-CSIDs (when partial failure handling is supported as specified in clause 4.6), Group IDs or SMF IP addresses, to (another) SMF(s) in the set proactively, without causing massing signalling (per PFCP session) towards UPF(s).

NOTE: The FQ-CSID can only be used in the procedure specified in this clause when the partial failure feature (using FQ-CSID) is deployed and used (not to force the NF to use a Group ID). For a network where the partial failure feature is not deployed, a Group ID or a SMF IP address needs to be used.

4.7.2 Allocation of Group Id or FQ-CSID to a PFCP session

To optimize the resource utilization for PFCP session(s), e.g. to meet different traffic requirements for different APNs/DNNs and/or DCNs/Network Slices, and also to facilitate moving a (sub)set of PDN connections/PFCP sessions among an SMF set, e.g. for a partial or complete SMF failure or a scale-in operation, an SMF in a SMF Set may:

- allocate a globally unique Group Id in the PFCP Session Establishment Request message for a PFCP session during a PFCP session establishment procedure and update the Group Id, if necessary, in subsequent PFCP Session Modification Request messages (see also clause 5.22.4 of 3GPP TS 29.244 [4]).

Alternatively, if partial failure handling is supported, the SMF may assign an FQ-CSID to a PFCP session as specified in clause 4.6.

Subsequently, e.g. when a partial or complete failure takes place affecting all PFCP sessions which are sharing either the same FQ-CSID or the Group ID (see clause 4.7.1), a PGW-C/SMF in a PGW-C/SMF Set may trigger the restoration procedure for those affected PFCP sessions as specified in clause 4.7.3.

4.7.3 Restoration of PFCP sessions associated with an FQ-CSID, Group ID or SMF IP Address

When there is a need to change the SMF controlling certain PFCP sessions, e.g. when a partial or complete failure takes place, the SMF (either the SMF serving the PFCP sessions or another SMF in the same Set taking over the control of the PFCP sessions) may send a PFCP Session Set Modification Request message to the UPF(s) to request the UPF(s) to send subsequent PFCP Session Report Request messages to the alternative SMF (as indicated in the Alternative SMF IP Address IE) for the PFCP sessions which are associated with the FQ-CSID(s) or Group ID(s), or which have their CP F-SEIDs containing the SMF IP Address as shown in Figure 4.7.3-1.

The SMF may instruct the UPF to move sessions associated with different SMF FQ-CSIDs, Group Ids or SMF IP addresses, to different SMF addresses.

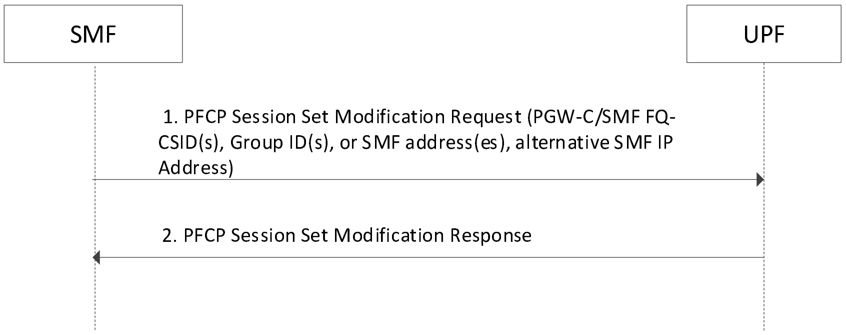
SMF
UPF
1. PFCP Session Set Modification Request (PGW-C/SMF FQ-CSID(s), Group ID(s), or SMF address(es), alternative SMF IP Address)
2. PFCP Session Set Modification Response

Figure 4.7.3-1: SMF initiated PFCP Session Set Modification procedure

5 Restoration Procedures related to the User Plane Interfaces N3 and N9

5.1 General

This clause specifies the procedures supported in the 5G System to detect and handle failures affecting the user plane interfaces N3 and N9

5.2 User Plane Failure Detection

5.2.1 Loss of GTP-U contexts

A GTP-U entity may lose its GTP-U contexts upon a failure or restart.

When a GTP-U node receives a G-PDU for which no corresponding GTP-U tunnel exists, the GTP-U node shall discard the G-PDU and return a GTP-U Error Indication to the sending node, as specified in clause 7.3.1 of 3GPP TS 29.281 [3].

The receipt of a GTP-U Error Indication is an indication for the sending GTP-U entity that the peer GTP-U entity cannot receive any more user plane traffic on the corresponding GTP-U tunnel.

5.2.2 User Plane Path Failure

A GTP-U entity may detect a user plane path failure by using GTP-U Echo Request and Echo Response messages, as specified in clause 20.3.1 of 3GPP TS 23.007 [2].

5.3 Restoration Procedures upon Loss of GTP-U contexts

5.3.1 General

The following clauses specify the behaviour of the different network entities when receiving a GTP-U Error Indication.

5.3.2 Procedure for GTP-U Error Indication received from 5G-AN

5.3.2.1 Principles

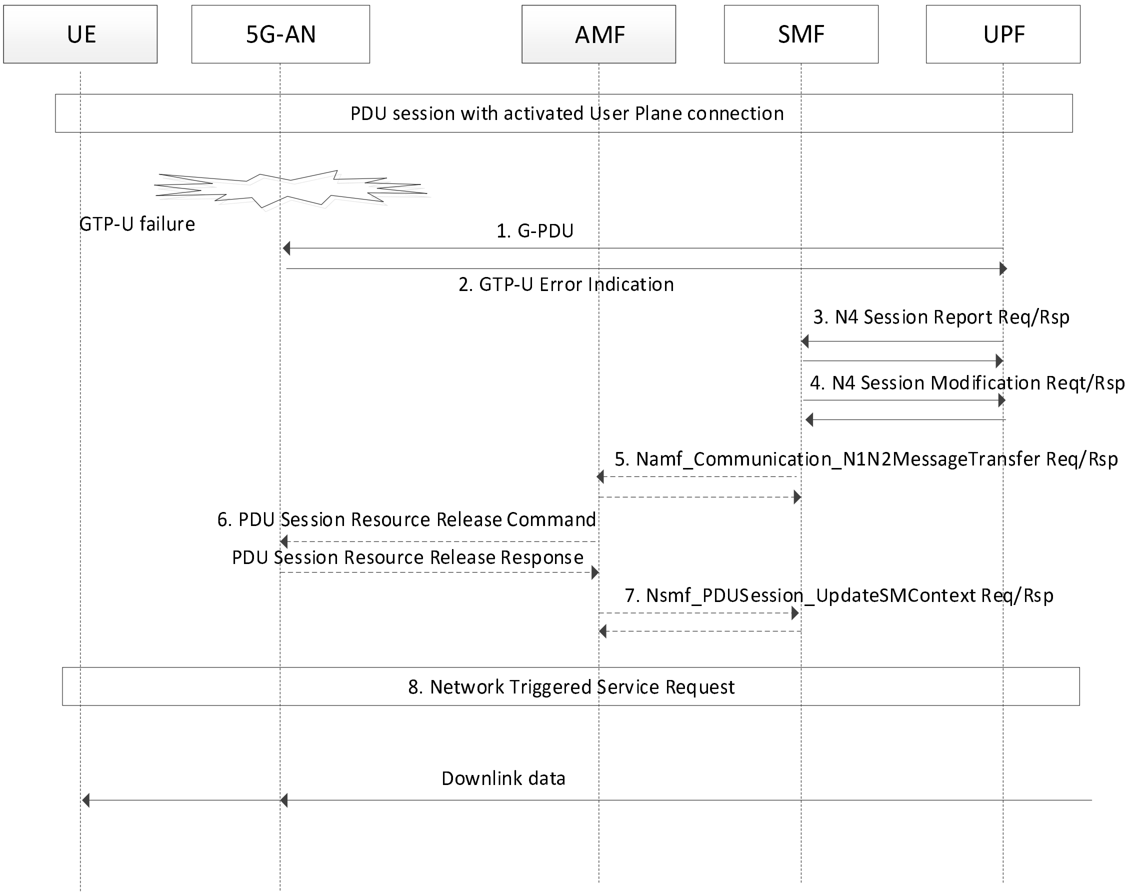
UE
5G-AN
AMF
SMF
UPF
PDU session with activated User Plane connection
GTP-U failure
1. G-PDU
2. GTP-U Error Indication
3. N4 Session Report Req/Rsp
4. N4 Session Modification Reqt/Rsp
5. Namf_Communication_N1N2MessageTransfer Req/Rsp
6. PDU Session Resource Release Command
PDU Session Resource Release Response
7. Nsmf_PDUSession_UpdateSMContext Req/Rsp
8. Network Triggered Service Request
Downlink data

Figure 5.3.2.1-1: GTP-U Error Indication from 5G-AN

1. The user plane connection of an existing PDU session is activated. Downlink G-PDUs are sent towards the 5G-AN.

2. The 5G-AN returns a GTP-U Error Indication if it does not have a corresponding GTP-U context (see clause 5.2).

3. Upon receipt of a GTP-U Error Indication, the UPF shall identify the related PFCP session and send an Error Indication Report to the SMF, as specified in clause 5.10 of 3GPP TS 29.244 [4].

4. For a GTP-U Error Indication received from a 5G-AN, the SMF shall modify the PFCP session to instruct the UPF to buffer downlink packets.

5. If the user plane connection of the PDU session is seen as activated by the SMF, the SMF shall initiate an Namf_Communication_N1N2MessageTransfer service operation to request the 5G-AN to release the PDU session's resources, as specified in clause 4.3.7 of 3GPP TS 23.502 [5].

6. Upon receipt of an Namf_Communication_N1N2MessageTransfer request to transfer the PDU Session Resource Release Command, the AMF shall:

  - proceed with the request, as specified in clause 5.2.2.3.1 of 3GPP TS 29.518 [6], if the UE is in CM-CONNECTED state for the Access Network Type associated to the PDU session;
  - otherwise, reject the request with an error indicating that the UE is in CM-IDLE state for the Access Network Type associated to the PDU session.

7. If the AMF sent a PDU Session Resource Release Command to the 5G-AN, the PDU session's resource release is acknowledged to the SMF.
8. The SMF initiates the Network Triggered Service Request procedure specified in clause 4.2.3.3 of 3GPP TS 23.502 [5], to re-activate the user plane connection of the PDU session.

5.3.3 Procedure for GTP-U Error Indication received from UPF

5.3.3.1 GTP-U Error Indication received by 5G-AN

Upon receipt of a GTP-U Error Indication, the 5G-AN shall proceed as follows:

- if the GTP-U Error Indication was received from an UPF over a NG-U tunnel that is not an indirect forwarding tunnel, the 5G-AN shall initiate a PDU Session Resource Notify procedure and release immediately the resources of the PDU session for which the Error Indication was received. The 5G-AN should indicate to the SMF that the release is due to receiving the GTP-U Error Indication from the NG-U tunnel.

  Upon receiving this information, the SMF may re-establish the PFCP session for the affected PDU session using the procedure specified in clause 4.3.2, if the related UPF is a PSA UPF or is an I-UPF controlled by the same SMF;

- if the GTP-U Error Indication was received from a peer5G-AN over a Xn-U direct forwarding tunnel or an UPF over a NG-U indirect forwarding tunnel, the 5G-AN may ignore the error indication or delete the forwarding tunnel context locally without deleting the corresponding PDU session and bearers.

NOTE: The 5G-AN behaviour for dual connectivity is not described in this specification.

5.3.3.2 GTP-U Error Indication received by another UPF

Upon receipt of a GTP-U Error Indication, the UPF shall identify the related PFCP session and send an Error Indication Report to the SMF, as specified in clause 5.10 of 3GPP TS 29.244 [4].

Upon receipt of an Error Indication Report from the UPF, the SMF shall identify the PDU session for which the Error Indication is received using the remote F-TEID included in the report.

For a GTP-U Error Indication received from another UPF, the SMF shall delete the PFCP session and PDU session, unless the UPF from which the Error Indication was received is controlled by the same SMF and the SMF is able to restore the user plane connectivity of the PDU session (e.g. Error Indication received from an Intermediate UPF controlled by the same SMF).

5.4 Restoration Procedures upon User Plane Path Failure

Upon detecting a GTP-U user plane path failure as specified in clause 5.2.2, the UPF shall report the user plane path failure to the SMF, by sending a PFCP Node Report Request (see 3GPP TS 29.244 [4]) including a User Plane Path Failure Report with the IP address of the remote GTP-U peer(s) towards which a failure has been detected. The UPF should also notify the GTP-U user plane path failure via the Operation and Maintenance system.

Upon detecting a failed GTP-U user plane path become recovered, the UPF shall report the user plane path recovery to the SMF, by sending a PFCP Node Report Request (see 3GPP TS 29.244 [4]) including a User Plane Path Recovery Report with the IP address of the remote GTP-U peer(s) associated with the recovered user plane path. The UPF should also notify the GTP-U user plane path recovery via the Operation and Maintenance system.

When the SMF receives the PFCP Node Report Request with a User Plane Path Failure Report, the SMF may:

- delete the PDU session contexts associated with the path in failure; or

- maintain the PDU session contexts associated with the path in failure during an operator configurable maximum path failure duration. The SMF shall delete the PDU session contexts associated with the path in failure if the path is still down when this duration expires; or

NOTE 1: During transient path failures (e.g. path failures not exceeding few minutes at most), maintaining the PDU session contexts associated with the peer's IP address enables the delivery of end user services (when the path is re-established again) and this also avoids unnecessary signalling in the network for restoring those PDU sessions.

NOTE 2: It is not intended to maintain PDU session contexts during long path failures (e.g. exceeding few minutes at most) as this would imply undesirable effects like undue charging.

- maintain the PDU session contexts associated with the path in failure if the path in failure is towards a 5G-AN. When deciding to maintain the PDU session contexts, it shall send a PFCP Session Modification Request message with changing Apply-Action from FORW to BUFF and NOCP for each affected PFCP session. In addition, upon receipt of subsequent downlink data notifications from the UPF or the service request from affected UE, the SMF will try to reestablish the PDU session resources in the NG-RAN. As an implementation option, the SMF may try to re-establish the PDU session resources in the NG-RAN for those PDU sessions associated with the user plane path in failure prior to receiving downlink data notifications from the UPF or service request from the affected UE.

NOTE 3: This approach (as above for user plane path failure towards a 5G-AN) allows to maintain the PDU session even for non-transient path failures. For a PDU session with I/V-SMF, the pause of charging (as specified in clause 4.4.4 of 3GPP TS 23.502 [5]) ensures that there is no undue charging.

When deciding to delete the PDU session contexts associated with the path in failure, the SMF shall modify or delete the affected PFCP sessions in the UPF.

NOTE 4: The SMF need to take care to smoothen the signalling load towards the UPF if a large number of PFCP sessions are affected by the user plane path failure.

5.5 Reporting of a Peer GTP-U Entity Restart

To reduce massive amount of N4 signalling to report the receiving of GTP-U Error Indication messages and to perform subsequent PFCP Session Modification for PFCP sessions affected by the peer GTP-U restart, a user plane function (UPF) and a control plane function (SMF) may optionally support reporting of a peer GTP-U entity restart.

A GTP-U entity, e.g. in a UPF, may detect the restart of the peer GTP-U entity as specified in clause 18A of 3GPP TS 23.007 [2].

When the user plane function detects the peer GTP-U entity has restarted via receiving one or more GTP-U Error Indication message(s) or Echo Request/Response message(s) containing a larger Recovery Time Stamp, and when the control plane function supports Reporting of a GTP-U Entity Restart, it shall send a PFCP Node Report Request message to the control plane function to report that:

- the peer GTP-U entity identified by Remote GTP-U Peer IE has restarted; and
- all PFCP sessions associated with the restarted peer GTP-U entity have been modified by the user plane function, i.e. the F-TEID(s) that had been allocated by the restarted GTP-U entity have been removed from the FARs and the Apply-Action in these FARs changed to BUFF and NOCP, if the restarted GTP-U entity is a 5G-AN.

NOTE: The UP function can learn if the restarted GTP-U entity is a 5G-AN by using the Destination Interface Type included in the Forwarding Parameters in the FAR (which contains the F-TEID that had been allocated by the restarted GTP-U entity).

The control plane function shall send a PFCP Node Report Response message to acknowledge the receipt of the report of the peer GTP-U entity restart; and the control plane may further behave as if it receives a Error Indication Report for those PFCP sessions affected by the peer GTP-U entity restart, e.g. to trigger a Network Triggered Service Request procedure if the restarted GTP-U entity is a 5G-AN. (See also clause 5.3.)

6 Restoration Procedures related to Service-Based Interfaces

6.1 General

A NF may detect a failure or a restart of a peer NF or NF service using the NRF as specified in clause 6.2.

A NF may also detect a restart of a peer NF or NF service by receiving recovery time information in signalling exchanged with that peer NF or NF service.

When NF (Service) Set is deployed in the network as specified in clauses 5.21.3 and 6.3.1.0 of 3GPP TS 23.501[9], an NF Service Producer in a NF (Service) Set creates resource contexts and the context data is shared by all the NF (Service) instances pertaining to the same NF (Service) set, i.e. the resource context is bound to the NF (Service) Set. So, requests targeting the resource may be served by any NF (Service) Instance within the NF (Service) set, unless the shared contexts are lost (which is further referenced in this specification as "the NF (Service) Set has failed or restarted").

In order to enable peer NFs to detect the loss of the resource contexts, i.e. the "restart of the NF (Service) Set or NF instance", and trigger appropriate restoration procedures, the NF Service Producer may provide a recovery timestamp associated to the highest resiliency level that it supports for the resource context, i.e. the binding entity with which the context data is shared (bound). Binding entities are sorted from the highest to the lowest resilience levels as follows: an NF Set, NF Instance, NF service set or NF service instance. The NF Service Producer may signal this recovery timestamp and its corresponding binding entity, in direct HTTP signalling or via the NRF.

NOTE 1: Signalling the recovery timestamp of an NF (Service) Set or an NF (Service) Instance via the NF profile in the NRF does not require the support of Binding Indication.

NOTE 2: Signalling the recovery timestamp and its corresponding binding entity in direct HTTP signalling requires the use of a Binding Indication (i.e. "3gpp-sbi-binding" HTTP header, see clause 5.2.3.2.6 of 3GPP TS 29.500 [10]). When multiple binding entities are present in a Binding Indication, the binding entity with the highest resiliency level is associated with the recovery timestamp; otherwise (if there is only one binding entity in a Binding Indication), the recovery timestamp is associated with that binding entity in the Binding Indication.

A NF may prioritize the contexts to restore based on operator's policy.

A NF should control/regulate the load induced on a peer NF or NF service when performing the restoration procedures.

The restoration procedures initiated when detecting a failure or a restart are not specified in this release.

6.2 NF (NF Service) Failure and Restart Detection using the NRF

6.2.1 General

This clause describes optional procedures that may be supported by NFs to detect the failure or restart of a NF or a NF service using the NRF.

6.2.2 NF (NF Service) Failure

Figure 6.2.2-1 describes a NF failure scenario and how other NFs can be notified of this failure.

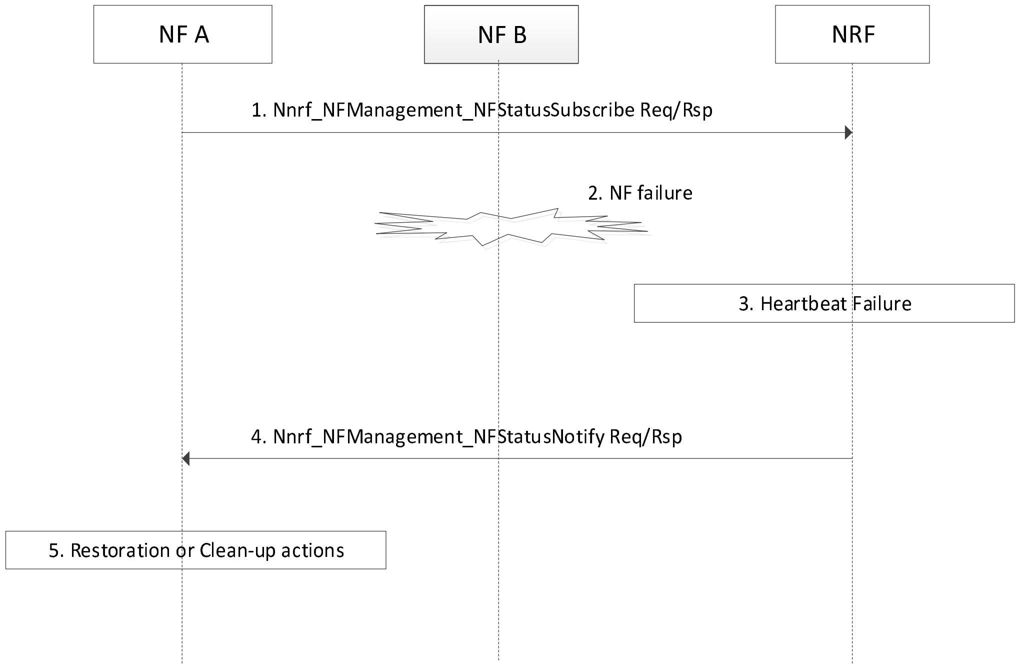
NF A
NF B
NRF
1. Nnrf_NFManagement_NFStatusSubscribe Req/Rsp
2. NF failure
3. Heartbeat Failure
4. Nnrf_NFManagement_NFStatusNotify Req/Rsp
5. Restoration or Clean-up actions

Figure 6.2.2-1: NF Failure Detection and Notification

1. NF A subscribes to the NRF to receive notifications of changes of the NF B Profile, as specified in 3GPP TS 29.510 [7].
2. A NF failure occurs at NF B.
3. The NRF detects that NF B is no longer operative using the NF Heart-Beat procedure as specified in clause 5.2.2.3.2 of 3GPP TS 29.510 [7]. The NRF changes the NFStatus of NF B to SUSPENDED.
4. The NRF notifies NFs having subscribed to receive notifications of changes of the NF B Profile that the NFStatus of NF B is changed to SUSPENDED.
5. NF A may trigger appropriate restoration or clean-up actions, if it cannot communicate with NF B.

Figure 6.2.2-2 describes a NF service failure scenario and how other NFs can be notified of this failure.

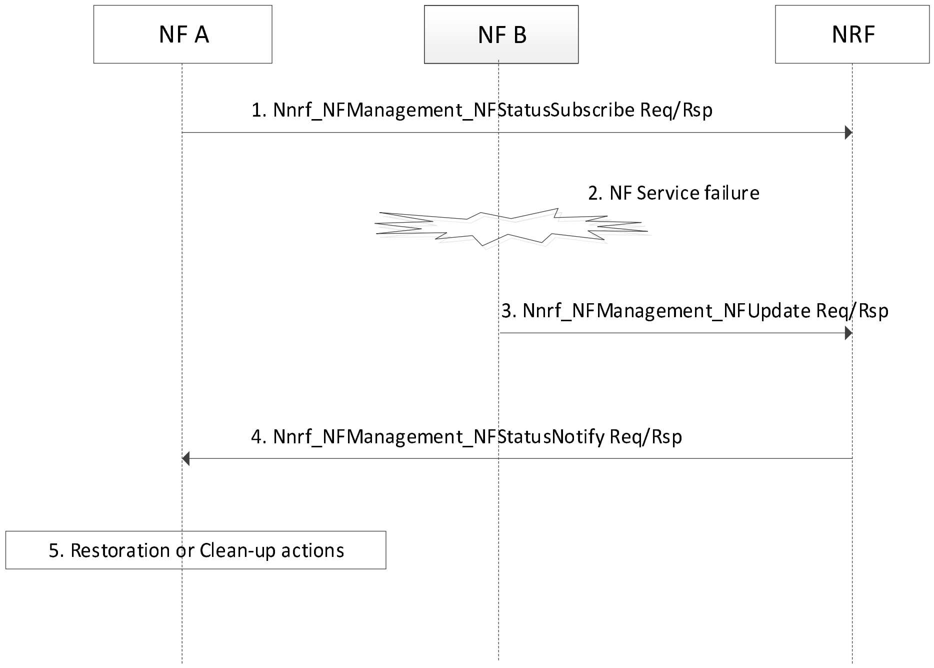
NF A
NF B
NRF
1. Nnrf_NFManagement_NFStatusSubscribe Req/Rsp
2. NF Service failure
3. Nnrf_NFManagement_NFUpdate Req/Rsp
4. Nnrf_NFManagement_NFStatusNotify Req/Rsp
5. Restoration or Clean-up actions

Figure 6.2.2-2: NF Service Failure Detection and Notification

1. NF A subscribes to the NRF to receive notifications of changes of the NF B Profile.

2. A NF Service failure occurs at NF B. NF B (other than the failed NF Service) is still operative.

3. NF B (or OAM) updates its NF Profile in the NRF, by setting the NFServiceStatus of the failed NF Service to SUSPENDED.

4. The NRF notifies NFs having subscribed to receive notifications of changes of NF B Profile that the NF Service status of the failed NF service of NF B is changed to SUSPENDED.

5. NF A triggers appropriate restoration or clean-up actions, if it cannot communicate with the NF B service.

6.2.3 NF (NF Service) Restart

Figure 6.2.3-1 describes a NF restart scenario and how other NFs can be notified of this restart.

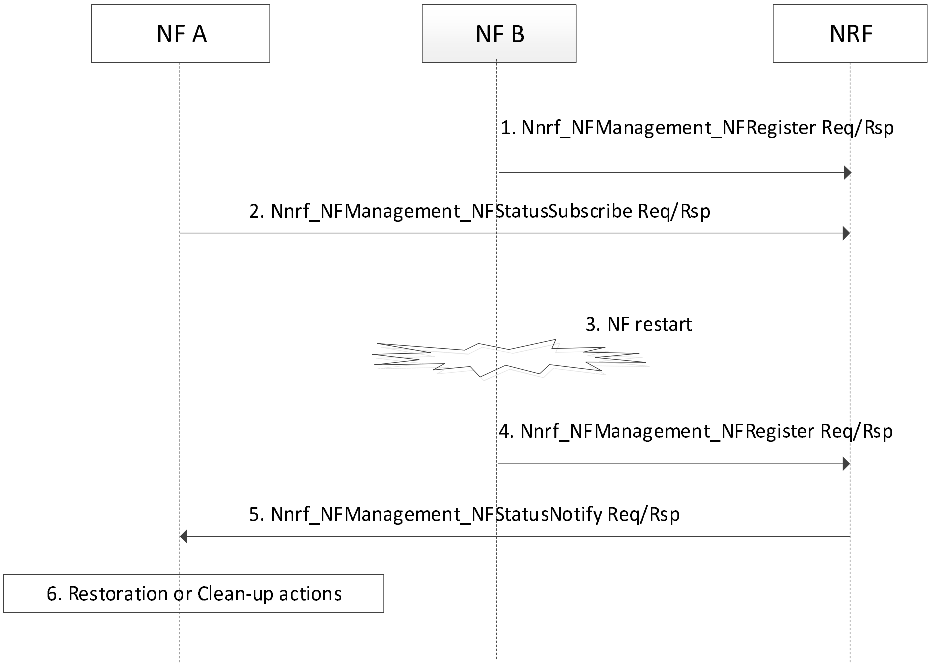
NF A
NF B
NRF
1. Nnrf_NFManagement_NFRegister Req/Rsp
2. Nnrf_NFManagement_NFStatusSubscribe Req/Rsp
3. NF restart
4. Nnrf_NFManagement_NFRegister Req/Rsp
5. Nnrf_NFManagement_NFStatusNotify Req/Rsp
6. Restoration or Clean-up actions

Figure 6.2.3-1: NF Restart Detection and Notification

1. NF B (or OAM) registers NF B Profile to the NRF. The NF B Profile may include the recoveryTime attribute, if a restart of NF B results in losing contexts.

   NF B Profile may include the recoveryTime attribute of the NF Set to which NF B pertains to, when NF B pertains to an NF Set, i.e. when the resource contexts created in the NF B is bound to the NF Set, i.e. resource contexts are accessible by all NF Instances within the NF Set.NOTE 1:The restart of an NF Set indicates that resource contexts bound to the NF Set (i.e. that are accessible by all NF Instances within the NF Set) have been lost.2 NF A subscribes to the NRF to receive notifications of changes of the NF B Profile.

3. NF B restarts.

4. If contexts are lost during the restart, NF B (or OAM) updates the recoveryTime in its NF Profile in the NRF.

   NF B Profile shall update the recoveryTime attribute of the NF Set to which NF B pertains to, if the whole NF Set has restarted and NF B has registered the recoveryTime for that NF Set.

5. The NRF notifies NFs having subscribed to receive notifications of changes of NF B Profile about the updated recoveryTime of the NF B Profile or updated recoveryTime of NF Set to which the NF B pertains to.

6. NF A may consider that all the resources created in the NF B before the NF B recovery time as have been lost. NF A triggers then appropriate restoration or clean-up actions.

Figure 6.2.3-2 describes a NF service restart scenario and how other NFs can be notified of this restart.

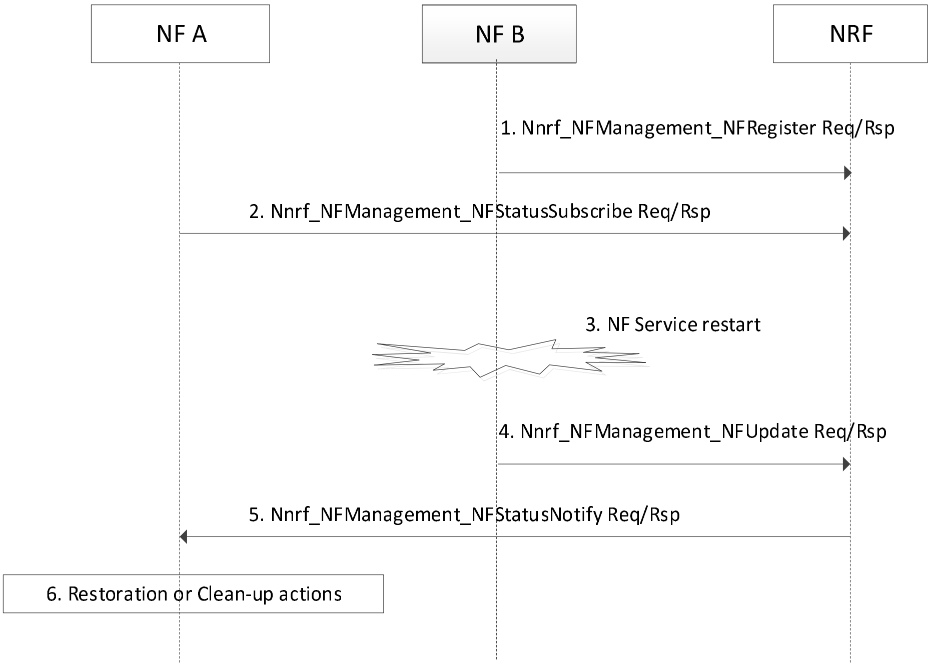
NF A
NF B
NRF
1. Nnrf_NFManagement_NFRegister Req/Rsp
2. Nnrf_NFManagement_NFStatusSubscribe Req/Rsp
3. NF Service restart
4. Nnrf_NFManagement_NFUpdate Req/Rsp
5. Nnrf_NFManagement_NFStatusNotify Req/Rsp
6. Restoration or Clean-up actions

Figure 6.2.3-2: NF Service Restart Detection and Notification

1. NF B (or OAM) registers its NF B Profile (and its services) to the NRF. The NF B Profile may include the recoveryTime attribute for the NF Services it supports, if a restart of a NF B service results in losing contexts. The NF B Profile may include the recoveryTime attribute of either the NF Service Set, NF Instance or NF Set to which the NF Service Instance pertains to, when the resource context for the NF Service created in NF B is bound to NF Service Set, or NF Instance, or NF Set respectively, i.e. accessible by all NF Service Instances within an NF Service Set, NF Instance or NF Set respectively (see clause 6.3.1.0 of 3GPP TS 23.501 [9]).

NOTE 2: The restart of an NF Service Set indicates that the resource contexts bound to the NF Service Set (i.e. accessible by all NF Service Instances within the NF Service Set) have been lost.

2 NF A subscribes to the NRF to receive notifications of changes of the NF B Profile.

3. A NF B service restarts.

4. If contexts are lost during the service restart, NF B (or OAM) updates the recoveryTime of the corresponding NF Service in the NRF. NF B (or OAM) shall update the recoveryTime attribute of the NF Service Set, NF Instance or NF Set to which the NF Service Instance pertains to, when the whole NF Service Set, NF Instance or NF Set has restarted respectively.

5. The NRF notifies NFs having subscribed to receive notifications of changes of the NF B Profile about the updated recoveryTime of the NF B Service or updated recoveryTime of the NF B Service Set, NF Instance or NF Set.

6. NF A may consider that all the resources created in the NF B service before the NF B service recovery time as have been lost. NF A triggers then appropriate restoration or clean-up actions.

6.3 NF Service Producer Restart Detection using direct signalling between NFs

6.3.1 General

This clause describes an optional procedure that may be supported by NFs to detect the restart of a peer NF service using direct signalling between NFs.

6.3.2 NF Service Producer Restart

Figure 6.3.2-1 describes a NF Service restart scenario of an NF Service Producer and how the NF Service Consumer can detect this restart.

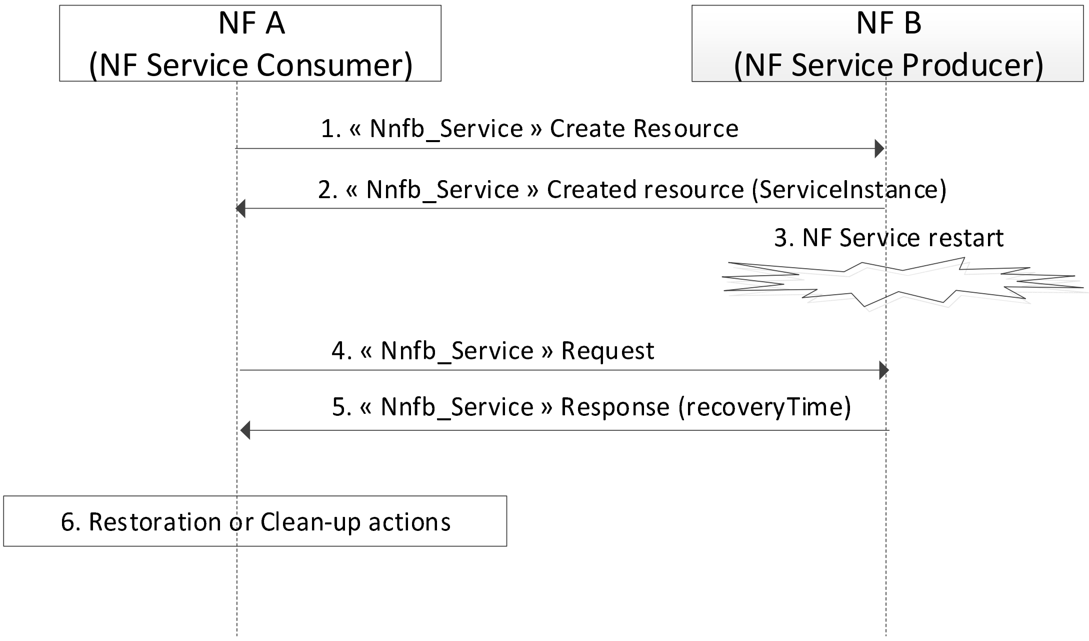
NF A
(NF Service Consumer)
NF B
(NF Service Producer)
1. « Nnfb_Service » Create Resource
2. « Nnfb_Service » Created resource (ServiceInstance)
3. NF Service restart
4. « Nnfb_Service » Request
5. « Nnfb_Service » Response (recoveryTime)
6. Restoration or Clean-up actions

Figure 6.3.2-1: NF Service Producer Restart Detection

1. NF A (NF Service Consumer) requests to create a resource in the NF B (NF Service Producer).

2. If the request is accepted, and if NF B implements the procedure specified in this clause, NF B shall return its NF B service instance ID in the response, and NF A shall associate the created resource with the NF B service instance if no Binding Indication is received from NF B.

   In the response message, the NF B that supports this procedure may include the recovery timestamp in the Binding Indication (i.e. in the "3gpp-sbi-binding" HTTP header). An NF A that supports this procedure shall associate the created resource with the binding entity and the recovery timestamp as specified in clause 6.1.

3. A NF service produced by NF B restarts, e.g. an NF Service Instance in NF B, an NF Service Set in NF B, NF B or the NF Set to which NF B pertains has restarted.

4-5. NF B Service Producer may include its last recovery timestamp in responses it sends to the NF A Service Consumer, if the restart of the NF service resulted in losing contexts and e.g. if the NF service has restarted recently.

6. NF A may consider that all the resource contexts are lost, which were created in the NF B service instance before the updated recovery timestamp, if the recovery timestamp was associated to the NF B service instance.

   If the recovery timestamp was associated to an NF Service Set, NF Instance or NF Set, NF A may consider that all the resource contexts are lost, which were created in these binding entities before the recovery, as indicated in the received recovery timestamp.

   NF A may trigger then appropriate restoration or clean-up actions.

NOTE 1: The recovery time signalled in this procedure is equivalent to the recovery time of the NF service of Figure 6.2.3-2. For an entire NF restart scenario, this procedure can be applied by each NF service instance of the NF.

NOTE 2: This procedure enables the detection of a restart of a peer NF service when sending signalling towards that NF Service. It can fasten the detection of a restart of a peer NF service when frequent signalling occurs towards that peer NF Service.

NOTE 3: In some use cases, NF A is not aware of the NF B Service Instance ID when creating the resource, e.g. a V-SMF just receives the H-SMF URI from the AMF to create a PDU session resource in H-SMF. Besides, for APIs supporting distributed collections (e.g. SMF), the response can contain a different Service Instance ID (that need not be registered in the NRF) than the one selected by NF A for sending the request.

6.4 NF Service Consumer Restart Detection using direct signalling between NFs

6.4.1 General

This clause describes an optional procedure that may be supported by NFs to detect the restart of a peer NF Service Consumer by NF Service Producer using direct signalling between NFs.

When NF (Service) Set is deployed in the network as specified in clause 5.21.3 and 6.3.1.0 of 3GPP TS 23.501[9], an NF Service Consumer in an NF (Service) Set may create a session context for callback (corresponding to the resource context in the NF Service Producer) when invoking a NF Service and the session context data is shared by all NF (Service) instances pertaining to the same NF (Service) set, i.e. the context is bound to the NF (Service) Set. So, any NF (service) instance within the NF (service) set is able to receive notifications or callback request from the NF Service Producer, unless the shared contexts are lost (which is further referenced in this specification as "the NF (Service) Set has failed or restarted").

In order to enable peer NF Service Producers to detect the loss of the session contexts in the NF Service Consumer, i.e. the "restart of the NF (Service) Set or NF instance", and trigger appropriate restoration procedures, the NF Service Consumer may provide a recovery timestamp associated to the highest resiliency level it supports for the context, i.e. the binding entitiy with which the context data is shared (bound). Binding entities are sorted from the highest to the lowest resilience levels as follows: an NF Set, NF Instance, NF service set or NF service instance. The NF Service Consumer may signal this recovery timestamp in direct HTTP signalling, using a Binding Indication.

6.4.2 NF Service Consumer Restart

Figure 6.4.2-1 describes a NF Service Consumer restart scenario and how the NF Service Producer can detect this restart.

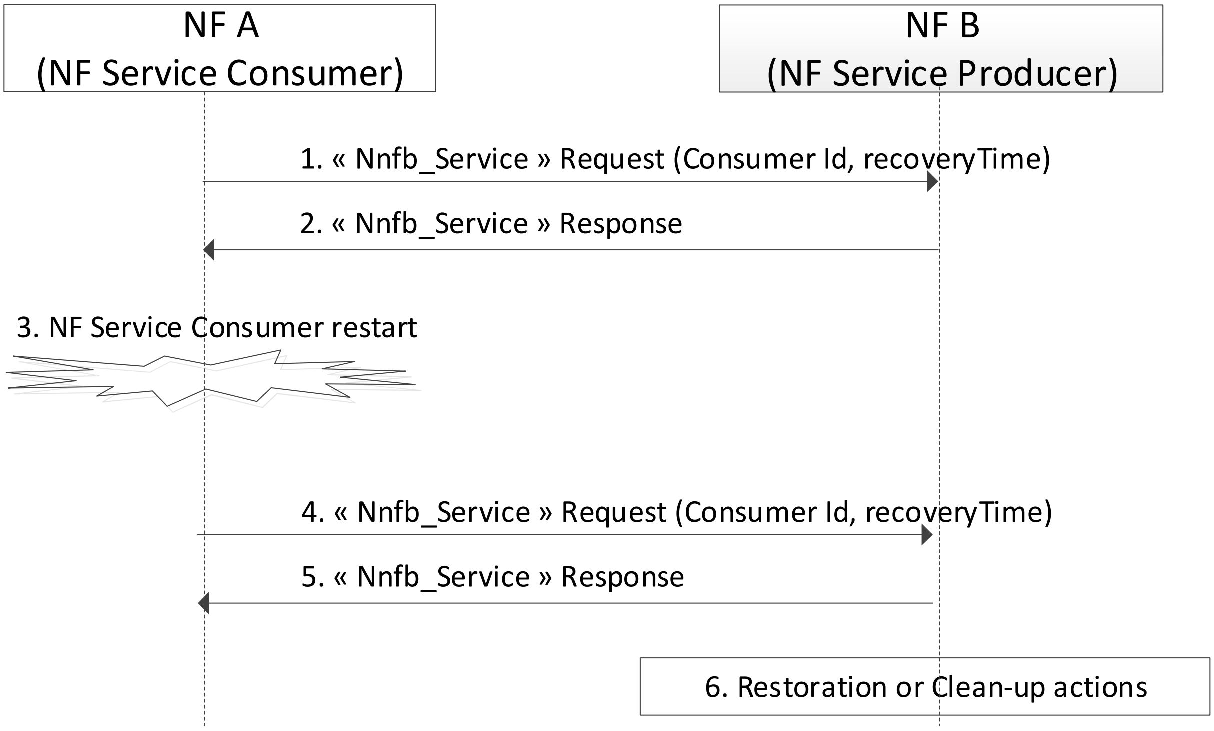
NF A
(NF Service Consumer)
NF B
(NF Service Producer)
1. « Nnfb_Service » Request (Consumer Id, recoveryTime)
2. « Nnfb_Service » Response
3. NF Service Consumer restart
4. « Nnfb_Service » Request (Consumer Id, recoveryTime)
5. « Nnfb_Service » Response
6. Restoration or Clean-up actions

Figure 6.4.2-1: NF Service Consumer Restart Detection

1. NF A (NF Service Consumer) requests to create a resource in the NF B (NF Service Producer). If NF A implements the procedure specified in this clause, it shall include a Consumer Id together with the last recovery timestamp in the request. The Consumer Id shall be identical for all service requests triggered by the NF service consumer for that service and shall be globally unique (e.g. using UUID).

   If NF A includes Binding Indication(s) (i.e. in the "3gpp-sbi-binding" HTTP header) in the request, NF A may include the recovery timestamp for the higher level binding entity indicated in the Binding Indication with the scope set to "callback" (see clause 5.2.3.2.6 of 3GPP TS 29.500 [10]).

2. If resource creation is successful, NF B as service producer shall store the received Consumer Id and recovery timestamp and associate the created resource with it.

   An NF B that supports this procedure shall associate the callback resource and the recovery timestamp to the higher level binding entity indicated in the received Binding Indication (with the scope set to "callback").

   If the Service Request contains Binding Indication(s) with the scope set to "other service", the NF B may use the binding information and associated recovery timestamp to detect whether resources that NF B has created in NF A have been lost, according to the principles specified in clause 6.3.2.

3. The NF service consumer in NF A restarts.

4. The NF service consumer in NF A shall include its last recovery timestamp together with the Consumer Id in the request when invoking service provided by NF B. The same Consumer Id shall be used after restarting.

   If NF A includes Binding Indication(s) in the request, NF A shall include the updated recovery timestamp for the higher level binding entity to which the callback resource context is bound in the Binding Indication with the scope set to "callback".

5. NF B as NF service producer may compare the received recovery timestamp with previous stored and detect the NF service consumer has restarted, if the received recovery timestamp is newer than the previous one.

The consumer Id for the resource or the Binding Indication with the scope set to "callback" may be updated if another service consumer took over the usage of the resource. e.g. if a new consumer Id is received during a service operation of a resource. NF B as NF service producer shall consider the service consumer handling the resource has changed and associate the resource with the new consumer Id or according to the new Binding Indication and with the corresponding recovery timestamp.

6. NF B may consider that the contexts in NF A corresponding to all the resources associated with the consumer Id or all resources bound to the entity (with which the recovery timestamp is associated) and the previous stored recovery time stamp have been lost. NF B triggers then appropriate restoration or clean-up actions.

NOTE 1: This procedure is only supported by NF services that support signalling the recovery timestamp attribute.

NOTE 2: This procedure can be used when the resource is exclusively used by an NF service consumer.

NOTE 3: This procedure enables the detection of a restart of a peer NF service consumer when sending signalling towards that NF service producer. It is helpful if the NF A as a pure service consumer without registration of its profile in NRF. If NF A does have a profile registered in NRF, it also can fasten the detection of a restart of a peer NF service consumer when frequent signalling occurs towards that peer NF Service.

6.5 NF Service Producer Instance Reselection

6.5.1 General

An NF Instance of an NF Service Producer may expose several service instances of the same NF Service (e.g., an UDM instance may expose several service instances of the "Nudm_SubscriberDataManagement" service).

An NF Service Consumer may discover, while an SCP shall be able to discover, via NRF Nnrf_NFDiscovery service, all available NF Service Instances for a given NF Service and select one of them.

6.5.2 NF Service Instance Reselection when a (Routing) Binding Indication is available

When using the Binding procedures specified in clause 6.12 of 3GPP TS 29.500 [10], Binding Indications and Routing Binding Indications include the Binding level and one or more Binding entity IDs representing all NF service instances that are capable to serve service requests targeting the resource, i.e. that share the same resource contexts.

When a Binding Indication or a Routing Binding Indication is available for a target resource, NF Service Instance selection and re-selection shall be supported as specified in clause 6.12 of 3GPP TS 29.500 [10].

6.5.3 NF Service Instance Reselection when a (Routing) Binding Indication is not available

If a formerly selected NF Service Instance becomes unavailable, the NF Service Consumer may, while the SCP shall be able to select a different instance of a same NF Service in:

- the same NF Instance, if the NF Instance indicates in its NF Profile that it supports the capability to persist their resources in shared storage inside the NF Instance, and if the new NF Service Instance offers the same major service version; or
- the same NF Set or NF Service Set, if the NF (service) instance indicates in its NF Profile that it belongs to an NF Set or an NF Service Set.

If so, the NF Service Consumer may, while the SCP shall be able to invoke service operations in the newly selected NF Service Instance by means of replacing the addressing parameters with those of the new service instance, and the new NF Service Instance in the NF Service Producer shall produce the same result as if the service request would have been successfully delivered to the former NF Service Instance.

NOTE 1: In some scenarios, the newly selected NF Service Producer might not produce the exact same result as the former NF Service Producer would have produced for the service request, e.g. when the former NF Service Producer failed before it could update a change in the resource context to the USDF.

For indirect communication, if the NF service consumer delegates target NF service instance reselection to the SCP (when the target NF service instance is not reachable), the NF Service Consumer shall include at least one of the 3gpp-Sbi-Discovery-target-nf-instance-id, 3gpp-Sbi-Discovery-target-nf-set-id, 3gpp-Sbi-Discovery-target-nf-service-set-id, 3gpp-Sbi-Discovery-amf-region-id and 3gpp-Sbi-Discovery-amf-set-id headers, and it should also include at least the following information in its request to the SCP:

- the target NF type, the service name, and the requested S-NSSAI in the corresponding "3gpp-Sbi-Discovery-*" request header(s) (see clause 6.10.3.2 of 3GPP TS 29.500 [10]).

NOTE 2: This is to allow the SCP to discover and reselect a target NF service instance from the target NF instance or target NF (service) set for the corresponding service request and supporting the requested S-NSSAI, e.g. when the NF service producer supports different NF service instances serving different network slices. Likewise, other "3gpp-Sbi-Discovery-*" request header(s), e.g. target-plmn-list, can also be included for the same purpose.

NOTE 3: The inclusion of the 3gpp-Sbi-Discovery-target-nf-instance-id in an HTTP request enables the SCP to discover the profile of the target NF instance and to possibly reselect a different target NF service instance from the same NF instance or from a different NF instance in the same set.

If so, the SCP shall use the information provided by the NF service consumer to perform a NF service discovery procedure and reselect a NF (service) producer instance as specified in the preceding bullets, if possible and if the target NF Service Instance indicated in the "3gpp-Sbi-Target-apiRoot" header or target URI is not reachable.

NOTE 4: This reselection mechanism is applicable only for the request/response service semantics, but not for notify/callback requests.

If the NF instance does not indicate in its NF Profile the support of the capability to persist their resources in shared storage across service instances of the same NF Service, inside the NF Instance, and if it does not indicate in its NF Profile that it belongs to an NF Set or an NF Service Set, the NF Service Consumer or SCP may still reselect any of the exposed service instances, but it shall not assume that the resources created in the former service instance are still valid.

6.6 NF Service Consumer Instance Reselection

6.6.1 General

When NF (Service) Set is deployed in the network as specified in clauses 5.21.3 and 6.3.1.0 of 3GPP TS 23.501[9], an NF Service Consumer in an NF (Service) Set may create a session context for callback (corresponding to the resource context in the NF Service Producer) when invoking a NF Service and the session context data is shared by all NF (Service) instances pertaining to the same NF (Service) set, i.e. the context is bound to the NF (Service) Set.

An NF Service Producer may, while the SCP shall be able to discover, via NRF Nnrf_NFDiscovery service, all available NF (Service) Instances within the NF (service) set that are capable to receive the notifications or callback requests and select one of them.

NOTE: When an NF service consumer changes, if the new NF service consumer does not support handling the notification or callback requests as described above, the new NF service consumer updates NF service producers with new URI as specified in clause 6.5.3.2 of 3GPP TS 29.500 [10].

6.6.2 NF Service Consumer Instance Reselection when a (Routing) Binding Indication is available

When using the Binding procedures specified in clause 6.12 of 3GPP TS 29.500 [10], Binding Indications and Routing Binding Indications include the Binding level and one or more Binding entity IDs representing all NF service consumer instances that are capable to receive the notifications or callback requests targeting the session context for callback (corresponding to the resource context in the NF Service Producer). See also clause 6.5.3.2 of 3GPP TS 29.500 [10].

When a Binding Indication or a Routing Binding Indication is available for a target context, NF Service Consumer selection and re-selection shall be supported as specified in clause 6.12 of 3GPP TS 29.500 [10].

6.6.3 NF Service Consumer Instance Reselection when a (Routing) Binding Indication is not available

When the target NF Service Consumer becomes unavailable, the NF Service Producer may, while the SCP shall be able to select a different instance of the Service Consumer which is capable to receive the notifications or callback requests targeting the session context for callback (corresponding to the resource context in the NF Service Producer) in:

- the same consumer NF instance, using an alternate endpoint address information if any is configured at the NF instance level, or at the NF service instance level when the name of the NF service to which these notifications are to be sent is known and the (consumer) NF instance registered in its NF Profile that it is capable to persist its resources in shared storage across NF service instances of the same NF Service;

- the same NF (service) Set or a backup NF Service Consumer if applicable.

NOTE 1: When binding procedures are not supported, the NF Service Consumer can provide in certain APIs the name of the NF service to which these notifications are to be sent. This service can be one of the service produced by the NF (if this NF Service Consumer can also serve as a NF Service Producer) and registered in the NRF, or a custom service registered in the NRF for the purpose of receiving these notifications). See clause 6.5.2.2 of 3GPP TS 29.500 [10].

NOTE 2: When the AMF serves as a NF Service Consumer, it can indicate to the NF Service Producer its backup AMF. See clause 5.21.2 of 3GPP TS 23.501 [9].

NOTE 3: NF Service Consumer Reselection when a (Routing) Binding Indication is not available is only supported when the NF Service Producer has the target NF Service Consumer information available, e.g. for APIs where the NF Service Consumer can communicate its NF Instance Id to the NF Service Producer in the service request message.

If so, the NF Service Producer may, while the SCP shall be able to send the notification or callback request to the newly selected NF Service Consumer Instance by means of replacing the addressing parameters with those of the newly selected instance. If the Callback URI included a prefix it shall be removed from the notification URI when using an alternate Consumer NF Service Instance and the callback URI prefix of the new Consumer NF Service Instance (if any) shall be added.

For indirect communication, if the NF service producer delegates target NF consumer instance reselection to the SCP (when the target NF consumer instance is not reachable), the NF service producer should include the target NF type (i.e. the type of the NF service consumer) in the corresponding "3gpp-Sbi-Discovery-*" request header, and may also include other 3gpp-Sbi-Discovery-*" headers in a notification or callback request, to enable the SCP to reselect a different NF service consumer instance as specified in the preceding bullets, if possible and if the NF service consumer instance indicated in the "3gpp-Sbi-Target-apiRoot" header or target URI is not reachable. If the Callback URI included a prefix, the NF service producer should also include the callback URI Prefix in the 3gpp-Sbi-Request-Info header.

6.7 Restoration of Profiles related to UDR

6.7.1 General

This clause describes an optional procedure that may be supported by UDR, UDR consumers (i.e. UDM, PCF, and NEF), and UDM consumers (e.g. AMF, SMF, SMSF, AUSF, NEF…) to re-synchronize profiles in UDR to those in UDR consumers and UDM consumers. When UDR detects corruption, loss, or inconsistency in temporary data stored in UDR, the UDR indicates it to its consumers. UDR should also send notifications to its consumers upon restart based on the deployment policy. If the UDR consumer is UDM, the UDM indicates it to its consumers. Then, those consumers initiate necessary procedures directly or via UDM towards UDR, so that related profiles are re-synchronized and adverse impacts on operator's service can be minimized.

NOTE 1: Notification can also be sent on other occasions than data corruption based on local policy.

Temporary data stored in UDR subject to restoration may be identified within the notification sent to UDR consumers and UDM consumers either by:

- Reset-ID (plus PLMN ID of the UDR): Reset-IDs of temporary data associated to SUPI ranges or GPSI ranges are assigned by UDR in an implementation specific way; e.g. a Reset-ID may identify a hardware resource and may contain a reset-counter. The Reset-ID is provided to UDR consumers and UDM consumers in the response of a request that has created temporary data (i.e. a resource) in UDR.

- SUPI or GPSI ranges.

- DNNs/S-NSSAIs (plus PLMN ID of the UDR).

- UDR or UDM Group ID (plus PLMN ID of the UDR).

- PLMN ID of the UDR.

The identifiers used in notifications are optional to be included when sent by UDR or by UDR consumers, but it is recommended that the notification includes some type of identifier to narrow down as much as possible the set of affected profiles. In particular, the notification to UDM consumers in PLMNs different from the PLMN of the UDM shall contain at least one of the identifiers. For the receivers of the notifications, all identifiers shall be supported.

If multiple identifiers are included in the notification, the set of affected profiles shall consider as a logical "AND" between all the included identifiers.

The notification sent to UDR consumers and UDM consumers also includes the following time values:

- lastReplicationTime: The last time when UDR replicated the temporary data identified to be potentially lost or corrupted, i.e. before the situation causing the potential data inconsistency occurred.

- recoveryTime: The time when UDR started working properly after the situation causing the potential data inconsistency occurred.

Resources related to temporary data stored in UDR are associated in the corresponding user profile stored at UDR consumers or UDM consumers with a timestamp of the time they were created or last modified; i.e. lastSynchronizationTime. Temporary data in UDR created or updated between the lastReplicationTime and the recoveryTime may be inconsistent with profiles in UDR consumers and UDM consumers. In order to avoid inconsistency of time due to different timezones, lastReplicationTime, recoveryTime and lastSynchronizationTime shall be identified using UTC.

UDR consumers and UDM consumers define callbackUri for data restoration in their NF profile. This is an endpoint to receive notification when potential UDR data inconsistency occurs. In addition, UDR consumers may inform their identity to UDR. Additionally, UDM consumers may inform their dataRestorationCallbackUri to UDM during registration in UDM (e.g. for AMF, SMF, SMSF); if so, such callback URI shall be the same as the URI registered by the UDM consumer in its NF Profile in NRF, and it shall be a same URI for the entire consumer's NF Instance (i.e., the UDM consumer shall not indicate different callback URIs per each UE registration).

When the UDR detects a potential data inconsistency of temporary data, the UDR notifies the UDR consumers of the potential data inconsistency event using the callbackUri of the UDR consumer.

The UDM may notify UDM consumers within its PLMN using the callbackUri included in the NF profile of the UDM consumer in NRF. This is, a UDM that receives a notification from UDR can discover the callbackURI of e.g. AMFs, SMFs, SMSFs or AUSFs within its PLMN and forward the notification to all of them. The UDM may also notify UDM consumers using the callbackUri if provided by UDM consumers during its registration in UDM based on local configuration.

NOTE 2: The option for UDM consumers to provide its dataRestorationCallbackUri during registration in UDM, and such UDM using these callbackUris to send subsequent notifications, is particularly beneficial to support roaming users connecting via UDM consumers in PLMNs different from the PLMN of the UDM (e.g. AMF, SMSF, and SMF in Local Break Out scenarios), since it avoids the task for UDM to perform an inter-PLMN service discovery.

The notification to UDR consumers and UDM consumers includes optionally the identifier of the temporary data subject to restoration (e.g. Reset-IDs), the lastReplicationTime and the recoveryTime. The UDR consumer or UDM consumer may then initiate the restoration of the temporary data identified to be potentially lost or corrupted when the last synchronization time recorded at consumer falls between the lastReplicationTime and the recoveryTime as provided by the producer, i.e. UDR or UDM.

6.7.2 Procedure

Figure 6.7.2-1 describes the procedure for restoration of profiles related to UDR.

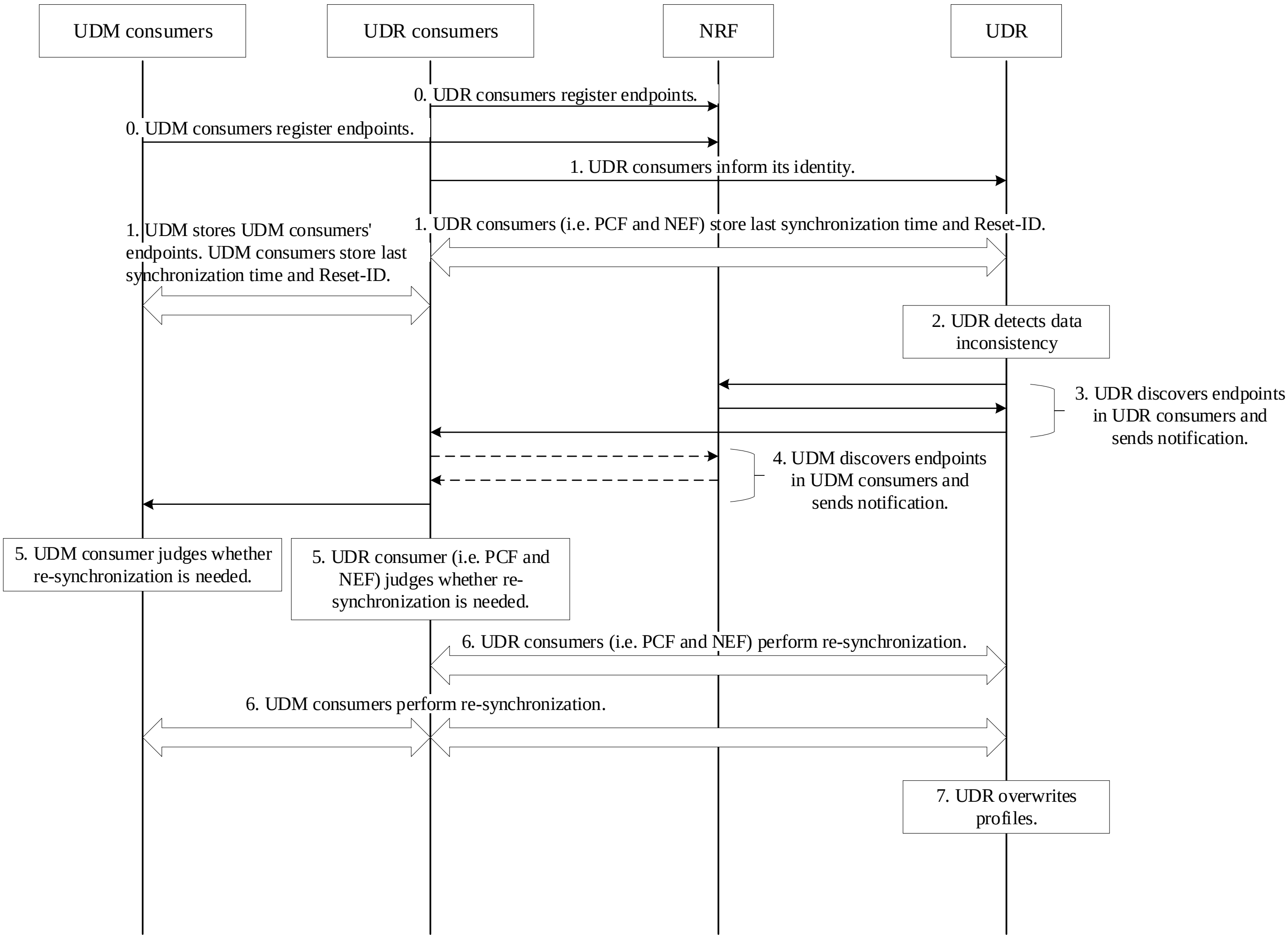
UDM consumers
UDR consumers
NRF
UDR
0. UDR consumers register endpoints.
0. UDM consumers register endpoints.
1. UDR consumers inform its identity.
1. UDM stores UDM consumers' endpoints. UDM consumers store last synchronization time and Reset-ID.
1. UDR consumers (i.e. PCF and NEF) store last synchronization time and Reset-ID.
2. UDR detects data inconsistency
3. UDR discovers endpoints in UDR consumers and sends notification.
4. UDM discovers endpoints in UDM consumers and sends notification.
5. UDM consumer judges whether re-synchronization is needed.
5. UDR consumer (i.e. PCF and NEF) judges whether re-synchronization is needed.
6. UDR consumers (i.e. PCF and NEF) perform re-synchronization.
6. UDM consumers perform re-synchronization.
7. UDR overwrites profiles.

Figure 6.7.2-1: Restoration of Profiles related to UDR

0. UDR consumers and UDM consumers define callbackUri for data restoration in the NF profile registered in NRF.

1. UDR consumers store temporary data in UDR. The UDR consumers may set its identity in the request to UDR, when accessing it for the first time. The UDR stores the received identity and creates for the UDR consumer a subscription on notification for the potential UDR data inconsistency. The UDR may provide to the UDR consumer the Reset-ID if assigned by the UDR for the temporary data stored in UDR.

   The UDM stores temporary data in UDR as requested by its consumers. UDM consumers may set dataRestorationCallbackUri in the request of their registration to UDM. In this case, the UDM stores the dataRestorationCallbackUri locally and creates for the UDM consumer a subscription on notification for the potential UDR data inconsistency. If received from UDR, the UDM also provides the Reset-ID assigned by the UDR to UDM consumers.

   When an NF other than UDM creates or updates a resource directly or via UDM in UDR, the NF sets or stores lastSynchronizationTime in a relevant profile. If the NF receives a Reset-ID directly or via UDM from UDR, the NF stores it in the profile.

2. UDR detects corruption, loss, or inconsistency in temporary data caused due to certain scenarios (e.g. failure and restart of the UDR, or migration of the data from an old UDR to a new UDR).

NOTE 1: The UDR can recover consistency by different means, e.g. by reloading data from its back-up.

3. UDR queries NRF based on the identity stored in step 1 and discovers callbackUri for data restoration in UDR consumers' NF profiles. If no UDR consumer impacted by the restoration event provided its identity in step 1, the UDR discovers via NRF the callbackUri of one suitable UDR consumer instance to send the notification to. The UDR sends Nudr_DR_Notification request to the callbackUri to notify potential UDR data inconsistency. The Nudr_DR_Notification request may contain temporary data identifier(s) (e.g. Reset-IDs) and an impacted period (i.e. lastReplicationTime and recoveryTime).

4. If UDR consumer is UDM, the UDM forwards the notification to UDM consumers. The UDM finds callbackUri for data restoration for UDM consumers within its PLMN in UDM consumers' NF profiles through querying NRF. Optionally, the UDM may find callbackUri for data restoration for UDM consumers (especially UDM consumers outside its PLMN) if provided by the UDM consumer during UDM consumer registration in UDM and locally stored in UDM in step1.

5. When a UDR consumer other than UDM (e.g. PCF, NEF) or a UDM consumer (e.g. AMF, SMF, SMSF) finds that a stored profile is affected by the potential loss or corruption of data, and that the last synchronization time of the profile falls into the impacted period in the notification, then the NF judges that the profile requires re-synchronization.

   UDR consumers other than UDM (e.g. PCF, NEF) initiates the re-synchronization of the impacted resources using Nudr_DataRepository service operations.

   UDM consumers initiate the re-synchronization for each impacted UE using different service operations depending on the UDM consumer type. UDM consumers shall include a flag ("udrRestartInd") indicating that the request is due to a re-synchronization event.

   - UDM consumers that register in UDM start re-synchronization by sending Nudm_UECM_Registration request for each impacted UE.

     In order to prevent storing obsolete registration information for a given user coming from UDM consumers that trigger resynchronization for the same user, UDM consumers may include the stored last synchronization time within the re-synchronization request. The lastSynchronizationTime provided by the UDM consumer may be used in UDM to compare it with current data stored in UDR and ensure that the registration from the most recent UDM consumer is kept (see step 7). However, if the UDM consumer ensures that its resynchronization is the most recent, accurate and correct (e.g. if the AMF triggers resynchronization upon detection of UE activity), the UDM consumer shall not include the lastSynchronizationTime within the resynchronization request and the UDM stores the UDM consumer registration in the UDR without further processing.

   - UDM consumers that subscribe to notification of subscription data changes in UDM start re-synchronization of these subscriptions in UDM by sending Nudm_SDM_Subscribe request for each impacted UE and subscription.

   - AUSF starts re-synchronization by sending Nudm_UEAuthentication_ResultConfirmation request containing the stored last synchronization timestamp of the authentication for each impacted UE.

   - NEF starts re-synchronization of the subscription to exposure events in UDM by sending Nudm_EE_ModifySubscription request for each impacted UE and subscribed event.

6. The UDR consumers and UDM consumers locally adjusts invocation timing of each of those procedures, in order not to cause congestion in the system. The NF invokes necessary procedures.

   UDM consumers select a UDM instance to send the re-synchronization signalling as defined in 3GPP TS 23.501 [9]. This is, the UDM consumer may not send the re-synchronization signalling to the UDM instance from which the UDM consumer received the notification.

7. If UDM receives Nudm_UECM_Registration request containing the "udrRestartInd" flag, the UDM overwrites the related profile in the UDR, or creates it if not available. If the registration request includes a lastSynchronizationTime, the related profile in UDR is overwritten only if the lastSynchronization time received from the UDM consumer is not older than the registration time stored in UDR before resynchronization. In this case, if the UDM replaces or creates the related profile in UDR, the UDM sets the registration time to the current time.

If UDM receives Nudm_SDM_Subscribe request containing the "udrRestartInd" flag the UDM sends a corresponding request to UDR, the UDR overwrites the related profile in the UDR or creates it if not available in UDR.

If UDM receives Nudm_UEAuthentication_ResultConfirmation request containing the "udrRestartInd" flag, the UDM sends a corresponding request to UDR, the UDR overwrites the related profile in the UDR or creates it if not available in UDR.

If UDM receives Nudm_EE_ModifySubscription request containing the "udrRestartInd" flag, the UDM sends a corresponding request to UDR, the UDR overwrites the related profile in the UDR or creates it if not available in UDR.

6.8 Restoration Procedures for Home Routed PDU Sessions or PDU sessions with an I-SMF

6.8.1 General

This clause specifies requirements in the AMF, the V/I-SMF and the (H-)SMF to restore Home Routed PDU Sessions or PDU sessions with an I-SMF.

During a PDU session establishment and update procedure, the V/I-SMF or the (H-)SMF shall:

- set the "Peer NF SET based Reselection"(PSETR) feature bit in the SupportedFeatures attribute if it supports the (re)selection of an alternative peer SMF using the binding indication of the resource/session contexts or based on the NF profile of the peer SMF;
- set the "Deployed Local SMF Set" (DLSET) feature bit in the SupportedFeatures attribute if the PDU session resource is not bound exclusively to the specific V/I-SMF or (H-)SMF NF service instance, i.e. if there is at least one alternative SMF service instance (in the same or a different SMF instance) that can take it over if the current serving SMF service instance becomes no longer operational (e.g. fails).

NOTE 1: A SMF can set the DLSET flag to "1" if it indicates in its NF Profile that it supports the capability to persist its resources in shared storage inside the NF Instance, i.e. if another SMF service instance with the SMF instance can take over the resource context even when NF (service) set is not deployed locally.

In the service request or response message towards the (new) AMF, the V/I-SMF shall set the "DLSET" feature bit if the PDU session resource can be taken over by an alternative V-SMF Service Instance. The V/I-SMF shall set the "anchorSmfPsetrSupportInd" attribute to "true" in the Update SM Context Response message towards the new AMF if the (H-)SMF supports the "PSETR" feature.

NOTE 2: The AMF needs to know if the V/I-SMF supports the DLSET feature and if the (H-)SMF supports the PSETR to take proper restoration actions when there is a V/I-SMF failure. See clause 6.8.2. The AMF can alternatively learn whether the (H-)SMF supports the PSETR feature when doing the SMF discovery/selection during the PDU Session Establishment procedure.

NOTE 3: The V/I-SMF indicates more generally all the features it supports to the AMF in the service request/response, including also setting the "PSETR" feature bit if it is able to reselect an alternative (H-)SMF when it detects the peer (H-)SMF has failed, but the AMF is not required to use this indication.

The requirements specified in subsequent clauses shall also be applied for N16a reference point by replacing the V-SMF with I-SMF, and H-SMF with SMF.

6.8.2 V-SMF failure

When the H-SMF detects the failure of the V-SMF, it shall retrieve all PDU sessions associated with the failed V-SMF and perform the following procedure for those PDU sessions:

- if the H-SMF supports the PSETR feature:
  - if the V-SMF supports the DLSET feature, the H-SMF shall keep the PDU session and should reselect an alternative V-SMF service instance, e.g. when it needs to send any request message to the V-SMF;

  - if the V-SMF doesn't support the DLSET feature, the H-SMF shall delete the affected PDU sessions locally.

- if the H-SMF does not support the PSETR feature:

  - the H-SMF shall delete the affected PDU sessions.

When the AMF detects the failure of the V-SMF, it shall retrieve all PDU sessions associated with the failed V-SMF and perform the following procedure for those PDU sessions:

- if the H-SMF supports the PSETR feature and if the V-SMF supports the DLSET feature, the AMF shall keep the PDU session and should reselect an alternative V-SMF service instance, e.g. when it needs to send any request message to the V-SMF.

- if the H-SMF doesn't support the PSETR feature while the V-SMF supports the DLSET feature, the AMF shall keep the PDU sessions, and may reselect an alternative V-SMF service instance to request the selected alternative V-SMF to delete the PDU session towards the UE and the UPF. The V-SMF may request the UE to reactivate the PDU session.

- for any other cases, the AMF may release the affected PDU session(s) locally and/or notify the UE about the release of the PDU session.

6.8.3 H-SMF failure

When the V-SMF detects the failure of the H-SMF, it shall retrieve all PDU sessions associated with the failed H-SMF and perform the following procedure for those PDU sessions:

- if the V-SMF does not support the PSETR feature, the V-SMF may release the affected PDU sessions towards the AMF and UE, and may request the UE to reactivate the PDU session;

- if the V-SMF supports the PSETR feature:

  - if the H-SMF supports the DLSET feature, the V-SMF shall keep the PDU session and may reselect an alternative H-SMF service instance, e.g. when it needs to send any request message to the H-SMF;

  - if the H-SMF doesn't support the DLSET feature, the V-SMF may release the PDU session towards the AMF and UE, and the V-SMF may request UE to reactivate the PDU session.

7 Restoration Procedures related to Public Warning System (PWS)

7.1 General

This clause specifies the procedures supported in the 5G System to handle failures affecting Public Warning System (PWS). The stage 2 architecture and procedures for PWS are specified in 3GPP TS 23.041 [8].

7.2 PWS operation failure in NG-RAN

The NG-RAN shall report that on-going PWS operation for one or more cells of the NG-RAN has failed by sending a PWS Failure Indication as specified in 3GPP TS 23.041 [8].

7.3 PWS operation restart in NG-RAN

After a NG-RAN (i.e. gNB or ng-eNB) has restarted, it shall delete all its warning message data. If the warning message service is operational in one or more cell(s) of the NG-RAN, the NG-RAN shall send a PWS Restart Indication message, which shall include the identity of the NG-RAN, the identity of the restarted cell(s), and the TAI(s) and Emergency Area Id(s) with which the restarted cell(s) are configured, to request the CBC to re-load its warning message data if applicable.

The NG-RAN should send the PWS Restart Indication message via two AMFs of the AMF Region, if possible, to ensure that the CBC receives the message even if one AMF cannot propagate it to the CBC (e.g. due to a path failure between the AMF and the CBC).

If the AMF interfaces with multiple CBCs, the AMF shall forward the PWS Restart Indication to all CBCs.

Upon receipt of a PWS Restart Indication message, the CBC shall consider that the warning message service is restarted in the reported cell(s), i.e. the service is operational and no warning messages are being broadcast in the cell(s). The CBC shall then re-send the warning message data (with the same message identifier and serial number) to the NG-RAN for these cells, if any. When doing so, the CBC:

- shall provide the identity of the NG-RAN received in the PWS Restart Indication when sending the Write-Replace-Warning-Request message(s) to the AMF, to enable the AMF to forward the message(s) only to the NG-RAN involved in the restart. The identity of the NG-RAN shall be included in:
  - the Write-Replace-Warning-Request message(s) sent to the PWS-IWF over the SBc interface; or
  - the globalRanNodeList IE of the NonUeN2MessageTransfer request message(s) sent to the AMF over the N50 interface (see clauses 5.2.2.4.1.3 and 6.1.6.2.9 of 3GPP TS 29.518 [6]) to request the transfer of the Write-Replace-Warning-Request message(s).
- should set the warning area list to the identities of the cell(s) to be reloaded which are relevant to the warning message data being reloaded; and
- may update the number of broadcasts requested, if necessary.

The CBC shall consider a PWS Restart Indication message received shortly after a preceding one for the same cell identity as a duplicate restart indication for that cell which it shall ignore.

NOTE: The broadcast of warning messages can be configured in the network per individual cell, TAI and/or Emergency Area Id. The CBC can use the list of cell(s), the TAI(s) and Emergency Area Id(s) received in the PWS Restart Indication to derive the list of warning messages to be broadcast in the respective cell(s), TAI(s) and Emergency Area Id(s).

Likewise, in other scenarios where the NG-RAN may need to reload its warning message data (e.g. when an individual cell is restarted), the NG-RAN shall send a PWS Restart Indication message (including the identity of the NG-RAN, the identity of the restarted cell(s), and the TAI(s) and Emergency Area Id(s) with which the restarted cell(s) are configured) to the CBC to request the CBC to re-load its warning message data if applicable. The NG-RAN, AMF and CBC shall then proceed as specified above for a NG-RAN restart.

8 Restoration Procedures for MBS

8.1 General

This clause specifies the procedures supported in the 5G System to detect and handle failures affecting any network entity involved in the delivery of broadcast and/or multicast service.

8.1A N4mb Failure and Restart Detection

Across PFCP based interfaces, an MB-SMF and MB-UPF shall utilize the PFCP Heartbeat Request and Heartbeat Response messages to detect a peer PFCP entity failure or restart as described in clause 19A of 3GPP TS 23.007 [2].

A PFCP function shall ignore the Recovery Timestamp received in PFCP Association Setup Request and PFCP Association Setup Response messages (see clause 6.2.6 of 3GPP TS 29.244 [4]).

8.2 Restoration procedures for MB-UPF failure with or without restart

8.2.1 General

When an MB-UPF fails, all its PFCP session contexts of the MBS sessions and all its PFCP associations affected by the failure may be lost.

The MB-SMF and MB-UPF may support the procedures specified in this clause to restore the multicast and broadcast MBS sessions affected by the failure.

8.2.2 Restoration Procedure for MB-UPF Restart

The MB-UPF should ensure that:

- when multicast transport is used on N3mb and/or N19mb, any N3mb and/or N19mb Low Layer Source Specific Multicast (LL SSM) addresses used by the MB-UPF before the MB-UPF restart are not immediately reused after the MB-UPF restart; and

- when unicast transport is used on N6mb and/or Nmb9, any N6mb and/or Nmb9 ingress tunnel addresses used by the MB-UPF before the MB-UPF restart are not immediately reused after the MB-UPF restart.

NOTE 1: This avoids inconsistent addresses allocation throughout the network and enable the restoration of PFCP sessions of MBS sessions affected by the failure. How this is ensured is implementation specific.

During or immediately after an MB-UPF Restart, the MB-UPF shall place a local UPF Recovery Time Stamp value in all Heartbeat Request/Response messages.

Immediately after the re-establishment of a PFCP association between the MB-SMF and the MB-UPF, the MB-SMF may start restoring the PFCP sessions of the affected MBS sessions in the MB-UPF, by following PFCP requirements for establishing a PFCP session over N4mb as specified in clause 5.34.2 of 3GPP TS 29.244 [4], with the following modifications:

- the MB-SMF shall include the MBS Restoration Indication in the PFCP Session Establishment Request message to indicate to the MB-UPF that this is a request to restore the PFCP session of an existing MBS session;

- If multicast transport is used on N3mb and/or N19mb, the MB-SMF shall additionally provide, in the Multicast Transport Information for N3mb and/or N19mb IE in the PFCP Session Establishment Request, the N3mb and/or N19mb LL SSM address and GTP-U Common TEID (C-TEID) that was previously used for the MBS session, and the MB-UPF shall allocate the same N3mb and/or N19mb LL SSM address and C-TEID to the PFCP session if possible. The MB-SMF shall not set the PLLSSM flag in the MBSN4mbReq-Flags IE in the PFCP Session Establishment Request.

- If unicast transport is used on N6mb and/or Nmb9, the MB-SMF shall additionally provide, in the "Local Ingress Tunnel" IE in the Create PDR IE or Create Tunnel Endpoint IE (for the downlink PDRs) in the PFCP Session Establishment Request, the N6mb and/or Nmb9 ingress tunnel address that was previously used for the MBS session, and the MB-UPF shall allocate the same N6mb and/or Nmb9 ingress tunnel address if possible. The MB-SMF shall not set the CHOOSE bit to "1" in the "Local Ingress Tunnel" IE".

If multicast transport is used on N3mb and/or N19mb and the MB-UPF cannot accept the requested N3mb and/or N19mb LL SSM address, or if unicast transport is used on N6mb and/or Nmb9 and the UPF cannot accept the requested N6mb and/or Nmb9 ingress tunnel address, because the requested address is not available at the MB-UPF, the MB-UPF shall reject the PFCP Session Establishment Request with the cause "PFCP session restoration failure due to requested resource not available". The MB-SMF may then proceed as specified for the restoration procedure for MB-UPF failure without restart, but possibly using the same or a different MB-UPF.

NOTE 2: The cause "PFCP session restoration failure due to requested resource not available" corresponds to scenarios where the requested address is no longer available at the MB-UPF, i.e. it cannot be assigned to any PFCP session, due to e.g. the address having been decommissioned by OAM from the MB-UPF or e.g. the address being no longer operational due to a partial hardware failure at the MB-UPF. This cause is not to be used for scenarios where the requested address would be available at the MB-UPF but would have been re-assigned to a different PFCP session, which is a scenario that is not expected to happen based on the requirements specified above.

8.2.3 Restoration Procedure for MB-UPF failure without Restart

Upon detecting that an MB-UPF fails without restart, the MB-SMF may restore the MBS sessions that were served by the failed MB-UPF by selecting an alternative MB-UPF and by restoring the PFCP sessions of the MBS sessions in the alternative MB-UPF, following PFCP requirements for establishing an N4mb PFCP session as specified in clause 5.34.2 of 3GPP TS 29.244 [4] with the following additions:

- the MB-SMF shall request the alternative MB-UPF to join the multicast tree towards the Source Specific Multicast (SSM) address information earlier provided by AF/AS or MBSTF, if multicast transport is used over N6mb and/or Nmb9;
- the MB-SMF shall request the alternative MB-UPF to allocate a new N6mb and/or Nmb9 ingress tunnel address, if unicast transport is used over N6mb and/or Nmb9;
- the MB-SMF shall request the alternative MB-UPF to allocate a new N3mb and/or N19mb LL SSM address and C-TEID, if multicast transport is used over N3mb and/or N19mb; and
- for each N3mb and/or N19mb endpoint expected to receice the MSB session data, the MB-SMF shall request the alternative MB-UPF to send data towards the N3mb and/or N19mb endpoint's DL F-TEID, if unicast transport is used over N3mb and/or N19mb.

For each MBS session, during the PFCP session establishment, the alternative MB-UPF will assign:

- a new N3mb and/or N19mb LL SSM address and C-TEID, if multicast transport is used on N3mb and/or N19mb; and/or
- a new N6mb and/or Nmb9 ingress tunnel address, if unicast transport is used on N6mb and/or Nmb9.

Then, for each MBS session:

- if multicast transport is used on N3mb:
    - the MB-SMF shall update the AMFs handling the multicast or broadcast MBS session, or location dependent component of the MBS session, about the new N3mb LL SSM address and C-TEID by sending:
        - an Namf_MBSCommunication_N2MessageTransfer request (Multicast Session Update Request including the new MB-UPF LL SSM address and C-TEID) for a multicast MBS session; and/or
        - an Namf_MBSBroadcast ContextUpdate Request (Broadcast Session Modification Request including the new MB-UPF LL SSM address and C-TEID) for a broadcast MBS session.
    - the AMFs shall forward the above information towards the NG-RAN nodes handling the MBS session (using the Multicast Session Update and Broadcast Session Modification procedures respectively);
    - the NG-RAN nodes shall join delivery from the new multicast transport address to receive MBS session data from the new MB-UPF and leave delivery from the previous multicast address in use for the MBS session.
- if multicast transport is used on N19mb, for a multicast MBS session:
    - the MB-SMF shall update the SMF handling the multicast MBS session, or location dependent component of the MBS session, about the new N19mb LL SSM address and C-TEID by sending an Nmbsmf_MBSSession_ContextStatusNotify request including an " MULT_TRANS_ADD_CHANGE" event and the new N19mb LL SSM address and C-TEID used for the MBS data delivery over N19mb;
    - the SMF shall update the UPF terminating the N19mb tunnel about the new LL SSM address and C-TEID;

  - the UPF shall join delivery from the new multicast transport address to receive MBS session data from the new MB-UPF and leave delivery from the previous multicast address in use for the MBS session.

- if unicast transport is used on N6mb and/or Nmb9:

  - the MB-SMF shall update the AF/NEF/MBSF about the new N6mb/Nmb9 ingress tunnel address to use for sending MBS data for a given MBS session, or location dependent component of the MBS session, by sending an Nmbsmf_MBSSession_StatusNotify request including an "Ingress Tunnel Address Change" event and the new N6mb/Nmb9 ingress tunnel address;

  - the AF/MBSF shall start sending MBS data to the new N6mb/Nmb9 ingress tunnel address.

Figures 8.2.3-1 and 8.2.3-2 depict the call flows for the case of a broadcast MBS session and a multicast MBS session respectively.

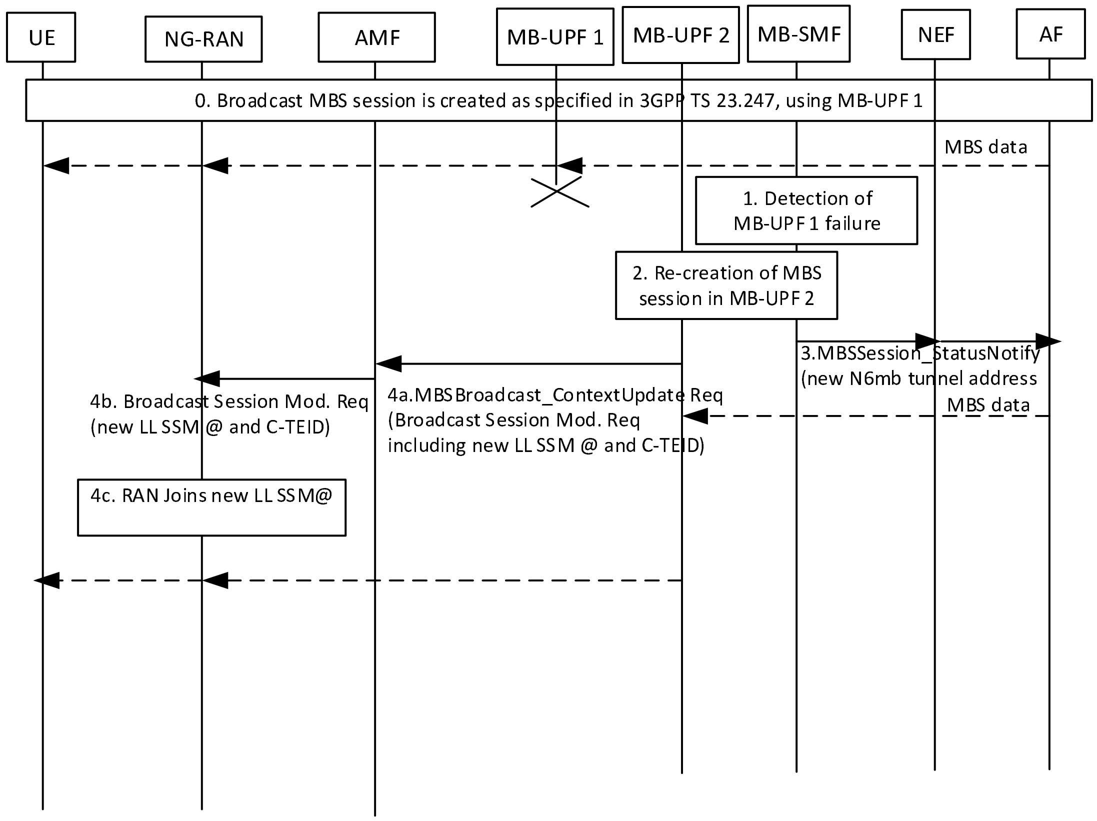
UE
NG-RAN
AMF
MB-UPF 1
MB-UPF 2
MB-SMF
NEF
AF
0. Broadcast MBS session is created as specified in 3GPP TS 23.247, using MB-UPF 1
MBS data
1. Detection of MB-UPF 1 failure
2. Re-creation of MBS session in MB-UPF 2
3.MBSSession_StatusNotify (new N6mb tunnel address
MBS data
4a.MBSBroadcast_ContextUpdate Req (Broadcast Session Mod. Req including new LL SSM @ and C-TEID)
4b. Broadcast Session Mod. Req (new LL SSM @ and C-TEID)
4c. RAN Joins new LL SSM@

Figure 8.2.3-1: Broadcast MBS session restoration upon MB-UPF failure without restart

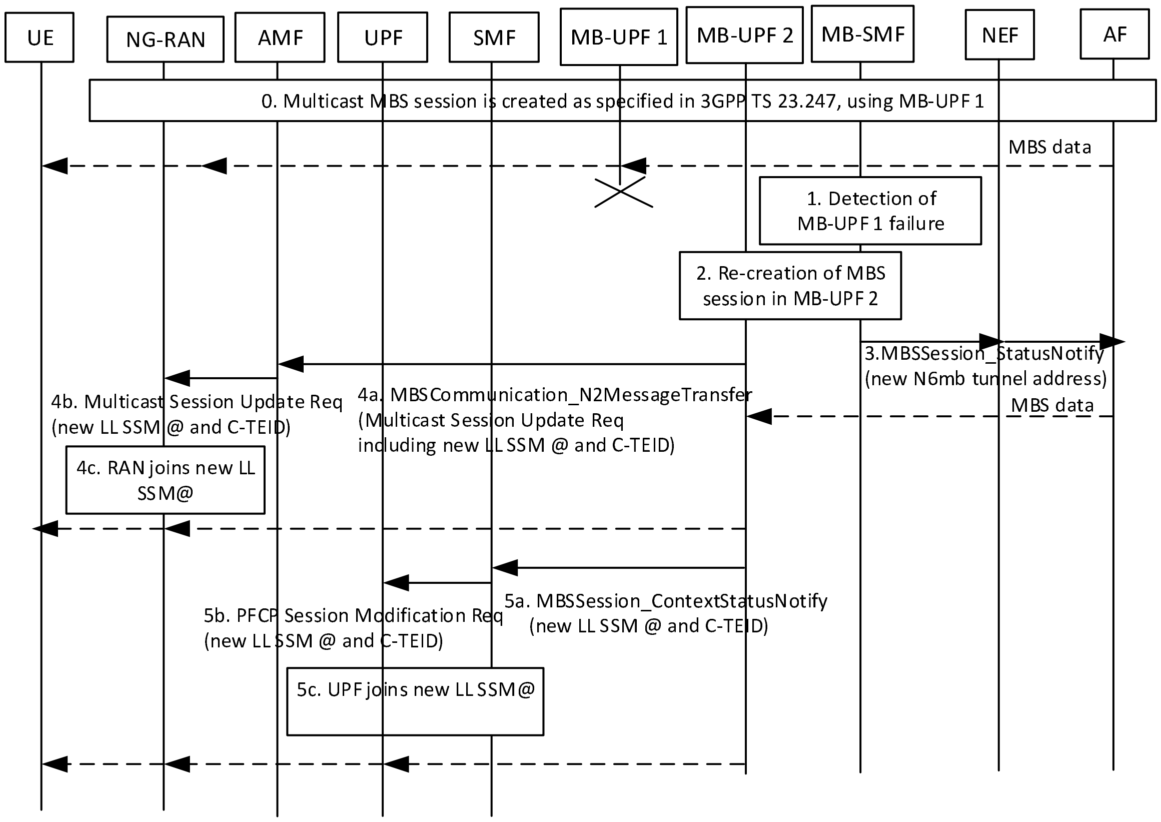
UE
NG-RAN
AMF
UPF
SMF
MB-UPF 1
MB-UPF 2
MB-SMF
NEF
AF
0. Multicast MBS session is created as specified in 3GPP TS 23.247, using MB-UPF 1
MBS data
1. Detection of MB-UPF 1 failure
2. Re-creation of MBS session in MB-UPF 2
3.MBSSession_StatusNotify (new N6mb tunnel address)
MBS data
4a. MBSCommunication_N2MessageTransfer (Multicast Session Update Req including new LL SSM @ and C-TEID)
4b. Multicast Session Update Req (new LL SSM @ and C-TEID)
4c. RAN joins new LL SSM@
5a. MBSSession_ContextStatusNotify (new LL SSM @ and C-TEID)
5b. PFCP Session Modification Req (new LL SSM @ and C-TEID)
5c. UPF joins new LL SSM@

Figure 8.2.3-2: Multicast MBS session restoration upon MB-UPF failure without restart

8.3 Restoration procedures for NG-RAN failure with or without restart

8.3.1 General

When an NG-RAN fails with or without restart, all its MBS session contexts may be lost, causing the interruption in the delivery of MBS data over the radio interface.

Restoration procedures for NG-RAN failure with or without restart are optional to support.

8.3.2 Broadcast MBS session restoration Procedure for NG-RAN failure with restart

8.3.2.1 General

MBS sessions affected by an NG-RAN failure with restart may be restored by the AMF as specified in clause 8.3.2.2 or by the MB-SMF as specified in clause 8.3.2.3.

8.3.2.2 Broadcast MBS session restoration by AMF

The procedure specified in this clause may be supported to restore a broadcast MBS session affected by an NG-RAN restart.

The AMF handling a broadcast MBS session is responsible for restoring the MBS session in a restarted NG-RAN, as shown in Figure 8.3.2.2-1.

NOTE 1: An NG-RAN restart is transparent to the MB-SMF (i.e. the restoration procedure does not cause any signaling to the MB-SMF) when multicast transport is used over N3mb.

NOTE 2: This procedure can also be used in other scenarios where an existing MBS session needs to be started in a new NG-RAN, e.g. an NG-RAN that is reconfigured by OAM to support a new TA that is part of the MBS service area of an existing MBS session.

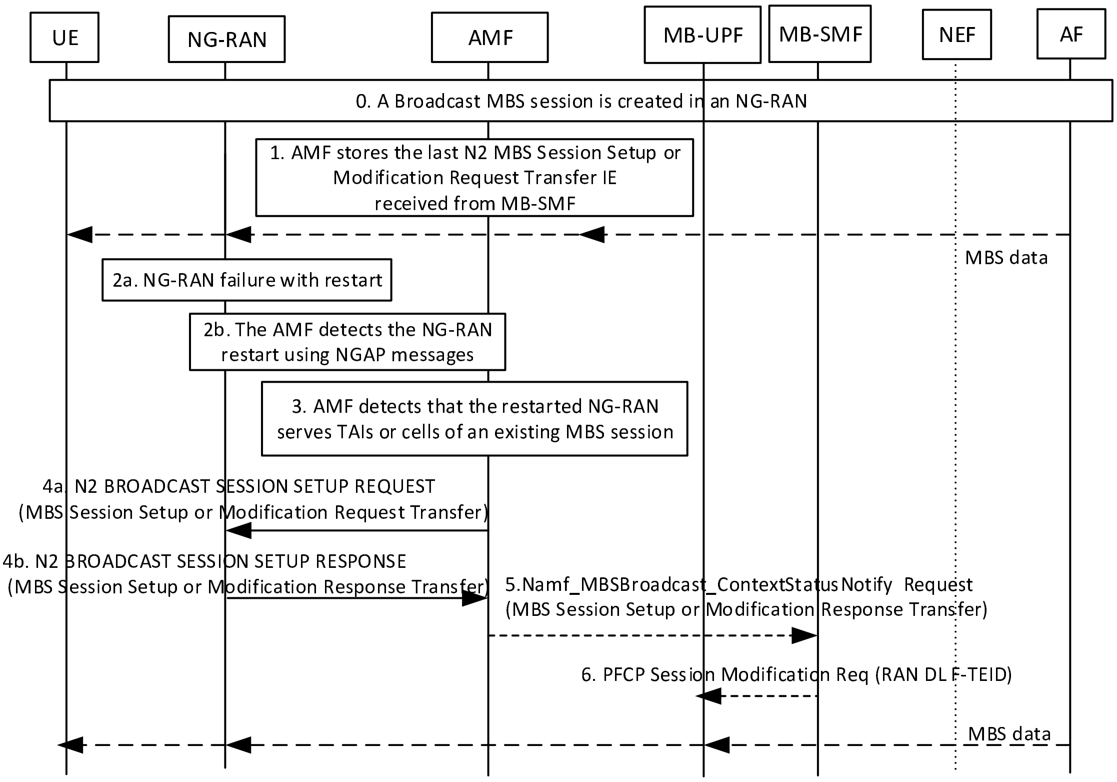
UE
NG-RAN
AMF
MB-UPF
MB-SMF
NEF
AF
0. A Broadcast MBS session is created in an NG-RAN
1. AMF stores the last N2 MBS Session Setup or Modification Request Transfer IE received from MB-SMF
MBS data
2a. NG-RAN failure with restart
2b. The AMF detects the NG-RAN restart using NGAP messages
3. AMF detects that the restarted NG-RAN serves TAIs or cells of an existing MBS session
4a N2 BROADCAST SESSION SETUP REQUEST (MBS Session Setup or Modification Request Transfer)
4b. N2 BROADCAST SESSION SETUP RESPONSE (MBS Session Setup or Modification Response Transfer)
5.Namf_MBSBroadcast_ContextStatusNotify Request (MBS Session Setup or Modification Response Transfer)
6. PFCP Session Modification Req (RAN DL F-TEID)
MBS data

Figure 8.3.2.2-1: Broadcast MBS session restoration by AMF upon NG-RAN restart

1. The AMF stores the last N2 MBS SM container (i.e. MBS Session Setup or Modification Request Transfer IE defined in 3GPP TS 38.413 [11]) received from the MB-SMF during the establishment of the broadcast MBS session or during a broadcast MBS session update. When unicast transport is used over N3mb, the MB-SMF stores the RAN-ID together with the DL F-TEID received from each NG-RAN.

NOTE 3: The N2 MBS SM container contains all the information to establish the broadcast MBS session (e.g. transport layer address if multicast transport is used over N3mb, QoS flows).

2. The NG-RAN restarts, causing the broadcast MBS service interruption.

3. The AMF detects that the NG-RAN has restarted (e.g. upon receiving NG Setup Request message) and that it serves at least one TAI or one cell being part of the MBS service area of an existing MBS session (or one of the MBS services areas of the MBS session in case of location dependent content).

4. The AMF re-establishes the broadcast MBS session in the restarted NG-RAN, by sending an NGAP Broadcast Session Setup Request including the last N2 (NGAP) MBS Session Setup or Modification Request Transfer IE that was stored.

   The NG-RAN establishes the broadcast MBS session and returns a response to the AMF. If unicast transport is used over N3mb, the NG-RAN response includes the DL F-TEID assigned by the NG-RAN to receive the MBS data from the MB-UPF within the N2 (NGAP) MBS Session Setup or Modification Response Transfer IE of the NGAP Broadcast Session Setup Response message. In deployments where multiple NG-RAN nodes share a common user plane entity and unicast transport is used over N3mb, the NG-RAN response may include an existing DL F-TEID signalled by other NG-RAN nodes during shared delivery setup.

The NG-RAN joins the delivery of the broadcast MBS session if multicast transport is used over N3mb.

5. If an N2 MBS SM Container (i.e. N2 (NGAP) MBS Session Setup or Modification Response Transfer IE) was received from the NG-RAN in step 4, the AMF sends an Namf_MBSBroadcast_ContextStatusNotify Request to the MB-SMF including the N2 MBS SM Container and the RAN-ID of the NG-RAN .

6. The MB-SMF modifies the PFCP session of the MBS session in the MB-UPF to start distributing MBS data towards the DL GTP-U F-TEID received from the NG-RAN, and to stop doing so towards the earlier DL GTP-U F-TEID that was used by the same NG-RAN before the NG-RAN restart.

   This step shall be skipped in deployments where multiple NG-RAN nodes share a common user plane entity, unicast transport is used over N3mb, and the MB-SMF that supports handling shared NG-U terminations determines that the DL F-TEID signalled by restarted NG-RAN node is already associated with other NG-RAN nodes.

8.3.2.3 Broadcast MBS session restoration by MB-SMF

The procedure specified in this clause may be supported to restore a Broadcast MBS session affected by an NG-RAN restart.

When the AMF detects an NG-RAN restart, or a (new) NG-RAN is deployed to serve a TAI that is part of the MBS session service area, e.g. using NG Setup Request message, as specified in 3GPP TS 38.413 [11], it shall report such event to the MB-SMF for each of MBS session(s) affected by this event, to enable the MB-SMF to (re)start the MBS session(s) in the concerning NG-RAN as further described in the Figure 8.3.2.3-1.

The MB-SMF shall run the following restoration procedure for each of Broadcast MBS sessions which were established in the restarted NG-RAN or a (new) NG-RAN.

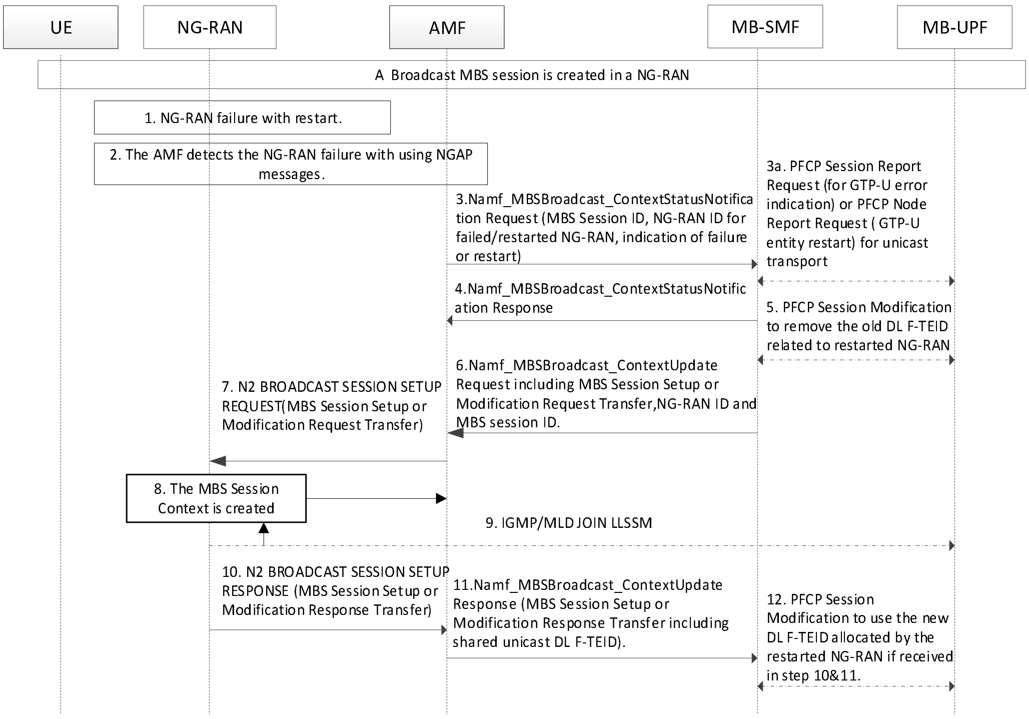
UE
NG-RAN
AMF
MB-SMF
MB-UPF
A Broadcast MBS session is created in a NG-RAN
1. NG-RAN failure with restart.
2. The AMF detects the NG-RAN failure with using NGAP messages.
3.Namf_MBSBroadcast_ContextStatusNotification Request (MBS Session ID, NG-RAN ID for failed/restarted NG-RAN, indication of failure or restart)
3a. PFCP Session Report Request (for GTP-U error indication) or PFCP Node Report Request (GTP-U entity restart) for unicast transport
4.Namf_MBSBroadcast_ContextStatusNotification Response
5. PFCP Session Modification to remove the old DL F-TEID related to restarted NG-RAN
6.Namf_MBSBroadcast_ContextUpdate Request including MBS Session Setup or Modification Request Transfer,NG-RAN ID and MBS session ID.
7. N2 BROADCAST SESSION SETUP REQUEST(MBS Session Setup or Modification Request Transfer)
8. The MBS Session Context is created
9. IGMP/MLD JOIN LLSSM
10. N2 BROADCAST SESSION SETUP RESPONSE (MBS Session Setup or Modification Response Transfer)
11.Namf_MBSBroadcast_ContextUpdate Response (MBS Session Setup or Modification Response Transfer including shared unicast DL F-TEID).
12. PFCP Session Modification to use the new DL F-TEID allocated by the restarted NG-RAN if received in step 10&11.

Figure 8.3.2.3-1: Broadcast MBS session restoration by MB-SMF upon NG-RAN failure with restart

1. The NG-RAN has failed with restart.

2. The AMF detects the NG-RAN has failed with restart, e.g., upon receiving NG Setup Request message.

3. The AMF sends Namf_MBSBroadcast_ContextStatusNotify Request message to the MB-SMF for each affected MBS session including the MBS Session ID, the NG-RAN ID and an indication of the event, either NG-RAN restart, or NG-RAN failure without restart, or a (new) NG-RAN getting into service to serve a TAI that is part of the MBS session service area.

3a. The MB-SMF receives a PFCP Node Report Request message from the MB-UPF to report NG-RAN has failed with restart or a PFCP Session Report Request message from the MB-UPF to report receiving GTP-U Error Indication for each affected MBS session when unicast transport was used for N3mb interface.

4. The MB-SMF returns a "204 No Content" response.

5. The MB-SMF modifies the PFCP sessions corresponding to the affected MBS sessions to remove the NG-RAN DL F-TEID for unicast transport over N3mb.

6. The MB-SMF sends Namf_MBSBroadcast_ContextUpdate Request message to the AMF to (re)start the MBS session in the related NG-RAN including the MBS Session Setup or Modification Request Transfer IE and the NG-RAN ID received in the step 3.

   If the notification is triggered due to receiving the PFCP Node Report Request message or the PFCP Session Report Request message from the MB-UPF as specified in step 3a, and the MB-SMF that supports handling shared NG-U terminations determines that multiple NG-RAN nodes share the restarted user plane entity, the Namf_MBSBroadcast_ContextUpdate Request message may include multiple corresponding NG-RAN IDs.

7. The AMF sends the N2 MBS Session Setup Request message to the NG-RAN node(s) including the MBS Session Setup or Modification Request Transfer IE.

8. The MBS session is created/restored in the NG-RAN node(s).

9. The NG-RAN node(s) joins the delivery of the broadcast MBS session if multicast transport is used over N3mb.

10. The NG-RAN node(s) responds with the N2 MBS Session Setup Response message including a MBS Session Setup or Modification Transfer IE if a Shared NG-U Unicast TNL Information needs to be allocated for unicast transport over N3mb interface.

11. The AMF responds with Namf_MBSBroadcast_ContextUpdate Response message with a MBS Session Setup or Modification Response Transfer IE if received.

12. The MB-SMF modifies the PFCP sessions corresponding to the MBS sessions to provision the new NG-RAN DL F-TEID if received in step 10.

8.3.2.4 Selecting an alternative AMF for a Broadcast MBS Session at AMF failure

When the AMF selected by the MB-SMF to start a Broadcast MBS Session fails without restart, to support the restoration procedure to restore an Broadcast MBS Session in a restarted NG-RAN as specified in 8.3.2.2 and 8.3.2.3, another AMF in the same AMF set needs to be selected to become the serving AMF for this broadcast MBS session and to be responsible for restoration. This may be done by one of the following solutions:

- another AMF is selected in the same AMF set by an AMF implementation specific mechanism, and this AMF sends a Namf_MBSBroadcast_ContextStatusNotify Request message to the MB-SMF to notify this optionally containing an updated binding indication; or

- when the MB-SMF detects that the AMF which was handling the Broadcast MBS session has failed without restart and no Namf_MBSBroadcast_ContextStatusNotify Request is received from any AMF of the AMF set as described in the first bullet, the MB-SMF may reselect an alternative AMF by sending a Namf_MBSBroadcast_ContextUpdate Request message with an indication that the alternative AMF needs not trigger any NGAP message to deliver the N2 container - MBS Session Setup or Modification Request Transfer, but just to store it for future potential NG-RAN restoration.

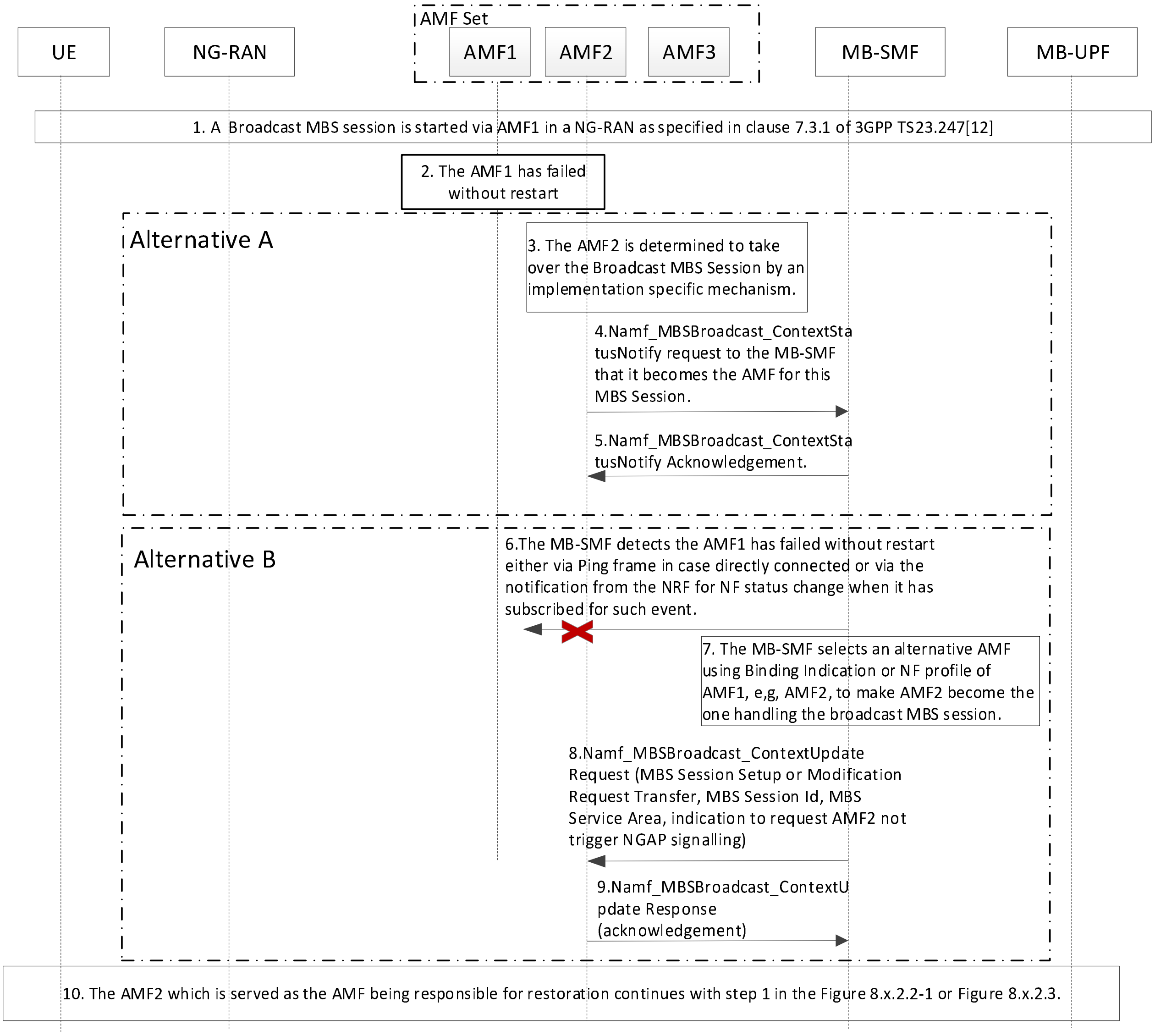
AMF Set
UE
NG-RAN
AMF1
AMF2
AMF3
MB-SMF
MB-UPF
1. A Broadcast MBS session is started via AMF1 in a NG-RAN as specified in clause 7.3.1 of 3GPP TS23.247[12]
2. The AMF1 has failed without restart
Alternative A
3. The AMF2 is determined to take over the Broadcast MBS Session by an implementation specific mechanism.
4.Namf_MBSBroadcast_ContextStatusNotify request to the MB-SMF that it becomes the AMF for this MBS Session.
5.Namf_MBSBroadcast_ContextStatusNotify Acknowledgement.
Alternative B
6.The MB-SMF detects the AMF1 has failed without restart either via Ping frame in case directly connected or via the notification from the NRF for NF status change when it has subscribed for such event.
7. The MB-SMF selects an alternative AMF using Binding Indication or NF profile of AMF1, e,g, AMF2, to make AMF2 become the one handling the broadcast MBS session.
8.Namf_MBSBroadcast_ContextUpdate Request (MBS Session Setup or Modification Request Transfer, MBS Session Id, MBS Service Area, indication to request AMF2 not trigger NGAP signalling)
9.Namf_MBSBroadcast_ContextUpdate Response (acknowledgement)
10. The AMF2 which is served as the AMF being responsible for restoration continues with step 1 in the Figure 8.x.2.2-1 or Figure 8.x.2.3.

Figure 8.3.2.4-1 Selecting an alternative AMF at AMF failure.

1. A Broadcast MBS Session has been established in the network.

2. The AMF1 has failed without restart.

3. Alternative A: another AMF2 in the same AMF set is selected by an AMF implementation specific mechanism.

4. The AMF2 sends Namf_MBSBroadcast_ContextStatusNotify to the MB-SMF that the AMF2 becomes the AMF controlling the Broadcast MBS Session context.

5. The MB-SMF acknowledges the notification and will send subsequent signalling message for this Broadcast MBS Session via the AMF2.

6. Alternative B: the MB-SMF detects that the AMF1 has failed without restart either via HTTP/2 PING Frame for directly connected, or via notifications from the NRF for the NF Status Change when it has subscribed such event, and that no Namf_MBSBroadcast_ContextStatusNotify Request is received from any AMF of the AMF set as described in Alternative A.

7. The MB-SMF selects an alternative AMF pertaining to the same AMF set using the Binding Indication provided by the old AMF or using the NF profile of the old AMF.

8. The MB-SMF sends a Namf_MBSBroadcast_ContextUpdate Request including a MBS Session ID, the corresponding MBS Service Area, a MBS Session Setup or Modification Request Transfer, and sets the "noNgapSignallingInd" to "true" to request the AMF2 to be the AMF for the Broadcast MBS Session to handle subsequent MBS session signaling and be responsible for triggering restoration procedures for NG-RAN failure with or without restart. The AMF may consider to not trigger any NGAP signalling towards NG-RANs covering the MBS service area.

NOTE 1: Upon receiving any subsequent NGAP Broadcast MBS Session signalling from an alternative AMF, the NG-RAN will send any later NG-RAN initiated MBS session signalling towards this alternative AMF.

NOTE 2: If the AMF does not trigger any NGAP signaling towards NG-RANs covering the MBS service area, before receiving any subsequent NGAP Broadcast MBS Session signalling from an alternative AMF, a NG-RAN can initiate a NGAP Broadcast MBS Session signaling procedure (e.g. Broadcast MBS Session Release Required) to a third AMF, e.g. AMF3, in which case the NG-RAN expects a response from AMF3. However, this does not affect that the AMF2 is the AMF responsible for the Broadcast MBS Session, e.g. to handle subsequent Namf_MBSBroadcast_ContextUpdate request messages or to restore the Broadcast MBS session at a NG-RAN restart. How the NGAP initiated Broadcast MBS Session signaling is handled between AMF3 and AMF2 is implementation specific (e.g. to update the broadcast MBS session context that the MBS session has been stopped in the NG-RAN).

9. The AMF responds the Namf_MBSBroadcast_ContextUpdate Request message.

10. The AMF2 continues with the procedures as specified in clauses 8.3.2.2 and 8.3.2.3.

8.3.3 Broadcast MBS session restoration Procedure for NG-RAN failure without restart

The procedure specified in this clause may be supported to restore a Broadcast MBS session affected by an NG-RAN failure without restart.

When the AMF detects NG-RAN failure without restart, e.g. using SCTP path failure detection mechanism, it shall report such event to the MB-SMF for each of MBS session(s) affected by this failure, to enable the MB-SMF to remove the DL F-TEID allocated by the failed NG-RAN in the MB-UPF when unicast transport is used over N3mb interface.

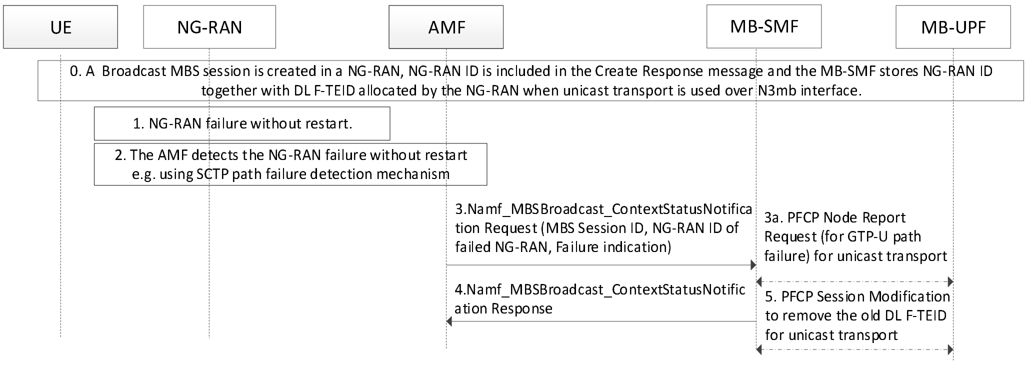
UE
NG-RAN
AMF
MB-SMF
MB-UPF
0. A Broadcast MBS session is created in a NG-RAN, NG-RAN ID is included in the Create Response message and the MB-SMF stores NG-RAN ID together with DL F-TEID allocated by the NG-RAN when unicast transport is used over N3mb interface.
1. NG-RAN failure without restart.
2. The AMF detects the NG-RAN failure without restart e.g. using SCTP path failure detection mechanism
3.Namf_MBSBroadcast_ContextStatusNotification Request (MBS Session ID, NG-RAN ID of failed NG-RAN, Failure indication)
3a. PFCP Node Report Request (for GTP-U path failure) for unicast transport
4.Namf_MBSBroadcast_ContextStatusNotification Response
5. PFCP Session Modification to remove the old DL F-TEID for unicast transport

Figure 8.3.3-1: Broadcast MBS session restoration by MB-SMF upon NG-RAN failure without restart

0. A Broadcast MBS session is created in a NG-RAN, the NG-RAN ID is inserted by the AMF in the N2MbsSmInfo attribute included in the Namf_MBSBroadcast_ContextCreate Response message to the MB-SMF and the MB-SMF stores the NG-RAN ID together with the DL F-TEID allocated by the NG-RAN when unicast transport is used over N3mb interface.

1. The NG-RAN has failed without restart.

2. The AMF detects the NG-RAN has failed without restart e.g. using SCTP path failure detection mechanism.

3. The AMF sends Namf_MBSBroadcast_ContextStatusNotify Request message to the MB-SMF for each affected MBS session including the MBS Session ID, the NG-RAN ID and an indication of the NG-RAN failure without restart event.

3a. The MB-SMF receives a PFCP Node Report Request message from the MB-UPF to report NG-RAN has failed without restart for each affected MBS session when unicast transport was used for N3mb interface.

4. The MB-SMF returns a "204 No Content" response.

5. The MB-SMF modifies the PFCP sessions corresponding to the affected MBS sessions to remove the NG-RAN DL F-TEID in case NG-RAN failure without restart for unicast transport over N3mb.

   The MB-SMF executes step 5 upon receiving either the notification from the AMF or from the MB-UPF.

   If the restoration procedure is triggered due to notification from AMF as specified in step 3, this step may be skipped in deployments where multiple NG-RAN nodes share a common user plane entity, unicast transport is used over N3mb, and the MB-SMF that supports handling shared NG-U terminations determines that the DL F-TEID is associated with other NG-RAN nodes too.

8.3.4 Multicast MBS session restoration Procedure for NG-RAN failure with or without restart

The procedure specified in this clause may be supported to restore a Multicast MBS session affected by an NG-RAN failure with or without restart.

When a UPF detects the NG-RAN failure with or without restart using Echo Request and Echo Response message which is sent towards the IP address in the DL F-TEID allocated by the failed NG-RAN, or upon receiving GTP-U Error Indication, it shall report such event to the SMF to enable the SMF to derive UEs who have joined the MBS sessions which are affected by the NG-RAN failure and initiates the restoration procedure for each of Multicast MBS session which were activated in the failed NG-RAN as described in Figure 8.3.4-1.

When unicast transport is used over N3mb interface for 5GC Shared MBS traffic delivery, the MB-UPF detects the NG-RAN failure with or without restart using Echo Request and Echo Response message which is sent towards the IP address in the DL F-TEID allocated by the failed NG-RAN, or upon receiving GTP-U Error Indication, it shall report such event to the MB-SMF, so that the MB-SMF removes the DL-TEID allocated by the failed NG-RAN.

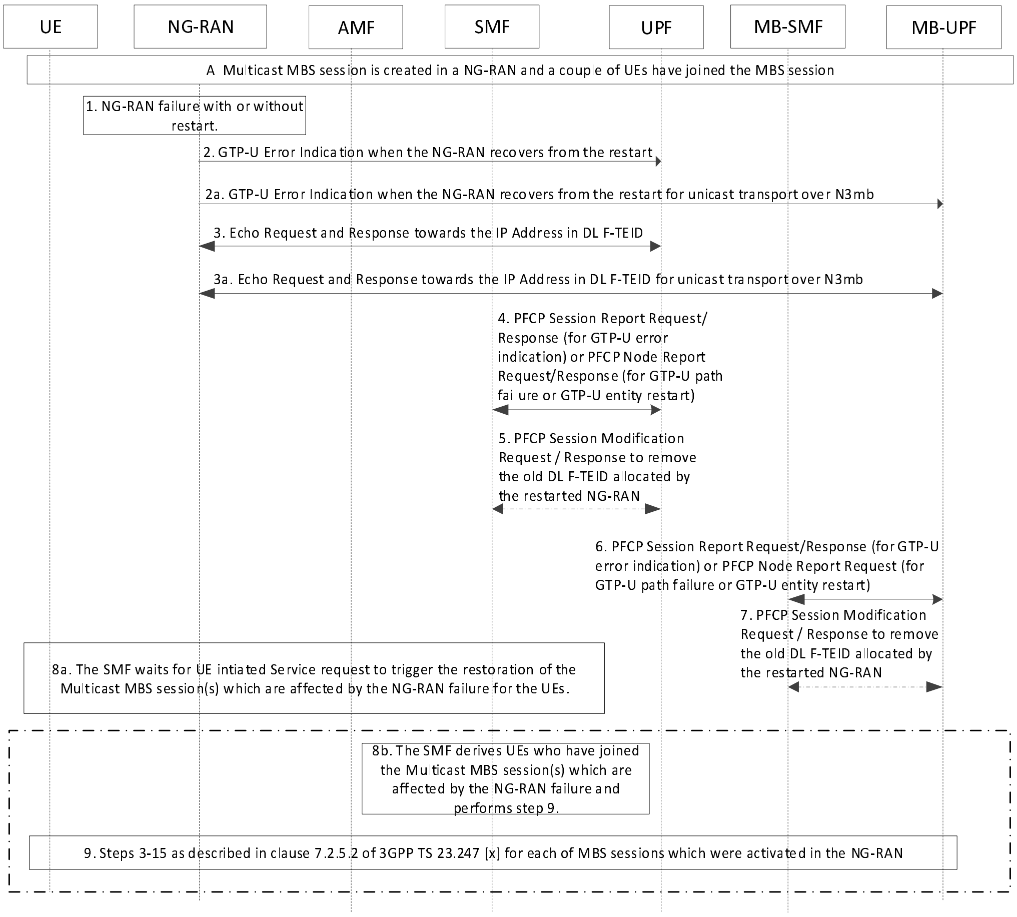
UE
NG-RAN
AMF
SMF
UPF
MB-SMF
MB-UPF
A Multicast MBS session is created in a NG-RAN and a couple of UEs have joined the MBS session
1. NG-RAN failure with or without restart.
2. GTP-U Error Indication when the NG-RAN recovers from the restart
2a. GTP-U Error Indication when the NG-RAN recovers from the restart for unicast transport over N3mb
3. Echo Request and Response towards the IP Address in DL F-TEID
3a. Echo Request and Response towards the IP Address in DL F-TEID for unicast transport over N3mb
4. PFCP Session Report Request/ Response (for GTP-U error indication) or PFCP Node Report Request/Response (for GTP-U path failure or GTP-U entity restart)
5. PFCP Session Modification Request / Response to remove the old DL F-TEID allocated by the restarted NG-RAN
6. PFCP Session Report Request/Response (for GTP-U error indication) or PFCP Node Report Request (for GTP-U path failure or GTP-U entity restart)
7. PFCP Session Modification Request / Response to remove the old DL F-TEID allocated by the restarted NG-RAN
8a. The SMF waits for UE intiated Service request to trigger the restoration of the Multicast MBS session(s) which are affected by the NG-RAN failure for the UEs.
8b. The SMF derives UEs who have joined the Multicast MBS session(s) which are affected by the NG-RAN failure and performs step 9.
9. Steps 3-15 as described in clause 7.2.5.2 of 3GPP TS 23.247 [x] for each of MBS sessions which were activated in the NG-RAN

Figure 8.3.4-1: Multicast MBS session restoration upon NG-RAN failure with or without restart

1. The NG-RAN has failed with or without restart.

2. The UPF receive GTP-U Error Indication when the NG-RAN recovers from its restart for 5GC Individual MBS traffic delivery.

2a. The MB-UPF receives GTP-U Error Indication when the NG-RAN recovers from its restart for unicast transport over N3mb for 5GC Shared MBS traffic delivery.

3. The UPF sends Echo Request message towards the NG-RAN using the IP address included in the DL F-TEID, thus the UPF detects the NG-RAN has failed with or without restart.

3a. The MB-UPF sends Echo Request message towards the NG-RAN using the IP address included in the DL F-TEID for unicast transport over N3mb, thus the MB-UPF detects the NG-RAN has failed with or without restart.

4. The UPF sends PFCP Session Report Request messages to the SMF to report receiving of GTP-U Error Indication message, or sends a PFCP Node Report Request message to the SMF to report the GTP-U path failure towards the NG-RAN or the remote GTP-U entity has restarted.

5. The SMF sends PFCP Session Modification Request message to request the UPF to remove DL-FTEID allocated by the failed NG-RAN and buffer the MBS session data for 5GC Individual MBS traffic delivery, except for an NG-RAN restart if the UPF has already removed the DL F-TEID on its own as specified in clause 5.5.

6. The MB-UPF sends PFCP Session Report Request messages to the MB-SMF to report receiving of GTP-U Error Indication message, or sends a PFCP Node Report Request message to the MB-SMF to report the GTP-U path failure towards the NG-RAN or the remote GTP-U entity has restarted, for unicast transport for N3mb.

7. The MB-SMF sends PFCP Session Modification Request message to request the MB-UPF to remove DL-FTEID allocated by the failed NG-RAN, except for an NG-RAN restart if the MB-UPF has already removed the DL F-TEID on its own as specified in clause 5.5.

8a. The SMF may wait for UEs who have joined the MBS session(s) which are affected by the NG-RAN failure to trigger a Service Request procedure to re-establish the user plane resource and then restore the Multicast MBS session in NG-RAN.

8b. Alternatively, the SMF may derive UEs who have joined the MBS session(s) which are affected by the NG-RAN failure (i.e. with a DL F-TEID matching the IP address of the NG-RAN node's to restore the MBS service and perform step 9.

9. When step 8b applies, the SMF continues with the MBS session activation procedure as specified in clause 7.2.5.2 of 3GPP TS 23.247 [12] starting from step 3 to restore the MBS sessions for affected UEs for each MBS session.

8.4 Restoration procedures for AMF failure

8.4.1 Multicast MBS session (de)activation or update after an AMF failure

8.4.1.1 General

Different NG-RAN nodes may establish shared delivery for the same MBS session via different AMFs of a same AMF set. During the shared delivery establishment:

- each AMF involved in the establishment of shared delivery stores in its multicast MBS session context the RAN-ID of the NG-RAN nodes that have established shared delivery via this AMF, for subsequent signaling related to the multicast MBS Session (Multicast MBS session activation, deactivation or update); and

- the MB-SMF stores in its multicast MBS session context the NF Instance ID of each AMF involved in the establishment of shared delivery to enable subsequent signalling towards these AMFs.

See clause 7.2.1.4 and Table 6.9.1-1 of 3GPP TS 23.247 [12].

The following procedure may be used to enable the MB-SMF to activate, deactivate or update the multicast MBS session, when an AMF of the AMF set through which one or more NG-RAN nodes had established shared delivery has failed with or without restart or is no longer reachable (e.g. due to networking issues, or because it has been de-instantiated from the AMF set).

8.4.1.2 N2 MBS session request distribution with list of NG RAN Node IDs provided by MB-SMF to AMF

During the shared delivery establishment procedure (see clause 7.2.1.4 of 3GPP TS 23.247 [12]), the MB-SMF stores, for each AMF involved in the establishment of shared delivery, the list of NG-RAN Node IDs having shared delivery established through the AMF.

The MB-SMF may then send any multicast MBS session activation, deactivation and update request towards the NG-RAN nodes that established shared delivery as defined in Figure 8.4.1.2-2.

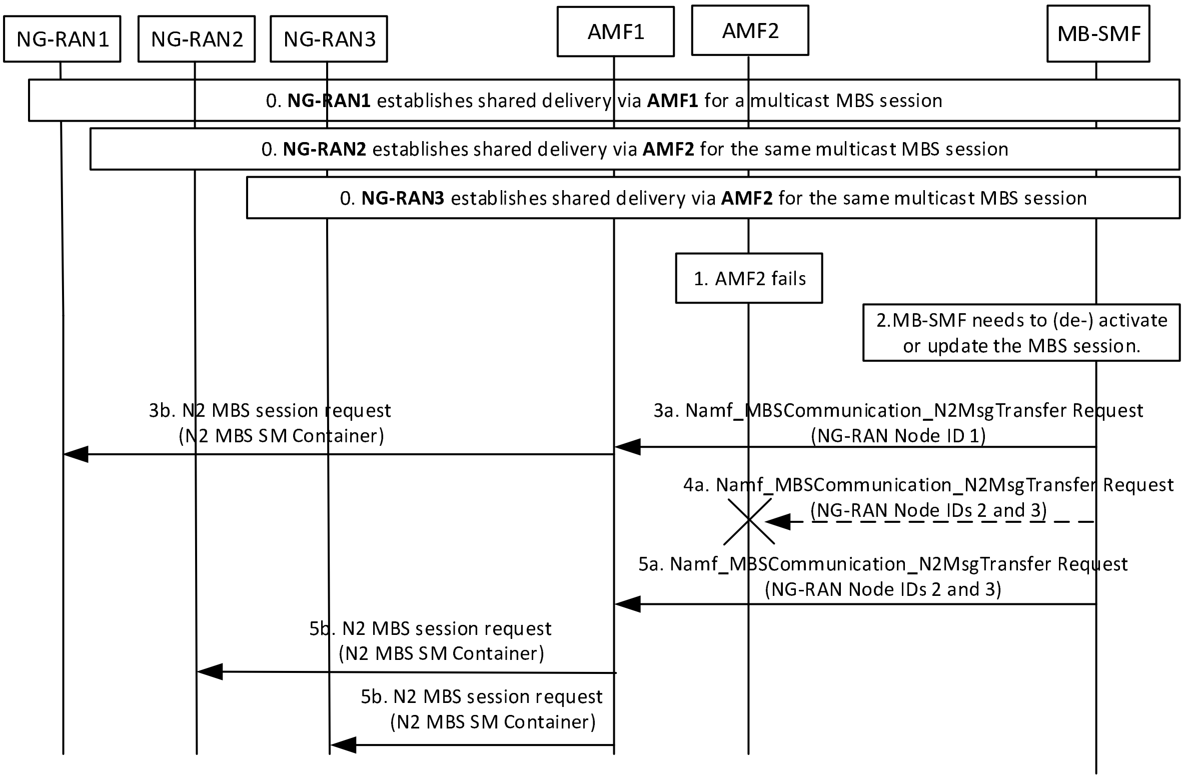
NG-RAN1
NG-RAN2
NG-RAN3
AMF1
AMF2
MB-SMF
0. NG-RAN1 establishes shared delivery via AMF1 for a multicast MBS session
0. NG-RAN2 establishes shared delivery via AMF2 for the same multicast MBS session
0. NG-RAN3 establishes shared delivery via AMF2 for the same multicast MBS session
1. AMF2 fails
2.MB-SMF needs to (de-) activate or update the MBS session.
3b. N2 MBS session request (N2 MBS SM Container)
3a. Namf_MBSCommunication_N2MsgTransfer Request (NG-RAN Node ID 1)
4a. Namf_MBSCommunication_N2MsgTransfer Request (NG-RAN Node IDs 2 and 3)
5a. Namf_MBSCommunication_N2MsgTransfer Request (NG-RAN Node IDs 2 and 3)
5b. N2 MBS session request (N2 MBS SM Container)
5b. N2 MBS session request (N2 MBS SM Container)

Figure 8.4.1.2-2: Multicast MBS session activation, deactivation or update via an alternative AMF of the AMF set

0. NG RAN1 establishes shared delivery for the multicast MBS session via AMF1. NG RAN2 and NG RAN3 do so via AMF2. MB-SMF stores corresponding information in its MBS session context.

1. AMF2 becomes no longer available/reachable.

2. The MB-SMF needs to activate, deactivate or update the MBS session.

3. The MB-SMF sends an Namf_MBSCommunication_N2MessageTransfer Request to every AMF of the same AMF set that was involved in the establishment of shared delivery, as specified in clauses 7.2.5.2, 7.2.5.3 and 7.2.6 of 3GPP TS 23.247 [12], but with the request further including the list of NG RAN Node IDs known by the MB-SMF to have established shared delivery through the respective AMF. AMF1 distributes the request to the list of NG-RAN nodes received from the MB-SMF, if any, otherwise to the list of the NG-RAN nodes it has stored locally, if any.

NOTE 1: In absence of AMF failures, an NG-RAN node receives requests to activate, deactivate and update the MBS session via the same AMF through which it established shared delivery.

NOTE 2: Including the list of NG RAN Node IDs in every Namf_MBSCommunication_N2MessageTransfer Request, even towards AMFs that are operational, enable to distribute the requests to the NG RAN nodes, even if these AMFs would have restarted and lost their list of NG RAN node IDs beforehand, or if the SCP would need to reselect a different AMF when using indirect communication.

4. If the MB-SMF is not yet aware that AMF2 has failed, it sends an Namf_MBSCommunication N2MessageTransfer Request to AMF2 as described in step 3 and detects that AMF2 is no longer available.

5. The MB-SMF sends an Namf_MBSCommunication_N2MessageTransfer Request to an alternative AMF (AMF1 in this example) of the same AMF set including the list of NG RAN Node IDs known by the MB-SMF to have established shared delivery through the failed AMF (AMF2). AMF1 distributes the request to the list of NG-RAN nodes received from the MB-SMF.

If the MB-SMF is already aware at the start of this procedure that AMF2 has failed, the MB-SMF may already include in step 3 the list of NG RAN Node IDs known by the MB-SMF to have established shared delivery through the failed AMF (AMF2).When using unicast transport over N3mb, the MB-SMF may determine that a NG-RAN node has failed or restarted as specified in clause 8.3.4. In this case, the MB-SMF shall remove this NG RAN node from its MBS session context.

NOTE 3: This avoids that the MB-SMF requests an AMF to send requests to NG RAN nodes that have failed or restarted, i.e. that have no more shared delivery established.

In scenarios where the MB-SMF would request an AMF to distribute an activate, deactivate or update request to a NG RAN node that has no longer shared delivery established (e.g. the NG RAN node has restarted but this has not been detected by the MB-SMF), the NG RAN will return an activation or update failure to the AMF. To enable the MB-SMF to be notified about this failure and to remove the NG RAN node ID from its MBS session context, the MB-SMF shall include a notification URI in every Namf_MBSCommunication_N2MessageTransfer Request it sends and the AMF shall notify a failure received from an NG RAN node towards the MB-SMF by sending an Namf_MBSCommunication_Notify request to the notification URI that was received in the request.

Likewise, if an AMF receives an Namf_MBSCommunication_N2MessageTransfer Request including a NG RAN Node ID and the AMF cannot send any N2 message towards this NG RAN node (e.g. the NG-RAN node has failed without restart), the AMF shall notify the failure to send N2 MBS session requests to the NG RAN node by sending an Namf_MBSCommunication_Notify request to the notification URI that was received in the request.

NOTE 4: When IP multicast is used over N3mb, the MB-SMF cannot detect via the MB-UPF that a NG RAN node has failed or restarted. So in this case, and also possibly even when using unicast transport, it can occur that the MB-SMF requests the AMF to send an activate, deactivate or update request to an NG RAN node that has no longer shared delivery established.

Annex A (informative): Change history

Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2018-07	CT4#85bis	C4-185034				Initial Draft and skeleton.	0.0.2
2018-07	CT4#85bis	C4-185407				N4 Failure and Restart Detection, Restoration procedures for User Plane interfaces N3 and N9 Implementation of C4-185409, C4-185410, C4-185411, C4-185412, C4-185413, C4-185414, C4-185527	0.1.0
2018-08	CT4#86	C4-186509				Implementation of C4-186233, C4-186406, C4-186408, C4-186413, C4-186488	0.2.0
2018-09	CT#81	CP-182082				Presented for Information and approval	1.0.0
2018-09	CT#81					Approved in CT#81	15.0.0
2018-12	CT#82	CP-183021	0003	-	F	GTP-U Error Indication received from 5G-AN	15.1.0
2018-12	CT#82	CP-183021	0004	4	F	NF service restart detection by direct signalling between NFs	15.1.0
2018-12	CT#82	CP-183021	0006	1	F	Restoration Procedure for Intermediate UPF Restart	15.1.0
2018-12	CT#82	CP-183021	0007	1	F	Restart detection by direct signalling between NFs	15.1.0
2018-12	CT#82	CP-183021	0008		F	PWS restoration procedures	15.1.0
2018-12	CT#82	CP-183021	0009	1	F	NF Service Instance Reselection	15.1.0
2019-03	CT#83	CP-190026	0010	-	F	NF Restart detection	15.2.0
2019-06	CT#84	CP-191038	0011	1	F	Corrections to Restoration procedures	15.3.0
2019-06	CT#84	CP-191044	0012	2	F	Clarifications on UPF restoration procedure	16.0.0
2019-06	CT#84	CP-191044	0013	1	F	Clarifications on GTP-U Error Indication received by 5G-AN	16.0.0
2019-09	CT#85	CP-192124	0014	-	F	Regulation of contexts restoration by NFs	16.1.0
2019-12	CT#86	CP-193045	0017	1	F	PFCP Association Setup Request with same Node ID	16.2.0
2019-12	CT#86	CP-193045	0018	2	F	Reestablishment of PFCP sessions after a UP function restart	16.2.0
2020-06	CT#88e	CP-201030	0019	2	B	Populating Recovery Information via Direct signalling from a Service Producer	16.3.0
2020-06	CT#88e	CP-201030	0021	2	B	Populating Recovery Information of NF (Service) Set via NRF	16.3.0
2020-06	CT#88e	CP-201030	0020	2	B	Populating Recovery Information via Direct signalling from a Service Consumer	16.3.0
2020-06	CT#88e	CP-201030	0023	-	F	NF Service Instance Reselection	16.3.0
2020-09	CT#89e	CP-202119	0024	1	F	Reselection when the Routing Binding Indication unavailable	16.4.0
2020-12	CT90e	CP-203054	0025	1	F	NF reselection by the SCP without Routing Binding Indication	16.5.0
2021-03	CT#91e	CP-210032	0027	-	F	Partial failure handling support over N4	17.0.0
2021-06	CT#92e	CP-211059	0031	1	A	Clarifications to NF service producer reselection procedure (w/o binding support)	17.1.0
2021-06	CT#92e	CP-211043	0030	2	B	Restoration of PFCP sessions affected by a partial or complete failure	17.1.0
2021-06	CT#92e	CP-211049	0029	5	B	I-SMF/V-SMF Restoration procedure	17.1.0
2021-12	CT#94e	CP-213086	0035	-	F	Mandating SCPs to support NF reselection for Model C/D delegated discovery	17.2.0
2021-12	CT#94e	CP-213122	0036	1	B	Void I-SMF/V-SMF Restoration procedure from normal specification clause	17.2.0
2021-12	CT#94e	CP-213120	0037	-	F	Update the reference	17.2.0
2022-03	CT#95e	CP-220035	0041	1	B	MBS session restoration upon MB-UPF failure with restart	17.3.0
2022-03	CT#95e	CP-220035	0042	1	B	MBS session restoration upon MB-UPF failure without restart	17.3.0
2022-03	CT#95e	CP-220036	0038	3	B	Stage 2 description on Restoration of Profiles related to UDR	17.3.0
2022-03	CT#95e	CP-220037	0039	1	B	Detection and reporting of the restart of a GTP-U entity	17.3.0
2022-03	CT#95e	CP-220086	0040	3	B	Enhanced handling at user plane path failure	17.3.0
2022-03						Editorial corrections	17.3.1
2022-06	CT#96	CP-221023	0044	1	F	Restoration procedure for MB-UPF restart	17.4.0
2022-06	CT#96	CP-221023	0048	1	B	Restoration of a Broadcast MBS session upon NG-RAN failure with or without restart	17.4.0
2022-06	CT#96	CP-221023	0049	1	B	Restoration of a Multicast MBS session upon NG-RAN failure with or without restart	17.4.0
2022-06	CT#96	CP-221024	0053	-	F	Removal of Editor's note for MB-UPF failure without restart	17.4.0
2022-06	CT#96	CP-221024	0056	1	B	Support of Broadcast MBS Session with an AMF set being deployed	17.4.0
2022-06	CT#96	CP-221025	0046	3	F	Updates on Stage 2 description on Restoration of Profiles related to UDR	17.4.0
2022-06	CT#96	CP-221045	0045	1	F	Failure to restore a PFCP session at UPF restart	17.4.0
2022-06	CT#96	CP-221045	0054	1	F	Target NF type in notification request for NF service consumer reselection by SCP	17.4.0
2022-06	CT#96	CP-221045	0055	-	F	Set Deletion procedure	17.4.0
2022-06	CT#96	CP-221061	0057	1	F	Restoration procedures for Home Routed PDU Sessions or PDU sessions with an I-SMF	17.4.0
2022-06	CT#96	CP-221061	0058	1	F	Restoration procedures for Home Routed PDU Sessions or PDU sessions with an I-SMF	17.4.0
2022-06						Editorial corrections	17.4.1
2022-09	CT#97e	CP-222031	0059	-	F	Corrections to the Broadcast MBS session restoration procedures	17.5.0
2022-09	CT#97e	CP-222035	0061	-	F	Updates on Stage 2 description on Restoration of Profiles related to UDR	17.5.0

2022-12	CT#98e	CP-223036	0062	-	F	Corrections on ContextStatusNofity event for multicast transport over N19mb	17.6.0
2022-12	CT#98e	CP-223036	0064	2	F	Impact of Shared NG-U Termination on MBS Restoration Procedures	17.6.0
2022-12	CT#98e	CP-223087	0063	-	B	Multicast MBS session (de)activation or update after an AMF failure	18.0.0
2023-09	CT#101	CP-232033	0065	1	B	Prefix in Callback URIs	18.1.0
2023-12	CT#102	CP-233056	0067	2	B	Restoration procedure for NG-RAN receiving a GTP-U Error Indication	18.2.0
2024-03	CT#103	CP-240053	0068	1	F	SMF restoration procedures for SMF in an SMF set	18.3.0
2024-03	CT#103	CP-240053	0069	-	F	Incorrect styles	18.3.0
2024-03	CT#103	CP-240053	0071	1	F	Reference updates	18.3.0

History

Document history		
V18.3.0	May 2024	Publication