Technical Report

TR-456

AGF Functional Requirements

Issue: 2 Corrigendum 1

Issue Date: July 2023

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is owned and copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be owned and/or copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER'S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

All copies of this Technical Report (or any portion hereof) must include the notices, legends, and other provisions set forth on this page.

Issue History

Issue Number	Approval Date	Release Date	Issue Editors	Changes
1	25 August 2020	25 August 2020	Bouchat Christele, Nokia Newton, Jonathan, Vodafone Group	Original
2	1 March 2022	1 March 2022	Bouchat Christele, Nokia Newton, Jonathan, Vodafone Group	Multiple IP session support for FN-RGs Additional authentication in the form of PAP/CHAP support for FN-RGs Support for FN-RG Static IPv4 Addressing Updates to VSNP procedures; NAS and AS messaging. Extensions for MTU and DSCP handling Fixes, clarifications and additional guidance for improved interoperability.
2 Corrigendum 1	19 July 2023	19 July 2023	Bouchat Christele, Nokia	Correction of the VSNP SDU message Different clarifications and improvements added

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org..

Editor: Christele Bouchat, Nokia

Work Area Directors: Christele Bouchat, Nokia
Manuel Paul, Deutsche Telekom

Project Stream Leader: Venkatesh Padebettu, Juniper

Table of Contents

Table of Figures

Executive Summary

This document contains the functional requirements of the Access Gateway Function (AGF), a key mediation function specified by BBF in the 5G Wireline Wireless Convergence (WWC) architecture for Fixed Mobile Convergence (FMC), jointly defined by 3GPP and BBF.

The 5G WWC architecture includes the set of functions and interfaces that realizes the use cases targeted by the BBF and 3GPP for the 3GPP Release 16, including network functions for adapting wireline access to the 5G-Core.

The Access Gateway Function is a logical function deployed between the physical access media (e.g., DSL, PON, GE) in the wireline access network and the 5G core network.

Functional requirements specified for the AGF in this document cover the deployment scenarios described in TR-470 [9]. Both Fixed Network-Residential Gateway (FN-RG) as well as 5G-Residential Gateway (5G-RG) devices are supported.

This document is a corrigendum. It does obsolete previous Issues. The main correction finds place in section 5.7.1 ‘VSNP message format’. This issue contains moreover clarification text and improvements.

1 Purpose and Scope

1.1 Purpose

In 2017-2018, the BBF WWC Work Area studied 5G Fixed Mobile Convergence and its impacts on interfaces being defined by 3GPP for release 16 and further releases. BBF concluded its study by December 2018. It resulted in series of liaisons with requests from BBF to 3GPP SA2. Those requests have been considered in the normative phase of 3GPP R16. The Access Gateway Function, AGF, that resides between fixed access networks and the 5G core network, serving both 5G-RG as well as FN-RG, will be described in this document.

1.2 Scope

The scope of this Technical Report is to describe the functional requirements of the AGF. The Access Gateway Function resides in between the aggregation network of fixed access nodes such as DSLAMs and PON OLTs, and the 5G core network. As such subscribers served by access equipment specified in TR-101 issue 2, TR-156 issue 4, TR-167 issue 3, TR-178 issue 2 and TR-301 issue 2 corr1 can be connected to the 5GC via an AGF. The AGF integrates a subset of BNG functions and new functions that together can allow it to serve both FN-RG and 5G-RG. In the current issue of this document, wholesale deployment scenarios (excluding third-party access networks and L2TP support); IPTV; considerations on AGF virtualization and deployment of virtual AGF; are all out of scope. They may be studied in future revisions of the document.

In addition, for the current issue of this document, the only VLAN model on the V interface (as per TR-101) that is considered for 5G-RG is 1:1 double tag. 1:1 single tag and n:1 for 5G-RG are for further study.

Hybrid access is supported by the overall architecture but does not add any AGF requirements.

CUPS for the AGF will be addressed by TR-458. For this issue of TR-456, the AGF is assumed to be an integrated implementation and the exact call flows between the AGF-CP and AGF-UP are FFS. The impact in TR-458 on these flows will be reflected in subsequent issues of this specification.

It should be noted that a same requirement in different issues might have a different number.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC 2119[38] RFC 8174 [53] when, and only when, they appear in all capitals, as shown here.

2.1.1 Special Convention for this document

Throughout this document, the AGF requirements that are common for a 5G-RG and an FN-RG use the template [R-1], …, [R-x].

The extra AGF requirements needed for the FN-RG use the template [R-FN-1], …, [R-FN-x].

The extra AGF requirements needed for the 5G-RG use the template [R-5G-1], …, [R-5G-x].

In case a given AGF only supports 5G-RG, then this AGF MUST support all requirements [R-1], …, [R-x] AND [R-5G-1], …, [R-5G-x].

In case a given AGF only supports FN-RG (in the example an operator would want to keep FN-RGs while still being able to connect to the 5GC) then this AGF MUST support all requirements [R-1], …, R-x] AND [R-FN-1], …, [R-FN-x].].

In case a given AGF supports both 5G-RG and FN-RG, then this AGF MUST support all requirements [R-1], …, R-x] AND [R-FN-1], …, [R-FN-x] AND [R-5G-1], …, [R-5G-x].

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-069 Amendment 6	CPE WAN Management Protocol	BBF	2018
[2] TR-181 Issue 2 Amendment 14	Device Data Model for TR-069	BBF	2020
[3] TR-101 Issue2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[4] TR-177 Corrigendum 1	IPv6 in the context of TR-101	BBF	2017
[5] TR-178 Issue 2	Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2017
[6] TR-124 Issue 6	Functional Requirements for Broadband Residential Gateway Devices	BBF	2020
[7] TR-146	Subscriber Sessions	BBF	2013
[8] TR-187 Issue 2	IPv6 for PPP Broadband Access	BBF	2013
[9] TR-470	5G Wireless Wireline Convergence Architecture	BBF	2022

[10] TR-458	CUPS for WWC	BBF	2023
[11] TS 24.501	Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage3	3GPP	For R16
[12] TS 24.502	Access to the *3GPP* 5G Core Network (5GCN) via non-*3GPP* access networks	3GPP	For R16
[13] TS 38.331	NR; Radio Resource Control (RRC); Protocol specification.	3GPP	For R16
[14] TS 38.410	NG-RAN, NG general aspects and principles	3GPP	For R16
[15] TS 38.412	NG-RAN, NG signaling transport	3GPP	For R16
[16] TS 38.413	NG-RAN; NG Application Protocol (NGAP)	3GPP	For R16
[17] TS 29.244	Interface between the control plane and the user plane nodes	3GPP	For R16
[18] TS 29.274	3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C)	3GPP	For R16
[19] TS 29.303	Domain Name System Procedures	3GPP	For R16
[20] TS 29.413	Application of the NG Application Protocol (NGAP) to non-3GPP access	3GPP	For R16
[21] TS 29.502	5G System; Session Management Services; Stage 3	3GPP	For R16
[22] TS 29.510	5G System; Network function repository services; Stage 3	3GPP	For R16
[23] TS 38.414	NG-RAN; NG data transport	3GPP	For R16
[24] TS 38.415	PDU Session User Plane Protocol	3GPP	For R16
[25] TS 23.316	Wireless and wireline convergence access support for the 5G System	3GPP	For R16
[26] TS 23.003	Numbering, addressing and identification	3GPP	For R16
[27] TS 33.501	Security architecture and procedures for 5G system	3GPP	For R16
[28] TS 23.501	System architecture for the 5G System (5GS)	3GPP	For R16
[29] TS 23.502	Procedures for the 5G System (5GS)	3GPP	For R16
[30] TS 23.503	Policy and charging control framework for the 5G System (5GS); Stage 2	3GPP	For R16
[31] TS 38.300	NR and NG-RAN Overall Description	3GPP	For R16
[32] RFC 8822	5G Wireless Wireline Convergence User Plane Encapsulation (5WE)	IETF	2021
[33] IEEE 802.1Q	Virtual Bridged Local Area Networks	IEEE	2018
[34] RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)	IETF	1992
[35] RFC 1570	PPP LCP Extensions	IETF	1994
[36] RFC 1877	PPP IPCP Extensions	IETF	1995
[37] RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)	IETF	1996
[38] RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[39] RFC 2153	“PPP Vendor Extensions”, IETF Informational Standard, May 1997. https://tools.ietf.org/html/rfc2153	IETF	1997
[40] RFC 8200	Internet Protocol, Version 6 (IPv6) Specification	IETF	2017
[41] RFC 2515	Definitions of Managed Objects for ATM Management	IETF	1999
[42] RFC 2516	“A Method for Transmitting PPP Over Ethernet	IETF	1999

	(PPPoE)", IETF Informational Standard, February 1999. Available at "https://tools.ietf.org/html/rfc2516"		
[43] RFC 1661	"The Point-to-Point Protocol (PPP)", IETF Internet Standard, July 1994, Available at "https://tools.ietf.org/html/rfc1661"	IETF	1994
[44] RFC 2661	Layer Two Tunneling Protocol "L2TP"	IETF	1999
[45] RFC 2865	Remote Authentication Dial In User Service (RADIUS)	IETF	2000
[46] RFC 3772	"Point-to-Point Protocol (PPP) Vendor Protocol", IETF Proposed Standard, May 2004. Available at "https://tools.ietf.org/html/rfc3772"	IETF	2004
[47] RFC 3931	Layer Two Tunneling Protocol - Version 3 (L2TPv3)	IETF	2005
[48] RFC 4282	The Network Access Identifier	IETF	2005
[49] RFC 4861	Neighbor Discovery for IP version 6 (IPv6)	IETF	2007
[50] RFC 4638	Accommodating a Maximum Transit Unit / Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)	IETF	2006
[51] RFC 4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)	IETF	2006
[52] RFC 6691	TCP Options and Maximum Segment Size	IETF	2012
[53] RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC2119 Key Words	IETF	2017
[54] RFC 6957	Duplicate DAD Detection Proxy	IETF	2013
[55] RFC 6221	Lightweight DHCPv6 Relay Agent	IETF	2011
[56] RFC 6788	The Line-Identification Option	IETF	2012
[57] RFC 2868	RADIUS Attributes for Tunnel Protocol Support	IETF	2000
[58] RFC 5515	Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions	IETF	2009
[59] RFC 8415	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	IETF	2018
[60] I.363.1	B-ISDN ATM ADAPTATION LAYER SPECIFICATION: TYPE 1 AAL	ITU-T	1996

2.3 Definitions

The following terminology is used throughout this Technical Report.

5G-RG	An RG acting as a 3GPP UE towards the 5GC. Note: This corresponds to the term 5G-BRG in [25].
5G VLAN	5G VLAN refers to the VLAN delineated access circuit that is used for NAS CP exchange and transport of all 5WE encapsulated UP traffic between a 5G-RG and an AGF. There is one 5G-VLAN provisioned per 5G-RG. This may also be the access circuit previously used for FN-RG support in migration scenarios. The 5G-RG is either configured with the VID to use for the 5G VLAN, or defaults to using NULL or priority tagged VLAN encapsulation for NAS and 5WE traffic.
5WE Session ID	5WE Session ID is the identifier of the 5WE session used in the user plane between 5G-RG and AGF corresponding to the 5G-RG's PDU session ID.
Access Network (AN)	A network used by a subscriber device to access a service edge, typically IP edge, i.e., BNG, P-GW, 5G core.
Access Gateway function (AGF)	A function connecting wireline ANs to the 5GC. AGF-CP is the control plane while AGF-UP is the user plane of the AGF. Note: This corresponds to the W-AGF in [25].
FN-RG	An RG connecting a home LAN to the WAN, which does not exchange N1 signaling with the 5GC. Note: This corresponds to an FN-BRG in [25].
Hybrid Access	Access that utilizes both wireline access networks and wireless access networks. From the perspective of an RG, 5G-RG or UE. This can either be exclusive or simultaneous access.
IP sessions	Where used, the term IP session refers to the BBF concept of an IP session as documented in TR-146 [7].
N1	Reference point between the 5G-RG and the AMF and between the AGF-CP and AMF in case of FN-RG.
N2	Reference point between W-5GAN and AMF. On the W-5GAN side, the termination point is the AGF-CP.
N3	Reference point between W-5GAN and UPF. On the W-5GAN side, the termination point is the AGF-UP.
PDU Session ID	PDU Session ID is the control plane identifier of each PDU session in the 5G system. It is administered by the 5G-RG.
Transport MTU	Is the MTU of the mobile network on the N3 and N9 interfaces. This is typically the infrastructure MTU less the overhead of GTP tunneling.
Wireline 5G Access Network (W-5GAN)	This is a wireline AN that can connect to a 5G core via the AGF. The egress interfaces of a W-5GAN form the border between access and core. The interfaces are N2 for the control plane and N3 for the user plane.

Wireline Access MTU	Is the maximum transfer unit established for the concatenated Y4/Y5 & V reference points. This would be 1492 for PPPoE (or in rare cases is negotiated), 1500 for IPoE and the negotiated value for 5WE.
Wireline Access Network	Access network conforming with TR-101/TR-178, that can be for example optical fiber or electrical cable. The egress interface of a wireline access network is the V interface. The wireline access network includes wireline access nodes and optionally some form of aggregation.
Wireless Access Network	In this document, is a 3GPP NG RAN, as specified in TS38.300 and/or TS36.300.

2.3.1 Definitions of 3GPP concepts:

The following definitions summarize 3GPP definitions. In case of inconsistency between the text in the following and 3GPP definition (please refer to the referenced documents in section 2.2), the 3GPP definition takes precedence.

5G System (5GS)	A system consisting of 5G Access Network (AN), 5G Core Network and UE.
Network Instance	Information identifying a domain. Used by the UPF for traffic detection and routing (definition from TS 23.501 [28]).
Network Slice	A logical network that provides specific network capabilities and network characteristics (definition from TS 23.501 [28]).
Network Slice Instance	A set of Network Function instances and the required resources (e.g., compute, storage and networking resources) which form a deployed Network Slice (definition from TS 23.501 [28]).
Network Slice Selection Assistance Information (NSSAI)	The NSSAI is a collection of S-NSSAIs (Single NSSAIs). An NSSAI may be a Configured NSSAI, a Requested NSSAI or an Allowed NSSAI. There can be at most eight S-NSSAIs in Allowed and Requested NSSAIs sent in signaling messages between the UE and the Network. The NSSAI is defined in TS 23.501 [28].
Allowed NSSAI	An NSSAI provided by the serving PLMN during e.g., a registration procedure, indicating the S-NSSAI's value that the UE could use in the serving PLMN of the current registration area. The Allowed NSSAI is defined in TS 23.501 [28].
Configured NSSAI	An NSSAI that has been provisioned in the 5G-RG applicable to one or more PLMN (the Configured NSSAI is defined in TS 23.501 [28]).
Requested NSSAI	An NSSAI provided by the UE to the Serving PLMN during registration. The Requested NSSAI is defined in TS 23.501 [28].
Subscribed NSSAI	An NSSAI based on subscriber information, which a UE is subscribed to use in a PLMN. The Subscribed NSSAI is defined in TS 23.501 [28] and the format of S-NSSAI is defined in TS 23.003 [26].

IP and PDU sessions	Where used, the term IP session refers to the BBF concept of an IP session as documented in TR-146 [7]. Where used, the term PDU session refers to the 3GPP concept as defined in TS 23.501 [28]. A PDU session is a temporal association between the UE and a Data Network that provides a PDU connectivity service. As described in TR-146 [7], IP session corresponds to a single protocol (IPv4 or IPv6) whereas a PDU session may provide dual stack support. An IP session may be IPoE based or negotiated by one or more network control protocols over a PPPoE session. Hence there is not necessarily a 1:1 correspondence between them, a PDU session may support two IP sessions; an IPv4 session and an IPv6 session.
Access & Mobility Management Function (AMF)	The AMF is a 5GC-CP function that in particular terminates N1 and N2. It is responsible for mobility and access-related functions. It acts as the security anchor point for a given UE. At PDU session establishment, it selects the SMF corresponding to the requested slice and targeted DN, and relays session related messages to this SMF. For detailed specification of AMF refers to 3GPP documents TS 23.316 [25] and TS 23.502 [29].
Session Management Function (SMF)	The SMF is a 5GC control plane function. For detailed specification of SMF refers to 3GPP documents TS 23.316 [25], TS 23.501 [28], TS 23.502 [29]. Its main functionalities include: • establishing, modifying and releasing sessions • maintaining tunnel(s) between the UPF and access network • UPF control and selection • address allocation • policy control via UPF • charging data collection and reporting
SSC modes	SSC mode determines how UPF of PDU session is managed during session lifetime with regard to the UE change of radio access anchor point. More details can be found in chapter 5.6.9 of TS 23.501 [28]. • SSC mode 1 preserves the UPF as IP anchor for the PDU session and the IP address of the PDU session doesn’t change if the UE changes radio anchor point. • With SSC mode 2, the network may break the connectivity and release PDU session before making a new one on a different UPF. In this case, the UE's IP address may be released and a new anchor UPF can be chosen for the new PDU session. • With SSC mode 3, the network ensures that UE does not lose connectivity by making a new connection before breaking the existing one, to allow service continuity. In this mode UE, IP address is not preserved as PDU session anchor changes.

User Plane Function (UPF)	The UPFs provide user plane functions, its main functionalities are: • PDU session point of interconnection to the Data network • packet routing & forwarding • packet inspection and UP part of Policy rule enforcement • uplink classifier to support routing traffic flows to a data network • branching point to support multi-homed PDU sessions in case of multiple serialized UPFs • QoS handling for UP, e.g., packet filtering, gating, UL/DL rate enforcement, transport level packet marking • Lawful intercept • Traffic Usage Reporting
Policy Control Function (PCF)	The PCF supports a unified policy framework to govern network behavior and provides policy rules to CP function(s) to enforce them. It utilizes subscription information relevant for policy decisions stored in a UDR. The detailed functionalities are described in TS 23.503 [30]. The specification for supporting W-5GAN are described in this document and in TS 23.316 [25].
User Data Management (UDM)	The UDM provides management of user data information including: • Subscription management • Support of de-concealment of privacy-protected subscription identifier (SUCI) • User Identification Handling (e.g., storage and management of SUPI for each subscriber in the 5G system) The UDM uses subscription information which may be stored in a User Data Repository.
5G-Global Unique Temporary Identifier (5G-GUTI)	The 5G-GUTI provides an unambiguous but temporary identification of the UE that does not reveal the UE or the user's permanent identity in the 5G System (5GS). The 5G-S-TMSI is a shortened form of the 5G-GUTI that only contains the identifier of the AMF within a region of a PLMN (<AMF Set ID><AMF Pointer>) and the temporary identifier of the UE <5G-TMSI>.
Globally Unique AMF Identifier (GUAMI)	The GUAMI uniquely identifies an AMF. It is defined in TS 23.501 [28] and the format of the GUAMI is defined in TS 23.003 [26].

2.4 Abbreviations

This Technical Report uses the following abbreviations:

5WE	5G Wireless Wireline Convergence User Plane Encapsulation
5GC	5G Core Network
5G-BRG	Broadband 5G-RG (3GPP terminology)
5G-RG	5G Residential gateway
5QI	5G QoS Identifier
AAA	Authentication, Authorization and Accounting
ACS	Auto-Configuration Server (TR-069 and TR-369)
AGF	Access Gateway Function
AMBR	Aggregate Maximum Bir Rate
AMF	Access and Mobility Management Function
AN	Access Network
API	Application Programming Interface
AS	Access Stratum
ATSSS	Access Traffic Steering, Switching and Splitting

AUSF	Authentication Server Function
BBF	Broadband Forum
BNG	Broadband Network Gateway
BPS	Bytes Per Second
CPE	Customer Premises Equipment
DAD	Duplicate Address Detection
DC	Data Center
DL	Data Link
DHCP	Dynamic Host Configuration Protocol
DN	Data Network
DNN	Domain Name News
EAP	Extensible Authentication Protocol
ES	End System
FFS	For Future Study
FMC	Fixed Mobile Convergence
FN-BRG	Broadband FN-RG (terminology from 3GPP)
FN-RG	Fixed Network Residential Gateway
FSM	Finite State Machine
GBR	Guaranteed Bit Rate
GLI	Global Line Identifier
GTP-U	GPRS Tunneling Protocol User Plane
GW	Gateway
IMSI	International Mobile Subscriber Identity
LCP	Link Control Protocol
LLA	Link Local Address
LTE	Long Term Evolution
MCC	Mobile Country Code
MFBR	Maximum Flow Bit Rate
MNC	Mobile Network Code
MS-BNG	Multi-Service BNG
NAS	Non-Access Stratum
NAT	Network Address Translation
NEF	Network Exposure Function
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
OAM	Operations, Administration and Management
OSS	Operations Support Systems
PCP	Priority Code Point
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PCO	Protocol Configuration Options
PID	Protocol Identifier
PIR	Peak Information Rate
PLMN	Public Land Mobile Network
PON	Passive Optical Networking
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
QFI	QoS Flow Identifier
RAN	Radio Access Network
RG	Residential Gateway
RG-LWAC	RG-Level Wireline Access Characteristics
RQI	Reflective QoS Indicator
RS	Router Solicitation
SDN	Software-Defined Networking
SMF	Session Management Function
SM	Session Management

SSC	Session and Service Continuity
STB	Set Top Box
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TCI	Tag Control Information
UE	User Equipment
UDM	Unified Data Management
UDR	User Data Repository
UE	User Equipment
ULI	User Location Information
UPF	User Plane Function
URSP	UE Route Selection Policy
USP	User Services Platform
VSNCP	Vendor Specific Network Control Protocol
VSNP	Vendor Specific Network Protocol
VSO	Vendor-Specific Option
W-5GAN	Wireline 5G Access Network
W-AGF	Wireline AGF (terminology used by 3GPP for an AGF)

3 WWC architecture with AGF

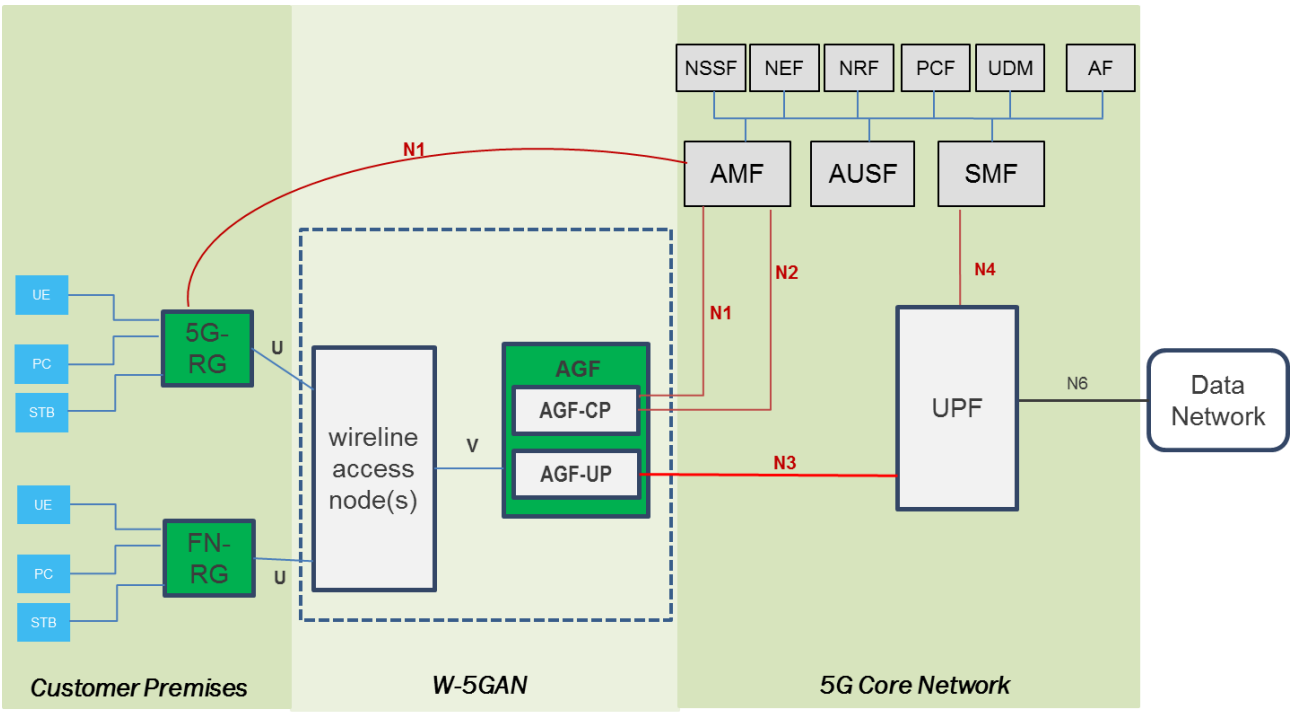

Figure 1: Architectural view of AGF connecting RGs to the 5GC through wireline only access networks.

Figure 1 illustrates an FN-RG and a 5G-RG connected to the 5GC through the Access Gateway Function, AGF. W-5GAN comprises of wireline access nodes and an adaption function for 5G convergence, i.e., the AGF. The AGF may be split into control plane, AGF-CP, and user plane, AGF-UP. The control plane and user plane separation (CUPS) of the AGF is out of scope of this document and is specified in TR-458 [10].

The converged 5G core network is used to deliver functions traditionally offered by the wireline core network as well as potential new 5G services.

The interfaces of the AGF towards the core are N1 (for FN-RG) and N2 for the control plane and N3 for the user plane. They form the border between access and core. These are defined in 3GPP documents referenced in [11], [16], [20] and [21].

In this Figure 1, the 5G-RG is connected via wireline access only to the 5GC. However, it is possible that a 5G-RG could use a NG-RAN as well to connect to the 5GC.

The user devices (i.e., UE, PC, and STB) access to the 5G Core Network through the 5G-RG or the FN-RG and W-5GAN.

N1 is supported by 5G-RGs and carried over the W-5GAN. To support an FN-RG, the AGF emulates the N1 interface. The AGF generates and exchanges the Non-Access Stratum (NAS) signaling to the AMF on behalf of the FN-RG.

The interface of the AGF towards the wireline access node is the V reference point as defined in TR-178 Issue 2 [5].

Note: The FN-RG is always identified by a Line ID/GLI based SUPI and 5G-RG is always identified by an IMSI based SUPI.

4 High-level requirements of an AGF

The AGF supports the following high-level requirements:

[R-FN-1] The AGF MUST support the N1 interface as defined in [11] and [25].

[R-1] The AGF MUST support the N2 interface as defined in [16], [20] and [25].

[R-2] The AGF MUST support the N3 interface as defined in [24] and [25].

[R-3] The AGF MUST support all W-AGF (3GPP terminology for AGF) functionalities described in TS 23.316 [25] that are not specific to a particular RG type.

[R-FN-2] The AGF MUST support all W-AGF (3GPP terminology for AGF) functionalities described in TS 23.316 [25] that are specific to the FN-RG and FN-BRG (3GPP terminology explicitly identifying a Broadband FN-RG).

[R-5G-1] The AGF MUST support all W-AGF (3GPP terminology for AGF) functionalities described in TS 23.316 [25] that are specific to the 5G-RG and 5G-BRG (3GPP terminology explicitly identifying a Broadband 5G-RG).

[R-4] The AGF MUST support all functionalities described in TS 23.316 [25] for the W-AGF (3GPP terminology for AGF).

[R-5] The AGF MUST support the V interface as defined in TS 23.316 [5].

[R-6] The AGF MUST be able to identify the Line ID as defined in TR-101 Issue2 [3] and TR-177 Corrigendum 1 [4] as signaled by the access network in order to provide location information to the 5GC.

[R-7] The AGF MUST be able to be configured to associate a Line ID source with a subscriber-facing interface. This may be at the granularity of interface/S-tag, interface or platform.

[R-FN-3] The AGF MUST support Layer 2 Tunneling Protocol (L2TP) from access node concentrator(s) as defined in RFC 2661 [44].

[R-8] The AGF MUST separately administer PPPoE and 5WE session IDs as distinct identifier spaces.

[R-9] The AGF MUST support RFC 4638 [50] procedures for negotiating PPP MTU.

[R-10] The AGF MUST be able to be administratively configured as to the maximum MTU to use in the access.

[R-11] The AGF MUST echo the received PPP-Max-Payload tag during PPPoE exchange if has been configured to support a PPP MTU greater than 1492 octets.

[R-12] The AGF MUST negotiate the PPP MTU for the access link as the MIN of that the AGF configured value and that the RG indicated it supported in the PPP-Max-Payload parameter.

[R-13] The AGF MUST set the 5WE MTU for the subscriber to that negotiated for the PPP MTU.

The following requirements are imported by reference from TR-101 Issue2[3] with BNG replaced with AGF:

[R-FN-4] The AGF MUST support R-190 and R-195.

[R-14] The AGF MUST support R-191 through R-194.

[R-15] The AGF MUST support R-196 to R-212.

Note: Security Functions and DHCP relay are FFS.

The following requirements are imported by reference from TR-177 Corrigendum 1 [4] with BNG replaced by AGF:

[R-16] The AGF MUST support R-37.

The following requirements are imported by reference from TR-187 Issue 2 [8] with BNG replaced by AGF:

[R-FN-5] The AGF MUST support R-46, R-47, R-49, R-51 to R-53, R-57, R-58.

Note: R-56 from TR-187 Issue 2 [8] with the RFC 8200 [40] link model is FFS.

5 NAS and AS Transport and Information Elements

5.1 Theory of operation

There are three classes of control information that are transported between a 5G-RG and an AGF. These are Authentication (AN), Non-Access Stratum (NAS) and Access Stratum (AS).

NAS information is the access independent signaling information exchanged between a 5G-RG and the 5G core NAS information is ciphered, opaque to the AGF, and it has its own reliability mechanisms. The majority of VSNP messages are expected to not require fragmentation, the exception being the communication of a SUCI due to the nature of the concealment algorithms.

AS information is access specific information communicated from the AGF to the 5G-RG. AS information is not ciphered. There are two classes of AS information communicated to the 5G-RG: subscription information and session information. Subscription information is communicated as part of the 5G-RG registration process and session information is communicated as either part of the PDU session establishment process, at the reactivation of PDU sessions as a result of a service request or as a result of policy control decisions in 5GC.

PPPoE version 1 (RFC 2516 [42]) is used as the underlying transport, carrying PPP (RFC 1661 [43]) and augmented with the BBF defined use of the vendor specific network protocol (VSNP, RFC 3772 [46]) for NAS and AS encapsulation. PPPoE v1 provides the following capabilities that are utilized in this application.

1. PPPoE PADI can be used to solicit connectivity from any class of service edge (BNG and or AGF) or may be used to explicitly solicit connectivity from an AGF via the use of the 5G service-name tag.

2. LCP is extended with a BBF specified vendor specific information element (VSO) to identify that the purpose of the session is 5G authentication, NAS and AS transport. Rejection of an LCP configuration request that contains the information element indicates that the peer does not support 5G-RG procedures.

3. LCP provides a signaling channel liveliness check in the form of LCP-ECHO. This is required as in most deployments an AGF will not be directly connected to a 5G-RG and will not have direct visibility of all link outages.

4. The BBF VSNP as the NCP as defined below provides a means of communicating authentication, NAS and AS messages between a 5G-RG and an AGF. The BBF VSNP is initiated by VSNCP procedures [46].

When combined with either 5WE session delineation in the UP, this results in an overall protocol suite as follows between a 5G-RG and an AGF:

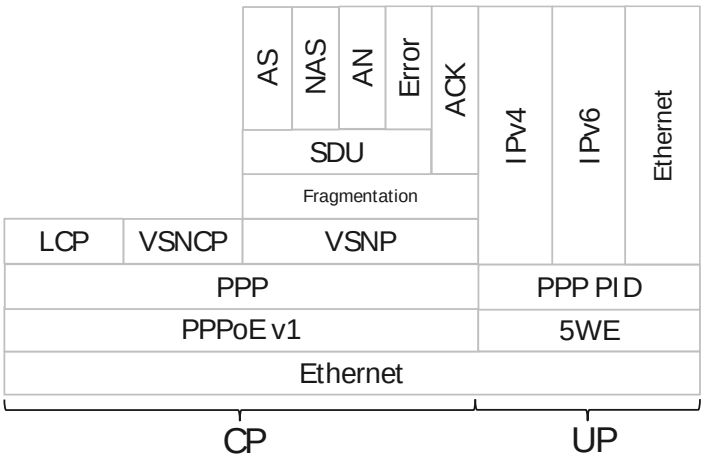

Figure 2: Protocol stacks between a 5G-RG and an AGF

Note that in this design, VSNP is the only NCP opened in the PPPoE v1 session and may only serve one NAS termination.

The encoding of all aspects of AN, NAS and AS communication uses network byte order.

Initiation of CP communication between a 5G-RG and an AGF has each layer brought up in the following sequence with the procedures specific to NAS and AS exchange outlined in the referenced standards and where appropriate augmented by the subsequent sections.

1. PPPoE procedures as documented in RFC 2516 [42] to establish a PPPoE session, and optionally explicitly require connectivity with an AGF.

2. PPP LCP procedures documented in RFC 1661 [43] augmented with:

    a. The 5G VSO (RFC 2153 [39]) to open the link and to permit 5G procedure support to be negotiated.

    b. The exclusion of the request to use an authentication protocol, corresponding to the default specified in Section 3.5 of RFC 1661 [43].

3. VSNCP procedures to open a VSNP channel as documented in RFC 3772 [46].

The BBF defined VSNP incorporates a fragmentation layer that offers a single datagram interface to the AN, NAS and AS layer above it. A datagram containing NAS. AS and or AN information and potentially an error indication is presented to the fragmentation layer for transmission is termed a VSNP message.

The fragmentation scheme fragments VSNP messages into zero or more middle fragments and an end fragment. An end fragment contains metadata about the VSNP message that permits the successful reassembly of the individual fragments back into the VSNP message to be verified by the receiver. The metadata includes:

1. A CRC-32 of the VSNP message that is used to validate that all fragments are present and received in the correct order.

2. A VSNP message length that permits the concatenation of SDUs (via the loss of an end fragment) to be detected and compensated for.

A VSNP message can be one of two types: SDU, or ACK.

VSNP exchange is bi-directional. NAS implements reliable transmission between the UE and the AMF and uses an additional reliability mechanism over the VNSP leg of the path from 5G-RG to AMF. This is a simple timeout and ACK approach.

A VSNP SDU message has a fixed header which identifies the message components. The components can be a NAS, AS or AN message and may include an error indication, Current use cases support an SDU containing a single class of message (NAS, AS, or AN) or the combinations NAS+AN and NAS+AS with the VSNP message containing one message from each identified class. When the error indication is set, only one other class of message is included in the SDU which is an echo of the message the error indication applies to.

Current use cases only have identified AS errors. The error indication is provided as a means of identifying AS messages that are not well formed and should not be needed in mature implementations.

AS messages are TLV encoded. AS TLVs are then broken down into sub-TLVs to distinguish subscription or session information. The design permits additional TLVs to be defined in the future.

An ACK message is a simple acknowledgement of the last SDU message received.

5.2 PPPoE procedures

The PPPoE transaction is a vehicle an RG uses to discover the AGF(s) and/or BNG(s) reachable within a L2 broadcast domain and to select one of them to start a PPP session. The first PPPoE message (PADI) allows the RG to also indicate whether it requests a particular service or any service. This is achieved via the “service-name tag” in the PADI packet, as documented in RFC 2516 [42].

With regards to WWC, the PADI packet sent by the RG over a broadcast domain, and the subsequent service offers (PADO) sent back by the network, can be considered implicit signaling for RG to select the most appropriate AGF or BNG as well as to settle the mode of operation of the RG. The final settlement of 5G-RG mode of operation is postponed to a real negotiation that takes place after the PPPoE transaction, in the PPP LCP phase, as documented in section “LCP procedures”.

How PPPoE transaction can be triggered depends on the RG. For completeness, hereafter both FN-RG and 5G-RG are considered.

- AN FN-RG typically sends a PADI with NULL length service-name tag to trigger the PPPoE transaction. It might also use other service-name tag, for example “DSL” to access the service provided by specific ISPs, but it is assumed to never use the special tag “5G”.

- A 5G-RG can trigger the PPPoE transaction in one of the two following ways:

    - Option a: Sending a PADI with NULL length service-name tag: this is used to solicit “any” AGF or BNG.

    - Option b: Sending a PADI with “5G” service-name tag: this is used to solicit a 5G AGF that offers access to the 5G system, providing NAS signaling exchange for control plane, and other capabilities.

‘Option a’ should be the default method a 5G-RG uses to start PPPoE and is better suited for AGF-only (AGF in Adaptive mode only, AGF in both direct and adaptive mode) or BNG-only deployments. Note that in a broadcast domain where both BNG and AGF in adaptive mode are deployed, ‘option a’ might bring uncertainty on the connection time experienced by the customers, because both AGF(s) and/or BNG(s) are able to reply to that PADI.

'Option b' is recommended if the 5G-RG sends the PADI in a broadcast domain where both BNG and AGF in direct mode are deployed. In order to do this, the 5G-RG must be explicitly configured to use the 5G service tag in PADI solicitations. In this case, according to RFC 2516 [42], a BNG is expected to silently discard the PADI, while an AGF will reply with a PADO echoing the service-name tag value; therefore the AGF will be selected by the 5G-RG as serving platform without impact on the connection time experienced by the customers.

The encoding of the 5G service-name tag is as per section 5 and appendix A of RFC 2516 [42]:

- Tag type (16-bit): 0x101 (service-name tag)
- Tag length (16-bit): 0x02
- Tag value: '5G' (encoded as ASCII, 0x35, 0x47)

In order to describe how the service selection is carried out by FN-RG and 5G-RG, and how 5G-RG identifies its mode of operation, it is necessary to distinguish among the possible behaviors of the AGF(s) and/or BNG(s) receiving the PADI. These behaviors depend on the network device capabilities and/or on their configuration as shown in Table 1. The following behaviors can be distinguished:

- AGF direct mode only
- AGF adaptive mode only
- AGF both modes
- BNG

Note that when AGF is configured to support both adaptive and direct modes, it will decide which mode is required to serve the RG only after the PPP LCP negotiation. No decision is taken at the end of the PPPoE transaction.

Note that a BNG would be expected to provide the same behavior as an AGF that is restricted to adaptive mode only.

RG type	Message sent by RG	AGF and BNG Behaviors			
		AGF direct mode only	**AGF adaptive mode only**	**AGF both modes**	**BNG (expected reaction)**
FN-RG	PADI with NULL length service-name tag	Silently Discard	Reply with a PADO with no tag	Reply with a PADO with no tag	Reply with a PADO with no tag
5G-RG	PADI with 5G service-name tag	Reply with a PADO with 5G service-name tag	Silently Discard	Reply with a PADO with 5G service-name tag	Silently Discard
	PADI with NULL length service-name tag	Silently Discard	Reply with a PADO with no tag	Reply with a PADO with no tag	Reply with a PADO with no tag

Table 1: Different AGF and BNG behaviors when replying to PADI.

5.3 LCP procedures

A 5G-RG requests the establishment of 5G control plane connectivity via the inclusion of the BBF defined 5G-RG VSO in the LCP configure-request message. The encoding of the VSO is as per RFC 2153 [39]:

- Type = 0
- Length = 6 (no values fields are present)

- OUI = BBF IEEE administered OUI 0x00256D
- Kind = 5 (5G-RG)

An AGF operating in direct mode responds to the Configure-Request containing 5G-RG VSO with a Configure-Ack, while a BNG or AGF operating in adaptive mode only that does not support 5-RGs responds with a Configure-Reject. A 5G-RG that receives an LCP Configure-Ack proceeds with the PPP VSNCP to enable the PPP VSNP, that transport the NAS messages for the 5G-RG registration. A 5G-RG that receives a Configure-Reject may revert to FN-RG mode of operation. If reverting to PPPoE operation, the 5G-RG continues the LCP phase negotiating a non-5G PPP session by removing the 5G VSO from the LCP Configure Request and the PPPoE service tag. If reverting to IpoE operation, the 5G-RG will issue a PADT to clean up the unused PPPoE session attempt.

Note that an AGF operating in direct mode only responds to the Configure-Request not containing 5G-RG VSO with a Configure-Ack, gracefully completing LCP negotiation before terminating the link via an LCP Terminate-Request.

Table 2 describes how the AGF and/or BNG replies based on both its capabilities and configurations and on the service requested by the RGs.

RG type	Message sent by RG	AGF and BNG Behaviors			
		AGF direct mode only	**AGF adaptive mode only**	**AGF both modes**	**BNG (expected reaction)**
FN-RG	LCP Configure-Request with no VSO	Reply with a Configure-ACK followed by a Terminate-Request	Reply with a Configure-ACK	Reply with a Configure-ACK and operate in adaptive mode	Reply with a Configure-ACK
5G-RG	LCP Configure-Request with 5G-RG VSO	Reply with a Configure-ACK	Reply with a Configure-Reject	Reply with a Configure-ACK and operate in direct mode	Reply with a Configure-Reject
	LCP Configure-Request with no VSO	Reply with a Configure-ACK followed by a Terminate-Request	Reply with a Configure-ACK	Reply with a Configure-ACK and operate in adaptive mode	Reply with a Configure-ACK

Table 2: Different AGF and BNG behaviors when replying to LCP Configure-Request.

The AGF or the 5G-RG may terminate CP communication between the 5G-RG and the AGF via closing the LCP NAS and AS channel. Upon completion of these steps the AGF or 5G-RG will issue a PPPoE PADT.

5.4 Void

This section is intentionally blank.

5.5 VNSCP & VSNP Procedures

The registration procedure with the 5G network takes places before the 5G-RG has any connectivity established. This requires that the NAS registration request message is carried from 5G-RG to AGF and forwarded to 5GC.

NAS and AS are communicated over the Vendor Specific Network Protocol (VSNP) which is part of the PPP protocol suite [46]. The VSNP channel is opened using VSNCP procedures. VSNCP permits the particular

protocol encapsulated in VSNP to be negotiated using the PPP negotiation state machine documented in RFC 1661 [43]. VSNP itself has no state machine and is simply an encapsulation. It is entirely dependent on the vendor defined extensions for all aspects of information transfer.

There are no options in the BBF specified VSNP application so the 5G-RG Configure Request that starts the negotiation simply encodes the BBF OUI to identify the protocol used with no additional data. The IEEE administered BBF OUI is 0x00256D (this has also been registered with IANA). Once VSNCP negotiation has successfully completed, NAS and AS can be communicated over VSNP using the procedures documented in this section.

5.6 VSNP Fragmentation Sub-Layer

5.6.1 Fragmentation sub-layer encoding

The Fragmentation sub-layer is encoded as a TLV. The type field is a 16-bit integer and identifies the message type. The length is a 16-bit unsigned integer that provides the octet count of the following fragment.

There are 2 message types used by the Fragmentation sub-layer:

Type = 0: Middle fragment

Encoding:

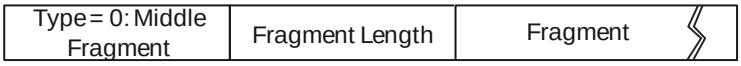

Figure 3 – VSNP fragmentation sub-layer middle fragment encoding

- Type: A 16-bit unsigned integer, explicitly set to 0.
- Fragment length: A 16-bit unsigned integer
- Fragment: ‘Fragment Length’ octets of message data

Type = 1: End fragment

Encoding:

Figure 4 – VSNP fragmentation sub-layer end fragment encoding

- Type: A 16-bit unsigned integer, explicitly set to 1.
- Fragment length: A 16-bit unsigned integer
- CRC: An unsigned 32-bit value computed as specified in section 9.2.1.2 of ITU-T recommendation I.363.1 [60].
- SDU length: A 16-bit unsigned integer
- Fragment: ‘Fragment Length’ octets of message data

5.6.2 Reassembly Buffer:

The receiver will implement a reassembly buffer or similar construct to handle reassembly of fragmented messages. The reassembly buffer can be dimensioned in an implementation as the maximum SDU length. The recommended value is 8188 octets as this corresponds to the maximum MTU of the 3GPP RRC layer.

5.6.3 Sender FSM:

The sender finite state machine (FSM) is as follows:

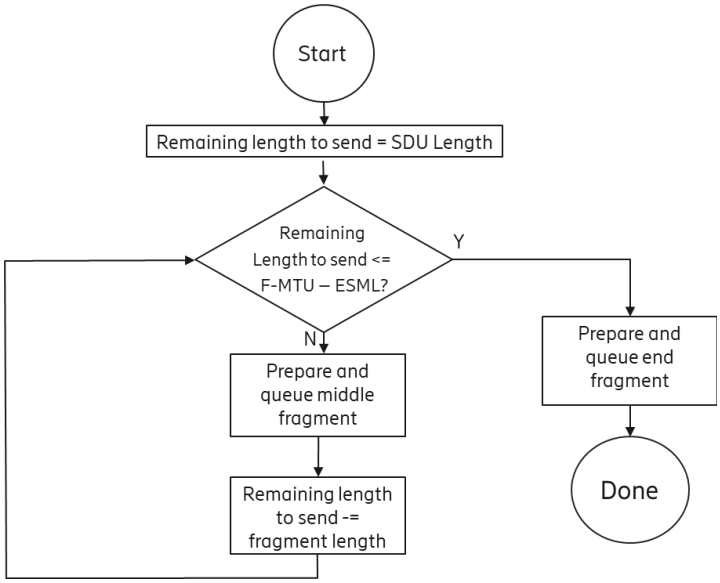

Figure 5 – Sender FSM

The sender partitions the SDU into one or more fragments and queues them for transmission.

The following variables are used:

SDU length: the length of an unfragmented message.

Remaining length to send: the length remaining net of any fragments already queued for transmission.

F-MTU: is the fragment MTU. For PPPoE with a 1500 bytes Ethernet frame the starting point to determine the MTU is typically 1492 octets. Due to the TLV structure of the fragmentation layer, this reduces the F-MTU value to 1488 octets. Note that this may be extended via procedures documented in RFC 4638 [50].

ESML: End segment metadata length is the length in octets of the end segment meta data (CRC, and SDU length). This is explicitly 6 octets.

5.6.4 Receiver FSM:

The receiver finite state machine is as follows:

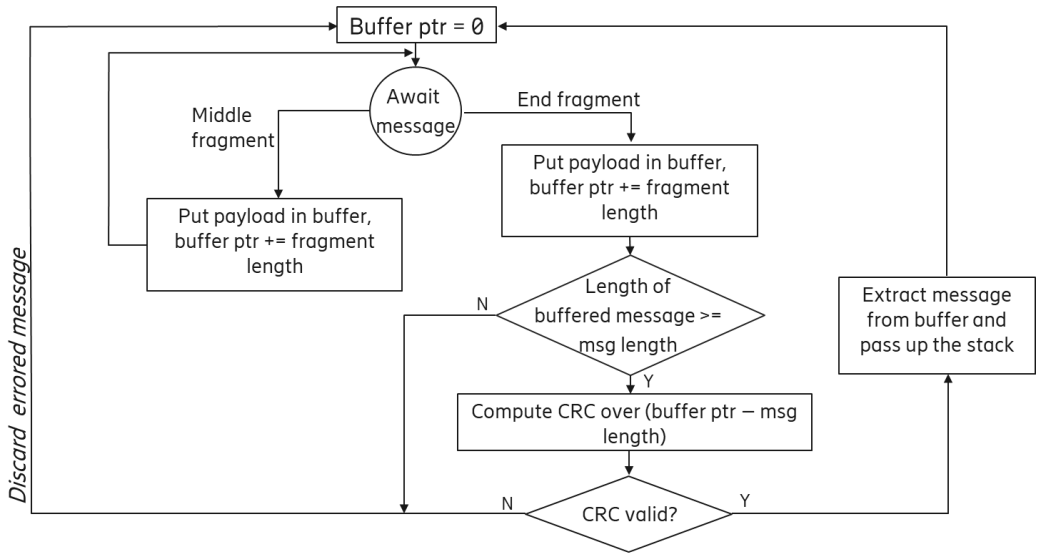

Figure 6 – Receiver FSM

The receiver copies message fragments into the reassembly buffer until an end-segment is received. The receiver uses the SDU length encoded in the end segment metadata to determine the start of the message in the reassembly buffer and if at least the number of octets in the SDU length has actually been received. If the received message is too short, the received data discarded. If sufficient data is present, it computes the CRC for the message and checks this against the CRC encoded in the end segment metadata. If the CRC is correct, then the message is passed to the higher layers for processing, else the message is discarded.

The following variables are used:

Buffer_ptr: current position of the next octet to be received in the reassembly buffer.

5.7 AN, NAS and AS message encoding

The AN, NAS and AS information is encoded and transmitted over the VSNP. A VSNP SDU message will typically contain only AN-Parameters or one NAS PDU or one AS message. However, under some circumstances (e.g., piggy backing of a NAS IE with an AS PDU session parameters TLV) a SDU may contain more than one message class.

The SDU is transported between the 5G-RG and the AGF with additional reliability in the form of a simple ACK or timeout and retry discipline; this is designed to overcome the long timeouts that are an artefact of the specification of NAS timers.

5.7.1 VSNP Message Format.

Octet 1 always indicates the message type. The following are the valid message types:

- SDU: Message Type = 1
- ACK: Message Type = 2

5.7.2 SDU Message Format.

The AS Parameters, AN Parameters and the NAS PDU are coded in SDU Message as specified in

Figure 7.

Bits 7	6	5	4	3	2	1	0	Octets
Message Type (SDU = 1)								1
0 Spare	0 Spare	0 Spare	ERR	ASPI	ANPI	NPI	NMTI	2
NAS-PDU Message Type								3
NAS-PDU length								4-5
NAS-PDU								6-a
AN-parameters length								(a+1)-(a+2)
AN-parameters								(a+3)-b
AS-parameters length								(b+1)-(b+2)
AS-parameters								(b+3)-c
Error String Length								(c+1)-(c+2)
Error String								(c+3)-d

Figure 7: SDU Message Format on VSNP

Octet 1: Value set to 1 (SDU)

Octet 2 bit 0: NAS PDU Message Type included field (NMTI).

0 NAS PDU Message Type is not present.

1 NAS PDU Message Type is present.

If the NMTI is set to 1 then:

- NAS-PDU Message Type: Indicates 5G MM/SM message carried in VSNP and is coded as specified in Section 9.7 of 3GPP TS 24.501 [11].

Octet 2 bit 1: NAS PDU included field (NPI).

0 NAS PDU and NAS-PDU length are not present.

1 NAS PDU and NAS-PDU length are present. If the NPI bit is set to 1 then:

- NAS-PDU length: Indicates the length of NAS-PDU field in octets.
- NAS-PDU: Contains a NAS message from the UE as specified in 3GPP TS 24.501 [11].

Octet 2 bit 2: AN Parameters included field (ANPI).

0 AN Parameters and AN-parameters length are not present.
1 AN Parameters and AN-parameters length are present.
If the ANPI bit is set to 1; then:

- AN-parameters length: Indicates the length of the AN-parameters field in octets
- AN-parameters field: Is coded according to figures 9.3.2.2.2-2 and 9.3.2.2.2-3 and tables 9.3.2.2.2-2 and 9.3.2.2.2-3 of 3GPP TS 24.502 [12].

Octet 2 bit 3: AS Parameters included field (ASPI).

0 AS-parameters and AS-parameters length are not present.
1 AS-parameters and AS-parameters length are present.
If the ASPI bit is set to 1; then:

- AS-parameters length: Indicates the length of the AS-parameters field in octets

- AS-parameters field: Is coded as described below.

The AS-parameters use a type-length-value (TLV) encoding. The type field is 16-bits. The length field is a 16-bit unsigned integer and specifies the length of the value field in octets.
The TLV structure of a AS-Parameters is as follows:

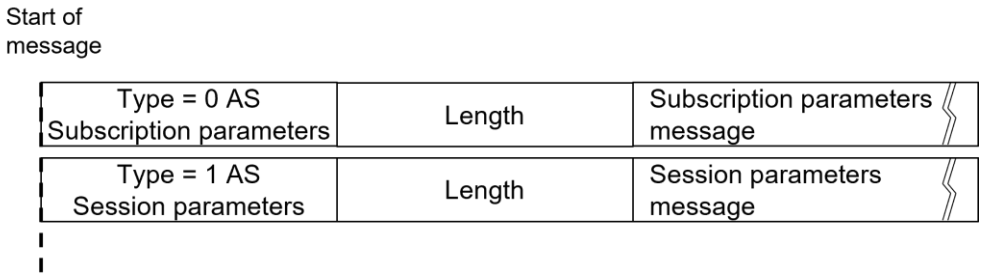

Figure 8 – AS Parameters TLV structure

Octet 2: bit 4 is the Error included field (ERR).

An error may be sent in response to a poorly formed AS message and may be sent in conjunction with echoing the AS message in question. It is only used in communication from a 5G-RG to the AGF.
0 Error String Length & Error String are not present.
1 Error String Length & Error String are present.
If the ERR bit is set to 1; then

- Error String Length: Error String length indicates the length of the Error String in octets
- Error String: Error String describes the error in an ascii coded string format.

Note: The Error could be reported along with echoing the AN Parameter(s) or AS Parameter(s) which triggered the error.

5.7.3 AS Parameters TLVs:

In messages from the AGF to the 5G-RG the valid AS TLVs are the subscription parameters TLV and the session parameters TLV.

All information exchanged via AS messages is idempotent.

AS Subscription Parameters TLV:

The subscription parameters TLV contains information communicated from the AGF to the 5G-RG at registration time. The subscription parameters TLV is encoded as follows:

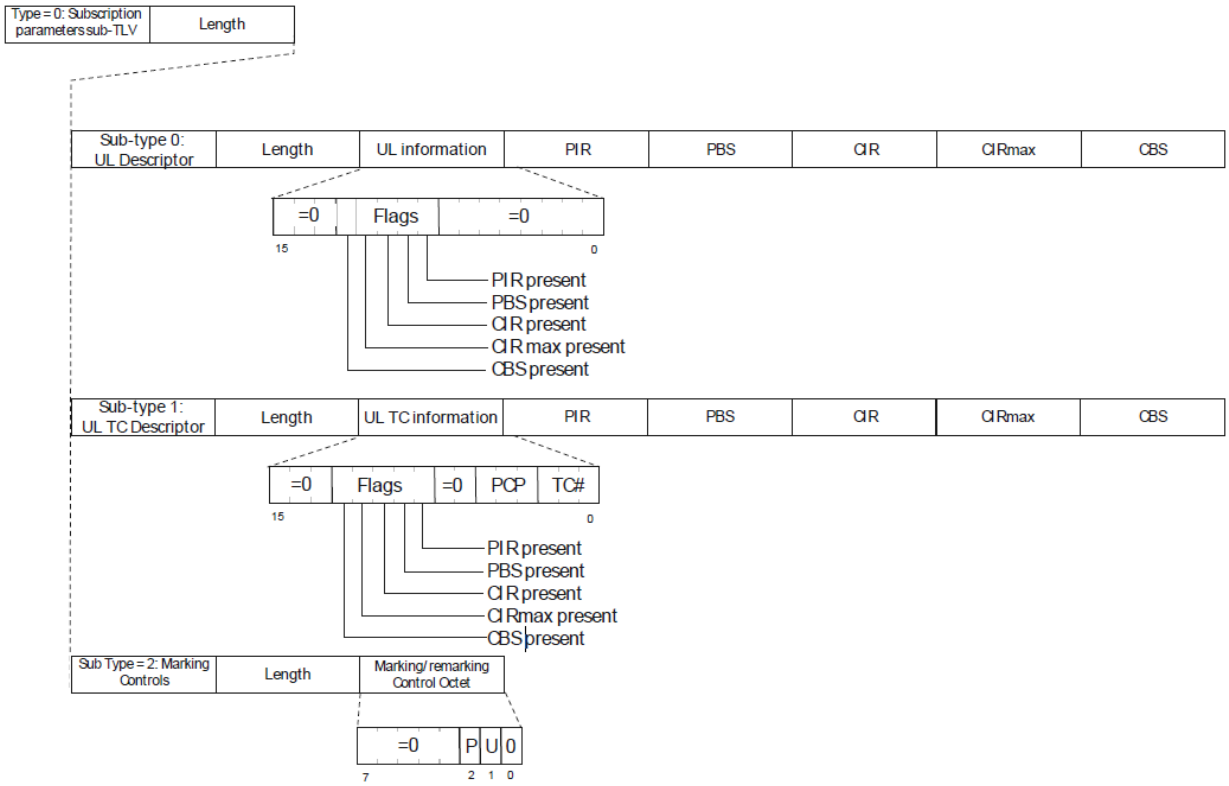

Figure 9 - AS subscription Parameters TLV encoding

The TLV is composed of three sub-TLVs, a single UL descriptor TLV and up to 8 UL traffic class descriptors and a marking control TLV. The first two are variable length depending on what fields are required to describe either the overall upstream characteristics, or the individual traffic class.

The traffic fields are:

PIR	peak information rate
PBS	peak burst size
CIR	committed information rate
CIRmax	maximum committed information rate
CBS	committed burst size

Sub-type is a 16-bit unsigned integer.

Length fields indicate the number of octets of the data portion of a (sub)TLV.

Sub-type = 0: The UL descriptor provides an overall description of the uplink traffic contract to which the resource envelope the sum of the traffic classes has to fit into.

- Length: A 16-bit unsigned integer
- UL information: A 16-bit unsigned integer
    - The flags in the UL information indicate what trailing fields are present
- PIR and CIR: 64-bit unsigned values expressed as bits per second
- CBS and PBS: 32-bit unsigned value expressed as the maximum burst size in bytes

Sub-type = 1: The UL TC descriptor provides a description of the uplink traffic class as well as the traffic class number as an identifier and the PCP marking to map the TC to queue, and permit QFI to TC mapping to be performed by a combination of the subscription and session parameters.

- Length: A 16-bit unsigned integer
- The UL TC information: A 16-bit unsigned integer
  - The flags in the UL information indicate what trailing fields are present
  - TC: TC number ranges 0-7
  - PCP: PCP marking ranges 0-7
- PIR and CIR: 64-bit unsigned values expressed as bits per second
- CBS and PBS: 32-bit unsigned value expressed as the maximum burst size in bytes

Sub-type = 2: The marking controls TLV indicates if PCP and/or DSCP marking of upstream traffic according to the QFI mapping information received in the session parameters TLV is performed. It encodes two bits:

- Length: A 16-bit unsigned integer
- 'P' bit: Indicates if priority tagging should be used to encode PCP as indicated in the session parameters TLV in the absence of a VLAN tag on the UNI:
  - 0 priority tagging MUST NOT be used
  - 1 priority tagging MUST be used
- 'U' bit: Indicates if remarking of IP DSCP is performed as indicated in the session parameters TLV.
  - 0 DSCP remarking MUST NOT be performed.
  - 1 DSCP remarking MUST be performed.

AS Session Parameters TLV:

The session parameters TLV communicates access layer specific information from the AGF to the 5G-RG at the time of PDU session initiation, or when a service request is being fulfilled. A session parameters TLV can contain one or more session records. A session record contains session binding information and one or more QFI mapping records.

The encoding of the session parameters TLV is as follows:

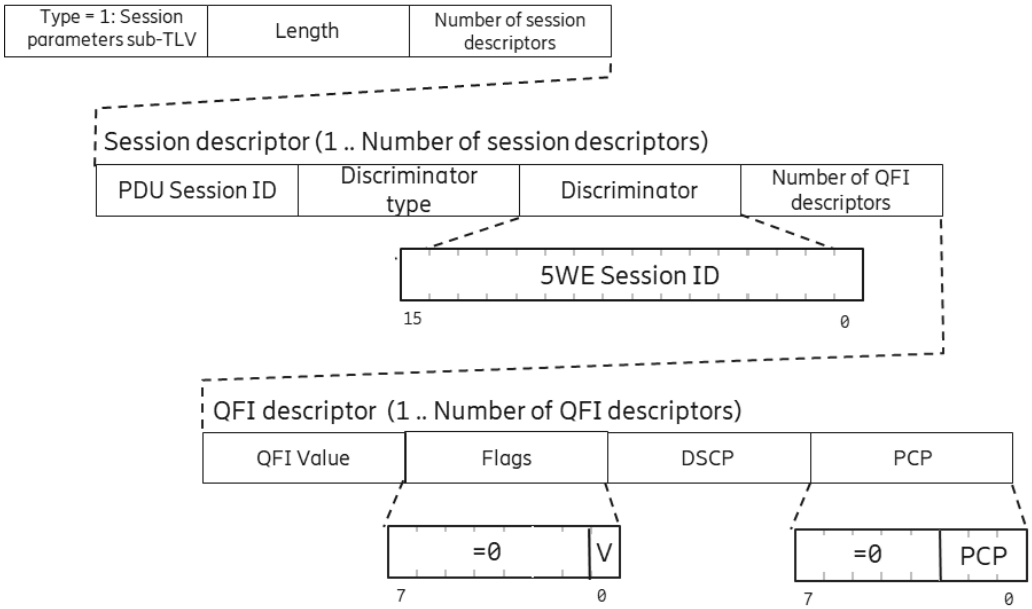

Figure 10 - AS Session Parameters TLV

- Number of session descriptors: A 16-bit unsigned value.

A session descriptor is a variable length record which encodes the following:

- PDU Session ID: An 8-bit unsigned integer

User plane session binding information:

- Discriminator type: An 8-bit unsigned value. Currently defined values are:

  0 5WE session ID as session discriminator

- Discriminator: A 16-bit integer, where the actual encoding depends on the Discriminator type as follows:

  '5WE session ID' discriminator type: The 5WE session ID is used with the VLAN ID assigned to NAS, AS and 5WE delineated PDU sessions. The VLAN ID is locally configured at both the 5G-RG and the AGF.

- Number of QFI descriptors: An 8-bit unsigned value that indicates the number of QFI descriptors that follow the session binding information. These are the valid QFI values for the PDU session and their corresponding incarnations at the IP and Ethernet layers. The first QFI descriptor is the default QFI for the PDU session.

A QFI descriptor is fixed length of 4 octets encodes as follows:

- QFI value: An 8-bit unsigned integer
- Flags: 8-bits where the upper 7-bits reserved and must be set to zero. The least significant bit ('V') indicates the validity of the following DSCP and PCP fields as follows:

  0 The DSCP and PCP information is not valid, and local configuration should be used. The DSCP and PCP fields must be set to zero.

  1 The following DSCP and PCP information should be used for layer 2 and layer 3 marking corresponding to the QFI.

- DSCP: An 8-bit IP DSCP value that corresponds to QFI value and is used for layer 3 marking.
- PCP: An 8-bit unsigned integer. The lower 3-bits encode the corresponding 802.1Q [32] PCP marking to use in the Ethernet frame which corresponds to the QFI value and used both for layer 2 marking and TCI for AN scheduling. The upper 5-bits MUST be set to zero.

5.7.4 ACK Message format

The ACK is coded in VSNP Message as specified in

Figure **7**.

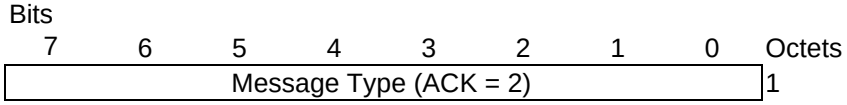

Figure 11: ACK Message format on VSNP

Octet 1: Value set to 2 (ACK)

5.8 VSNP Reliability

VSNP SDU messages that flow between the AGF and the 5G-RG and are acknowledged by the peer on successful receipt of the reassembled message once reassembly processing is complete. The acknowledgement serves to only indicate a successful message receipt.

AS messages are idempotent, therefore duplicate detection is not required. NAS and AN messages incorporate their own duplicate detection mechanisms.

VSNP Reliability FSM:

The AGF FSM for VSNP Reliability handling is as follows:

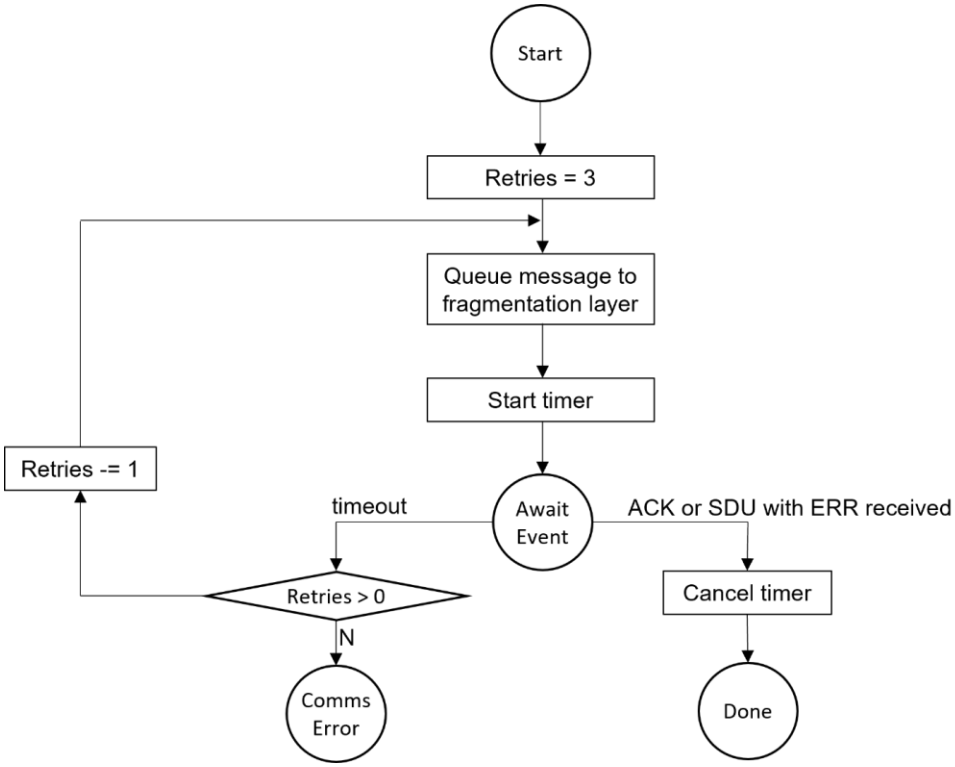

Figure 12 - VSNP reliability handling FSM

When the AGF initiates sending a VSNPSDU message it initializes a retry counter to 3 retries and starts a timer. The timer value is FFS. If the timer expires before an ACK or an SDU containing error string message is received, the retry counter is decremented, and if not zero, the message is resent.

The AGF will not initiate communication of any additional VSNP messages while the disposition of the current VSNP message is unknown.

6 Functional features and requirements

6.1 Authentication/Authorization/identity management for FN-RG support

6.1.1 Primary Authentication

In order to access to 5GC, each subscriber is allocated one 5G Subscription Permanent Identifier (SUPI) for use within the 3GPP system. The SUPI is the permanent identity that identifies the subscriber and it is used only inside the 3GPP system. The procedures for SUPI privacy are defined in TS 33.501 [27] and in TS 23.003 [26]. The SUPI, in respect to the 5G system, is never provided by UE to the network element, but it is confined to the core network and exchanged between the NF(s) in the core network. The UE in the procedure communicates its Subscription Concealed Identifier (SUCI). The exception is the case of Emergency Services, where the identification of UE, take precedence over the privacy requirements. TR-470 [9] section 7.5 (SUPI/SUCI for FN-RG) provides additional background information about SUPI and SUCI usage for FN-RG.

[R-FN-6] The AGF MUST generate the SUCI as defined in TS 23.003 [26] clause 2.2B, and encode its parts as follows: SUPI-type=2 (Global Line ID); Home Network Identifier=MCC+MNC of the AGF's PLMN (as defined in TR-470 [9] section 7.5); Routing Indicator=0; Protection Scheme ID=0 (NULL scheme); Scheme Output=Global Line ID (as defined in TR-470 [9] section 7.2).

[R-FN-7] The AGF MUST be able to use DHCPv4 option 82 inserted by the AN as specified in [3] as source information for the Global Line ID.

[R-FN-8] The AGF MUST be able to use PPPoE Circuit and Remote ID tags inserted by the AN as specified in [3] as source information for the Global Line ID.

[R-FN-9] The AGF MUST be able to use DHCPv6 option 18 via LDRA functionality in the access node as specified in [4] as source information for the Global Line ID.

[R-FN-10] The AGF MUST be able to use the Line ID Option (LIO) in RS messaging as specified in [4] as source information for the Global Line ID.

[R-FN-11] The AGF MUST be able to use the Circuit ID AVP and/or the Remote ID AVP in the ICRQ message, as specified in RFC 5515 [58] as source information for the Global Line ID.

[R-FN-12] AGF acting in Adaptive Mode MUST discard the packet and report an error to management if a GLI cannot be generated for an FN-RG.

Requirements related to 5G-RG and N1 support are specified in TR-124 Issue 6 [6].

Hereafter it is explained how the identity of an FN-RG is derived and encoded by the AGF.

SUCI Encoding for FN-RG in AGF

The procedure for encoding a SUCI for an FN-RG is described in TR-470 [9] section 7.5 'SUPI/SUCI for FN-RG' and is communicated using the NULL encryption scheme.

[R-FN-13] The AGF MUST encode the SUCI derived from Line ID for an FN-RG using null protection scheme as defined in TS 23.003 [26].

6.1.2 Additional Authentication

An AGF supporting PPPoE will be configured to require either PAP or CHAP authentication and will negotiate this during LCP procedures. An AGF in the absence of either an attached RADIUS server or the presence of additional authentication information in RG-LWAC will always treat PAP or CHAP authentication attempts as valid and reply in kind. As such an AGF may be configured to promiscuously accept PAP/CHAP authentication in lieu of having access to network support.

[R-FN-14] An AGF configured to accept PAP authentication MUST always respond to a PAP Authenticate-Request with an Authenticate-ACK upon successful registration with the 5GC.

[R-FN-15] An AGF MUST initiate a CHAP Challenge to the PPP peer. Upon receipt of the CHAP Response, an AGF configured to accept CHAP authentication MUST always respond with a CHAP Success upon successful registration with the 5GC.

Additional authentication beyond the primary authentication may be performed for an FN-RG. This may be achieved by a combined AGF/BNG using existing RADIUS infrastructure, or for a combined AGF/BNG or standalone AGF, via the dissemination of PAP/CHAP credentials information encoded in Additional Authentication Credentials Information (AACI) in the RG-LWAC data structure obtained from UDM at registration time, see section 7.6 of TR-470 [9]. The NAI in an AACI is expected to be unique for a given subscriber, such that no two AACI TLVs in a given RG-LWAC will contain a common NAI.

[R-FN-16] An AGF SHOULD support PAP/CHAP procedures using the AACI information provided in the RG-LWAC.

[R-FN-17] An AGF that supports AACI MUST treat the absence of AACI information as meaning additional authentication is not performed and MUST treat all PAP/CHAP transactions as authorized.

[R-FN-18] An AGF that supports AACI MUST reject IP session initiation when the additional authentication procedures are unsuccessful in validating the credentials presented by the FN-RG.

[R-FN-19] An AGF that supports AACI that rejects IP session initiation whereby that IP session initiation also triggered registration SHOULD de-register the FN-RG.

[R-FN-20] An AGF that is either configured to accept PAP/CHAP authentication, or has validated PAP/CHAP credentials, MUST set “Authenticated Indication” flag in N2 Initial UE Message towards AMF indicating that the FN-RG is authenticated by AGF. Please refer to clause 7.2.1.3 of TS 23.316 [25].

6.2 Security

6.2.1 N1 (NAS) Security for AGF in adaptive mode

Unlike NAS messages generated by 5G-RG, integrity protection and ciphering for NAS messages generated by the AGF on behalf of FN-RG are not required because the AGF is assumed to be in the same domain as the 5GC. Scenarios where the AGF is in a different domain to the 5GC are FFS.

[R-FN-21] The AGF MUST only use Null Integrity Protection Algorithm for NAS messages generated on behalf of an FN-RG, as defined in TS 33.501 [27].

The AGF will only encode 5G-EA0 for Ciphering Algorithm and 5G-IA0 for Identity protection of the NAS PDUs in the UE Security Capability IE (See TS 33.501 [27])

Procedure for Security mode Command for FN-RG:

Case 1: Null ciphering configured in AMF:

AMF will send the security mode command with 5G-EA0 – AGF will agree and send Security Mode Complete.

Case 2: Null ciphering not configured in AMF:

AMF can send the security mode command with 5G-EA0 – AGF will agree and send Security Mode Complete.

-OR-

AMF can send the security mode command without 5G-EA0 – AGF will send Security Mode Reject. AMF can reinitiate a security mode or stop going forward.

The same is applicable for the Identity protection algorithm.

[R-FN-22] The AGF MUST only use Null Ciphering Algorithm for NAS messages generated on behalf of an FN-RG, as defined in TS 33.501 [27].

6.2.2 N2 Security

The following section describes the encryption requirements for N2 reference point. More details can be found in TS 33.501 [27]).

It is an Operator's decision whether to implement encryption on N2. Encryption on N2 can be implemented on the AGF or can be achieved via an external security gateway.

Note: The AMF already supports negotiation of null cyphering, hence there is no new requirement on AMF to support this model.

For Wireline Access (AGF), an external security gateway (SEG) on the access side can be used to provide IPSec/DTLS based encryption support in case the Operator wants to secure the N2 endpoints.

The SEG is an external device and it is not managed by AGF or 5G Control Plane.

6.2.3 User Plane Data Security (N3)

TS 33.501 [27] Clause 9.3 provides option to use SEG to terminate the IPSec tunnel for N3 Endpoint on the core network side (UPF).

In case of Wireline Access, a SEG can be used to terminate the IPSec tunnel for N3 Endpoint on the AGF side.

6.2.4 Protection of AGF from Denial-of-service attacks

There is a need to protect AGF from multicast and broadcast packets injected at user ports.

[R-FN-23] The AGF MUST be able to rate-limit the traffic destined to its control plane (PPPoE Agent, DHCP L2 Agent, IGMP, ARP Proxy, etc.) that is received on user-ports. See section 5.4.8 of TR-178 Issue 2 [5]

[R-FN-24] The AGF MUST support R-135 to R-138 from TR-178 Issue 2 [5] with ‘AGF’ replacing ‘EAN’

[R-17] The AGF MUST be able to rate-limit the traffic from AMF (5GC) over the N2 Interface

6.2.5 Source IP Spoofing

A malicious user might try to spoof an IP address by sending ARP messages (both ARP requests and replies) indicating the binding of its MAC address to the spoofed IP address.

[R-FN-25] The AGF MUST support R-220 to R-224 from TR-101 Issue2 [3], with 'AGF' replacing 'BNG'

[R-FN-26] The AGF MUST support R-53 to R-57 from TR-177 Corrigendum 1 [4], with 'AGF' replacing 'BNG'

Editor's Note: This section needs to be updated when addressing Framed Route support as anti-spoofing might filter the packets belonging to the framed addresses. Evaluate the case where AGF and UPF are co-located.

6.3 User plane

6.3.1 User plane for 5G-RG

The user plane encoding employed for PDU exchange between an AGF and a 5G-RG will be the IP packet or Ethernet frame appropriate to the PDU session type encapsulated in the '5G WWC Encapsulation'(5WE), defined in [32], and then adapted into TR-101/178 ([3], [5]) Ethernet transport.

The user plane connection is established via the PDU session establishment procedure described in section 8.2.3. This procedure is initiated by the 5G-RG sending PDU Session Establishment request. A PDU Session ID is generated by the 5G-RG. The PDU Session ID generated by the 5G-RG is communicated to the AMF by the NAS message which is transparent to the AGF. The 5GC informs the AGF of the PDU session ID in the N2 PDU Session Resource Setup Request. Afterwards, the AGF assigns a 5WE session ID and binds it to the PDU session ID. How the AGF administers pools of 5WE session IDs (e.g., per subscriber, per interface, per platform etc.) is up to implementation. This 5WE session ID and PDU session ID binding is communicated to the 5G-RG. The 5G-RG uses this 5WE session ID going forward to identify the UP packets of the PDU session.

As shown in Figure 13, the 5WE encapsulation is used to encode the 5WE session ID, QFI/RQI and the encapsulated protocol (IPv4, IPv6 or Ethernet). Note that RQI is optional (RG may decide not to support it or 5GC may decide not to use it). The VLAN used for 5WE encapsulated session traffic is known as the 5G VLAN. The VID to use for the 5G-VLAN is preconfigured on the 5G-RG and will default to the untagged or priority tagged VID.

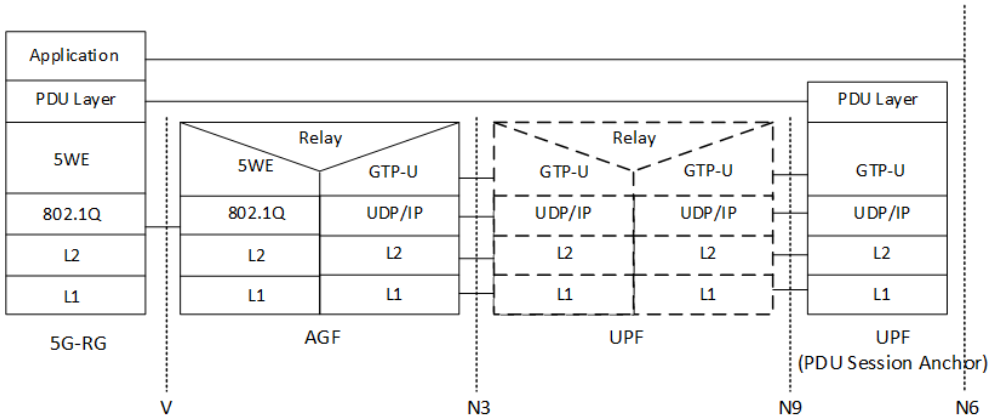

Figure 13: User Plane via AGF for 5G-RG.

The AGF needs to maintain a context per PDU session for each 5G-RG. The following information is maintained by the AGF associated with a PDU Session ID:

- The Line ID associated with the 5G-RG subscription
- The PDU session ID assigned by the 5G-RG,
- The 5WE session ID assigned by the AGF,
- The IEEE 802 MAC address of the 5G-RG that terminates the PDU session,
- The VLAN tag control information (TCI) at V interface, as specified in IEEE 802.1Q [33], associated with the access circuit connecting the AGF to the 5G-RG.
- Fully qualified TEIDs (see definition in TS 29.274 [18] section 8.22) for upstream and downstream of the N3 interface instance associated with the PDU session.
- The mapping of permissible PDU session QFI values to Ethernet Priority Code Point (PCP) and DSCP values.
    - PCP marking is always used for downstream traffic.
    - The remarking of packet DSCP is configurable for downstream traffic either via information in RG-LWAC or local configuration.
- The allowable protocols for the PDU session, e.g.: IPv4 Type, IPv6 Type, or Ethernet Type.

The 5GC informs the AGF of the relationship between QFI and 5G QoS Identifier (5QI) in QoS profile(s) in the N2 PDU Session Resource Setup/Modify/Release Request. By combining this with either local configuration or the RG-LWAC mapping information for 5QI to 802.1Q PCP and DSCP values (identified in the marking controls TLV (note that the 5QI descriptor TLV is depreciated)), the AGF derives the access transport layer priority/traffic class marking (e.g., 802.1Q PCP) and optionally any DSCP remarking for the QFI identified QoS flows. There are 254 5QIs and only up-to-eight traffic classes, each represented by an 802.1Q PCP value. The mapping between 5QI and 802.1Q PCP is N:1. At a given point of time, a maximum of 64 QoS flows exist in a PDU Session and each uniquely identified by a QFI.

The applicability of marking/remarking of packets/frames is communicated to the 5G-RG as part of the subscription parameters information communicated to the 5G-RG at registration time. The QFI to PCP/DSCP mapping values are communicated to the 5G-RG by the AGF, for each active QoS flow as part of the PDU session establishment/modification. This combination allows the 5G-RG to use this direct mapping to derive any PCP/DSCP marking to be used in uplink packets.

For a Non-GBR QoS flow, if the Reflective QoS Attribute (RQA, as defined in TS 38.300 [31]) is associated with a QFI, the 5G-RG can derive the IP-5 tuple filter and associated QFI from the received downstream packets. Otherwise, the 5G-RG MUST obtain the mapping rules for uplink packets to QoS flows/QFIs from PDU session establishment/modification related N1 messages. Note: support for dynamic 5QI Descriptors is FFS

[R-5G-2] The AGF MUST forward the list of QFI and PCP/DSCP mapping pair to the 5G-RG and update it when any changes are applied. This information is to be encoded in AS session parameter TLVs as defined in section 5.7 (AN, NAS and AS).

5WE uses NAS signaling for session establishment, therefore any PPPoE discovery messages sent with a 5WE header version are invalid.

[R-18] The AGF MUST silently discard any PPPoE discovery messages (EtherType 0x8863) received with a 5WE header.

6.3.1.1 Construction of 5WE header by the AGF for downstream information transfer

In the downstream direction, the AGF when relaying a received GTP-U packet from the UPF anchoring a PDU session populates the 5WE header as follows:

Note that where the following requirements in this section differ from [32], the latter is the authoritative source.

[R-5G-3] The 5WE version number MUST be set to 2 indicating this is WWC.

[R-5G-4] The 5WE type field MUST be set to 1.

[R-5G-5] The 5WE QFI field MUST be copied from the GTP encapsulation of the PDU session.

[R-5G-6] The 5WE RQI field MUST be copied from the GTP encapsulation of the PDU session.

[R-5G-7] The AGF MUST map the received N3 encapsulated packet to the local PDU session context, on the basis of the local F-TEID.

[R-5G-8] The 5WE session ID MUST be set to the value assigned by the AGF in the PDU session context.

[R-5G-9] The 5WE length field MUST be set to the length of the packet data unit received over the N3 interface plus 2 bytes for the protocol ID.

[R-5G-10] The 5WE Protocol ID MUST be set to the protocol encapsulated for the PDU session. The permissible values are drawn from the IANA PPP DLL Protocol Numbers registry and are:

- 0x0021 - IPv4 Packet
- 0x0031 - IEEE 802 Ethernet Frame
- 0x0057 - IPv6 Packet.

In the case of collocated UPF, described in section ‘Combined AGF/UPF’, the internal N3 interface may not implement GTP-U. However, UPF collocation is transparent to the user plane interface between AGF and 5G-RG. This means, from a downstream user plane perspective, the combined AGF/UPF behaves in the same way as an AGF with an external UPF. The requirements above also apply to the combined AGF/UPF, with the understanding that the N3 interface is internal. For example, in the case of an internal N3 interface that does not implement GTP-U encapsulation, the 5WE QFI is set to the QFI that a UPF would have applied on GTP-U packet, based on N4 and/or UPF local configuration.

6.3.1.2 Encapsulation of 5WE encoded packet in Ethernet for downstream transfer

The 5WE encapsulated PDU session packet or frame is then adapted onto the Ethernet transport via the imposition of the Ethernet MAC header and the tag control information from the PDU session context.

[R-5G-11] The AGF MUST be able to encapsulate the 5WE encapsulated PDU session packet with an IEEE 802 Ethernet MAC header.

[R-5G-12] The SA of the MAC frame MUST be set to the AGF-UP’s 5G-RG facing MAC address when relaying the frame in the downstream direction.

[R-5G-13] The DA of the MAC frame MUST be set to the MAC address of the 5G-RG obtained from the PDU session context

[R-5G-14] The VLAN tag control information for the access circuit connecting the AGF and the 5G-RG obtained from the PDU session context MUST be encoded in the Ethernet frame.

[R-5G-15] The Ethernet 802.1Q Priority Code Point value MUST be set to that corresponding to the 5QI value of the QoS flow associated with the QFI value received by the AGF in the GTP-U encapsulation. Note that this may result in packets from multiple QoS flows having the same 802.1Q PCP value.

6.3.1.3 Construction of N3 header by the AGF for upstream information transfer

The PDU session packet/frame is extracted from received Ethernet frames with 5WE encapsulation and relayed via the N3 interface to the UPF anchor point for the session.

[R-5G-16] The AGF MUST be able to map a received 5WE frame to a PDU session context. This is on the basis of 5WE session ID. Note that depending on the AGF implementation, it may be discriminated also by VLAN tag control information, port of arrival and/or SA MAC address.

[R-5G-17] The AGF MUST silently discard any frames received that it is not able to successfully map to a session context.

[R-5G-18] The AGF MUST silently discard any PDUs received that do not have a permissible protocol ID for the PDU session.

[R-5G-19] The AGF MUST be able to construct a GTP-U encapsulated session packet/frame using the payload of the 5WE encapsulated packet/frame and local PDU session context information (UPF IP address, TEID etc.).

[R-5G-20] A GTP-U packet produced by the AGF MUST comply with TS 38.414 [23] and TS 38.415 [24].

[R-5G-21] The AGF MUST be able to map the 802.1Q PCP value of an Ethernet frame received on the ‘V’ interface to a traffic class policer in the AGF.

6.3.2 User plane for FN-RG

The user plane encoding employed for PDU exchange between an AGF and an FN-RG is based on the traditional wireline protocols documented in TR-101/178 ([3], [5]) (such as IPoverPPP and IPoE). The protocol stack used for user plane is shown in Figure 14.

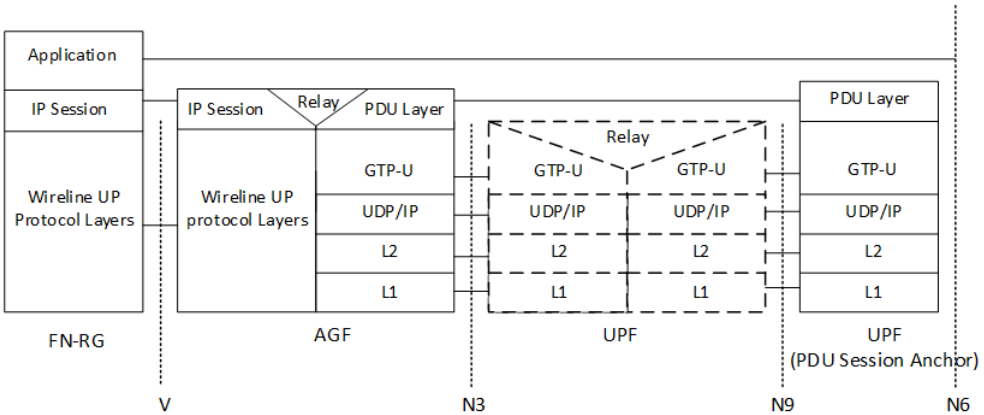

Figure 14: User Plane via AGF for FN-RG.

The user plane connection between FN-RG and AGF follows the IP-session lifecycle management as defined in TR-101/TR-178 and between the AGF and UPF follows the PDU session management as defined in TS 23.502 [29]. AGF proxies the FN-RG to establish the user plane connection to the 5GC by initiating PDU Session establishment.

6.3.2.1 L2/L3 Interworking

[R-FN-27] An AGF MUST perform a proxy ARP response offering the AGF's FN-RG facing MAC address in response to an ARP request from the FN-RG seeking to resolve the gateway address.

[R-FN-28] The AGF MUST glean an IPoE FN-RG's LLA from transaction that triggers IP session initiation (indirectly from DHCPv4 or directly from DAD, RS or DHCPv6) and encode it in the "suggested interface identifier" IE in the PDU SESSION ESTABLISHMENT REQUEST.

In the case of a DHCPv4 trigger for a v4/v6 PDU session, the information to construct an LLA can be gleaned from the triggering DHCPv4 source MAC address.

Note: The 5GC will acknowledge the Interface Identifier IE and echo the IPoE FN-RG's LLA in the PDU SESSION ESTABLISHMENT ACCEPT.

[R-FN-29] An AGF MUST use the SMF IPv6 LLA received in the PDU SESSION ESTABLISHMENT ACCEPT message as the source address for all proxied IPv6 ND responses for IPoE and the network LLA in IPv6CP negotiation for PPPoE.

[R-FN-30] An AGF that does not implement proxy DAD MUST silently discard all IPv6 DAD solicitations from IPoE FN-RGs.

[R-FN-31] An AGF that supports N:1 VLAN model SHOULD maintain a proxy DAD database and be able to appropriately respond to DAD solicitations from IPoE FN-RGs as per RFC 6957 [54].

[R-FN-32] An AGF MUST respond to an IPv6 neighbor solicitation for its link local address received from an IPoE FN-RG offering its own FN-RG facing MAC address.

[R-FN-33] When configured to support IPoE over N:1 VLAN, an AGF MUST resolve all IPv6 ND destination multicast addresses received from the SMF to the FN-RG unicast MAC address when adapting the ND message to Ethernet. (This is consistent with the spirit of R-44 in TR-177corr1 and necessary for the support of N:1 VLANs).

6.3.2.2 Static IPv4 for FN-RG

The requirements in this section are derived from section 8.1.14. Some of the requirements are touching the control plane but are left here for coherence.

The AGF may support handling of an FN-RG configured with a static IP Address.
Note: This is an Enterprise use case and is commonly deployed in the 1:1 VLAN access model.

If the AGF supports an FN-RG configured with a static IP Address, then [R-FN-34] to [R-FN-38] apply.

[R-FN-34] AGF MUST support local configuration of an IPv4 Address on a PORT/VLAN that is deployed in a 1:1 VLAN access model to be used for identifying the packets from FN-RG.

[R-FN-35] AGF MUST support the association of a unique Circuit ID and/or Remote ID with the IP Address configured as per [R-FN-34].

[R-FN-36] AGF MUST generate the Line ID, SUPI, SUCI using the Circuit ID and/or Remote ID for an FN-RG using static IPv4 Address.

[R-FN-37] AGF MUST prevent access towards the DNN for an FN-RG using a static IPv4 address if the IP Address assigned by the 5GC does not match the SRC IP Address of the packet from the FN-RG which triggered the FN-RG Registration.

[R-FN-38] AGF MUST release any user plane resources for the FN-RG and flush the local 3GPP context in case of any failures in REGISTRATION or PDU Session Setup Procedures.

6.3.3 Fragmentation and reassembling

Due to possible mismatch between the N3/N9/N6 interfaces MTU and V interface MTU, AGF might need to fragment and/or reassemble and perform path MTU processing.

[R-19] The AGF MUST support IP fragmentation and IP path MTU discovery for PDU sessions carrying IPv4 traffic downstream from an N3 interface towards a V interface.

[R-20] A combined AGF/UPF MUST support fragmentation and IP Path MTU discovery for PDU sessions carrying IPv4 traffic downstream from an N6 or N9 interface towards the V interface.

Note: If the PDU session carries Ethernet traffic, a minimum transport or DN MTU of 1522 bytes is required to accommodate MAC header, VLAN tag control information and a 1500 byte frame payload.

[R-21] The AGF MUST support IP fragmentation and IP path MTU discovery for PDU sessions carrying IPv4 traffic upstream from a V interface towards an N3 interface

[R-22] A combined AGF/UPF MUST support fragmentation and IP path MTU discovery for PDU sessions carrying IPv4 traffic upstream from a V interface towards an N6 or N9 interface.

Note: These two requirements above address the upstream case where the Wireline MTU is greater than the N3/N6/N9 MTU and the lesser of the two values has not been communicated to the CPE.

[R-23] AGF MUST support the IPv6 Path MTU Discovery procedure as defined in RFC 8201 as follows:

- For downstream IPv6 traffic of a PDU session exceeding a V-interface limit, the AGF generates an ICMPv6 Packet Too Big error message.
- The AGF handles any ICMPv6 Packet Too Big message destined to one of its local GTP-U IP addresses to learn an MTU for the GTP-U peer. The AGF MUST further enforce this MTU in one of the following ways:
    - By fragmenting the GTP-U packets toward the peer after encapsulation
    - By fragmenting upstream IPv4 traffic of a PDU session, generating an ICMP Packet Too big message for upstream IPv4 traffic of a PDU session, and by generating an ICMPv6 Packet Too big message for upstream IPv6 traffic of a PDU session.

[R-24] AGF MUST support IPv4 fragmentation and reassembly of GTP-U packet on the N3 interface.

[R-25] Combined AGF/UPF MUST support IPv4 fragmentation and reassembly of GTP-U packet on the N9 interface.

[R-26] AGF SHOULD be able to be configured to manipulate the TCP Maximum Segment Size of subscriber traffic as documented in RFC 6691 [52]

[R-27] The AGF interfaces MUST have configurable MTU.

[R-28] The UPF in a combined AGF/UPF SHOULD constrain the downstream MTU to the wireline access MTU for single access PDU sessions supporting RGs that only have a wireline interface. Note: how the combined AGF/UPF determines if this is a single access RG is FFS.

[R-29] The UPF in a combined AGF/UPF SHOULD constrain the downstream MTU to the MIN of the wireline access MTU and the transport MTU of the mobile network for ATSSS multi-access PDU sessions and RGs that support both wireline and wireless interfaces.

Note: how the combined AGF/UPF determines if this is a multiple access RG is FFS.

[R-30] An AGF MUST constrain the upstream MTU to that of the transport MTU of the mobile network for any sessions relayed over an N3 or N9 interface.

[R-31] A combined AGF/UPF SHOULD constrain the upstream MTU to that of a local N6 interface for PDU sessions where the combined UPF is the ultimate UPF.

6.3.4 Common QoS Marking Aspects

The following requirements apply to AGF support of both 5G-RGs and FN-RGs.

[R-32] The AGF MUST only support Standardized and Pre-configured 5QI values, i.e., support Non-dynamic 5QI Descriptors as defined in TS 38.413 [16] clause 9.3.1.28, without the optional parameters.

[R-33] For each PDU session, the AGF MUST derive and maintain an up-to-date list of QFI and PCP/DSCP mapping pair for downstream traffic and QFI and DSCP mapping pair for upstream traffic. For this, the AGF MUST use the mapping information in the RG-LWAC and the QFI-5QI mapping information received from the 5GC, in QoS flow management related messages (N2 PDU session resource setup/modification/release requests).

[R-34] If downstream remarking of IP DSCP is indicated by either local configuration or the RG-LWAC marking controls TLV. The AGF MUST remark the IP packet with the configured DSCP for the 5QI.

[R-35] The AGF MUST mark the PCP of downstream traffic sent on the ‘V’ interface to correspond to the traffic class for the 5QI of the packet. This may be:

- On the basis of received QFI mapped to 5QI via and either local configuration or mapping information in RG-LWAC
- On the basis of tunnel DSCP received on the N3 interface
- On the basis of QoS flow classification performed by a combined AGF/UPF

[R-36] If upstream remarking of IP DSCP is indicated by either local configuration or the RG-LWAC marking controls TLV the AGF MUST remark the IP packet with the configured DSCP for the 5QI.

[R-37] If upstream remarking of IP DSCP of the GTP-U encapsulated packet on N3 is indicated by local configuration the AGF MUST remark the IP Header of the GTP-U encapsulated IP Packet on the N3 interface with the configured DSCP for the 5QI.

[R-38] If upstream reflection of IP DSCP is indicated by local configuration the AGF SHOULD remark the IP Header of the GTP-U encapsulated IP Packet on the N3 interface with the IP DSCP of the incoming packet.

6.4 Control plane

Control plane traffic is originated by an AGF on behalf of an FN-RG or relayed as NAS PDUs between a 5G-RG and an AMF.

[R-39] The AGF must support Point-to-Point Protocol (PPP) as defined in RFC 1661 [43].

[R-40] The AGF MUST be able to receive the Line ID from the AN.

[R-41] The AGF MUST be able to construct the Global Line ID (GLI) as defined in TR-470 [9] by using the Line ID.

[R-42] The AGF MUST be able to encode the GLI into a User Location Information as define in TS 23.003 [26] and TS 38.413 [16].

[R-43] The AGF MUST be able to construct a Global W-AGF ID to globally identify an AGF node and populate the Global RAN Node ID in N2 messages, as defined in TS 38.413 [16] and TS 29.413 [20].

The AGF determines the class of RG it is supporting on the basis of session initiation traffic received by the AGF from the RG. This is described in detail in section 5.2 of this document. The formal requirements for detection of class of RG are as follows:

[R-FN-39] The AGF that is configured to support adaptive mode MUST reply to a PADI containing a NULL length service-name tag with a PADO containing a NULL length service-name tag.

[R-5G-22] The AGF that is configured to support direct mode MUST reply to a PADI containing the 5G service name tag with a PADO containing the 5G service-name tag.

[R-44] The AGF that is configured to support only direct mode MUST silently discard any PADIs received with a NULL length service tag.

[R-45] The AGF that is configured to support only adaptive mode MUST silently discard any PADIs received with the 5G service tag.

[R-FN-40] The AGF that is configured to support adaptive mode MUST reply to an LCP Configure-Request not containing the LCP 5G VSO with a Configure-Ack.

[R-5G-23] The AGF that is configured to support direct mode MUST reply to an LCP Configure-Request containing the LCP 5G VSO with a Configure-Ack.

[R-46] The AGF that is configured to support only direct mode MUST reply to an LCP Configure-Request not containing the LCP 5G VSO with a Configure-Ack followed by a Terminate-Request.

[R-47] The AGF that is configured to support only adaptive mode MUST reply to an LCP Configure-Request containing the LCP 5G VSO with an LCP Configure-Reject.

6.4.1 Control plane for 5G-RG

An AGF implements 5G control plane connectivity with a 5G-RG using PPPoE. The actual protocol and procedural aspects as well as the information elements are documented in section 5 (NAS and AS Transport and Information Elements) of this document. How NAS and AS exchange is integrated into procedures for registration management and PDU session management is documented in section 8 (Procedures and call flows). Large NAS packets may be fragmented by the Fragmentation sub-layer as specified in section 5.6 (VSNP Fragmentation Sub-Layer).

The protocol stacks used for control plane are shown in Figure 15:

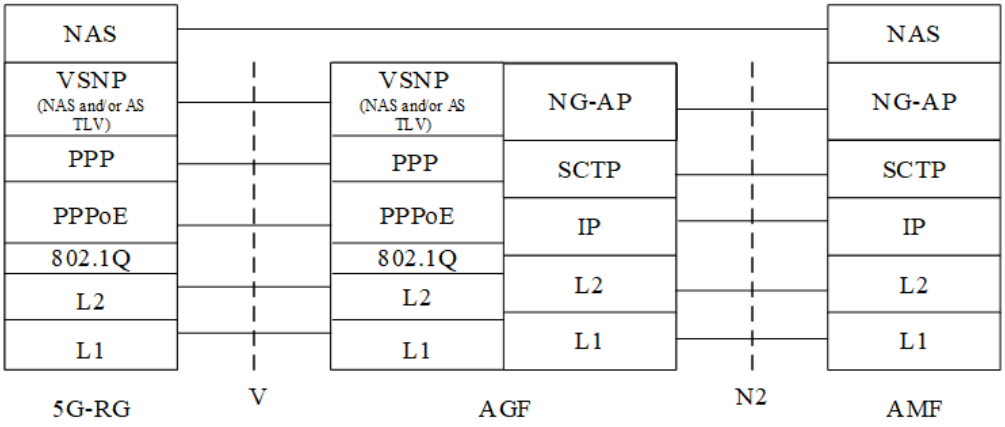

Figure 15: Control Plane between the 5G-RG and the AMF

The control plane is established by the 5G-RG starting the PPPoE procedure as specified in RFC 2516 [42]. The VLAN used at the U interface is that configured at the 5G-RG for NAS and 5WE exchange, which is called 5G VLAN. The VLAN used at the V interface is that associated with the access circuit connecting the AGF to the 5G-RG. After the PPPoE discovery stage, a PPPoE Session ID will be assigned by the AGF and communicated to the 5G-RG. The 5G-RG will use this Session ID to encapsulate the PPP as specified in RFC 1661 [43] for carrying the NAS message. The following procedures such as LCP, VSNCP and VSNP are all encapsulated in the PPP with the Protocol field specified based on different stages as per registration procedure:

- 0x0C21 – LCP (Step 5)
- 0x805b – VSNCP (Step 6)
- 0x405b – VSNP (After Step 6)

The AGF needs to maintain a 5G-RG context (N2 specific) for the 5G-RG's control plane. The following information is maintained by the AGF associated with a 5G-RG (identified as a 5G-RG context):

- The Line ID associated with the 5G-RG
- The MAC address of the 5G-RG
- The AN parameters as received from the 5G-RG, e.g., GUAMI, Requested NSSAIs, etc.,
- The Line ID based GLI as constructed by the AGF
- The User Location Information as encoded with GLI by the AGF
- The Global W-AGF ID as constructed by the AGF for globally identifying an AGF
- The VLAN tag control information (TCI) at V interface, as specified in IEEE 802.1Q, associated with the access circuit connecting the AGF to the 5G-RG
- The PPPoE Session ID assigned by the AGF
- The N2 interface identifier for the 5G-RG at the AGF side, i.e., the RAN UE NGAP ID [16] allocated by the AGF.
- The N2 interface identifier for the 5G-RG at the AMF side, i.e., the AMF UE NGAP ID.

[R-5G-24] The AGF MUST be able to use the 5G-RG Line ID to construct the GLI, from the PADI message sent by the 5G-RG initiating the PPP session that transports the NAS and the AS messages.

[R-5G-25] The AGF MUST support RFC 2516 [42] PPPoE for the exchange of NAS and AS information with a 5G-RG [42].

[R-5G-26] The AGF MUST use the 5G-RG MAC address from the 5G-RG context as the L2 5G-RG address when populating the PDU session context.

[R-5G-27] The AGF MUST populate the RG MAC address in the 5G-RG context with the 5G-RG MAC address gleaned from the PADI that initiates the PPPoE CP session.

[R-5G-28] The AGF MUST be able to allocate a PPPoE Session ID to identify the 5G-RG control plane association over the V interface.

[R-5G-29] The AGF MUST NOT include in the LCP Configure Request the Authentication-Protocol.

[R-5G-30] The AGF MUST use the PPPoE session ID to associate the received AN parameters (GUAMI, Requested NSSAIs, etc.) with the local 5G-RG context.

[R-5G-31] The AGF MUST be able to allocate a unique ID for the 5G-RG that will be used in the RAN UE NGAP ID as defined in TS 38.413 [16] to identify the 5G-RG association over the N2 interface.

[R-5G-32] The AGF MUST map the received N2 encapsulated packet to the local 5G-RG context, on the basis of the RAN UE NGAP ID.

[R-5G-33] The AGF MUST forward the received NAS message from the 5G-RG to the AMF on the basis of binding relationship between N2 interface and PPPoE Session ID.

[R-5G-34] The AGF MUST forward the received NAS message from the AMF to the 5G-RG on the basis of binding relationship between PPPoE Session ID and N2 interface.

[R-5G-35] The AGF MUST be able to send the N2 parameters (ULI, Global W-AGF ID, etc.) to the AMF via the N2 interface for the 5G-RG.

[R-5G-36] The AGF MUST support the exchange of NAS UE Registration Management Procedure messages encapsulated within PPP VSNP as specified in TS 24.502 [12].

[R-5G-37] The AGF MUST support the exchange of NAS UE PDU Session Establishment Procedure and AS Procedure messages encapsulated within PPP VSNP as specified in TS 24.502 [12].

[R-5G-38] The AGF MUST supervise the connectivity of the PPPoE session that transports NAS and AS messages using periodic LCP Echo Requests.

[R-5G-39] The AGF MUST consider that the PPPoE session specified in [R-5G-38] has terminated (and the connectivity with the 5G-RG has been lost) upon observing missed replies to a configurable number of consecutive LCP Echo Requests, with a default value of 3.

[R-5G-40] The periodicity of LCP Echo Requests specified in [R-5G-38] MUST be configurable. It MUST at least include the range from 30 seconds to 3600 seconds.

[R-5G-41] The AGF MUST use a default periodicity of 30 seconds for the LCP Echo Requests specified in [R-5G-40]

Note: An implementation may consider the reception of VSNP encapsulated traffic as the equivalent of a successful LCP Echo Reply and adjust LCP Echo Requests timers/counters accordingly

[R-5G-42] Upon detecting a fault, either due to a 5G-RG failure or to a loss of connectivity on the PPP link carrying NAS and AS, the AGF MUST start the “AN Release” procedure towards the AMF, as documented in section 8.2.8, and in TS 23.316 [25] clause 7.2.5.2.

6.4.1.1 IPoE DHCP Negotiation over the PDU Session

For a 5G-RG IPv4 or IPv4v6 PDU session that negotiates an IP address and session options using DHCP, the Access Node operates as a Layer2 DHCP Relay Agent, as specified in TR-101 Issue2 [3] section 3.9.1 and 3.9.3. The AGF is not required to snoop the DHCP control packet exchanges and transparently forwards the exchanges between the 5G-RG and SMF. When the 5G-RG initiates negotiation over the PDU Session, the broadcast DHCP DISCOVER (and subsequent REQUEST) is forwarded by the AGF to the SMF via N3. After processing the packet, the SMF will send the downstream DHCP OFFER or ACK packet to the 5G-RG as a broadcast or unicast packet, per the broadcast bit in the DISCOVER packet, via N3. All downstream DHCP control packets are transparently forwarded by the AGF to the 5G-RG. Hence, the 5G-RG appears directly connected to the SMF.

The PDU session exchanges between the 5G-RG and SMF via the AGF and UPF is summarized in Figure 16:

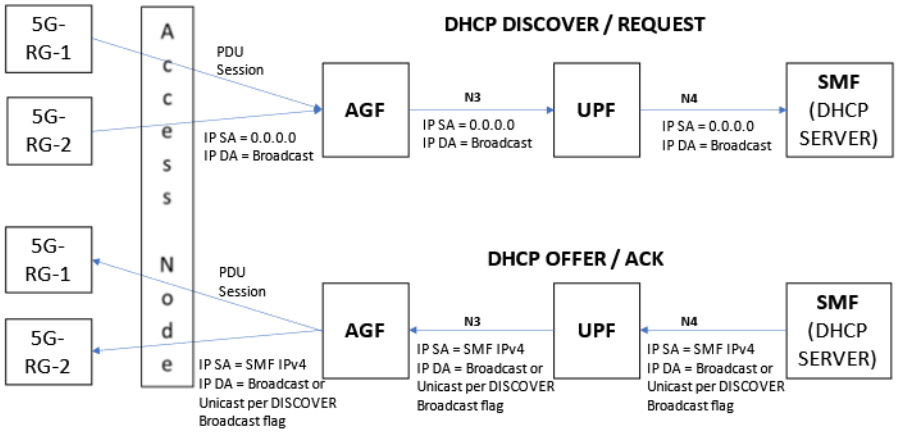

Figure 16: 5G-RG PDU Session DHCP Control Packet Exchanges

The AGF forwards the broadcast upstream DHCP control packets over N3 to the UPF, which forwards over N4 to the SMF to process as a DHCP server. The SMF sends the corresponding DHCP control packet responses over N4, using its IP address as the IP SA and sets the IP DA per the broadcast bit setting received in the DISCOVER. The AGF will transparently forward the downstream DHCP control packets to the 5G-RG over the 5WE encapsulated PDU session.

The following requirement applies to 5G-RG PDU Session DHCP control packet exchanges between the 5G-RG and 5GC via the AGF:

[R-5G-43] An AGF MUST transparently forward 5G-RG PDU Session DHCP control packet exchanges between the 5G-RG and 5GC.

6.4.1.2 IPoE DHCPv6 Negotiation over the PDU Session

For a 5G-RG IPv6 or IPv4v6 PDU session that negotiates an IPv6 address or prefix or session options using DHCPv6, the AGF is not required to snoop the DHCPv6 control packet exchanges and transparently forwards the exchanges between the 5G-RG and SMF. When the 5G-RG initiates negotiation over the PDU Session, the multicast DHCPv6 SOLICIT (and subsequent REQUEST) is forwarded by the AGF to the SMF

via N3. After processing the packet, the SMF will send the corresponding DHCPv6 ADVERTISE or REPLY response packet to the 5G-RG, via N3. Hence, the 5G-RG appears directly connected to the SMF

The packet exchanges between the 5G-RG and SMF via the AGF and UPF is summarized in Figure 17:

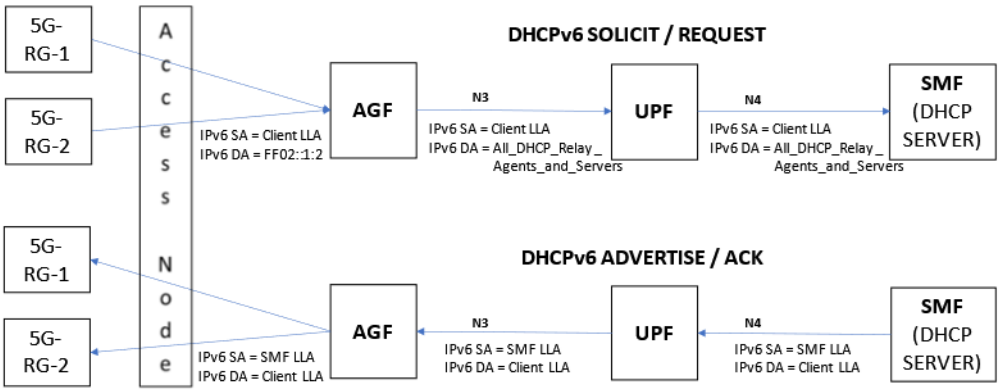

Figure 17: 5G-RG PDU Session DHCPv6 Control Packet Exchanges

The AGF forwards the upstream DHCPv6 control packets with an IPv6 DA of the All_DHCP_Relay_Agents_and_Servers multicast address over N3 to the UPF, which forwards over N4 to the SMF to process as a DHCPv6 server. The SMF sends the corresponding DHCPv6 control packet responses over N4, using its IPv6 LLA as the IPv6 SA and the client's LLA as the IPv6 DA. The AGF will transparently forward the downstream DHCPv6 control packets to the 5G-RG over the 5WE encapsulated PDU session.

Note that it is potentially possible in some cases that an element such as an AN will insert a RELAY-FORW header, per RFC 6221 [55], containing option 18 (Interface-ID), option 37 (Remote-ID) and possibly option 17 (Vendor-Specific Information). Hence, the DHCPv6 control packet exchange between the 5G-RG and SMF via the AGF would be encapsulated in a single RELAY-FORW or RELAY-REPL message, but the above description otherwise applies.

The SMF is the IPv6 gateway for the 5G-RG and thus responds to Neighbor Solicitation requests from the 5G-RG and always originates unsolicited and solicited IPv6 Router Advertisements to the 5G-RG. Depending on the IPv6 addressing mode (i.e., the use of DHCPv6 to assign an IPv6 address), the Router-Advertisement may contain a Prefix Information Option carrying a /64 IPv6 prefix. The AGF will transparently forward Neighbor Discovery and Router Advertisement exchanges between the 5WE PDU session and corresponding N3 interface.

The following requirements apply to 5G-RG PDU Session IPv6 control packet exchanges between the 5G-RG and 5GC via the AGF:

[R-5G-44] An AGF MUST transparently forward 5G-RG PDU Session DHCPv6 control packet exchanges between the 5G-RG and 5GC.

[R-5G-45] An AGF MUST transparently forward 5G-RG PDU Session IPv6 Neighbor Discovery and Router Advertisement control packet exchanges between the 5G-RG and 5GC.

6.4.2 Control plane for FN-RG

An AGF proxies 5G control plane connectivity for an FN-RG. The protocol stack used for control plane is shown in Figure 18:

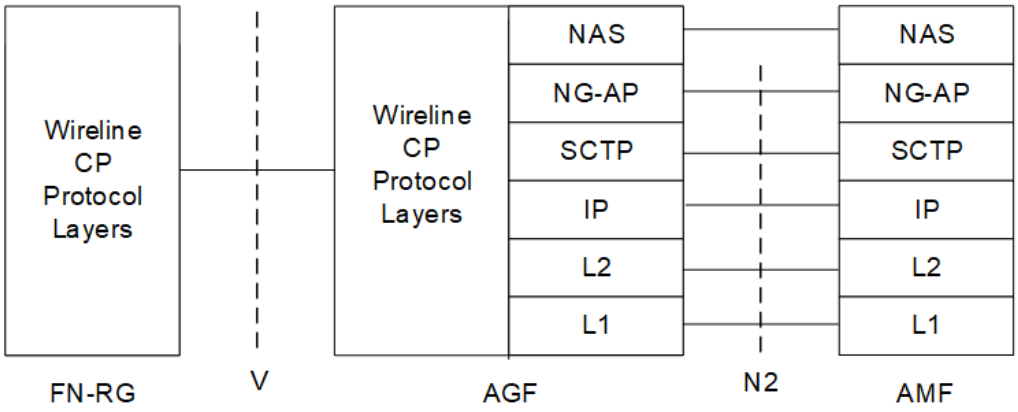

Figure 18: Control Plane signaling stack between the FN-RG and the AMF

FN-RG initiates the connection with the AGF-CP as described in TR-101. The V interface used for FN-RG connection follows the requirements as defined in TR-101 Issue2 [3] for BNG. The AGF-CP treats the IP session initiation as a trigger to perform a proxy registration for the FN-RG and establishes the NAS connection with the AMF where the NAS message overlays the N2 interface as defined for 5G-RG.

In addition to the N2 specific 5G-RG context, the AGF needs to maintain N1 specific context for the FN-RG's control plane.

SSC modes: SSC mode 2 and SSC mode 3 requires behaviors in PDU session life cycle management that cannot be coordinated with an IPoE session. Therefore, for IPoE FN-RG support only SSC mode 1 is used. SSC mode 2 could be supported with PPPoE.

Note: The reason why SSC mode 2 can be supported with PPPoE, but cannot be supported with IPoE is that PPPoE protocol has mechanisms to let the network break the connectivity in the access segment (e.g., PADT), while in case of IPoE there aren't mechanisms to break the access connectivity on purpose. SSC mode 3 is not supported with PPPoE nor with IpoE, because the network cannot make a new connection on its own.

[R-FN-41] An AGF initiating a PDU session in response to an IpoE based IP session trigger MUST request SSC mode 1.

[R-FN-42] An AGF initiating a PDU session in response to an PPPoE based IP session trigger MUST NOT request SSC mode 3.

6.4.2.1 IpoE DHCP FN-RG

For an IpoE FN-RG that negotiates using DHCP, the Access Node operates as a Layer2 DHCP Relay Agent, as specified in TR-101 Issue2 [3] section 3.9.1 and 3.9.3, and the AGF operates as a DHCP relay. When the FN-RG initiates negotiation, the DHCP DISCOVER can be used to initiate proxy UE Registration and PDU Session Establishment Procedures. Upon signaling completion, the AGF converts the broadcast DHCP DISCOVER to an IP unicast packet, including setting the GIADDR to the AGF Ipv4 address. The AGF is thus the gateway for the FN-RG and will perform a proxy ARP response to an ARP of the gateway address or server IP address. All downstream DHCP control packets are directed to the AGF, such that the GIADDR is set to the AGF Ipv4 address. After processing the packet, the AGF will forward the downstream packet to the client as a broadcast or unicast packet, per the broadcast bit in the DISCOVER packet.

This behavior allows a lease associated with a PDU session to have a common lifetime and fate share with AGF, SMF and any external server when the SMF is not operating as DHCP server.

The packet exchanges between the AGF and SMF via the UPF is summarized in Figure 19.

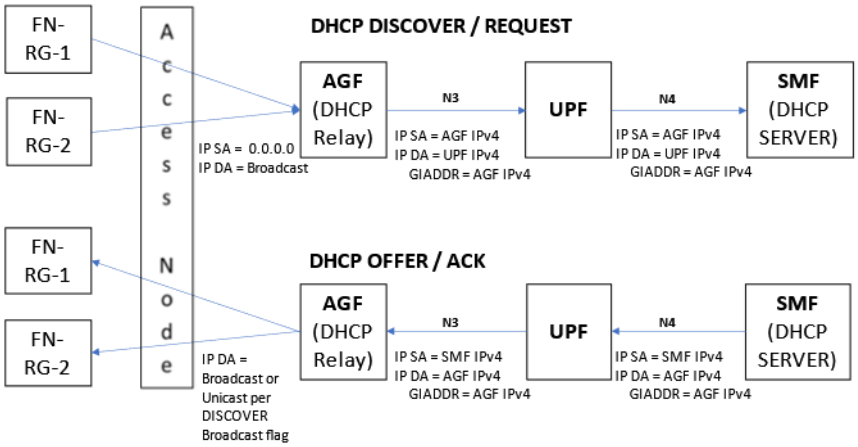

Figure 19: DHCP FN-RG Control Packet Exchanges

The AGF converts broadcast upstream DHCP control packets to unicast, using its address as the IP SA and the UPF endpoint as the IP DA, and sets the GIADDR to its IP address. The upstream DHCP control packets are forwarded by the UPF over N4 to the SMF to process as a DHCP server. The SMF sends the corresponding DHCP control packet responses over N4, using its IP address as the IP SA and the AGF as the IP DA and returns the GIADDR unmodified. The AGF will forward the downstream DHCP control packets to the FN-RG client, adhering to the broadcast bit setting received in the DISCOVER.

The following requirements apply to AGF processing of a IpoE FN-RG using DHCP:

[R-FN-43] An AGF MUST be able to proxy UE registration and PDU session establishment procedures upon receipt of a DHCP DISCOVER from the FN-RG.

[R-FN-44] An AGF MUST be able to operate as a DHCP relay, converting upstream broadcast DHCP control packets to IP unicast packets and setting the GIADDR to the AGF Ipv4 address before forwarding over N3 to the SMF.

[R-FN-45] An AGF MUST be able to receive and process downstream DHCP control packets addressed to it, including the GIADDR set to the AGF Ipv4 address.

6.4.2.2 IpoE DHCPv6 FN-RG

For an IpoE FN-RG that negotiates using DHCPv6, the Access Node operates as a Lightweight DHCP Relay Agent (LDRA), as specified by TR-177 Corrigendum 1 [4] section 5.6.1 and RFC 6788 [55], and the AGF operates as a DHCPv6 relay. When the FN-RG initiates negotiation, the DHCPv6 SOLICIT is received with a RELAY-FORW header added by the Access Node and can be used to proxy UE Registration and PDU Session Establishment Procedures. Upon signaling completion, the AGF-CP adds its own RELAY-FORW header, per RFC 8415 [59], before relaying the DHCPv6 SOLICIT to the 5GC. Hence, the SMF receives upstream DHCPv6 control packets with two layers of RELAY-FORW header.

All downstream DHCPv6 control packets are sent as a RELAY-REPL to the AGF relay, containing the client response (e.g., ADVERTISE) in its own RELAY-REPL header. After processing the packet, the AGF will decapsulate the outer REPLY-REPL header before forwarding the downstream packet to the client.

This behavior allows a lease associated with a PDU session to have a common lifetime and fate share with AGF, SMF and any external server when the SMF is not operating as DHCP server.

The packet exchanges between the AGF and SMF via the UPF is summarized in Figure 20:

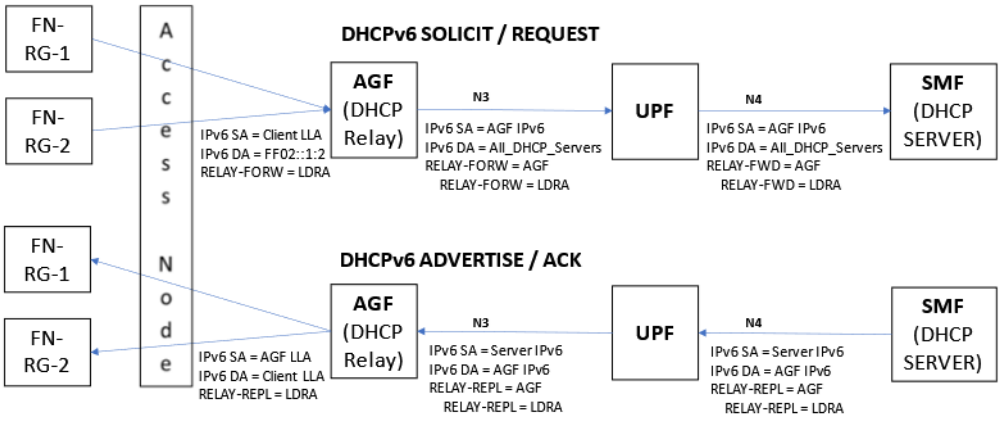

Figure 20 : DHCPv6 FN-RG Control Packet Exchanges

The AGF receives the DHCPv6 SOLICT and REQUEST messages with an Ipv6 DA of the All_DHCP_Relay_Agents_and_Servers multicast address and a RELAY-FORW header inserted by the Access Node as an LDRA. The AGF encapsulates the packet with a RELAY-FORW header and uses its address as the Ipv6 SA and the All_DHCP_Servers multicast address as the Ipv6 DA. The upstream DHCPv6 control packets are forwarded by the UPF over N4 to the SMF to process as a DHCPv6 server. The SMF sends the corresponding DHCPv6 control packet responses over N4, using its Ipv6 address as the Ipv6 SA and the AGF as the Ipv6 DA. The AGF decapsulates its RELAY-REPL header before forwarding the downstream DHCPv6 control packets to the FN-RG client.

The AGF is the Ipv6 gateway for the FN-RG and thus should use its MAC address and a consistent local LLA to respond to Neighbor Solicitation requests from the FN-RG and sending solicited and unsolicited router advertisements which originate from the SMF.

Note that Ipv6 addressing for an FN-RG may solely be satisfied by stateful means via DHCPv6 such that the SOLICIT contains either or both the IA_NA (non-temporary address) option and IA_PD (delegated prefix) option. As this is a common addressing mode for wireline IpoE networks, the Router Advertisement will not contain a Prefix Information option in this case. Regardless of whether an Ipv6 Prefix needs to be assigned, the SMF will always originate solicited and unsolicited Ipv6 Router Advertisements, optionally containing a Prefix Information Option carrying a /64 Ipv6 prefix.

The following requirements apply to AGF processing of a IpoE FN-RG using DHCPv6:

[R-FN-46] An AGF MUST be able to proxy UE registration and PDU session establishment procedures upon receipt of a DHCPv6 SOLICIT from the FN-RG.

[R-FN-47] An AGF MUST be able to operate as a DHCPv6 relay, encapsulating the packet with an LDRA RELAY-FORW header with its own RELAY-FORW header before forwarding over the N3 interface to the SMF.

[R-FN-48] An AGF MUST be able to receive and process downstream DHCPv6 control packets encapsulated as a RELAY-REPL message addressed to it, containing the client response (e.g., ADVERTISE) in its own RELAY-REPL header.

6.4.2.3 PPPoE-based FN-RG

For a PPPoE FN-RG, the Access Node operates as a PPPoE Intermediate Agent, as specified by TR-101 Issue2 [3] section 3.9.2, and the AGF terminates the PPP session, which may be transported directly over ethernet or encapsulated over L2TP. It negotiates IP NCP and/or Ipv6 NCP. In case of L2TP, the PPPoE

Intermediate Agent information received by the LAC must be conveyed to the AGF in the role of LNS, via the ICRQ message, per RFC 5515 [58].

When the FN-RG initiates negotiation, as PPP LCP is used to discriminate 5G-RG from FN-RG, PPP authentication protocol triggers proxy UE Registration and PDU Session Establishment Procedures such that the PPP authentication acknowledgement response is contingent on completing signaling with 5GC.

Note that, during PDU Session Establishment Procedures, the AGF will request an IP address via NAS signaling. The Ipv6 WAN address may be sourced from the SMF's Ipv6 Router Advertisement containing a /64 prefix in the Prefix Information Option. Additionally, DHCPv6 may be negotiated to establish a LAN prefix (delegated prefix) and other options needed by the FN-RG client. AGF processing of the DHCPv6 negotiation is as described in section 6.4.2.2.

The IP address, Ipv6 Interface Identifier and optionally Ipv6 Router Advertisement /64 prefix must be signaled by 5GC before the corresponding PPP NCP may be negotiated.

The following requirements apply to AGF processing of PPP when encapsulated in PPPoE or L2TP:

[R-FN-49] An AGF MUST be able to proxy UE registration and PDU session establishment procedures upon receipt of a PPP authentication protocol message (i.e., PAP Authentication-Request or CHAP Challenge-Response) from the FN-RG.

[R-FN-50] An AGF MUST support DHCPv6 as a DHCPv6 relay as described in section 6.4.2.2.

6.5 QoS

6.5.1 RG level QoS Provisioning

TR-101 wireline access networks inherently have end-to-end QoS characteristics that are typically managed on a per-subscriber / household level basis. These QoS characteristics are based on subscription or service tiers and traffic types and flows to and from the subscriber that are specified by an external authority (RADIUS, PCRF, etc.) and/or local configuration. Wireline access QoS, typically represented by the RG as the subscriber, prescribes treatment of traffic to and from the subscriber, including an aggregate downstream and upstream rate.

For 5G WWC similar QoS mechanisms are expected on a per-subscriber or RG-level basis for wireline access to accommodate legacy FN-RG QoS characteristics and QoS characteristics of 5G flows for 5G-RGs. This means the AGF will serve the role of accepting QoS characteristics from the 5GC, applying and enforcing these characteristics, and communicating relevant upstream information to the 5G-RG to enforce. To configure the QoS characteristics of the legacy access networks on the AGF, the AGF receives information from the 5GC known as the RG-Level Wireline Access Characteristics (RG-LWAC). As noted in TS 23.316 [25], these parameters are transparent to the 5GC; it neither interprets nor acts on these parameters, thereby preserving existing 3GPP behavior. The RG-LWAC thus serves as means to map 5G QoS management to a wireline access model.

RG-Level Wireline Access 5G QoS Characteristics

In a PDU session, the QoS flow is used for QoS differentiation in the AN. Each 5G QoS flow has a QoS class identity (5QI) that reflects its traffic forwarding treatment as defined in clause 5.7.2.1 in TS 23.501 [28], albeit the AGF will only support standardized and pre-configured (non-standardized) 5G QoS characteristics. The AGF will adapt the 3GPP QoS concept to wireline QoS mechanism. This is done by mapping the 5G QoS Characteristics as defined in TS23.501 [28] clause 5.7.3 to wireline traffic classes and shaping/policing characteristics (e.g., CIR, PIR, etc.). This is achieved using the information encoded in the RG-Level Wireline Access Characteristics (RG-LWAC) data structure possibly augmented with local configuration. The RG-LWAC is provisioned at the UDR, communicated to the AGF during Registration time, and can be updated by the operator anytime.

[R-48] The AGF MUST be able to be locally configured with up to 8 default RG facing traffic class descriptors.

[R-49] The AGF MUST be able to be locally configured with default 5QI to DSCP/PCP mappings.

[R-50] The AGF MUST be able to be locally configured with default PCP to traffic class mappings.

[R-51] The AGF MUST override local configuration of traffic class and mappings on a per subscriber basis with information received in the RG-LWAC data structure.

In the standard 5QI table (Table 5.7.4-1, from TS 23.501 [28]), the following three parameters: Packet Error Rate (PDR), Packet Delay Budget, and Averaging Window are not applicable to wireline technology. In wireline, the physical transport medium:

- Typically, do not experience Realtime degradation. The Quality of the transport does not change over time.
- Signal to Noise Ratio is not contributed by the external environment (ie. temperature, weather, other radio interferences) or external moving objects.

The 5QI parameters provide a minimum requirement for the wireless transport medium which may experience these interferences. Compared to the wireless environment, the transport is static and stable and therefore, some 5QI parameters are not applicable to wireline.

For Packet Error Rate: As specified in TS 23.501 “PER defines an upper bound for a rate of non-congestion related packet losses” and “The purpose of the PER is to allow for appropriate link layer protocol configurations (e.g., RLC and HARQ in RAN of a 3GPP access).” For wireline link layer, within the standard Ethernet and the PPP protocol stack, there are no alternative mechanism to enforce better error code handling or retransmission.

For Averaging Window: As specified in TS 23.501 “The Averaging window represents the duration over which the GFBR and MFBR shall be calculated (e.g., in the (R)AN, UPF, UE).” And “Every standardized 5QI (of GBR and Delay-critical GBR resource type) is associated with a default value for the Averaging window (specified in QoS characteristics Table 5.7.4.1).” These are only applicable to GBR type of traffic. For wireline, GBR or committed traffic are modeled with a strict scheduler as a committed information rate (CIR) to guarantee packet delivery. Once the PDU session establishes, the wireline CIR is designed to guarantee the rate without external environment influence. The averaging window therefore is not applicable to wireline, where there isn’t a time restriction placed on CIR.

For Packet Delay Budget: As specified in TS 23.501 “upper bound for the time that a packet may be delayed between the UE and the UPF that terminates the N6 interface.” In addition, “In the case of 3GPP access, the PDB is used to support the configuration of scheduling and link layer functions (e.g., the setting of scheduling priority weights and HARQ target operating points)”. The requirements are based on GBR which in wireline is a guaranteed rate. Further, there are no retransmission mechanism at layer 2 which would add to packet transmission delay.

For a standalone AGF or B-UPF, the above parameters do not apply. However, when the AGF is combined with AN, the above parameters may apply and is for FFS.

[R-52] The RG-LWAC MUST contain only Standardized and Pre-configured 5QI values, i.e., support Non-dynamic 5QI Descriptors as defined in TS38.413 [16] clause 9.3.1.28, without the optional parameters.

The RG-LWAC provides the relationship between each 5QI value the operator intends to use for the RG and an 802.1Q PCP and/or a DSCP value. The 802.1Q PCP value represents one of up-to-8 traffic classes that the wireline AN support (e.g., based on its configuration) for the given RG. The 5QI to PCP/DSCP mapping in RG-LWAC, or local configuration, is used in combination with the 5QI-QFI mapping information as received per PDU session basis.

Besides the 5QI to PCP/DSCP mapping, the RG-LWAC may contain further information applicable for each wireline traffic characteristics for traffic class specific bandwidth limits, shaping and policing configuration. These may supersede or augment local configuration, or the RG-LWAC may be empty and the parameters default to local configuration.

The following tables specify parameters that may be returned in the RG-LWAC. They are defined such that no one parameter is mandatory to allow flexibility of configuring the RG interface from a combination of local AGF configuration combined with parameters sourced from the UDM in these constructs. It also offers flexibility for varying AGF vendor implementations. In the event of a conflict, RG-LWAC configuration SHOULD take precedence over local AGF configuration. This implies the RG-LWAC "blob" is not a fixed-sized construct and can be variable in size to only provide those needed parameters from the AMF.

The following table defines UE (RG) Level QoS characteristics that allow for shaping or policing. All parameters are optional. Note that this is a framework that should not necessarily prevent additional and/or vendor-specific parameters.

Feature	Parameter	Description
DL Descriptor	-	UE-Level downstream shaper applied on the AGF
	Shaping-Rate	QoS Peak Information Rate (PIR) in BPS
	Shaping-Rate-Burst	Peak Burst Size in bytes
	Guaranteed-Rate	Maximum committed burst rate (CIRmax) in BPS
	Guaranteed-Rate-Burst	Committed Burst Size (CBS) in bytes
	TC-Queue-Profile	Profile specifying explicitly configured bandwidth and scheduling characteristics for up to 8 traffic classes to satisfy supported QFIs. This references the name of a profile/template configured on the AGF that simplifies UDM-sourced configuration. Per TC configuration in the table that follows may be used to prescribe per TC configuration in lieu of this attribute
	Shaping-Profile	Profile specifying Shaping-Rate, Shaping-Rate-Burst, Guaranteed-Rate, Guaranteed-Rate-Burst and TC-Queue-Profile. This references the name of a profile/template configured on the AGF that simplifies UDM-sourced configuration by allowing a single parameter to reference AGF local configuration that fully configures RG-level DL QoS characteristics.
UL Descriptor	-	UE-Level upstream shaper communicated to the RG by the AGF during AS procedures.
	Shaping-Rate	QoS peak information rate (PIR) in BPS
	Shaping-Rate-Burst	Peak Burst Size in bytes
	Guaranteed-Rate	Maximum committed burst rate (CIRmax) in BPS
	Guaranteed-Rate-Burst	Committed Burst Size in bytes
UL Policing Descriptor	-	UE-Level upstream policer applied on the AGF
	Bandwidth-Limit	Rate limit bandwidth in BPS
	Burst-Size-Limit	Burst size limit in bytes
	Policer-Template	Template specifying policer attributes, including rate limit value(s), action when rate limit is exceeded, etc. This references the name of a policer template configured on the AGF that simplifies UDM-sourced configuration by allowing a single parameter to reference AGF local configuration that fully configures RG-level UL QoS characteristics.

Table 3 - UE Level QoS characteristics

The following table defines per Traffic Class QoS characteristics that define up to 8 traffic classes on which QFIs are mapped. Only those traffic classes that are used or require configuration are specified. All parameters are optional. Note that this is a framework that should not necessarily prevent additional and/or vendor-specific parameters.

Feature	Parameter	Description
DL TC Descriptor	-	Per-Traffic Class QoS Configuration
	TC-Queue-Name	Name of the queue representing this Traffic Class. Up to 8 entries are allowed, where this attribute serves as the key
	TC-Shaping-Rate	QoS peak information rate (PIR) in BPS
	TC-Shaping-Rate-Burst	PBS in bytes
	TC-Guaranteed-Rate	Maximum committed burst rate (CIRmax) in BPS
UL TC Descriptor	-	Per-Traffic Class QoS Configuration communicated to the RG by the AGF during AS procedures.
	TC-Queue-Name	Name of the queue representing this Traffic Class. Up to 8 entries are allowed, where this attribute serves the key
	TC-Shaping-Rate	QoS peak information rate (PIR) in BPS
	TC-Shaping-Rate-Burst	PBS in bytes
	TC-Guaranteed-Rate	Maximum committed burst rate (CIRmax) in BPS
DL TC Policing Descriptor	-	Per-Traffic Class Downstream policer applied on the AGF. This is optional but may be used in lieu of or in conjunction with DL TC Shaper feature
	TC-Name	Traffic Class name
	TC-Policer-Name	Name of the policer corresponding to this Traffic Class
	TC-Bandwidth-Limit	Rate limit bandwidth in BPS
	TC-Burst-Size-Limit	Burst size limit in bytes
	Aggregate-Policer-Template	Template specifying policer attributes, including rate limit value(s), action when rate limit is exceeded, etc. for each Traffic Class. This references the name of the policer template configured on the AGF that simplifies UDM-sourced configuration by allowing a single parameter to reference AGF local configuration. This may be used in lieu of configuring per TC policer configuration attributes.
UL TC Policing Descriptor	-	Per-Traffic Class Upstream policer communicated to the RG by the AGF during AS procedures. This is a placeholder and FFS with respect to the RG.
	TC- Name	Traffic Class name
	TC-Policer-Name	Name of the policer corresponding to this Traffic Class
	TC-Bandwidth-Limit	Rate limit bandwidth in BPS
	TC-Burst-Size-Limit	Burst size limit in bytes

Table 4 - Per Traffic Class QoS characteristics

The mapping of 5G QFI to Traffic class is achieved by the mapping of QFI to 5QI provided with the PDU session parameters, and then the 5QI is mapped to traffic class using a combination of local configuration and information in the RG-LWAC data structure. The mapping may be sourced from local AGF configuration

as it is anticipated to be common among a class of subscribers, where the number of different subscriber classes, and thus different mappings, is expected to be small. Like other parameters described above, it is conceivable to reference an AGF-local 5G QFI to Traffic Class mapping as a profile or template reference in the RG-LWAC.

The following requirements apply:

[R-53] The AGF MUST support applying and enforcing downstream QoS configuration received from the AMF in the RG-LWAC as part of the RG registration process or in the Subscriber Data Update Notification procedure. This includes RG node level and per Traffic-Class configuration as described in the above tables.

[R-54] The AGF SHOULD support applying and enforcing downstream RG-LWAC QoS configuration received from the AMF along with local AGF RG QoS configuration. The AMF-sourced RG-LWAC QoS configuration should override or supplement local AGF configuration.

[R-55] The AGF SHOULD support applying and enforcing downstream RG-LWAC QoS configuration sourced from local AGF Configuration in absence of receiving downstream RG-LWAC QoS configuration from the AMF.

[R-56] The AGF MUST support applying and enforcing upstream QoS configuration received from the AMF in the RG-LWAC. This includes RG node level and per Traffic-Class configuration as described in the above tables.

[R-57] The AGF SHOULD support applying and enforcing upstream RG-LWAC QoS configuration received from the AMF along with local AGF RG QoS configuration. The AMF-sourced RG-LWAC QoS configuration should override or supplement local AGF configuration.

[R-58] The AGF SHOULD support applying and enforcing upstream RG-LWAC QoS configuration sourced from local AGF Configuration in absence of receiving upstream RG-LWAC QoS configuration from the AMF.

[R-5G-46] The AGF MAY support local AGF configuration of upstream RG-Level QoS configuration that can be communicated to the 5G-RG during AS procedures. This may be used in absence of receiving upstream configuration in the RG-LWAC from the AMF during RG procedures.

[R-5G-47] The AGF MUST support communicating upstream RG-LWAC QoS configuration received from the AMF to the 5G-RG using AS procedures as part of RG registration.

[R-5G-48] The AGF MAY support communicating to 5G-RG upstream QoS configuration based on a combination of RG-LWAC QoS configuration from the AMF and local AGF RG QoS configuration, where AMF-sourced RG-LWAC QoS configuration overrides or supplements local AGF configuration, using AS procedures.

PDU Session Level QoS Characteristics

TS 23.316 [25] specifies that each PDU Session of a 5G-RG or FN-RG may be configured with a Session-AMBR that limits the aggregate bandwidth for all Non-GBR QoS Flows for the Session. This is retrieved from the UDM via the SMF during Session Initiation and signaled to the UPF over N4. These QoS characteristics are enforced on the UPF. For a collocated AGF and UPF, the PDU session appears as an additional scheduling layer in the QoS hierarchy. Session-AMBR is only enforced at the 5G-RG and UPF.

FN-RGs do not support GBR functionality as defined by 3GPP, i.e., cannot enforce GBR or MFBR in the upstream direction. Therefore, for FN-RG, only downlink GBR QoS flow traffic filters can be enforced; this is enforced in the same way in AGF as for a 5G-RG. Note: For upstream direction, GBR-like behavior may be achieved using FN-RG configuration via ACS. However, this is static behavior and not controlled by the 5GC.

During PDU Session Initiation or PDU session modification, for a GBR QoS flow, the AGF will receive GBR QoS Flow Information. The information element contains MFBR for UL, MFBR for DL, GFBR for UL and GFBR for DL as mandatory, and Notification control, maximum downlink packet loss rate, maximum upstream packet loss rate as optional. The GBR QoS flows are subject to Call Admission Control (CAC) by the AGF based on RG-LWAC (for example, GFBR/MFBR for UL is subject to UL Policing Descriptor and GFBR/MFBR for DL is subject to DL Descriptor), while non-GBR QoS flows are not.

[R-5G-49] For GBR QoS flows, the AGF MUST support GBR QoS Flow Information shown as mandatory as defined in TS38.413 [16] clause 9.3.1.10.

[R-5G-50] The AGF MUST store the GFBR and MFBR value for each GBR QoS flow, as received in N2 PDU Session Resource Setup/Modification Request, for the QFI.

[R-5G-51] When receiving a request for establishing a GBR QoS flow, the AGF MUST exercise admission control.

- The AGF MUST then determine the TC that the newly requested GBR QoS flow must be mapped to, based on its 5QI value
- The AGF MUST then ensure that:
  (a) the sum of DL GFBR values of the previously established GBR QoS flows mapped to that TC, plus the DL GFBR of the actually requested QoS flow do not exceed the available CIR capacity belonging to the TC, as defined in the RG-LWAC.
  (b) the sum of UL GFBR values of the previously established GBR QoS flows mapped to that TC, plus the UL GFBR of the actually requested QoS flow do not exceed the available CIR capacity belonging to the TC, as defined in the RG-LWAC.
- If either the sum of DL or UL GFBR would exceed the PIR value, the AGF MUST execute pre-emption procedure based on the Allocation and Retention Priority parameter of each GBR flow, as defined in TS38.413 [16], clause 8.2.1.2. The AGF MUST release the pre-empted QoS flow(s).

[R-5G-52] The AGF SHOULD police the upstream TC for GBR QFIs to the sum of the resource commitments for that TC (which will be less than or equal to the CIR/EIR for the TC).

[R-5G-53] The AGF MUST use the combination of the TC descriptor, the QFI to 5QI to TC mapping and the received per packet IP precedence information as an input into queue management.

[R-FN-51] The AGF SHOULD support GBR QoS flows for FN-RG, if the QoS flow includes only DL traffic filters. In this case, functionality equivalent to [R-5G-49], [R-5G-50] and [R-5G-51] is to be supported.

Network Access Model

Applying RG-level 5G QoS characteristics implies the RG is represented as an interface on the AGF on which these QoS characteristics are enforced. This is more natural for a customer (1:1) VLAN but requires means to uniquely identify subscribers (RGs) on an N:1 VLAN. RG type specific considerations follow:

5G-RG: This consists of a PPPoE control session, used for NAS and AS procedures and session liveness detection, and one or more PDU sessions, where the combination of the PPPoE control session and PDU sessions are subject to the RG-level QoS characteristics.

FN-RG: An L3 RG is assumed with a single VLAN supporting one IPoE based IP session or multiple PPPoE based IP sessions, in both cases supporting dual stack. For the service (N:1) VLAN access model (i.e., separate VLANs to the RG for data, voice, IPTV, etc.), it is modelled as a separate

subscription per VLAN therefore a separate traffic contract represented in a separate RG-LWAC instance per VLAN is assumed.

For a collocated AGF and UPF, the SMF configures each PDU session with a session-AMBR that limits the aggregate bandwidth for Non-GBR QoS Flows for that session. This is retrieved from the UDM via SMF during session Initiation and signaled to the combined AGF + UPF over N4. This means each PDU session may be represented by its own interface to enforce PDU session level QoS characteristics and support accounting or usage-based monitoring requirements. These PDU sessions are, in turn, subject to RG-level QoS characteristics applied by the AGF during RG Registration over N2 that precedes PDU session Initiation.

QoS Representation on AGF

Multiple QoS models should be assumed, influenced by provider network topologies and QoS requirements for their network. Service providers with a traditional BNG migrating to WWC using 5GC may have a heterogeneous mix of 5G-RGs and FN-RGs and may potentially want to converge on a common QoS model for ease of migration and management of the subscribers.

A common wireline network technique used by providers represent the subscriber RG as an interface on which a shaper is applied with traffic classes represented as queues with configured attributes to honor the QoS requirements commensurate with a subscription plan, service tier, or contracted arrangement with a third-party access provider. Nevertheless, the approach should allow for a policer to be used in lieu of or in combination with a shaper. In the upstream direction a policer is typically used.

A provider typically has a relatively small set of subscription plans or service tiers that can be realized from a combination of local configuration and external authority, where external authority can supplement, override or fully source the QoS characteristics for the subscriber. Means to source the information from external authority can be in the form of individual parameters or references to locally configured templates, profiles or containers, each configured with the required QoS characteristics to meet the service plan. A similar technique should be supported on the AGF to avoid having to source all RG-level configuration from UDM, which, as features and use cases continue to be identified, will only expand over time. Thus, means to combine and reconcile AMF-sourced RG-LWAC with AGF-local configuration maximizes flexibility while avoiding redundant and excessive operator configuration of UDM under scale.

Finally, AGF vendor differences in representing and applying RG-LWAC QoS characteristics is to be expected, which means either “converting” RG-LWAC QoS characteristics to align with the AGF (-U) QoS implementation or providing flexibility to source vendor specific attributes. Referencing the name of a template, profile or container configured on the AGF that specifies QoS configuration and other supporting configuration suitable for the vendor’s implementation is an option to help accommodate such differences. Vendor differentiation and/or operational practice may also require AGF local implementation that is used in conjunction with or in lieu of RG-LWAC information. This technique should prove useful for providers that are already accustomed to configuring common profiles/templates assigned to groups or classes of subscribers for conventional, wireline broadband access that may be supplemented or overridden on a per-subscriber basis from external authority.

6.6 AGF functions for core network signaling

[R-59] The AGF MUST support the same functions for control plane signaling over the N2 interface as defined in TS 23.501 [28] and TS 38.410, 412,413 ([14], [15], [16]). In these reference documents, NG-RAN is to be replaced by AGF.

Note: The TS 29.413 [20] defines how to apply the NGAP protocol (TS 38.413 [16]) for non-3GPP access.

A summary is provided here about the relevant functions, procedures and protocol aspects defined in the above specifications and how they are applicable for AGF. In any case of conflict, the referenced 3GPP R16 specifications have precedence.

- The AGF must support functions to discover, connect and maintain reliable and redundant connections to multiple sets of AMFs, serving one or more network slices.

    a. The AGF must be able to derive and maintain a list of AMFs, to which it must maintain connections over N2 interface. At least one of the below options must be supported:

        i. DNS based discovery as defined in TS 29.303 [19] , clause 7.2 and Annex F.

        ii. Configuration knowledge of AMFs.

    b. AGF must support IP and transport layer requirements for N2 interface, as defined in TS 38.412 [15].

        i. AGF should support multiple SCTP associations (TNLA) towards an AMF and add new ones as requested by AMF. The AGF must request adding additional endpoints using the “RAN configuration update procedure” (see below).

        ii. The AGF must support NGAP UE-TNLA-binding as described in TS 23.501 clause 5.21 [28].

- The AGF must support the following major functions as listed in clause 5 of TS 38.410 [14], with the corresponding procedures defined in clause 8, and N2 messages defined in clause 9.2 of TS 38.413 [16] – as detailed below:

    a. Non-UE-associated services

        i. NG Interface Management functions (TS 38.413 [16] clause 8.7 and 9.2.6) that allows resetting the N2 connection, handling different implementation versions and protocol errors.

        ii. AMF Management function to support AMF planned removal (TS23.501 [28], clause 5.21.2.2 and TS38.413 [16] clause 8.7.6.2) and AMF auto-recovery (TS23.501 [28], clause 5.21.2.3),

        iii. Multiple TNL Associations Support function, supported via AMF and RAN configuration update procedure (TS38.413 [16], clause 9.2.6.4-9) to add/remove SCTP end point on AGF and AMF side and load balance the UE associated signaling across these associations.

        iv. AMF Load Balancing function (TS 38.413 [16] AMF relative capacity in clause 8.7.1 and 8.7.3 and 9.2.6.2/9.2.6.7) to support the indication by the AMF of its relative capacity to the AGF in order to achieve load-balanced AMFs within the pool area.

    b. UE-associated services

        i. NAS Node (i.e., AMF) Selection function (TS 23.501 [28] clause 6.3.5 and 5.15.5.2), to ensure that the AMF supports the requested network slices. For the selection, the AGF must take the AMF configuration and status information into account.

        ii. AMF Re-allocation function (TS 38.413 [16] clause 8.6.5 and 9.2.5.5), to allow that the RG gets served by a different AMF than the one that initially received the registration request.

        iii. NAS Transport function (TS 38.413 [16] clause 8.6 and 9.2.5), which supports transport and reroute of NAS messages between 5G-RG and AMF, or AGF-adaptive mode for FN-RG and AGF, respectively.

        iv. UE Context Management function (TS 38.413 [16] clause 8.3 and 9.2.2), which enabled the AMF to establish, modify and release UE context in the AMF and the AGF for individual RG related signaling.

Note: RRC state notifications are N/A for AGF.

v. PDU Session Management function (TS 38.413 [16] clause 8.2 and 9.2.1) for establishing, modifying and releasing the involved PDU session related AGF/W-5GAN resources for user data transport once a UE context is available in the NG-RAN node.

vi. Trace function (TS 38.413 [16] clause 8.11 and 9.2.10) to control trace sessions in AGF.

Note: the other functions in clause 5 of TS38.410 [14], Paging, Mobility Management, Warning Message Transmission, Configuration Transfer, Location Reporting, UE Radio Capability Management, Report of Secondary RAT data volumes and RIM Information Transfer functions are not applicable for AGF.

6.7 N2 connections

The AGF needs to fulfil the following requirements about N2 interface:

[R-60] The AGF MUST support Transport Network Layer Associations (TNLA) as defined in TS 38.412 [15].

[R-61] The AGF SHOULD support multiple TNLAs per AMF and TNLA load balancing.

[R-62] The AGF MUST support dynamic AMF discovery either via DNS (TS29.303 [19]) or statically via OAM based configuration.

[R-63] The AGF MUST support NGAP UE-TNLA-binding as described in 23.501 [28] clause 5.21.

[R-64] The AGF MUST support NGAP as defined for W-AGF (3GPP terminology for AGF) in TS 29.413 [20].

[R-65] The AGF (acting as a NG RAN as defined in TS 38.413 [16] and for the features to be supported by a Non 3GPP AN as defined in TS 29.413 [20]) MUST support maintaining up-to-date information of the AMFs it is connected to, in terms of:

- Served GUAMIs
- Backup AMF name
- Supported network slices
- Relative capacity
- Overload status
- Operational status.

6.8 AGF support for slicing and AMF selection

This section specifies the requirements for AGF support of slicing and AMF selection.

The AGF makes use of the Requested NSSAI and GUAMI to select an AMF. For FN-RG, in the current issue of specification, the AGF does not need the Requested NSSAI to select the AMF.

While for an FN-RG these parameters have to be set or retrieved directly by the AGF, for a 5G-RG, the AGF retrieves them within PPP VSNP (see sections 8.2.1 and 8.2.2) sent by the 5G-RG itself. In case the 5G-RG does not send any of these parameters or the corresponding AMF(s) cannot be determined or reached, then the AGF might end up with selecting an AMF among a set of default AMFs.

The 5G-RG or the AGF acting as a UE on behalf of an FN-RG and the AGF acting as a 5G AN follow the 5GC procedures specified by 3GPP for network slicing (specified in TS23.501 [28] clause 5.15).

[R-66] As a 5G AN, the AGF MUST support AMF selection as specified by TS 23.501 [28] clause 6.3.5 (AMF discovery and selection), clause 5.15 (Slice impacts on AMF selection).

[R-5G-54] If the AGF can reach an AMF corresponding to the GUAMI received from the 5G-RG (refer to TS 23.316 [25] clause 7.2.1.1 5G-RG registration procedure via W-5GAN or TS 23.316 [25] clause on Service Request), then the AGF MUST run the NGAP Initial UE procedure to establish an NGAP association for the 5G-RG with this AMF and forward the NAS signaling received from the 5G-RG to this AMF over N2. Otherwise, the AGF MUST select an AMF based on the requirements [R-5G-56] and [R-5G-57].

[R-5G-55] The AGF MUST support GUAMI identifying an individual AMF or GUAMI identifying multiple AMF(s) (within an AMF set).

[R-5G-56] If the AGF cannot reach an AMF corresponding to the GUAMI received by the 5G-RG or does not receive a GUAMI from the 5G-RG, then as specified by TS 23.501 [28] clause 5.15, the AGF MUST select an AMF on the basis of the Requested NSSAI, and run the NGAP Initial UE procedure (as defined in TS 29.413[20]/38.413[16]) to establish an NGAP association for the 5G RG with this AMF and forward the NAS signaling received from the 5G-RG.

[R-5G-57] If the AGF is not able to select an AMF based on the Requested NSSAI or based on the GUAMI received from the 5G-RG or does not receive these parameters from the 5G-RG, then the AGF MUST select from a set of default AMFs (configured locally) and run the NGAP Initial UE procedure (as defined in TS 29.413[20]/38.413[16]) to establish an NGAP association for the 5G RG with this AMF and forward the NAS signaling received from the 5G-RG.

[R-67] The AGF MUST be able to receive over N2 from current AMF the request to redirect an Initial NAS message to a different AMF, according to the Reroute NAS Request procedure defined in clause 8.6.5 of TS 38.413 [16].

[R-FN-52] The AGF MUST store the GUAMI of the serving AMF when the N2 connection for the RG is established.

[R-FN-53] When the AGF performs a Registration procedure on behalf of an FN-RG, the AGF SHOULD NOT provide any Requested NSSAI.

[R-FN-54] For a PPPoE based FN-RG, if an NAI was presented with the credentials in the PPP authentication phase, and the IP session initiation was successfully authenticated by any additional authentication procedures, the NAI realm MUST be compared with any DNN route selection policy URSP rules:

- If a DNN selection URSP Route Selection Descriptor is associated with the rule, that DNN is used in the PDU Session Establishment Request
- If a network slice selection URSP Route Selection Descriptor is associated with the rule, that value will be provided as the S-NSSAI

Where either DNN or S-NSSAI is not indicated by the URSP rules, it is left to the AMF to provide the defaults.

Note: The use of URSP in both a route selection descriptor and in a policy rule is currently precluded in TS23.503, but relaxing this restriction is currently under consideration by 3GPP.

[R-FN-55] When the AGF performs a PDU SESSION ESTABILISHMENT REQUEST (documented in clause 7.3.4 of TS 23.316 [25]) on behalf of an IPoE FN-RG, the AGF SHOULD provide as S-NSSAI the Allowed S-NSSAI that the 5GC indicated in the REGISTRATION ACCEPT.

[R-FN-56] The AGF MUST NOT include any DNN in the PDU SESSION ESTABLISHMENT REQUEST made on behalf of an IPoE FN-RG.

Note: The network operator MUST ensure that a default DNN is provisioned for the default S-NSSAI of the FN-RG's UDM record. The AMF will use that DNN for the PDU session

[R-FN-57] When the AGF performs a PDU SESSION ESTABILISHMENT REQUEST (documented in clause 7.3.4 of TS 23.316 [25]) on behalf of a PPPoE based FN-RG where NAI information was not presented in the PPP authentication phase, the AGF MUST NOT include DNN or S-NSSAI information in the PDU SESSION ESTABLISHMENT REQUEST allowing the AMF to establish the DNN and slice based upon the subscription defaults and local policy.

If a change in the subscription information occurs that implies a slice-specific authentication and authorization failure or revocation, as documented in TS 24.501 clause 5.5.2.3.1, the AGF as proxy UE will be requested from the 5GC to de-register the FN-RG via a DEREGISTRATION REQUEST, which indicates the rejected NSSAI IE. The 5GC also indicates whether a re-registration is needed or not.

[R-FN-58] The AGF MUST support NETWORK-INITIATED DEREGISTRATION procedure due to slice-specific authentication and authorization failure or revocation, as documented in TS 24.501 clause 5.5.2.3.1. In case the NETWORK-INITIATED DEREGISTRATION REQUEST indicates that a re-registration is needed, the AGF MUST start a new Registration.

If a change in the subscription information about the DNN associated with the Allowed NSSAI occurs, the AGF as proxy UE will be requested from the 5GC to release the PDU session via a NETWORK-INITIATED PDU SESSION RELEASE REQUEST.

[R-FN-59] The AGF MUST support a NETWORK-INITIATED PDU Session release procedure due to slice specific authorization failure. After the PDU session release, the AGF SHOULD initiate PDU session.

6.9 Connection Management State on AGF

Connection Management depicts UE status with respect to its signaling with AMF 5G Core Node and influences the NAS signaling messages the AGF sends to 5GC on behalf of the FN-RG to manage the connections.

When the AGF operates in adaptive mode, it maintains both Connection Management state and Registration Management state on behalf of the FN-RG along with FN-RG's N1 Proxy PDU Session Context(s).

TR-456 issue 2 introduces the possibility for an FN-RG to request multiple PDU sessions. However, the CM state of the AGF is mainly influenced by the first or the last session fate.

Figure 21 shows the CM state machine of an AGF playing the role of proxy UE for an FN-RG in case of a single PDU session, or of the first and final remaining session. In case of incoming or outgoing sessions other than the first or the final ones, the CM state for the FN-RG does not change. The diagram details the allowed state transitions with the triggers (on the user side) and the relevant actions taken by the AGF.

Note that, with reference to the event of outage (e.g., KA failure) of the last session, the diagram represents two different options of AGF behavior, which may result in different implementations, both compatible with the 3GPP 5G recommendations.

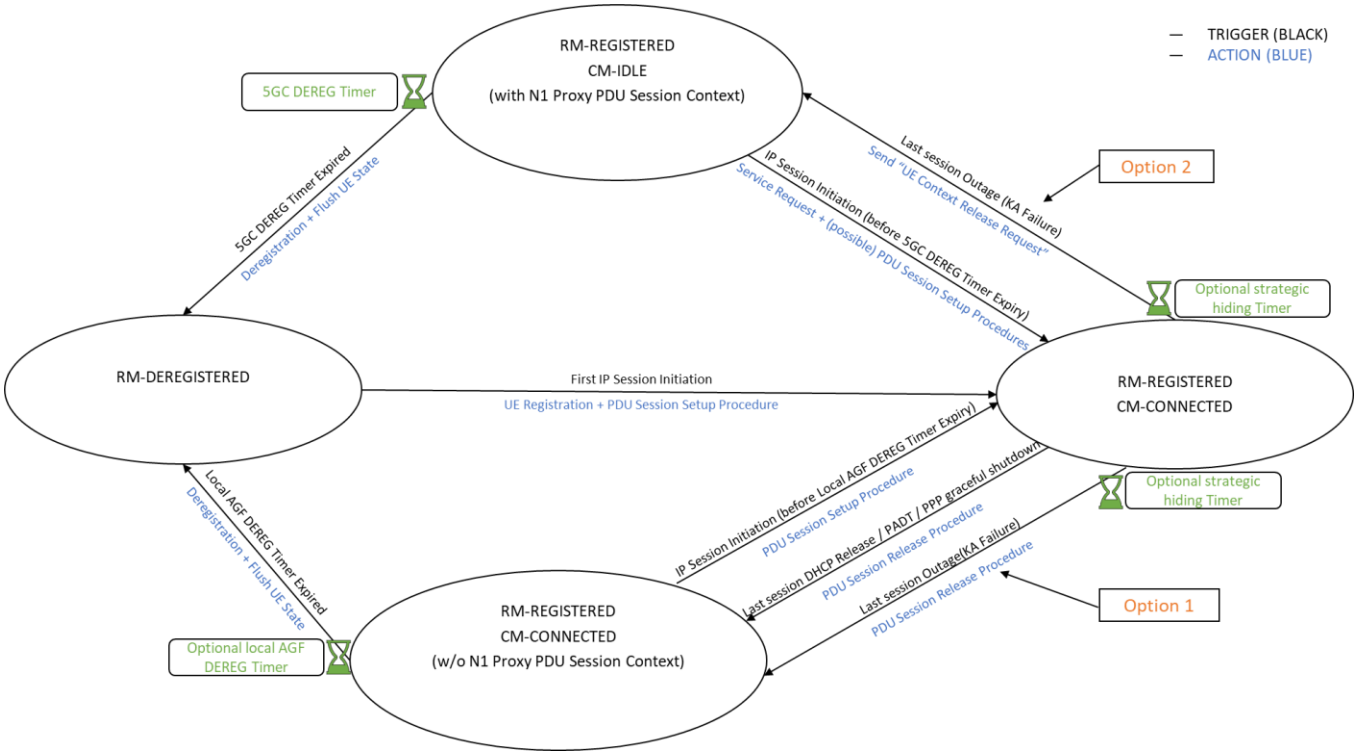

Figure 21: RM/CM state transitions for FN-RG with Single/Last PDU Session

In addition to the non-3GPP Deregistration timer foreseen by the 3GPP 5G recommendations, which starts when the AGF transitions to the CM-IDLE state (Option 2), the AGF may hold a local deregistration timer (Local AGF DEREG Timer) for FN-RG when maintaining the CM-CONNECTED state with no PDU sessions (bottom state in Figure 21). In this case, 5GC does not run the non-3GPP deregistration timer as the UE appears connected to 5GC. The local DEREG AGF timer helps in reducing the signaling towards the 5GC in case of flapping on the access side.

Note that in the AGF state machine there may be an internal transition between two flavors of the “CM-CONNECTED state”, which, from the point of view of 5GC, is not detected as a transition of CM state. Moreover, while in CM-CONNECTED state with at least one PDU session in place (right state in Figure 21), the AGF may implement a strategic hiding timer triggered by the (last) IP connection failure before taking any action (either Option 1 or Option 2). Strategic hiding is an implementation choice that may also help in reducing the signaling towards the 5GC.

The AGF CM state machine can be further simplified if the last session release or outage triggers a direct Deregistration instead than a PDU Session Release followed by a Deregistration. This is also possible with no impact on the 5GC point of view. If an Implementer chooses this simplified state machine, the two optional timers (Strategic hiding and Local AGF DEREG timers) collapse.

Finally, note that when transitioning to CM-IDLE state as a result of the UE Context Release procedure (Option 2), both the AGF and 5GC will start the non-3GPP deregistration timer.

6.9.1 PPPoE based FN-RG

An FN-RG based on PPPoE can access more than one DNN/Slice pair using different PPPoE sessions, see section 6.11. The change of state can be triggered by various events that may happen on the access side (e.g., connection faults detected by PPP keepalive failures) or in the AGF (e.g., timer expiration), or by the reception of explicit signaling messages such as PPPoE session requests, PPP graceful shutdown or PADT messages. The change of state can be triggered also by network-initiated procedures.

Table 5 describes the triggers for AGF change of state and the actions the AGF might take toward the 5GC due to these triggers. For simplicity, the underlying assumption for Table 5 is that each AGF action with 5GC is successful.

Initial AGF State	Trigger	Actions taken by AGF	Final AGF State
RM-Deregistered	PPPoE session request	Registration Request followed by PDU Session Establishment Request	RM-Registered, CM-Connected
RM-Registered, CM-Connected	PPPoE session request for a new service (i.e., another DNN/Slice pair)	PDU Session Establishment Request for the new DNN/Slice	RM-Registered, CM-Connected
	PPP graceful shutdown or PADT for other than the last PPP session	PDU Session Release	RM-Registered, CM-Connected
	Keepalive failure for other than the last PPP session	PDU Session Release	RM-Registered, CM-Connected
	PPP graceful shutdown or PADT for the last PPP Session	PDU Session Release followed by a Deregistration optionally executed after an internal timer expiration. A variation can be a direct Deregistration, optionally executed after an internal timer expiration.	RM-Deregistered
	Keepalive failure for the last PPP session	OPTION 1: PDU Session Release followed by a Deregistration optionally executed after an internal timer expiration. A variation can be a direct Deregistration, optionally executed after an internal timer expiration.	RM-Deregistered
		OPTION 2: UE Context Release procedure optionally executed after an internal timer expiration	RM-Registered, CM-Idle
	Network Requested PDU Session Release for other than the last PPP session	Withstanding the network request for PDU Session Release	RM-Registered, CM-Connected
	Network Requested PDU Session Release for the last PPP session	PDU Session Release followed by a Deregistration optionally executed after an internal timer expiration	RM-Deregistered
	Any triggers for Deregistration (see section 8.1.9 for the list)	Withstanding the network request	RM-Deregistered
RM-Registered, CM-Idle	PPPoE session request	Service Request (to re-establish the NAS connectivity), possibly followed by a PDU Session Establishment Request	RM-Registered, CM-Connected
	Implicit Deregistration timer expires	Deregistration Request	RM-Deregistered
	Any triggers for Deregistration (see section 8.1.9 for the list)	Withstanding the network request	RM-Deregistered

Table 5: CM State Transitions for PPPoE based FN-RG

6.9.2 IPoE based FN-RG

This section considers DHCPv4 as a trigger to initiate an IP session. This is extendable to DHCPv6 and SLAAC as triggers but not documented.

An FN-RG based on IPoE can access only one DNN/Slice pair. The change of state can be triggered by various events that may happen on the access side (e.g., connection faults detected by BFD, ping, or other methods) or in the AGF (e.g., timer expiration), or by the reception of explicit signaling messages such as a DHCP Release. The change of state can be triggered also by network-initiated procedures.

Table 6 describes triggers for AGF state change and the actions the AGF might take towards the 5GC due to these triggers. For simplicity, the underlying assumption for Table 6 is that each AGF action with 5GC is successful.

Initial AGF State	Trigger	Actions taken by AGF	Final AGF State
RM-Deregistered	DHCP discover	Registration Request followed by PDU Session Establishment Request	RM-Registered, CM-Connected
RM-Registered, CM-Connected	DHCP lease expiry	AGF acts as a DHCP relay and allows the SMF/DHCP server to take actions. The SMF is expected to trigger the Network Requested PDU Session Release procedure. After that, the AGF performs a Deregistration, optionally after an internal timer expiration.	RM-Deregistered
	IP connectivity fault detected (via BFD, ping, etc)	OPTION 1: PDU Session Release followed by a Deregistration optionally executed after an internal timer expiration. A variation can be a direct Deregistration, optionally executed after an internal timer expiration.	RM-Deregistered
		OPTION 2: UE Context Release procedure optionally executed after an internal timer expiration	RM-Registered, CM-Idle
	Network Requested PDU Session Release	PDU Session Release followed by a Deregistration optionally executed after an internal timer expiration	RM-Deregistered
	Any triggers for Deregistration (see section 8.1.9 for the list)	Withstanding the network request	RM-Deregistered
RM-Registered, CM-Idle	DHCP discover	Service Request Procedure. Possibly followed by a PDU Session Establishment Request (for example if the old IP address lease expired in the SMF/DHCP server).	RM-Registered, CM-Connected
	Implicit Deregistration timer expires	Deregistration Request	RM-Deregistered
	Any triggers for Deregistration (see section 8.1.9 for the list)	Withstanding the network request	RM-Deregistered

Table 6: CM State Transitions for IPoE based FN-RG

6.9.3 AGF Connection Management State requirements

With regards to the AGF CM state changes, the following requirements apply to AGF for both IPoE and PPPoE based FN-RGs:

[R-FN-60] The AGF SHOULD supervise the wireline connectivity in cases of IP session initiation with PPPoE and in cases of IP session initiation with IPoE.

[R-FN-61] Upon detecting a loss of connectivity for all active IP sessions, the AGF SHOULD start the AN Release procedure as documented in TS 23.316 [25] clause 7.2.5.3 and in clause 8.1.12 (FN-RG AN Release via W-5GAN).

Note: As an alternative, the AGF may initiate a PDU Session Release followed by a Deregistration, optionally executed after an internal timer expiration. A variation of this alternative is a direct De-Registration Procedure.

In all cases, when the last access-side session has been detected as lost, an optional internal timer may be started before starting the AN Release or the PDU Session Release or the Deregistration procedure. Waiting for the timer expiration reduces the signaling load toward 5GC in case of access flapping.

[R-FN-62] Upon receiving the N2 UE Context Release command from the AMF, the AGF SHOULD flush the FN-RG N2 context, keeping the N1 context until the non-3GPP Implicit Deregistration timer expires.

[R-FN-63] Upon receiving the N2 UE Context Release command from the AMF, the AGF proxy NAS termination that acts on behalf of the FN-RG SHOULD change state from (RM-REGISTERED, CM-CONNECTED) to (RM-REGISTERED, CM-IDLE).

[R-FN-64] The non-3GPP Implicit Deregistration timer MUST use the default value or the value received from the AMF in the NAS Registration Accept message (as documented in TS 24.501[11] clause 8.2.7.17).

[R-FN-65] When the non-3GPP Implicit Deregistration timer expires, the AGF MUST enter the RM-DEREGISTERED state and flush the local 3GPP context.

While the AGF is in (RM-REGISTERED, CM-IDLE) state, it may receive an IP connection request; this will always trigger a Service Request procedure and have the effect of re-establishing the NAS. However, if the IP connection request is for a dormant session (i.e., a session already requested before the AGF entered CM-IDLE state), the AGF will be able to serve the request with data previously received from the 5GC and stored locally. Otherwise, if the IP connection request is for a service never accessed since its registration or the IP address previously assigned expired in the 5GC, the AGF will have to issue a PDU Session Establishment request via NAS to let the user access that service.

[R-FN-66] While in (RM-REGISTERED, CM-IDLE) state, if the AGF receives an IP connection request, the AGF proxy NAS termination MUST issue a Service Request on behalf of the FN-RG on the N1 interface to restore the NAS and become aware of the state of the PDU sessions on 5GC, avoiding a new Registration on 5GC.

[R-FN-67] In case from the Service Request procedure the AGF determines there are no PDU sessions active on the 5GC related to the requested service, the AGF MUST issue a PDU Session Establishment request to service the IP connection request from the FN-RG.

[R-FN-68] While in (RM-REGISTERED, CM-IDLE) state, upon resuming the PDU session or establishing a new one, the AGF MUST transition back to the (RM-REGISTERED, CM-CONNECTED) state.

[R-FN-69] If the wireline connectivity is restored after expiration of the AGF Implicit Deregistration timer, the AGF SHOULD start a NAS initial Registration procedure, as documented in TS 23.316 [23] Clause 7.2.1.3 and section 8.1.6 (Registration Management Procedure for FN-RG).

6.10 Detection of FN-RG equipment change

[R-FN-70] Upon receipt of a PPPoE PADI for a given Line ID, if the FN-RG is in the RM-REGISTERED state, the AGF MUST check whether the FN-RG MAC in the PADI message corresponds to the MAC address associated with the registration. If different, the AGF performs FN-RG deregistration procedures.

[R-FN-71] Upon receipt of a DHCPv4 discover for a given Line ID, if the FN-RG is in the RM-REGISTERED state the AGF MUST check the client-identifier option 61, if present, or chaddr field in the DHCP discover message against the last registered client-identifier option 61 or chaddr for the FN-RG. If different, the AGF performs FN-RG deregistration procedures.

[R-FN-72] Upon receipt of a DHCPv6 Solicit for a given Line ID, if the FN-RG is in the RM-REGISTERED state the AGF MUST check the DUID field in the DHCP solicit message against the last registered DUID for the FN-RG. If different, the AGF performs FN-RG deregistration procedures.

[R-FN-73] Upon receipt of an ICMPv6 RS (SLAAC) for a given Line ID, if the FN-RG is in the RM-REGISTERED state the AGF MUST check the FN-RG MAC Ethernet header against the last registered MAC for the FN-RG. If different, the AGF performs FN-RG deregistration procedures.

[R-FN-74] When an IP session trigger is received in the RM-DEREGISTERED/CM-IDLE state, the AGF MUST store the identity of the FN-RG gleaned as per [R-FN-70] through [R-FN-72] for the duration of the Registration.

6.11 FN-RG IP session initiation requirements

The following requirements apply when an AGF is performing FN-RG IP session initiation procedures:

[R-FN-75] The AGF, when formulating the PDU Session Establishment Request documented in clause 7.3.4 of TS 23.316 [25] on behalf of an FN-RG, MUST be able to determine the PDU Session Type by a local configuration.

[R-FN-76] The AGF MUST support configuration of the PDU Session Type (IPv4, IPv6 or IPv4v6) on a logical or physical interface. The default PDU session type is IPv4v6.

[R-FN-77] When establishing the PDU session, the AGF MUST conform to the Selected PDU Session Type indicated by the PDU Session Establishment Accept received from the 5GC.

[R-FN-78] The AGF, when formulating the PDU Session Establishment Request documented in clause 7.3.4 of TS 23.316 [25] on behalf of an FN-RG using PPPoE or PPPoL2TP encapsulation, MUST use the Extended Protocol Configuration Option “IP address allocation via NAS signaling”.

[R-FN-79] The AGF, when formulating the PDU Session Establishment Request documented in clause 7.3.4 of TS 23.316 [25] on behalf of an FN-RG using IPoE encapsulation, MUST NOT request IP addressing via NAS signaling. In the PCO container the AGF MUST explicitly indicate its willingness to have a deferred IP address allocation mode.

[R-FN-80] If when the IP session has been initiated with PPPoE or PPPoL2TP, the PDU Session Establishment Accept indicates that FN-RG is not allowed to use IPv4 stack (Selected PDU Session Type=IPv6), the AGF MUST reply to the FN-RG IPCP Configuration Request with an LCP Protocol Reject.

[R-FN-81] If when the IP session has been initiated with PPPoE or PPPoL2TP, the Session Establishment Accept indicates that FN-RG is not allowed to use IPv6 stack (Selected PDU Session Type=IPv4), AGF MUST reply to the FN-RG IPv6CP Configuration Request with an LCP Protocol Reject.

[R-FN-82] When the IP session has been initiated with PPPoE or PPPoL2TP, the AGF MUST assign the IPv4 address received from the 5GC in the PDU Session Establishment Accept to the FN-RG when replying to the FN-RG IPCP Configuration Request.

[R-FN-83] When the IP session has been initiated with PPPoE or PPPoL2TP, the AGF MUST NOT acknowledge the initial IPv6CP Configuration Request sent by the FN-RG, replying with a Configuration-Nak.

[R-FN-84] In the IPv6CP Configuration-Nak specified in [R-FN-83], the AGF MUST assign to the FN-RG the Interface Identifier received from the 5GC in the PDU Session Establishment Accept.

[R-FN-85] When the IP session has been initiated with PPPoE or PPPoL2TP, and the FN-RG is allowed to use IPv6 stack (Selected PDU Session Type=IPv6 or IPv4v6), the AGF MUST send an IPv6CP Configuration Request to FN-RG, self-assigning as Interface Identifier the SMF IPv6 LLA information received from the 5GC in the PDU Session Establishment Accept.

[R-FN-86] The AGF MUST forward the Router Advertisement containing the IPv6 Prefix assigned to the FN-RG by the 5GC.

Note: RFC 4861 [49] would require the 5GC to start sending RAs as soon as possible. This will occur in parallel to any DHCPv6 exchange and start as soon as a PDU session is set up as the SMF is the source of RAs, regardless of whether an IPv6 Prefix is assigned. Therefore, RAs will occur in advance of or in parallel with DHCPv6 exchange.

[R-FN-87] If the Router Advertisement specified in [R-FN-86] includes the Source Link-Layer Address Option and the FN-RG uses PPPoE or PPPoL2TP encapsulation, the AGF MUST remove the option before forwarding the RA message to the FN-RG.

[R-FN-88] If the FN-RG allowed session type is IPv6 or IPv4v6, the AGF SHOULD forward any Router Solicitation sent by the FN-RG to the 5GC.

[R-FN-89] If the access protocol suite is IPv6oE and the Router Solicitation sent by the FN-RG as specified in [R-FN-88] contains the Source Link-Layer Address Option, the AGF SHOULD remove it before sending the message to the SMF.

[R-FN-90] The AGF MUST relay the DHCPv6 messages exchanged between 5GC and the FN-RG if the session type is IPv4v6 or IPv6.

Note: [R-FN-86], [R-FN-87], [R-FN-88], [R-FN-89] and [R-FN-90] apply to both session initiation and maintenance throughout session lifetime

For FN-RG procedures, the Line ID information is a requirement for Registration and PDU Session Initiation. As described in TR-470 section 7.1, the Line ID is derived from metadata added by deployed access equipment that allows the client-facing interface to be identified. This metadata information is inserted by the Access Node in every eligible message transmitted by the FN-RG to initiate an IP session (including PPPoE PADI and PADR, Router Solicitation, DHCPv4 control packets such as DISCOVER, REQUEST, etc. and DHCPv6 control packets such as SOLICIT, REQUEST, etc.).

In the FN-RG IP session initiation procedures described in the section 8.1, the Access Node must be configured to add the relevant metadata necessary to derive the FN-RG Line ID. This is actually a necessary condition, without which the AGF cannot serve FN-RGs.

Depending on the encapsulation protocol used and possibly on the type(s) of IP stack(s) requested by the FN-RG, the following cases can occur:

1. FN-RG uses PPPoE encapsulation. In this case, the Access Node is expected to support the PPPoE Intermediate Agent function, as FN-RG uses PPPoE encapsulation specified in TR-101 issue 2 section 3.9.2 and 3.9.3. This is a necessary condition to allow the AGF to serve an FN-RG that requests the IPv4 stack or the IPv6 stack or both using PPPoE protocol.

2. FN-RG uses PPPoE encapsulation and the backhaul to the AGF uses L2TP. In this case, the Access Node is expected to support the PPPoE Intermediate Agent function. The L2TP Access

Concentrator opening the L2TP tunnel is required to add the Circuit ID AVP and/or the Remote ID AVP extracted from the PPPoE messages to the ICRQ message, as per RFC 5515 [58], sent to the L2TP Network Server (LNS) serving as an AGF.

3. FN-RG uses IPoE encapsulation. In this case, the Access Nodes must support:

   a. The Layer2 DHCP Relay Agent function, as specified in TR-101 issue 2 section 3.9.1 and 3.9.3. This is a necessary condition to allow the AGF to serve an FN-RG that requests the IPv4 stack using DHCPv4 protocol.

   b. The Lightweight DHCPv6 Relay Agent (LDRA) function, as specified in TR-177 Issue 1 Corrigendum 1 section 5.6.1 and as per RFC 6221 [55]. This is a necessary condition to allow the AGF to serve an FN-RG that requests the IPv6 stack directly using DHCPv6 protocol.

   c. The Line Identification Option (LIO) insertion in the Router Solicitation messages as requested by TR-177 Issue 1 Corrigendum 1 and as per RFC 6788 [56]. This is a necessary condition to allow the AGF to serve an FN-RG that requests the IPv6 stack using SLAAC. Note that subsequently the FN-RG could use DHCPv6 protocol to request a Delegated Prefix.

Note: For FN-RGs not using PPPoE encapsulation, there is not uniform behavior about the use of a Router Solicitation (RS) or a DHCPv6 Solicit as a first indication of the intention to establish an IPv6 session: some FN-RGs require receipt of an RA prior to initiating DHCPv6 procedures, some others send a DHCPv6 Solicit message without having received any RA.

Any order in the stack requests by the FN-RG is possible: a dual-stack FN-RG might request IPv4 stack prior to IPv6 or vice versa, and it might also request only one of the two stacks.

A dual-stack FN-RG using PPPoE encapsulation will indicate the intention to initiate an IPv4 IP session using an IPCP Configuration Request and the intention to initiate an IPv6 IP session using an IPv6CP Configuration Request: both types of requests are sent within the context of the same PPP session. The AN will insert the metadata necessary to derive the FN-RG Line ID in the PADI and PADR messages that initiate the session. Therefore, the metadata are inserted once, independently of the number and the order of the stacks requested by the FN-RG.

For a dual-stack FN-RG using IPoE encapsulation, there is not an underlying layer that binds the stack requests coming from the same FN-RG. The FN-RG will indicate the intention to initiate an IPv4 IP session using a DHCPv4 Discover and the intention to initiate an IPv6 IP session using either a DHCPv6 Solicit or a Router Solicitation possibly followed by a DHCPv6 Solicit. The AN, on its part, will insert the metadata necessary to derive the FN-RG Line ID in each eligible upstream control packet that initiates a request for a stack. For a dual-stack FN-RG, that means the AN will insert the metadata:

- in the DHCPv4 Discover message and in the RS message, or
- in the DHCPv4 Discover message and in the DHCPv6 Solicit message, or
- in the DHCPv4 Discover message, in the RS message and in the DHCPv6 Solicit message (if any).

Note: Receiving independent messages with common Line ID allows the AGF to discriminate households even if the N:1 VLAN model is used. In case of 1:1 VLAN model, the logical interface on the access side where the various initiation messages are received would be sufficient to allow the AGF to correlate the independent session initiation procedures with a common subscription and PDU session.

Given the AN behavior and the different encapsulation types the FN-RG might use, the AGF will have to handle all possible cases with regard to the type and the order of IP stack requests.

A PPPoE based FN-RG may initiate more than one PPP based IP session and will use NAI realm information in the credentials presented during the PPP authentication phase to indicate the DNN and slice

the IP session should map to. If NAI realm information is not present and there is not an existing session to the defaulted DNN and Slice, then the DNN and S-NSSAI for the PDU session will not be communicated by the AGF to the AMF and revert to a combination of subscription defaults and local policy at the AMF.

An IPoE based FN-RG may initiate more than one IP session where each session is VLAN delineated. This is modelled as multiple subscriptions in the 5G System with each subscription having a default DNN and slice associated with it. This is achieved by the use of a unique GLI based SUPI per subscriber VLAN.

If the FN-RG state is RM-DEREGISTERED/CM-IDLE on the AGF, any message initiating an IP session (PADI, DHCPv4 Discover, DHCPv6 Solicit, Router Solicitation) sent by the FN-RG will trigger the registration as well as the PDU session establishment procedure on the AGF. By means of the reply to the latter request, the AGF is made aware of the types of IP stacks the user subscription permits and maps the allowed IP sessions with a single PDU session, supporting those stacks. While the FN-RG is in RM-REGISTERED state on the AGF, any other message initiating an IP session never triggers a new registration.

Once in RM-REGISTERED state, the FN-RG may transition between CM-IDLE and CM-CONNECTED states as explained in section 6.9 (Connection Management State on AGF). The transitions may be triggered not only by detected changes in the wireline connectivity, but also by the receipt of a new PADI, or DHCPv4 Discover, or DHCPv6 Solicit, or Router Solicitation.

When detecting one of these messages, the AGF determines if there has been a change of the FN-RG equipment, checking one or more of the following information fields (if present): the source MAC address at the Ethernet layer of the packet, the Option 61 or the Client Hardware field (alias chaddr) in the DHCPv4 Discover, the DHCP Unique Identifier (alias DUID) in the DHCPv6 Solicitation, the FN-RG Link Local Address (LLA) and any other indication that it may be useful to the scope.

In the following text, the information used by the AGF to identify the specific FN-RG is termed as “customer equipment identifier” irrespective of the source parameter used (for example, the MAC address, option 61 client-identifier, or DUID).

If the FN-RG state is RM-REGISTERED/CM-IDLE on the AGF, a message initiating an IP session (PADI, DHCPv4 Discover, DHCPv6 Solicit, Router Solicitation) sent by the FN-RG triggers the AGF NAS proxy acting on behalf of the FN-RG to perform the Service Request Procedure, if the customer equipment identifier is the same used for the Registration.

Besides triggering the Service Request Procedure, the AGF establishes the requested IP session(s) and restores the user plane continuity between the GTP-U on the network side and the IP session(s) on the access side. In the case of PPPoE, the association is made on the basis of the presence or absence of an NAI realm in the credentials presented during the PPP authentication phase. The NAI realm is used in conjunction with URSP rules to associate the NAI realm with the PDU session on the basis of DNN and S-NSSAI. At the end, the FN-RG state on the AGF is RM-REGISTERED/CM-CONNECTED. Else if the customer equipment identifier of the packet initiating the new IP session is different from the one used for the Registration, the AGF triggers a De-Registration and enters the RM-DEREGISTERED/CM-IDLE state. Subsequently, the AGF can register the FN-RG and issue a PDU session establishment again, moving to RM-REGISTERED/CM-CONNECTED state.

If the FN-RG state is RM-REGISTERED/CM-CONNECTED on the AGF, it means the AGF has in place at least an IP session mapped to a PDU session. If it receives a message initiating an IP session (PADI, DHCPv4 Discover, DHCPv6 Solicit, Router Solicitation) from the FN-RG, this might be the sign of one of a number of different scenarios. Here a distinction is needed on the basis of the FN-RG encapsulation.

1) FN-RG using PPPoE encapsulation – The new PADI can be

    a) an indication of a change of the FN-RG device,

    b) an indication of the restoration from a fault not detected by the AGF,

c) an indication of an additional PPP based IP session initiation request from the same household.

- If the customer equipment identifier is different from the one used for Registration, then the AGF assumes the customer has changed FN-RG device. The AGF will therefore trigger a De-Registration and enter the RM-DEREGISTERED/CM-IDLE state. Subsequently, the AGF can register the FN-RG and issue a PDU session establishment again, moving to RM-REGISTERED/CM-CONNECTED state.

- If the customer equipment identifier is the same used for Registration, and the DNN and S-NSSAI associated with the presented NAI realm correspond to that of an IP session already mapped to the PDU session, then the AGF may issue immediately an ICMP echo request to check the liveliness of the FN-RG on the PPP session already in place. If it receives a reply, then the AGF assumes the PADI as a new session request and it will ignore it. If it does not receive any reply, then the AGF assumes the PADI as an indication of the restoration from an undetected fault.

  In the latter case, the default behavior of the AGF is performing a De-Registration followed by a new Registration and a new PDU session establishment request.

  Optionally, when the AGF becomes aware of an undetected fault, the AGF may setup a new PPP session with the same information context of the previous PPP session and map it to the PDU session already in place. It will use the stored session state in the proxy NAS termination for NCP exchange etc. with the FN-RG.

  As an alternative to the use of ICMP echo requests, the AGF may simply wait for the pre-existing session LCP Echo Requests to expire. A PADI received in the CM-CONNECTED case is silently discarded.

- If the customer equipment identifier is the same used for Registration, and the DNN and S-NSSAI associated with the presented NAI realm do not correspond to an established IP session already mapped to the PDU session, then the IP session initiation will proceed with the AGF using the stored parameters associated with the PDU session, if available, when opening the NCPs for the IP session and the IP session will be mapped to the PDU session. If the parameters are not available, the AGF will send a PDU-SESSION-ESTABLISHMENT REQUEST with the new requested DNN and NSSAI.

  In all cases, the FN-RG ends up in the RM-REGISTERED/CM-CONNECTED state.

2) FN-RG using IPoE encapsulation – The new DHCPv4 Discover or DHCPv6 Solicit or Router Solicitation can be an indication the FN-RG requests to add a new stack, or an indication of a change of the FN-RG device, or an indication of the restoration from a fault not-detected by the AGF, or an indication of a second IP session request from the same household.

- If customer equipment identifier is different from the one used for Registration, then the AGF assumes the customer has changed FN-RG device. The AGF will therefore trigger a De-Registration and enter the RM-DEREGISTERED/CM-IDLE state. Subsequently, the AGF can register the FN-RG and issue a PDU session establishment again, moving to RM-REGISTERED/CM-CONNECTED state.

- If customer equipment identifier is the same used for Registration and the message initiates a different type of stack, then the AGF may simply map the IP session to the existing PDU session, if this is IPv4v6 type.

- If customer equipment identifier is the same used for Registration and the AGF has already mapped the requested IP stack with the PDU session, the new message will be handled by the IP addressing function of the 5GC. It is assumed this function will limit the IP addresses and IPv6 prefixes assigned to the FN-RG aligning with the number of PDU session requested by the AGF

(which in this specification issue is limited to one). It is also assumed this function behaves as a standard DHCPv4/DHCPv6 server and therefore gracefully accepts renegotiation without any N1 signaling.
Optionally, when the AGF becomes aware of an FN-RG renegotiation intention, the AGF may perform a De-Registration followed by a new Registration and a new PDU session establishment request.

The following requirements codify the description above:

[R-FN-91] The AGF MUST be able to map the IPv4 and IPv6 IP sessions initiated by the same FN-RG to a common DNN and S-NSSAI to a common IPv4v6 PDU session.

[R-FN-92] The AGF MUST NOT initiate more than one PDU session to a given DNN/S-NSSAI tuple on behalf of an FN-RG.

[R-FN-93] If the AGF has in place a PDU session to a given DNN/S-NSSAI tuple, it MUST ignore subsequent IP session initiations from the FN-RG towards the same DNN/S-NSSAI tuple, unless it detected loss of connectivity in the access segment on that IP session. In this case the AGF MUST either release the existing PDU session and start over coordinating the PDU session initiation with the IP session initiation; OR map the IP session initiation to the existing PDU session using stored session context.

[R-FN-94] If the FN-RG state is RM-DEREGISTERED on the AGF, and if the AGF receives a message initiating an IP session (and in the case of PADI, subsequent exchange until the RG type can be ascertained by LCP exchange), the AGF MUST perform the Registration Procedures in addition to the PDU session establish procedures on behalf of the FN-RG.

Note: the messages initiating an IP session can be the following: PPPoE PADI, DHCPv4 Discover, DHCPv6 Solicit, or ICMPv6 Router Solicitation.

[R-FN-95] If the FN-RG state is RM-REGISTERED/CM-IDLE, if the AGF receives a message initiating an IP session and the customer equipment identifier is the same used for the Registration, then the AGF SHOULD perform the Service Request procedure on behalf of the FN-RG. The AGF will use the retained state in the proxy NAS termination to correctly associate the IP session initiation with the PDU session that is restored by the service request procedures.

Note: the messages initiating an IP session can be the following: PPPoE PADI, DHCPv4 Discover, DHCPv6 Solicit, or ICMPv6 Router Solicitation.

[R-FN-96] If the FN-RG state is RM-REGISTERED/CM-IDLE and the FN-RG uses IPoE encapsulation, if the AGF detects a resumption of traffic from the FN-RG, then the AGF SHOULD perform the Service Request procedure on behalf of the FN-RG and map the FN-RG IP session to the appropriate PDU session instance

[R-FN-97] While the FN-RG state is RM-REGISTERED/CM-CONNECTED on the AGF, if the AGF has in place an IP session mapped to an IPv4v6 PDU session and receives from the FN-RG a message initiating a different stack, the AGF MUST add the second stack to the mapping as per [R-FN-91].

[R-FN-98] While the FN-RG state is RM-REGISTERED/CM-CONNECTED on the AGF and the FN-RG uses IPoE encapsulation, if the AGF receives a trigger to initiate an IP session for a protocol not supported by the PDU session type, the AGF will silently discard the message.

[R-FN-99] While the FN-RG is in the RM-REGISTERED state on the AGF, if the FN-RG has initiated an IPv6 session via an RS or a DHCPv6 Solicitation and in the PDU SESSION ESTABLISHMENT ACCEPT the 5GC indicates that FN-RG is not allowed to use the IPv6 stack (Selected PDU Session Type=IPv4), the AGF SHOULD NOT deregister the FN-RG.

[R-FN-100] While the FN-RG is in the RM-REGISTERED state on the AGF, if the FN-RG has initiated an IPv4 session via a DHCPv4 Discover and in the PDU SESSION ESTABLISHMENT ACCEPT the 5GC indicates that FN-RG is not allowed to use the IPv4 stack (Selected PDU Session Type=IPv6), the AGF SHOULD NOT deregister the FN-RG.

6.11.1 NAS back off timers and FN-RG support

In normal 5G enabled end system, the NAS timers are tightly coupled to NAS behaviours. NAS timers can be associated with control plane congestion, or the rejection of requests as a result of policy (lack of resources or business issues). In general, the purpose of these timers is to protect the 5GC against spurious requests not likely to be honoured due to some temporary constraint by getting the UEs to “back off”.

In an AGF running in adaptive mode, the NAS stack is only loosely coupled to IP session initiation transactions originating with an FN-RG. But some degree of loose coupling needs to be maintained. Therefore, the action an AGF takes is to silently discard IP session initiation attempts from an FN-RG when a timer indicating a “back off” as a consequence of a previous rejection is still active. Further, upon expiry of the timer the AGF simply resumes accepting IP session initiation requests from the FN-RG instead of taking any independent action. This is in order to preserve some coupling with FN-RG behaviour. The silent discard of IP session requests can have varying granularity depending on the previous rejection. This can range from all requests to only requests pertaining to a specific DNN and slice. The circumstances of the initiation of NAS “back off” timers are documented in TS. 24.501 [11]. The timers of interest for WWC are listed in the appendix 10.1.

[R-FN-101] An AGF MUST silently discard an IP session initiation attempt if any of the following NAS timers are running that indicate either rejection or control plane congestion: T3247, T3346 or T3502 [11].

[R-FN-102] An AGF MUST silently discard an IP session initiation attempt to a specific DNN if any of the following NAS timers are running for that DNN that indicate control plane congestion: T3396 timer [11] or the “generic back off” timer.

[R-FN-103] An AGF MUST silently discard an IP session initiation attempt to a specific DNN & slice if the T3584 timer [11] (insufficient resources) is running for that DNN/slice.

[R-FN-104] An AGF MUST silently discard an IP session initiation attempt to a specific slice if the T3585 timer [11] (insufficient resources) is running for that slice.

[R-FN-105] Upon expiry of all of the above-mentioned timers, an AGF MUST resume processing of IP session initiation attempts.

6.12 Void

This section is intentionally blank.

6.13 Combined AGF/UPF

AGF and UPF functions can be combined into a single implementation. The UPF is then called “co-located”. Co-location happens on a per PDU session basis. This model is described in detail in TR-470 section ‘Combined AGF/UPF’, including the concept of AGF identities parameter (WAgfInfo), as defined by 3GPP in TS 38.413 clause 9.2.5.3 [16] and TS 29.510 [22].

[R-68] When an AGF does not support UPF co-location, it MUST NOT send the WAgfInfo parameter to the AMF.

When the AGF supports UPF co-location, the following requirements apply:

[R-69] The AGF MUST send the WAgfInfo parameter to AMF in the N2 message transporting the PDU Session Establishment Request as described in TS 23.316 [25] clause 7.3.4 (step 1).

[R-70] The AGF MUST send the WAgfInfo parameter to AMF in the N2 message transporting the Registration Request message as described in TS 23.316 [25] clause 7.2.1.

[R-71] The combined AGF-UPF MUST support UPF as specified in TS 23.501 [28], as well as the specific aspects linked to wireline access described in TS 23.316 [25].

[R-72] The AGF MUST support an externally connected UPF via an N3 interface to support the case where SMF does not select the co-located UPF.

[R-73] The combined AGF-UPF MUST support framed routing.

[R-74] The combined AGF-UPF MUST indicate to SMF the support of framed routing by setting the FRRT flag in the UP Function Features IE, as documented in TS 29.244 [17].

7 Migration consideration

Operational simplicity for support of migration and reverse migration between FN-RGs and 5G-RGs is achieved by the deployment of an AGF that supports both direct and adaptive modes of operation and can auto-sense the class of CPE that is currently connected to a subscriber drop.

Autosensing of the CPE is a feature of the protocol design such that the initiation of 5G-RG registration procedures can be distinguished from FN-RG session initiation. Similarly, the procedures have been designed such that a 5G-RG can detect if it is being served by an AGF or a legacy BNG.

The AGF then tracks the CPE class on a per Line ID basis. This is formally described in section 7.1 (The Migration state machine).

7.1 The Migration state machine

An AGF that is configured to support both Direct and Adaptive modes, maintains a state table for each Line ID. This does not have to be persistent across AGF restarts as it is assumed that upon failure followed by restoration the RG will reinitiate either registration or session initiation procedures and therefore identify the class of CPE to the AGF. The Line ID is considered to be invariant through the migration process as it is unaffected by the class of CPE served. It is assumed that only one class of CPE may be connected to an access facility identified by a Line ID at any one time.

When FN-RG based subscribers are initially migrated to the 5GC but prior to CPE upgrade, the UDM will be prepopulated with subscription information where each subscription is indexed by a SUPI constructed from the associated Line ID, or IMSI based SUPI for which the Line ID is used as pseudonym. At this point, the subscriber connectivity in the access network may be re-directed to a standalone AGF, either via network provisioning, or steering to an AGF implemented internal to a BNG.

At the time of forward migration an independent subscription record is created in UDM with a SUPI created from the IMSI of the 5G-RG. Alternatively, the existing IMSI based SUPI can be reused to identify also the 5G-RG subscription. At this point the migration (and possible reverse migration) process between the specifically identified 5G-RG and an FN-RG becomes fully automated and may occur with no further network provisioning. This enables a customer self-install model.

The state machine involves three states:

A. Class of CPE is unknown.

B. Class of CPE is FN-RG

C. Class of CPE is 5G-RG

A transition from a previous known CPE state to another state includes the explicit or implicit de-registration of the CPE in the previous known state. For example, if a Line ID was in the FN-RG state and the AGF detected the initiation of 5G-RG registration procedures, it would de-register the FN-RG subscription.

The actual state machine implemented per Line ID in the AGF is illustrated in Figure 22:

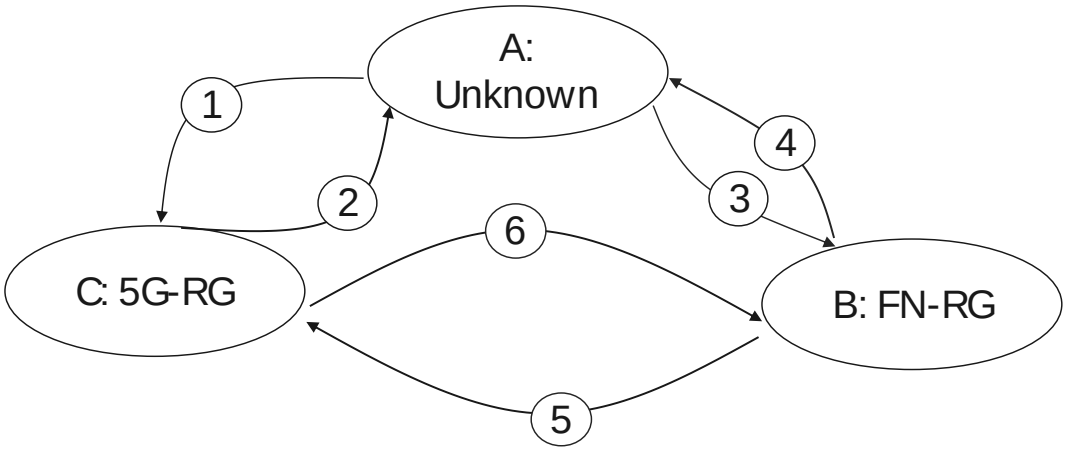

Figure 22: AGF Migration State Machine

A direct C-B transition can only occur when an FN-RG authoritatively indicates it is initiating an IP session and this has occurred prior to the AGF detecting a loss of the CP PPPoE session connectivity, which implies a loss of NAS connectivity between the 5G-RG and the AMF. This is achieved if the FN-RG initiates a PPPoE session without the LCP 5G VSO present during LCP negotiations. In this scenario the AGF reports loss of the wireline connectivity to the AMF via an N2 Context Release Request and the AMF starts the deregistration timer for the 5G-RG. In parallel, the AGF starts the FN-RG registration.

Table 7 details the set of triggers for a state transition between the states shown in Figure 22. In the following table, it is assumed that the FN-RG or 5G-RG comply with the LCP procedure described in section 5.3 to allow AGF autodetect the type of RG that is initiating the connection. A further possibility is that an IPoE based FN-RG is auto-detected by the AGF via the receipt of IPoE DHCP or SLAAC transactions as described in section 6.9.2.

It should be noted that these transitions are AGF-centric. Scenarios may exist whereby both an FN-RG and 5G-RG subscription may be in the registered state simultaneously as far as the overall 5G system is concerned: one class of RG being in the CM-CONNECTED state and homed on an AGF, and one in the CM-IDLE state and not associated with an AGF and with an associated deregistration timer. These scenarios are expected to be transitional.

#	Transition	Trigger (external from AGF)	Steps with References	Result
1	Unknown → 5G-RG	5G-RG initiates registration procedures	5G-RG Registration Requirements: sect. 6.4.1 Procedure call flows: sect. 8.2.1	5GC: 5G-RG is in RM-REGISTERED, CM-CONNECTED state. AGF supports the subscription associated with the Line ID in direct mode.
2	5G-RG → Unknown	Case 1) 5G-RG or 5GC performs de-registration procedures Case 2) Loss of connectivity in the wireline network detected	Case 1: Explicit deregistration Requirements: 6.4.1 Procedure call flows: 8.2.5 Case 2: AN release when loss of	(Case 1) 5GC: 5G-RG is put into RM-DEREGISTERED state (Case 2) 5GC: 5G-RG is put into CM-IDLE state and will be deregistered when deregistration timer expires. (Steps 3-5 of section 8.2.5) AGF is agnostic with regard

			connectivity detected Requirements: 6.4.1 Procedure call flows: 8.2.8	to the Class of CPE associated to the Line ID.
3	Unknown → FN-RG	FN-RG performs IP session initiation	IP session initiation Requirements: 6.11 PPP Procedure Call Flows: 8.1.1, 8.1.2 IPoE Procedure Call Flows: 8.1.3, 8.1.4	5GC and AGF: FN-RG is put into RM-REGISTERED, CM-CONNECTED state AGF supports the subscription associated with the Line ID in adaptive mode.
4	FN-RG → Unknown	Case 1: Abnormal session termination due to loss of connectivity Case 2: IP sessions is explicitly terminated by the FN-RG or 5GC initiates de-registration procedures	(Case 1) AGF may perform the AN Release procedure or may de-register the FN-RG after a timer expiration (see section 6.9) Requirements: Sect. 6.9.3 Call flow: Section 8.1.12 (Case 2): The AGF proxy UE or 5GC initiates deregistration procedures Requirements: 6.9.3 Call flow: Section 8.1.9	(Case 1) 5GC and AGF: FN-RG is put into CM-IDLE state and will be deregistered when timers expire. Alternatively, AGF hides the fault until an internal timer expires, and then de-register the FN-RG (Case 2) 5GC: FN-RG is put into RM_DEREGISTERED state AGF is agnostic with regard to the Class of CPE associated to the Line ID.
5	FN-RG → 5G-RG	5G-RG initiates registration procedures with FN-RG currently registered	Step 1) FN-RG AGF initiated deregistration: Requirements: sect. 6.9 Procedure Call Flows: sect. 8.1.9 Step 2) 5G-RG Registration Requirements: sect. 6.4.1 Procedure call flows: sect. 8.2.1	5GC: FN-RG is put into RM_DEREGISTERED state 5GC: 5G-RG is put into RM-REGISTERED, CM-CONNECTED state AGF supports the subscription associated with the Line ID in direct mode.
6	5G-RG → FN-RG	FN-RG initiates IP session with 5G-RG currently registered	Step 1) AGF reports loss of 5G NAS connectivity Requirements: Sect 6.4.1 Procedure call flows: Sect. 8.2.8 Step 2) AGF proxy performs registration & PDU session establishment Requirements: 6.11 PPP Procedure Call Flows: 8.1.1, 8.1.2	5GC: 5G-RG is put into CM-IDLE state and deregistration timer started. 5GC: FN-RG is put into RM-REGISTERED, CM-CONNECTED state AGF supports the subscription associated with the Line ID in adaptive mode.

Table 7: Triggers for AGF state machine transitions

Note: these are high level transitions, a failure to complete a state change once initiated results in a transition to the “Unknown” state.

Note: in the “Unknown” state, no UP packets or frames are relayed by the AGF

[R-FN-106] The AGF SHOULD always proceed with de-registration in case of detection of a new Class of CPE on a line with a certain Line ID, even if it is able to implement mechanisms to postpone the proxy UE initiated de-registration (see section 6.9).

8 Procedures and call flows

This section discusses procedures and call flows for FN-RG and 5G-RG. Some AGF-CP/AGF-UP steps which are further described in TR-458 [10] are not shown here.

8.1 For an FN-RG

Note the following procedures only apply to an AGF that has been configured to support adaptive mode. In all the FN-RG IP session initiation procedures documented in this section, for simplicity, the process that allows the AGF to auto-detect the RG operating as FN-RG is not detailed.

8.1.1 FN-RG IP Session Initiation with PPPoE

Figure 23 shows the call flow for the FN-RG IP session initiation with the AGF based on PPPoE message exchange.

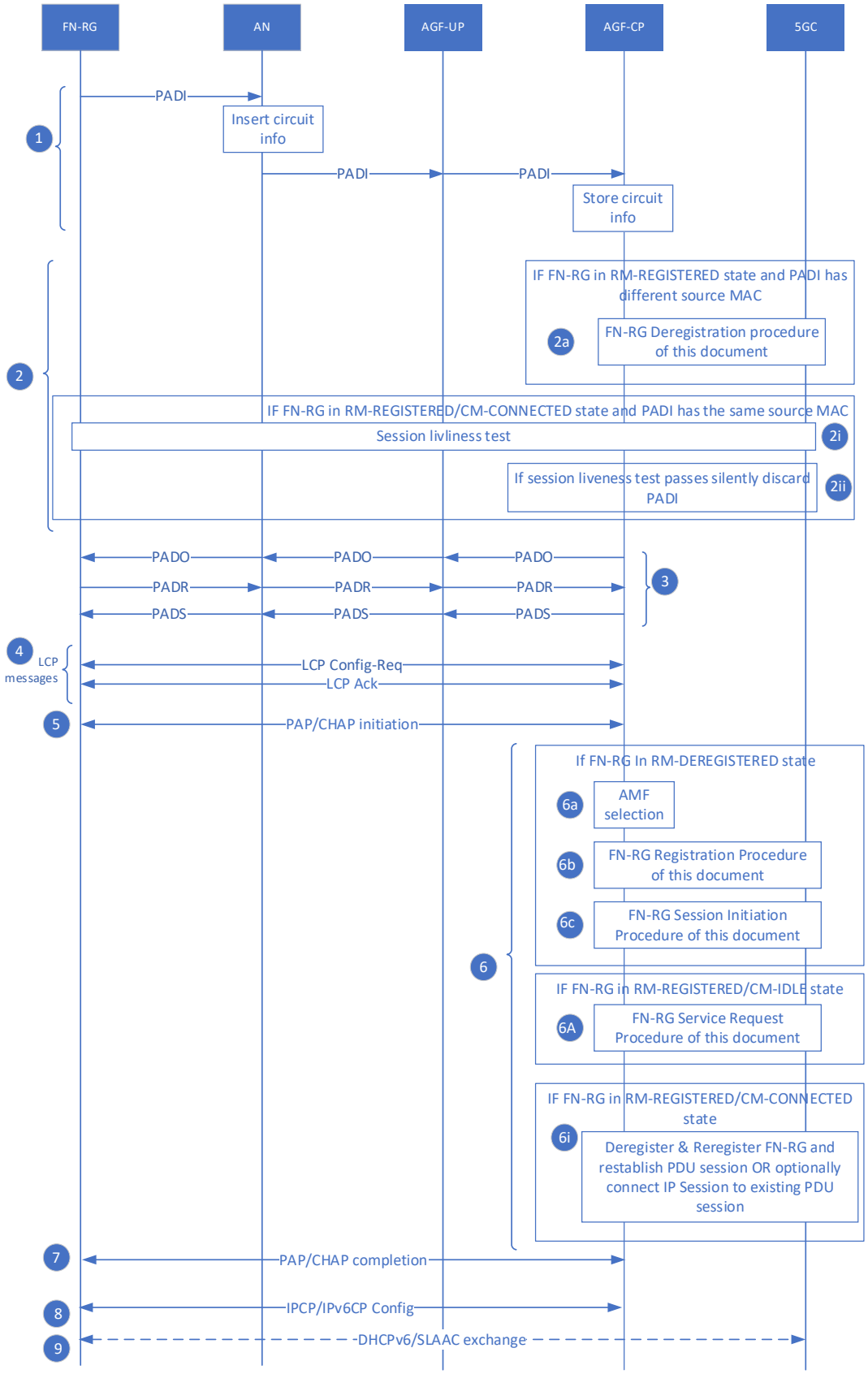

Figure 23: Call flow for FN-RG IP session initiation with PPPoE

1. The FN-RG starts a PPPoE session and begins with a PADI message based on section 5 of RFC 2516 [42].

   The AN receives the PPPoE PADI message and inserts PPPoE tags into the PADI message and forwards the entire message to the AGF-CP. The PPPoE tags include the PPPoE Circuit and Remote ID tag as defined in TR-101 issue 2. This PPPoE tags are treated as Line ID as specified in TR-470 [9].

   On receiving the PADI message, the AGF-CP will store the subscriber's information (FN-RG MAC address, TCI, port & Line ID) obtained from the Ethernet header and PPPoE tags.

2. The AGF will check the validity of the PADI.

   2a. If the MAC address of the FN-RG in the PADI has changed and the FN-RG is in the RM-REGISTERED state, the AGF interprets this as an equipment change and executes the AGF-CP initiated FN-RG Deregistration Procedure described in this document before proceeding to step 3.

   2i. If the MAC address is the same, and the FN-RG is in the RM-REGISTERED state the AGF may ensure this is not a second session initiation by performing an ICMP Ping on any pre-existing session.

   2ii. If the ICMP ping elicits a response from the FN-RG, then this PADI is silently discarded, else the previous IP session is assumed to have failed.

   Note: An alternative technique would be to simply silently discard a PADI received in the RM-REGISTERED/CM-CONNECTED state. This requires the existing LCP-ECHO supervision mechanism to put the existing session into the CM-IDLE state before a PADI is accepted.

3. The PPPoE discovery process completes with the exchange of PADO, PADR and PADS messages between the FN-RG and the AGF.

4. After the PPPoE discovery process completes, both the AGF-CP and FN-RG establish the link layer with LCP packet message exchanges as described in section 5 of RFC 1661 [43].

   The LCP Configure-Request and Configure-Ack messages are exchanged between the FN-RG and AGF-CP via the AN.

   > For an FN-RG, there is no 5G Vendor Specific Option (VSO) included in the LCP Configure-Request, and it is the absence of the VSO that permits an FN-RG to be distinguished from a 5G-RG.

5. The PPP authentication phase starts with either a PAP message from the RG or a CHAP challenge issued by the AGF and a CHAP challenge response from the FN-RG

6. The AGF will then handle the IP session initiation according to the current registration and connection state:

   <u>If the state is RM-DEREGISTERED</u>

   > 6a. The AGF-CP selects an AMF as described in section 6.8 (based on TS 23.316 [25], clause 7.2.1.3).

6b. The FN-RG is registered into the 5GC based on the registration procedure described in section 8.1.6 (based on TS 23.316 [25], clause 7.2.1.3).

6c. Upon successful registration, the AGF validates the credentials presented by the FN-RG with either RADIUS or AACI information in the RG-LWAC. PDU session initiation does not proceed upon unsuccessful validation of credentials. That may result in immediate deregistration of the FN-RG, or transition to the CM-IDLE state. Upon successful validation of credentials, the AGF establishes a PDU session as defined in section 8.1.8 (based on TS 23.316 [25] clause 7.3.4). The formulation of PDU SESSION ESTABLISHMENT REQUEST by the AGF proxy NAS termination must adhere to the requirements documented in sections 6.8 (AGF support for Slicing and AMF Selection) and 6.11 (FN-RG IP session initiation requirements).

The 5GC, when formulating the reply to PDU SESSION ESTABLISHMENT REQUEST, considers the PDU session type requested by the AGF and the user's subscription data stored in UDM: the latter are authoritative.

From the PDU SESSION ESTABLISHMENT ACCEPT received by the 5GC the AGF learns the type of PDU session that the subscriber is permitted to: this information is in the Selected PDU Session Type field. One of the following three cases occur:

a. If the Selected PDU Session Type is IPv4, the 5GC network provides also an IPv4 address to the AGF. This IPv4 address can be fixed or dynamic, according to the user subscription. The AGF passes this IPv4 address to the FN-RG replying to the FN-RG IPCP Configuration Request and including it as value of the IP Address Option.

b. if the Selected PDU Session Type is IPv6, the 5GC in the PDU SESSION ESTABLISHMENT exchange will support LLA assignment as per the requirements in section 6.3.2.1 (L2/L3 Interworking).

   The AGF will store this information at least until the IPv6CP phase is completed.

c. If the Selected PDU Session Type is IPv4v6, the AGF will use all the information passed by the 5GC in the PDU SESSION ESTABLISHMENT ACCEPT to configure the FN-RG IPv4 address, the FN-RG IPv6 Interface Identifier and its own IPv6 LLA, as explained in the previous items a and b.

<u>If the state is RM-REGISTERED/CM-IDLE</u>

6A. The AGF performs the Service Request Procedure for FN-RG in this document upon successful validation of any user credentials.

<u>If the state is RM-REGISTERED/CM-CONNECTED</u>

6i. Upon successful validation of any user credentials supplied, if the S-NSSAI and DNN correspond to an existing PDU session, the AGF may deregister and re-register the FN-RG and reestablish the PDU session (if this was the only PDU session active) OR MAY simply connect the IP session to the existing PDU session.

If the S-NSSAI and DNN associated with the IP session initiation do not correspond to an existing PDU session, PDU session establishment procedures are performed as described in step 5c above.

7. The AGF communicates the result of PAP/CHAP authentication to the FN-RG.

   Note: If the selected PDU session type is IPv6 or IPv4v6, the 5GC is expected to initiate an unsolicited Route Advertisement (RA) that may contain a RA prefix. In any case, the RA will be sent as a response to the RS initiated by the FN-RG.

8. The FN-RG will then proceed into opening the NCPs for the IP session.

   If the PDU SESSION ESTABLISHMENT ACCEPT indicates that FN-RG is not allowed to use IPv4 stack (Selected PDU Session Type=IPv6), AGF will reply to the FN-RG IPCP Configuration Request with an LCP Protocol Reject. Else in the IPCP phase over PPP the address information obtained from the original PDU SESSION ESTABLISHMENT ACCEPT is provided to the FN-RG.

   If the SESSION ESTABLISHMENT ACCEPT indicates that FN-RG is not allowed to use IPv6 stack (Selected PDU Session Type=IPv4), AGF will reply to the FN-RG IPv6CP Configuration Request with an LCP Protocol Reject and the remaining steps are skipped. Else in the IPv6CP phase over PPP:

   - The FN-RG will typically construct an Interface Identifier and the LLA from the WAN MAC address and offer the Interface Identifier in a Configuration Request. The AGF will not acknowledge the request and will provide the Interface Identifier received from the 5GC.

   - The AGF will also send an IPv6CP Configure Request to FN-RG including the Interface Identifier from the SMF IPv6 LLA information obtained from the PDU SESSION ESTABLISHMENT ACCEPT message.

   Note: The IPv6 LLA of the SMF is not negotiable nor is the assigned FN-RG Interface Identifier provided to the AGF by the SMF.

9. This step might occur only if the IPv6 Interface Identifier gets configured in the IPv6CP phase session. If so, the AGF will pass the IPv6 control traffic exchanged between the FN-RG and the 5GC, changing the encapsulation type from PPP to GTP-U and vice versa. The 5GC will remain responsible for any allocation of IPv6 addresses to the FN-RG, regardless of if via SLAAC or DHCPv6. The FN-RG will receive RA and DHCPv6 messages sourced by the SMF IPv6 LLA; the SMF will receive RS and DHCPv6 messages sourced by the FN-RG LLA.

   a. SLAAC: An ICMPv6 Router Advertisement (RA) containing an Ipv6 Prefix (default prefix length is /64) is signaled by the SMF to UPF and sent by UPF to AGF via the downlink GTP-U tunnel associated with the PDU Session. The Ipv6 prefix can be fixed or dynamic, according to the user subscription. The AGF-UP forwards the RA to the FN-RG, changing the underlaying encapsulation.

      If the RA from the SMF contains the Source Link-Layer Address Option, the AGF removes it before sending the message to FN-RG.

      Note: any RS message sent by the FN-RG will be forwarded to the 5GC by the AGF, which will change the underlaying encapsulation. If the RS from the FN-RG contains the Source Link-Layer Address Option, the AGF removes it before sending the message to the SMF.

      Note: the AGF may snoop the RA sent by the SMF for troubleshooting and/or security purposes.

b. DHCPv6: the FN-RG sends a DHCPv6 Solicit containing either a DHCPv6 IA_NA or a DHCPv6 prefix delegation option to request an Ipv6 address and/or an Ipv6 delegated prefix. The AGF-UP relays the DHCPv6 messages exchanged between 5GC and the FN-RG, changing the underlaying encapsulation.

8.1.2 FN-RG IP session initiation using L2TP

In 5GC interworking, the LNS is replaced by the AGF function which provides the control and user plane for mobile and fixed network traffic. This section outlines the procedural steps for legacy FN-RG interworking between the AGF and existing access nodes implementing an L2TP integration. This section details the authentication and session management procedures.

Note: Unlike the scenarios whereby the AGF is directly connected to an Ethernet ‘V’ interface, the AGF will have no direct visibility of the Ethernet layer. This means the use of the FN-RG MAC address as a PEI and to detect equipment change is not an option.

The Figure 24 shows the full call flow for the registration management of an FN-RG and also session establishment. It utilizes PPPoE concatenated with an L2TP tunnel to start NAS registration with the 5GC, through the AGF interworking.

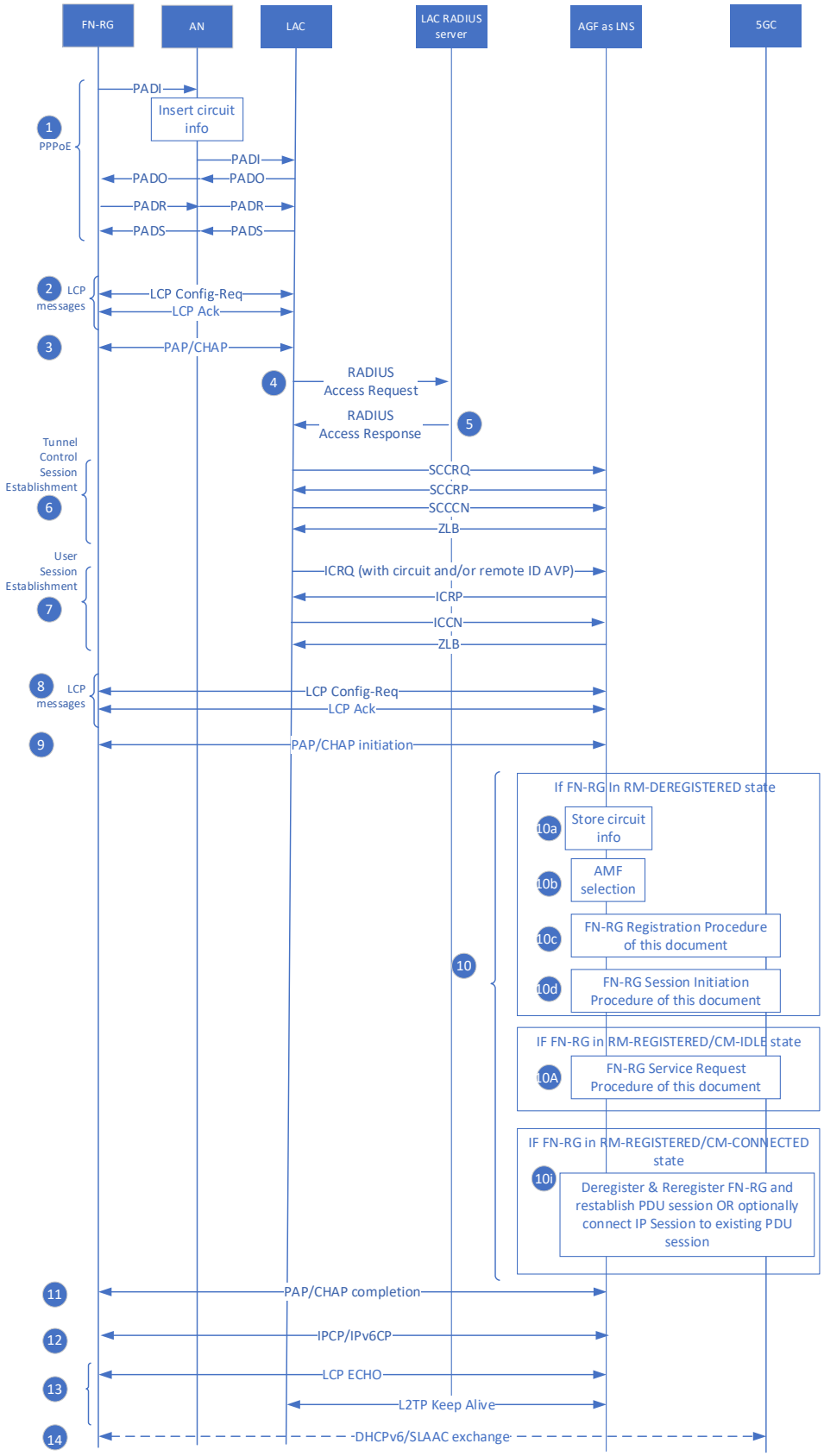

Figure 24: Call flow for the registration management procedure of an FN-RG (Legacy L2TP support).

The procedural steps as documented in Figure 24 follow their respective RFCs. In summary:

1. FN-RG initiates PPPoE client authentication initiation as per RFC 2516 [42] using Agent Remote ID or username as the service identifier, as in TR-101issue 2[ref].
2. PPP Link Control Protocol determines and agrees the standards of the ensuing data transmission, as in RFC 1661 [ref]
3. Authentication challenge (username/password) as (RFC 1661[43] & RFC 1994 [37])
4. LAC generates RADIUS Access Request (RFC 2865 [45])
5. RADIUS response specifies parameters for the L2TP tunnel to be established (RFC 2661 [44], & RFC 2868 [57])
6. L2TP tunnel control session established between LAC and LNS (RFC 2661 [44])
7. L2TP user sessions established between LAC and LNS (RFC 2661 [44])
8. (Optional) LCP re-negotiation procedures may take place with new network and per user parameters, if required, for the data plane; this requires the necessary functionality and can be triggered typically by the LNS device
9. The PPP authentication phase starts with either a PAP message from the RG or a CHAP challenge issued by the AGF and a CHAP challenge response from the FN-RG
10. The AGF will then handle the IP session initiation according to the current registration and connection state:

    If the state is RM-DEREGISTERED

    10a. The AGF-CP stores the circuit information associated with the registration. This would include LAC address, tunnel particulars, and line ID.

    10b. The AGF-CP selects an AMF as described in clause 7.2.1.3 of TS 23.316 [25].

    10c. The FN-RG is registered into the 5GC based on the registration procedure described in section 8.1.6 (based on TS 23.316 [25], clause 7.2.1.3).

    10d. Upon successful registration, the AGF validates the credentials presented by the FN-RG with either RADIUS or AACI information in the RG-LWAC. PDU session initiation does not proceed upon unsuccessful validation of credentials. That may result in immediate deregistration of the FN-RG, or transition to the CM-IDLE state. Upon successful validation of credentials, the AGF establishes a PDU session as defined in section 8.1.8 (based on TS 23.316 [25] clause 7.3.4). The formulation of PDU SESSION ESTABLISHMENT REQUEST by the AGF proxy NAS termination must adhere to the requirements documented in section 6.8 (AGF support for Slicing and AMF Selection) and section 6.11 (FN-RG IP session initiation requirements).

    The 5GC, when formulating the reply to PDU SESSION ESTABLISHMENT REQUEST, considers the PDU session type requested by the AGF and the user's subscription data stored in UDM: the latter are authoritative.

    From the PDU SESSION ESTABLISHMENT ACCEPT received by the 5GC the AGF learns the type of PDU session that the subscriber is permitted to: this information is in the Selected PDU Session Type field. One of the following three cases occur:

    - If the Selected PDU Session Type is Ipv4, the 5GC network provides also an Ipv4 address to the AGF. This Ipv4 address can be fixed or dynamic, according to the user subscription. The AGF passes this Ipv4 address to the FN-RG replying to the FN-RG IPCP Configuration Request and including it as value of the IP Address Option.

- if the Selected PDU Session Type is Ipv6, the 5GC in the PDU SESSION ESTABLISHMENT exchange will support LLA assignment as per the requirements in section 6.3.2.1 (L2/L3 Interworking).

  The AGF will store this information at least until the Ipv6CP phase is completed.

- If the Selected PDU Session Type is Ipv4v6, the AGF will use all the information passed by the 5GC in the PDU SESSION ESTABLISHMENT ACCEPT to configure the FN-RG Ipv4 address, the FN-RG Ipv6 Interface Identifier and its own Ipv6 LLA, as explained in the previous items a and b.

If the state is RM-REGISTERED/CM-IDLE

10A. The AGF performs the Service Request Procedure for FN-RG in this document upon successful validation of any user credentials.

If the state is RM-REGISTERED/CM-CONNECTED

10I. Upon successful validation of any user credentials supplied, if the S-NSSAI and DNN correspond to an existing PDU session, the AGF may deregister and re-register the FN-RG and reestablish the PDU session (if this was the only PDU session active) OR MAY simply connect the IP session to the existing PDU session.

If the S-NSSAI and DNN associated with the IP session initiation do not correspond to an existing PDU session, PDU session establishment procedures are performed as described in step 10d above.

11. The AGF communicates the result of PAP/CHAP authentication to the FN-RG.
12. IPCP configures Internet Protocol over PPP (RFC1332 [34]) and DNS resolver (RFC1877 [36])
13. The user session established, and data exchanged. Periodic PPP and L2TP keepalives are exchanged (RFC 1661[43] / RFC 2661 [44])
14. (Optional Ipv6 support) ICMPv6 RS/RA and/or DHCPv6 Exchange may take place to agree on Ipv6 addressing requirements for the session

Once a session is established, any changes in parameters, in-flight or through session restarts, arising from the AMF (5GC) will now be handled by AGF similar to any other type of FN-RG.

8.1.3 FN-RG IP Session Initiation with DHCPv4

Figure 25 shows the call flow for the FN-RG IP session initiation with the AGF based on DHCPv4, which subsequently leads to registration and session initiation procedures.

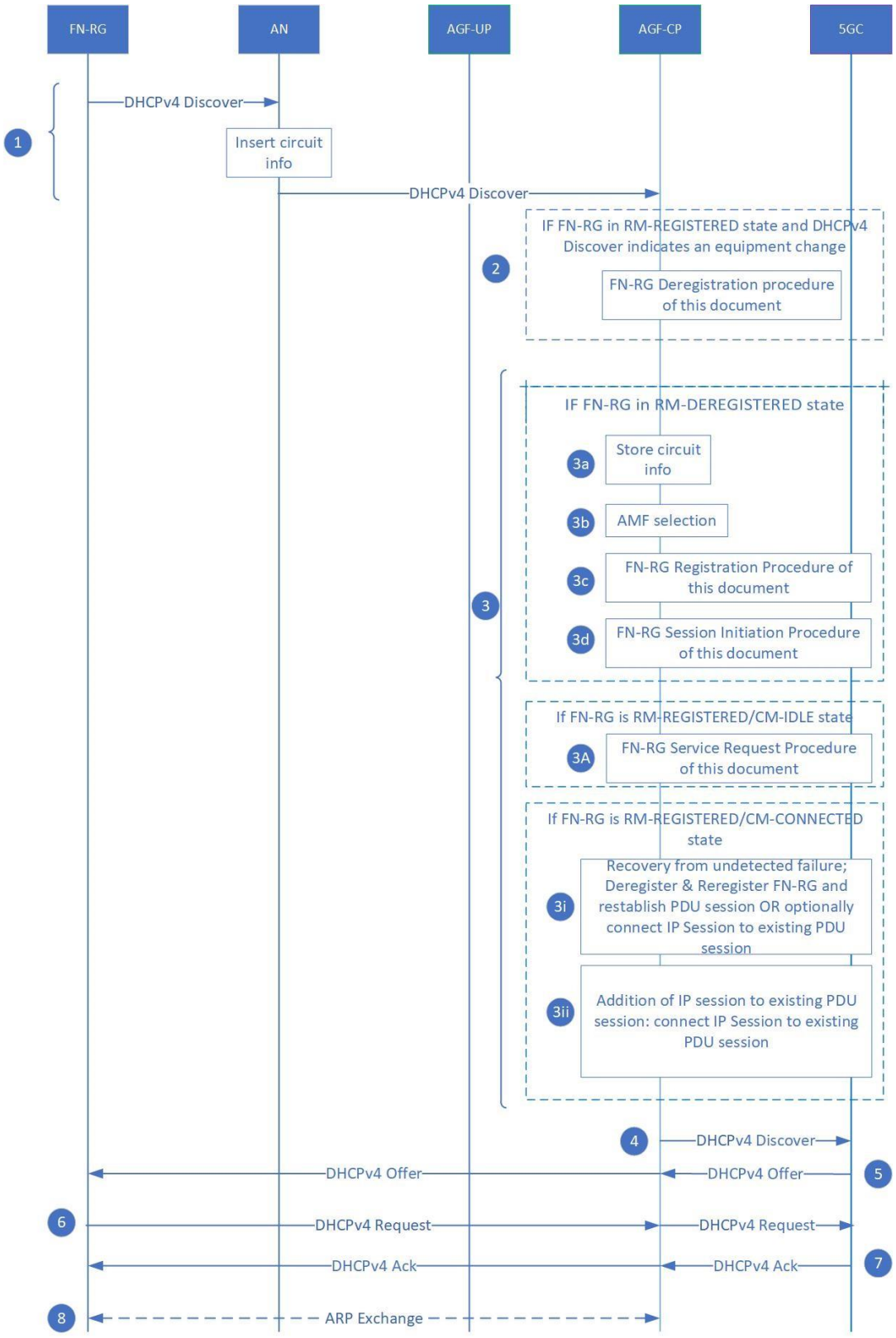

Figure 25: Call flow for FN-RG IP session initiation with DHCPv4

1. The FN-RG sends a DHCPv4 Discover message to the AGF-CP via the AN based on section 5.6.2 of TR-146.

   The AN receives the DHCPv4 Discover message. It inserts Line ID information in option 82 into this message and forwards the entire message to the AGF-CP as per section 3.8.2 of TR-101 Issue2.

2. On receiving DHCPv4 Discover message, if the FN-RG is in the RM-REGISTERED state, the AGF-CP checks the client-identifier option 61, if present, or the RG MAC address. The MAC address may be gleaned from the Ethernet header or from the DHCPv4 chaddr field. If the gleaned information identifying the FN-RG is different than that recorded for the current registration, the AGF interprets this as an equipment change and executes the AGF-CP initiated FN-RG Deregistration Procedure described in this document before proceeding.

3. The AGF will then handle the IP session initiation according to the current registration and connection state:

   If the state is RM-DEREGISTERED:

   3a. The AGF stores the subscriber's information including the FN-RG customer equipment identifier, line identification, TCI, and port identification metadata.

   3b. The AGF-CP selects an AMF as per step 2 in TS 23.316 [25] subclause 7.2.1.3.

   3c. The FN-RG is registered into the 5GC based on the registration procedure described in section 8.1.6 (based on TS 23.316 [25], clause 7.2.1.3).

   3d. A PDU session is established.

   The AGF establishes a PDU session as defined in section 8.1.8 (based on TS 23.316 [25] clause 7.3.4). The formulation of PDU SESSION ESTABLISHMENT REQUEST by the AGF will adhere to the requirements in section 6.11 (FN-RG IP session initiation requirements).

   When the AGF requests PDU session type Ipv4v6, it must also facilitate the possible reuse of the PDU session for Ipv6 stack. In this case, the AGF will handle the LLA assignment as per the requirements in section 6.3.2.1.

   The PDU session ID is allocated by the AGF.

   The 5GC, when formulating the reply to PDU SESSION ESTABLISHMENT REQUEST, considers the PDU session type requested by the AGF and the user's subscription data stored in UDM: the latter are authoritative.

   From the PDU SESSION ESTABLISHMENT ACCEPT received by the 5GC the AGF learns the type of PDU session that the subscriber is permitted to: this information is in the Selected PDU Session Type field.

   If the Selected PDU Session Type is Ipv4or Ipv4/v6, the AGF will act as a DHCP Relay for all the DHCPv4 messages from the FN-RG to 5GC. The SMF is responsible for all Ipv4 address allocation and network parameters (like Gateway, DNS, etc.).

   If the PDU SESSION ESTABLISHMENT ACCEPT indicated that FN-RG is not allowed to use Ipv4 stack (Selected PDU Session Type=Ipv6), the AGF will discard the current and any further DHCPv4 messages from that FN-RG on the basis of its Line ID, for the duration of the registration.

   If the state is RM-REGISTERED/CM-IDLE and the selected PDU session type is Ipv4 or Ipv4/Ipv6:

   3A. The AGF performs the Service Request Procedure for FN-RG in this document, possibly followed by PDU session establishment request.

   If the state is RM-REGISTERED/CM-CONNECTED and the selected PDU session type is Ipv4 or Ipv4/Ipv6:

3i. Recovery from undetected failure: The AGF will deregister and re-register the FN-RG and reestablish the PDU session OR MAY simply connect the IP session to the existing PDU session.

3ii. Addition of IP Session to existing PDU Session: Connecting the IP session to an existing PDU session applies to the scenario where the PDU session is Ipv4v6 and the IP session initiation is for the addition of the Ipv4 stack (e.g., the FN-RG initiated Ipv6 operation first).

4. This is followed by the relaying of the DHCPv4 Discover message by the AGF to the 5GC via the established PDU session. The AGF will have set the GIADDR field to the Ipv4 address of the AGF as the L3 DHCP relay agent.
5. The 5GC in turn sends a DHCP offer message to the FN-RG via the AN and AGF. This message echoes the GIADDR IP address received from the AGF.
6. The FN-RG will accept the offer with a DHCP request.
7. The 5GC will confirm the DHCP lease with a DHCP ack
8. The FN-RG will then typically resolve the MAC address of the default gateway with an ARP request (where the AGF proxies a reply with its own MAC address) as required in section 6.3.2.1 (L2/L3 Interworking).

8.1.4 FN-RG IP Session Initiation with DHCPv6

Figure 26 shows the call flow for the FN-RG IP session initiation with the AGF initiated by DHCPv6, which subsequently leads to registration and session initiation procedures.

This procedure applies to FN-RGs that are able to start DHCPv6 negotiation without having received a RA with either ‘M’ or ‘O’ ‘flag set to 1. In case the FN-RG does not have this ability, the procedure that applies is the one that requires the FN-RG sending a RS documented in section 8.1.5.

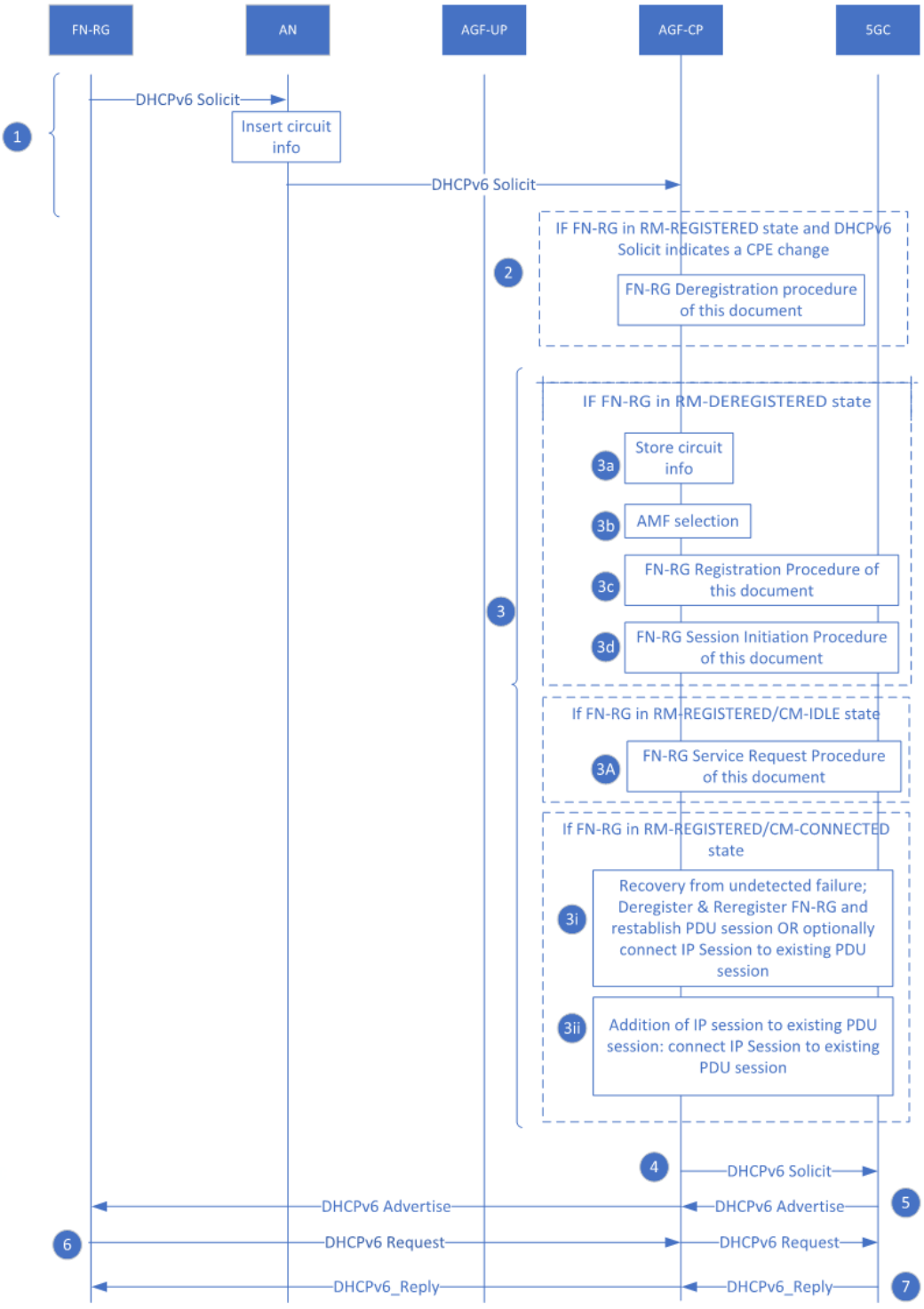

Figure 26: Call flow for FN-RG IP session initiation with DHCPv6

1. The FN-RG sends a DHCPv6 Solicit message to the AGF-CP via the AN based on section iWAN.Ipv6 in TR-124.

   The AN receives the DHCPv6 Solicit message. The AN will insert option 18 and/or option 37 ‘line identification information’. The AN then forwards the entire message to the AGF-CP.

2. On receiving DHCPv6 Solicit message for an FN-RG in the RM-REGISTERED state, AGF-CP checks the DUID within the DHCPv6 message or the RG MAC address. The MAC address may be gleaned from the Ethernet encapsulation or the RGs LLA. If the gleaned information indicates that the FN-RG is different than that recorded for the current registration, the AGF interprets this as an equipment change and executes the AGF-CP initiated FN-RG Deregistration Procedure described in this document before proceeding.
3. The AGF will then handle the IP session initiation according to the current registration and connection state:

   If the state is RM-DEREGISTERED

   3a. The AGF stores the subscriber's information including the FN-RG MAC address, line identification, TCI and port identification metadata.

   3b. The AGF-CP selects an AMF as per step 2 in TS 23.316 [25] subclause 7.2.1.3.

   3c. The FN-RG is registered into the 5GC based on the registration procedure described in section 8.1.6 (based on TS 23.316 [25], clause 7.2.1.3).

   3d. A PDU session is established.

   The AGF establishes a PDU session as defined in section 8.1.8 (based on TS 23.316 [25] clause 7.3.4). The formulation of PDU SESSION ESTABLISHMENT REQUEST by the AGF will adhere to the requirements in section 6.11 (FN-RG IP session initiation requirements).

   The PDU session ID is allocated by the AGF.

   The 5GC, when formulating the reply to PDU SESSION ESTABLISHMENT REQUEST, considers the PDU session type requested by the AGF and the user's subscription data stored in UDM: the latter are authoritative.

   The modifications to procedures for the assignment of LLAs as part of PDU session establishment is as per the requirements in section 6.3.2.1 (L2/L3 Interworking).

   From the PDU SESSION ESTABLISHMENT ACCEPT received by the 5GC the AGF learns the type of PDU session that the subscriber is permitted to: this information is in the Selected PDU Session Type field.

   If the Selected PDU Session Type is Ipv6 or Ipv4v6, the AGF will act as a DHCP Relay for all the DHCPv6 messages from the FN-RG to 5GC. The SMF is responsible for Ipv6 prefix allocation and network parameters.

   Moreover, the AGF will act as an ND Proxy for the FN-RG as documented in the L2/L3 interworking requirements in this document.

   If the PDU SESSION ESTABLISHMENT ACCEPT indicated that FN-RG is not allowed to use Ipv6 stack (Selected PDU Session Type=Ipv4), the AGF will discard the current DHCPv6 solicit and any further DHCPv6 or ND messages from that FN-RG on the basis of its Line ID, for the duration of the registration.

   If the state is RM-REGISTERED/CM-IDLE and the selected PDU session type is Ipv6 or Ipv4/Ipv6:

   3A. The AGF performs the Service Request Procedure for FN-RG in this document.

   If the state is RM-REGISTERED/CM-CONNECTED and the selected PDU session type is Ipv6 or Ipv4/Ipv6

   3i. Recovery from undetected failure: The AGF will deregister and re-register the FN-RG and reestablish the PDU session OR MAY simply connect the IP session to the existing PDU session.

3ii. Addition of IP Session to existing PDU Session: Connecting the IP session to an existing PDU session also applies to the scenario where the PDU session is Ipv4v6 and the IP session initiation is for the addition of the Ipv6 stack (e.g., the FN-RG initiated Ipv4 operation first).

4. The AGF-CP relays the DHCPv6 Solicit message to the 5GC.
5. The 5GC in turn sends a DHCPv6 Advertise Message to the FN-RG via the AN and AGF.
6. The FN-RG responds with a DHCPv6 Request Message.
7. The 5GC confirms the DHCPv6 lease with a DHCPv6 Reply Message.

8.1.5 FN-RG IP Session Initiation with RS followed by DHCPv6

Figure 27 illustrates the scenario when an RS is the first indication of Ipv6 IP session initiation. DHCPv6 exchange may follow. This covers the scenarios of SLAAC-only and RA followed by DHCPv6 to either negotiate a delegated prefix (IA_PD) or obtain other attributes such as DNSv6 addresses using DHCPv6 INFORM.

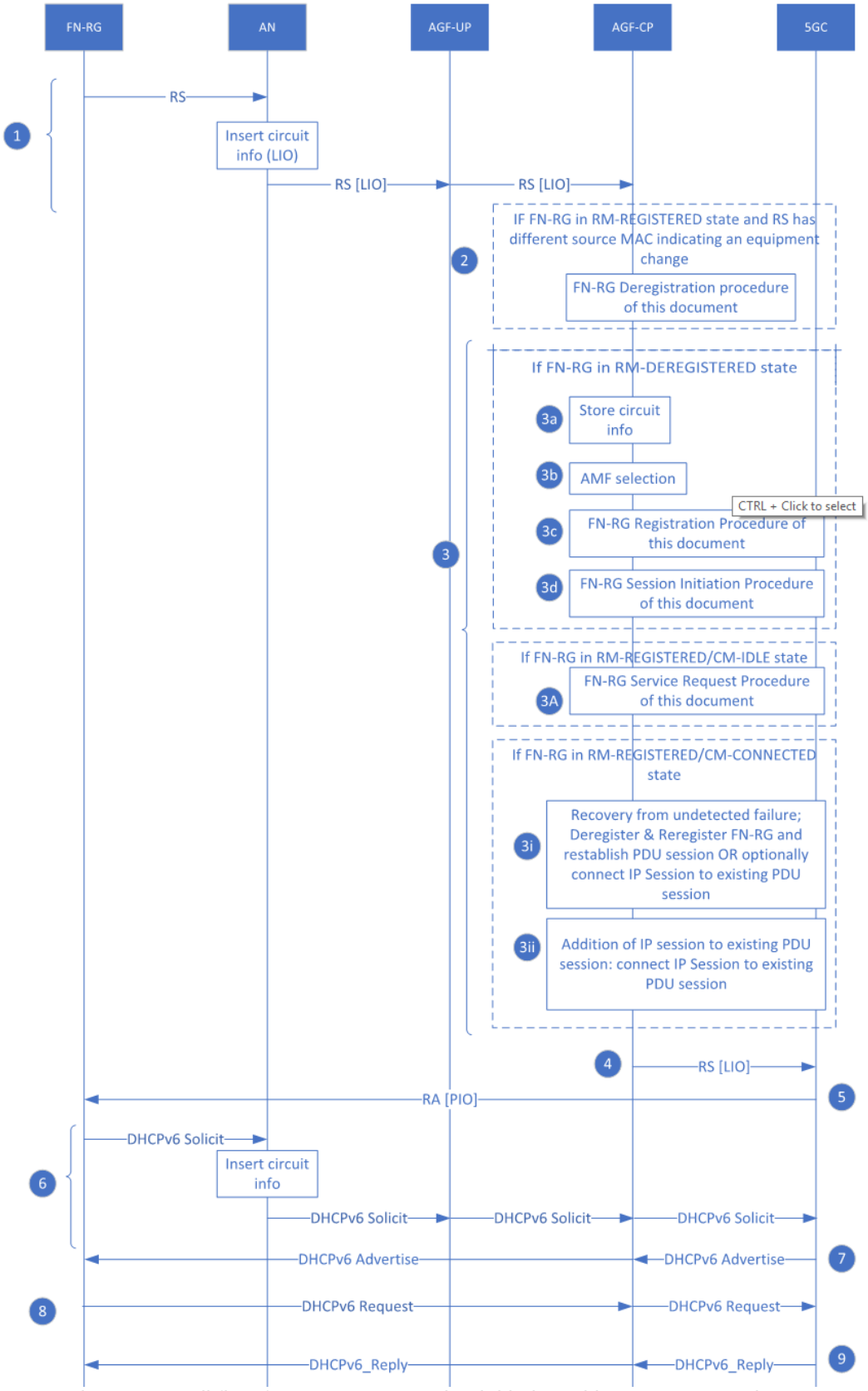

Figure 27: Call flow for FN-RG IP session initiation with SLAAC procedures

1. The FN-RG sends a Router Solicit (RS) message to the AGF-CP via the AN based on section 5.6.2 of TR-146.

   The AN receives the Router Solicit message. It inserts the Line ID option as per Annex 'A' of TR-177 Corrigendum 1 and in turn forwards the entire message to the AGF-CP.

2. On receiving the RS message, if the FN-RG is in the RM-REGISTERED state, the AGF-CP checks the RG MAC address. This may be gleaned from the Ethernet header or RG's LLA. If the gleaned information indicates that the FN-RG is different than that recorded for the current registration, the AGF interprets this as an equipment change and executes the AGF-CP initiated FN-RG Deregistration Procedure described in this document before proceeding.

3. The AGF will then handle the IP session initiation according to the current registration and connection state:

   If the state is RM-DEREGISTERED

   3a. The AGF stores the subscriber's information including the FN-RG MAC address, line identification, TCI, and port identification metadata.

   3b. The AGF-CP selects an AMF as per step 2 in TS 23.316 [25] subclause 7.2.1.3.

   3c. The FN-RG is registered into the 5GC based on the registration procedure described in section 8.1.6 (based on TS 23.316 [25], clause 7.2.1.3).

   3d. A PDU session is established.

   The AGF establishes a PDU session as defined in section 8.1.8 (based on TS 23.316 [25] clause 7.3.4). The formulation of PDU SESSION ESTABLISHMENT REQUEST by the AGF will adhere to the requirements in 6.11 (FN-RG IP session initiation requirements).

   The PDU session ID is allocated by the AGF.

   The 5GC, when formulating the reply to PDU SESSION ESTABLISHMENT REQUEST, considers the PDU session type requested by the AGF and the user's subscription data stored in UDM: the latter are authoritative.

   The modifications to procedures for the assignment of LLAs as part of PDU session establishment is as per the requirements in section 6.3.2.1 (L2/L3 Interworking).

   From the PDU SESSION ESTABLISHMENT ACCEPT received by the 5GC the AGF learns the type of PDU session that the subscriber is permitted to: this information is in the Selected PDU Session Type field.

   If the Selected PDU Session Type is Ipv6 or Ipv4/v6, the AGF will relay the RS message from the FN-RG to the 5GC. The SMF is responsible for prefix allocation and network parameters.

   Moreover, the AGF will act as an ND Proxy for the FN-RG as documented in the L2/L3 interworking requirements in this document.

   If the PDU SESSION ESTABLISHMENT ACCEPT indicated that FN-RG is not allowed to use Ipv6 stack (Selected PDU Session Type=Ipv4), the AGF will discard the current RS and any further DHCPv6 or ND messages from that FN-RG on the basis of its Line ID.

   If the state is RM-REGISTERED/CM-IDLE and the selected PDU session type is Ipv6 or Ipv4/Ipv6

   3A. The AGF performs the Service Request Procedure for FN-RG in this document.

   If the state is RM-REGISTERED/CM-CONNECTED and the selected PDU session type is Ipv6 or Ipv4/Ipv6

3i. Recovery from undetected failure: The AGF will deregister and re-register the FN-RG and reestablish the PDU session OR MAY simply connect the IP session to the existing PDU session.

3ii. Addition of IP Session to existing PDU Session: Connecting the IP session to an existing PDU session applies to the scenario where the PDU session is Ipv4v6 and the IP session initiation is for the addition of the Ipv6 stack (e.g., the FN-RG initiated Ipv4 operation first).

4. The AGF-CP relays the RS to the 5GC, removing the Source Link Layer Address option, if present.
5. The 5GC sends a router advertisement (RA) to the FN-RG. This may (as a consequence of local configuration) include a prefix information option (PIO). For N:1 VLAN, the AGF when forwarding the RA uses the unicast MAC address of the FN-RG (refer to section 6.2.6 of RFC 4861 [49]). The AGF forwards the RA towards the FN-RG making sure to insert, if missing, or rewrite, if present, the Source Link Layer Address option.
6. The FN-RG sends a DHCPv6 Solicit message to the AGF-UP via the AN. The AN will insert option 18 and/or option 37 line identification information (this will only be of further significance for N:1 VLAN support). If a received RA did not contain a prefix information option, the DHCPv6 Solicit asks for both IA_NA and IA_PD. If the received RA did contain a prefix information option, the DHCPv6 Solicit asks for IA_PD only. The AGF receives the DHCPv6 Solicit and by the Line-Id or by the VLAN it recognizes as coming from an FN-RG already mapped to a PDU session supporting Ipv6. Therefore, it will simply relay the DHCPv6 message to the 5GC.
7. The 5GC in turn sends a DHCPv6 Advertise Message to the FN-RG via the AN and AGF.
8. The FN-RG responds with a DHCPv6 Request Message.
9. The 5GC confirms the DHCP lease with a DHCPv6 Reply Message.

Note: Steps from 6 to 9 may or may not occur, depending on the FN-RG behavior.

8.1.6 Registration Management Procedure for FN-RG

Figure 28 shows the call flow for the registration management of an FN-RG. Since FN-RG is a legacy device that does not support N1, the AGF handles NAS signaling on behalf of the FN-RG.

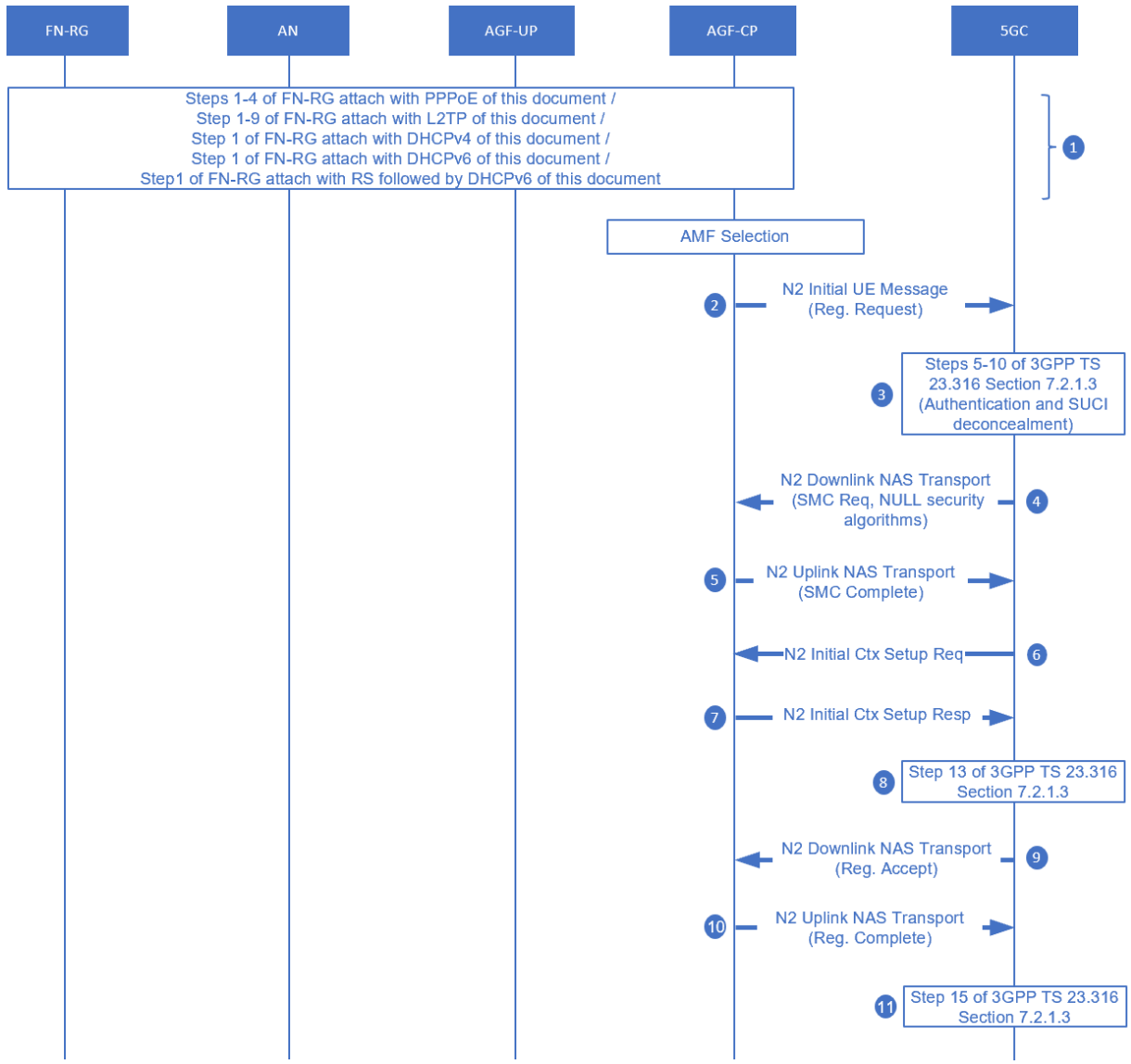

Figure 28: Call flow for the Registration Management Procedure for an FN-RG

1. In order to carry out the registration procedure, it is a pre-requisite that a connection exists between the FN-RG and AGF-CP via PPPoE, DHCP or SLAAC using one of:
    a. Steps 1-4 of FN-RG IP session initiation with PPPoE (Section 8.1.1)
    b. Steps 1-9 of FN-RG IP session initiation using L2TP (Section 8.1.2)
    c. Step 1 of FN-RG IP session initiation with DHCPv4 (Section 8.1.3)
    d. Step 1 of FN-RG IP session initiation with DHCPv6 (Section 8.1.4)
    e. FN-RG IP session initiation with RS followed by DHCPv6 (Section 8.1.5).

    After authentication, the AGF-CP selects an AMF based on the AN parameters and local policy.

2. The AGF-CP constructs a registration request to be forwarded to the 5GC on behalf of the FN-RG as specified in step 3 of TS 23.316 [25] subclause 7.2.1.3. As per step 3 of TS 23.316 [25] subclause 7.2.1.3, this registration request contains an authentication indication for the 5GC indicating that the FN-RG has been authenticated by the AN.

3. The next steps involve authentication by the 5GC which includes AUSF selection and SUCI deconcealment in the 5GC as per steps 4-9 in TS 23.316 [25] subclause 7.2.1.3.
4. On successful authentication by the 5GC, the 5GC initiates a NAS Security Mode Command procedure towards the AGF-CP based on step 10a of TS 23.316 [25] figure 7.2.1.3-1. The SMC request has NAS security algorithms – integrity protection algorithm and ciphering algorithm set to NULL.
5. The AGF-CP responds with a NAS Security Mode Complete message and a NAS security context is created between the AGF and 5GC.
6. The 5GC next sends an N2 Initial Context Setup Request message to the AGF-CP. This may include the RG Level Wireline Access Characteristics.
7. The FN-RG context is created and is indicated by the AGF-CP to the 5GC via the Initial Context Setup Response.
8. The 5GC performs step 13 as in TS 23.316 [25] figure 7.2.1.3-1.
9. The 5GC sends a NAS Registration Accept message to the AGF-CP.
10. The AGF-CP responds with a NAS Registration Complete message.
11. 5GC performs step 15 as in TS 23.316 [25] subclause 7.2.1.3.

8.1.7 Service Request Procedure for FN-RG

The Service Request Procedure described below is initiated by the AGF-CP when the state of the FN-RG on the AGF is (CM-IDLE, RM-REGISTERED). This procedure aims at re-establishing the NAS connectivity between AGF as proxy UE and the AMF, in case it was previously released or lost.

Note: In general, the service request procedures may also be initiated for the CM-CONNECTED case. This document does not address this use case as it does not apply to FN-RGs.

The procedure is as per clause 7.2.2.2 of TS 23.316 [25] with the following details:

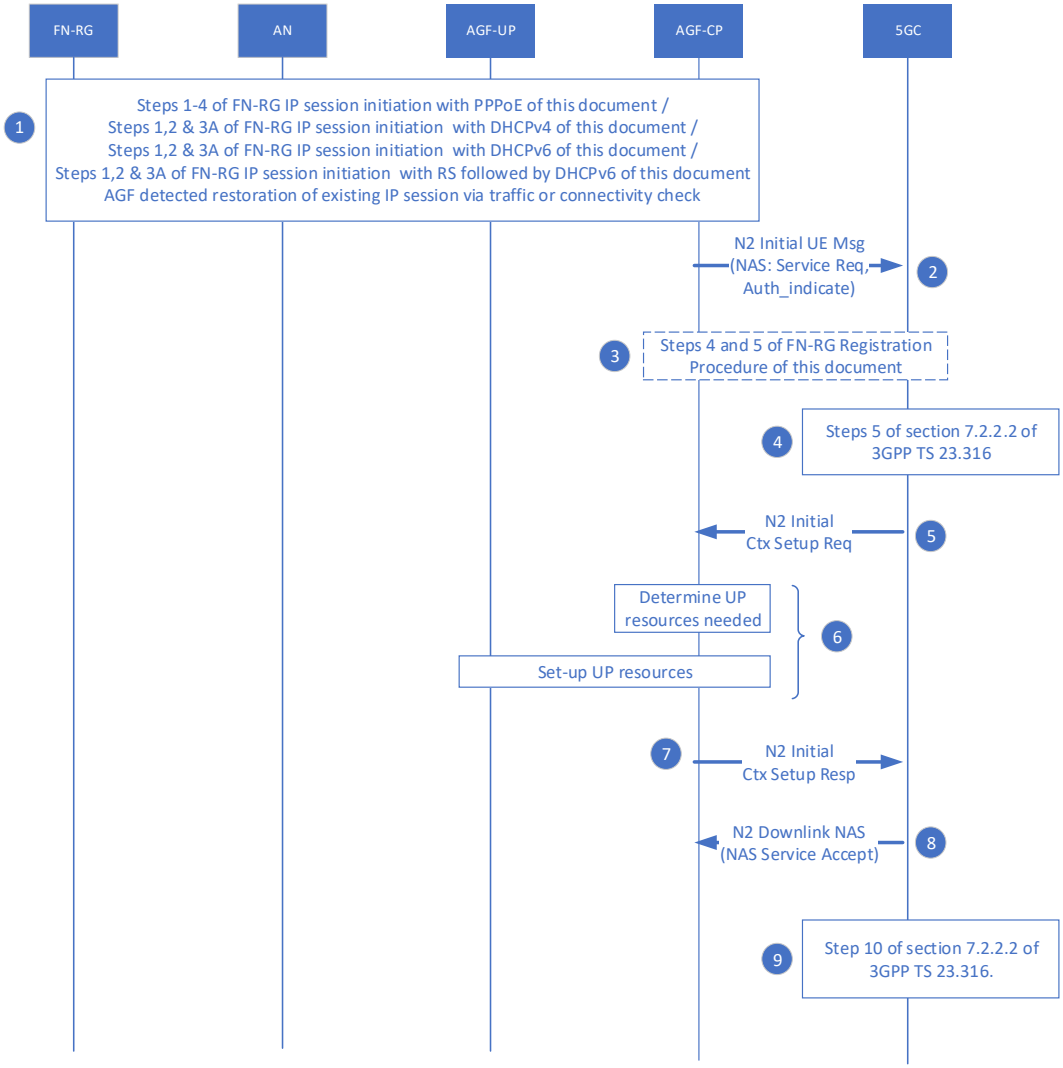

Figure 29: FN-RG Service Request Procedure via W-5GAN

1. The FN-RG connects to the AGF-CP via PPPoE, DHCP or SLAAC using one of:
    a. Steps 1-4 of FN-RG IP session initiation with PPPoE (Section 8.1.1)
    b. Steps 1-9 of FN-RG IP session initiation using L2TP (Section 0)
    c. Step 1 of FN-RG IP session initiation with DHCPv4 (Section 8.1.3)
    d. Step 1 of FN-RG IP session initiation with DHCPv6 (Section 8.1.4)
    e. FN-RG IP session initiation with RS followed by DHCPv6 (Section 8.1.5).

    OR the FN-RG has not detected the outage and resumes using the existing IP session

    The AGF detects a resumption in connectivity via the reception of well-formed traffic on an existing Ipv4oE or Ipv6OE session.
2. The AGF-CP sends the AN parameters and a Service Request message on behalf of FN-RG within an N2 Initial UE message as per step 3 of clause 7.2.2.2 of TS 23.316 [25].
3. The 5GC may initiate the security mode command procedure as per steps 4 and 5 of section 8.1.6.

    After successful establishment of the signaling connection, the AGF-CP and the 5GC can exchange NAS signaling

4. Step 5 of clause 7.2.2.2 in TS 23.316 [25] is executed in the 5GC.
5. The 5GC sends a N2 UE Initial Context Setup Request message as per step 6 of clause 7.2.2.2 of TS 23.316 [25] which contains the N2 SM information received from SMF(s), RG Level Wireline Access Characteristics, and other parameters intended for the FN-RG. All the parameters received from the 5GC in this step may not be applicable for AGF and can be left for implementation. The parameters in the INITIAL CONTEXT SETUP REQUEST, as defined in clause 5.3 of TS 29.413 [20], are not applicable to this step.

   Note: This single message can setup the UP for several PDU sessions, but this is FFS.
6. The AGF-CP determines the UP resources and sets-up the UP resources together with the AGF-UP. This corresponds to step 7 of clause 7.2.2.2 of TS 23.316 [25].
7. After setting up the UP resources, the AGF-CP sends a N2 Initial Context Setup Response to the 5GC as per step 8 of clause 7.2.2.2 of TS 23.316 [25].
8. The 5GC sends a NAS Service Accept message to the AGF-CP as per step 9 of clause 7.2.2.2 of TS 23.316 [25].
9. Further steps are executed in 5GC as per step 10 of clause 7.2.2.2 of TS 23.316 [25] .

8.1.8 Session Initiation Procedure for FN-RG

This procedure aims at initiating the PDU session for an FN-RG.

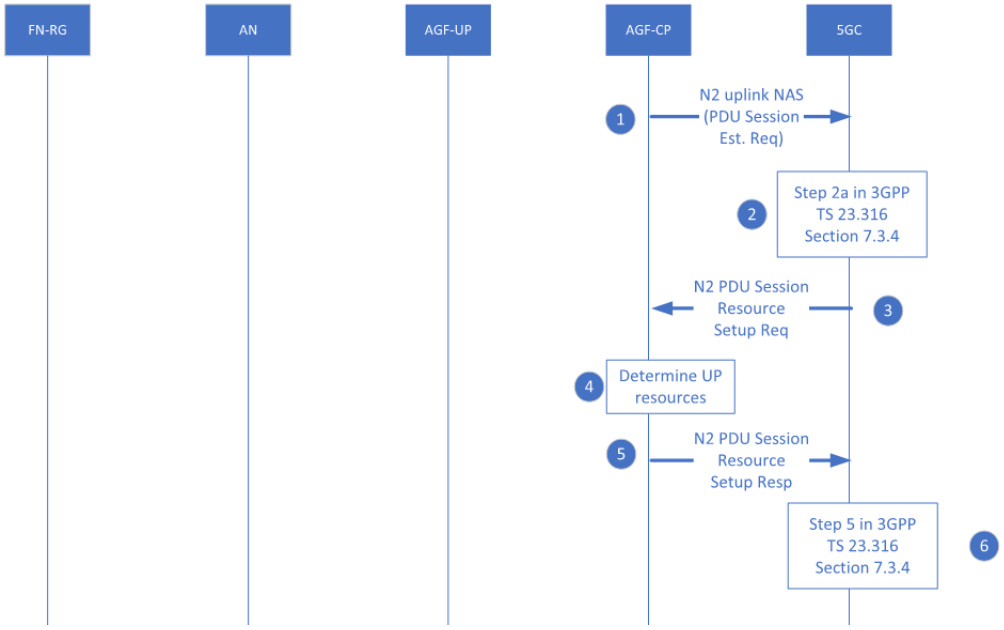

Figure 30: Call flow for the PDU Session Initiation Procedure for an FN-RG

1. The AGF-CP is triggered to send an N2 uplink NAS message with a PDU Session Establishment Request to the 5GC. The session request formulation adheres to the requirements documented in section 6.11 (FN-RG IP session initiation requirements)
2. The 5GC performs step 2a of TS 23.316 [25] clause 7.3.4.
3. The 5GC sends a N2 PDU Session Resource Setup Request to the AGF-CP as step 2b of TS 23.316 [25] clause 7.3.4.

4. This N2 PDU Session Resource Setup Request is used by the AGF to assign UP resources in the AN based on the AN specific subscription information in the RG-LWAC which describes the resource model for the circuit serving the FN-RG.
5. The AGF responds to the 5GC with a N2 PDU Session Resource Setup Response.
6. The 5GC performs step 5 as in TS 23.316 [25] clause 7.3.4 (step 6a of Figure 30).

8.1.9 Deregistration Procedure for FN-RG

Figure 31 shows the call flow for the deregistration of an FN-RG from the 5GC. The deregistration procedure can either be AGF-CP initiated or 5GC-initiated.

The triggers for UE initiated deregistration may include:

- Detecting a change of FN-RG equipment since the last registration, e.g., shown by a new MAC address in the signaling packets initiating a new IP session.
- Detecting a 5G-RG attempting to register on the same Line ID (migration scenario).
- The termination of the last IP session by PPPoE based FN-RG.
- Receipt of a DHCPv4 Release for a PDU session type IPv4.
- Receipt of a DHCPv6 Release for a PDU session type IPv6.
- Receipt of both a DHCPv4 Release and DHCPv6 release for a PDU session type IPv4v6.

The triggers from an AGF in the role of proxy UE may include:

- The expiration of the internal timer in CM-CONNECT mode without PDU session context.
- The expiration of the AGF deregistration timer.

The triggers for network-initiated deregistration include:

- Termination of the subscription in 5GC, e.g., triggered by non-payment.
- The expiration of the AMF deregistration timer.

Note: If the state of FN-RG in the AMF is CM-IDLE and the deregistration timer initiated upon the transition to CM-IDLE expires, then the 5GC or AMF simply considers the FN-RG to be deregistered and no explicit signaling occurs among the network nodes. This can be considered as network-initiated deregistration which does not involve any message exchanges between the AMF and the AGF. However, if the loss of connectivity to the FN-RG is kept local to AGF-CP until a specified outage duration is exceeded, then this can be UE-initiated deregistration initiated by the NAS proxy in the AGF.

This procedure is similar to the 5G-RG deregistration procedure described in section 8.2.5 (Deregistration Procedure for 5G-RG), with the difference that the AGF-CP acts on behalf of an FN-RG as an endpoint for N1 NAS signaling.

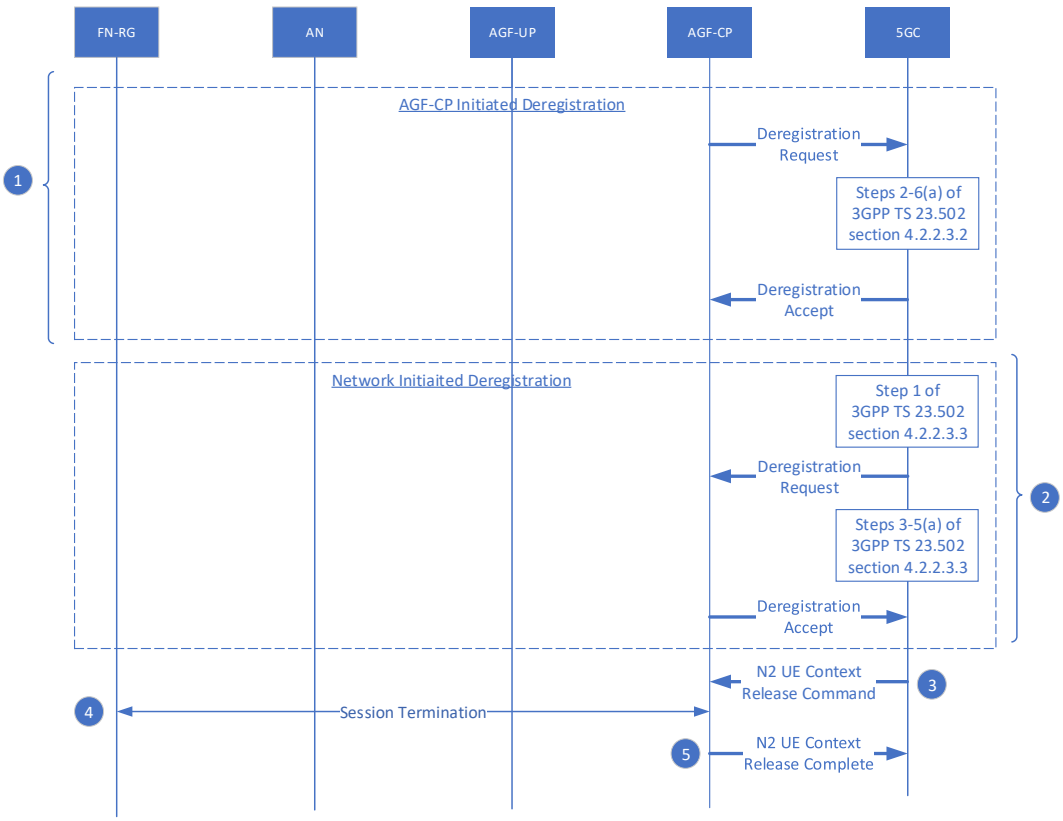

Figure 31: Call flow for Deregistration Procedure for FN-RG

1. The deregistration procedure for the FN-RG can be initiated by the AGF-CP on behalf of FN-RG and is triggered by one of the events described at the beginning of this section. The deregistration is specified in clause 7.2.1.4 in TS 23.316 [25], which is in turn based on UE-initiated deregistration procedure in TS 23.502 [29], clause 4.2.2.3.2.

Note: Scenarios where the DHCP lease does not fate share with the PDU session, for example when the DHCP server is not integrated with the 5GC, are FFS.

   The AGF-CP sends a deregistration request towards the 5GC on behalf of the FN-RG. This is followed by session release and policy termination mechanisms in 5GC. The 5GC then sends a deregistration accept message which is terminated at the AGF-CP.

   De-Registration Request will release all the PDU Sessions associated with the RG and release the N2 UE context. This can be preceded by PDU Session Release Procedure in case the N2 UE context needs to be retained.

2. The 5GC can also initiate the deregistration procedure towards the FN-RG which is specified in clause 7.2.1.4 in TS 23.316 [25], which is in turn based on section Network-initiated deregistration procedure in clause 4.2.2.3.3 of TS 23.502 [29].

   The AGF-CP sends a deregistration accept message to the 5GC on behalf of the FN-RG.

3. The 5GC next sends a N2 UE Context Release Command to the AGF-CP as in step 3 of section 8.2.5 (or step 2 of clause 7.2.1.2 in TS 23.316 [25]).

4. The AGF-CP uses an LCP Terminate Request followed by a PPPoE PADT to terminate any active PPPoE session with the FN-RG in line with step 4 of section 8.2.5 (or step 3 of clause 7.2.1.2 in TS 23.316 [25]).

5. After terminating active PPPoE sessions with the FN-RG, the AGF-CP sends a N2 UE Context Release Command message to the 5GC as in step 4 of clause 7.2.1.2 in TS 23.316 [25].

Note: Steps 4 and 5 only apply to PPPoE based IP sessions. Communicating IP session termination for IPoE is FFS.

8.1.10 FN-RG or Network Requested PDU Session Modification via W-5GAN

PDU session modification cannot be supported by an FN-RG. Any trigger such as subscription change will not take place until a new PDU session is established.

The Network Requested PDU Session Modification can be initiated by the SMF, possibly triggered due to a subscription change. There does not appear to be an actual use case where an FN-RG can do anything to trigger an AGF action, it is included here for completeness.

This procedure is as per clause 7.3.6 of TS 23.316 [25], which is in turn referring to clause 7.3.2 of TS 23.316 [25]. Applicable use cases and wireline specific clarifications are FFS.

8.1.11 FN-RG or Network Requested PDU Session Release via W-5GAN

The PDU session release procedure is triggered by:

- DHCP lease expiry for IpoE,
- graceful shutdown of a PPP session by the FN-RG
- keepalive failure of the PPP session
- IpoE connectivity fault detected via BFD, ping, etc.
- receipt of a PADT for PPPoE from the FN-RG

  Note: both graceful shutdown of a PPP session or a PADT received by the FN-RG trigger the FN-RG Deregistration as per section 8.1.10.
- 5GC action for deregistration

This procedure is as per clause 7.3.7 of TS 23.316 [25], which is in turn referring to clause 7.3.3 with the following clarifications:

1. For initiating this procedure, it is a prerequisite that connectivity exists between the FN-RG and AGF-CP and has at least one IP session mapped to a PDU session established between the AGF and UPF as per step 1 of clause 7.3.3 of TS 23.316 [25].

   The AGF-CP creates a PDU Session Release Request towards the 5GC on behalf of FN-RG as per bullet 3 in clause 7.3.7 in TS 23.316 [25].
2. The 5GC executes step 3 as in clause 7.3.3 in TS 23.316 [25].
3. The AGF-CP receives N2 Resource Release Request from 5GC as per step 4 of clause 7.3.3 in TS 23.316 [25].
4. Upon receiving the N2 Release Request message, the AGF-CP triggers the release of the corresponding UP resources as per bullet 4 of clause 7.3.7 in TS 23.316 [25].

If the PDU Session Release is network requested, and the session is PPPoE based, the AGF-CP sends a PADT to the FN-RG to terminate the IP session. If the session is IpoE based, then the AGF will release the user plane resources regardless of the inability to inform the FN-RG of this release. The 5GC may issue a DHCP Force Renew to trigger a renew request by the FN-RG and then reject it.

5. The AGF-CP sends a N2 Release Ack towards the 5GC as per step 6 of clause 7.3.3 in TS 23.316 [25].
6. Step 7 is executed in 5GC as per clause 7.3.3 in TS 23.316 [25].
7. The AGF-CP directly creates an Uplink NAS Transport Message towards the 5GC, which contains the PDU Session Release Ack as per bullet 5 in clause 7.3.7 in TS 23.316 [25].
8. Step 11 is executed in 5GC as per clause 7.3.3 in TS 23.316 [25].

8.1.12 FN-RG AN Release via W-5GAN

The AN Release Procedure for the FN-RG is used to release the NG-AP signaling connection and the associated N3 user plane connections between the W-5GAN and the 5GC.

The AN release procedure may be triggered by a loss of connectivity with the FN-RG detected by the AGF. It may be started by the AGF with a N2 UE Context Release Request to the AMF. Upon receiving the N2 UE Context Release command as a reply from the AMF, the AGF flushes the FN-RG N2 context, the N3 resources and the IP session resources, retaining the N1 context as proxy UE. Besides that, the AGF starts a local non-3GPP Implicit Deregistration timer using the default value or the value received from by the AMF in the in NAS Registration Accept message (as documented in TS 24.501 [11] clause 8.2.7.17). The N1 context related to the FN-RG is retained by the AGF as proxy UE until the non-3GPP Implicit Deregistration timer expires.

The AN Release procedure is as per clause 7.2.5.3 of TS 23.316 [25], which is in turn referring to clause 7.2.5.2 with the following clarifications:

1. It is a prerequisite that the FN-RG is registered into the 5GC. The AGF may have a PDU session established on behalf of the FN-RG as per step 1 of clause 7.2.5.2 in TS 23.316 [25].

   The AGF-CP detects that the FN-RG is unreachable, which serves as the trigger for initiating this procedure as per step 2 in clause 7.2.5.2 in TS 23.316 [25]. This may be via liveness detection means (e.g., LCP Echo Requests).

2. The AGF-CP sends a N2 UE Context Release Request to 5GC as per step 3 of clause 7.2.5.2 in TS 23.316 [25].
3. The AGF-CP receives a N2 UE Context Release Command from the 5GC as per step 4 of clause 7.2.5.2 in TS 23.316 [25].
4. The AGF-CP initiates the release of the IP session local resources as per bullet 2 of clause 7.2.5.3 in TS 23.316 [25]. The release process is entirely a local action and involves the release of state and scheduler appearances at the AGF.
5. The AGF-CP next sends a N2 UE Context Release Complete to the 5GC as per step 6 of clause 7.2.5.2 in TS 23.316 [25].
6. This is followed by PDU session user plane deactivation in the 5GC as per step 7 of clause 7.2.5.2 in TS 23.316 [25].

8.1.13 Configuration Update Procedure for FN-RG

This procedure is used by the network to update the FN-RG configuration which consists of:

- Access and mobility management related parameters provided by the AMF.
- FN-RG related Policy provided by the PCF. The use of URSP to determine PDU session type, DNN and NSSAI is FFS.

This procedure is similar to the 5G-RG configuration update procedure described in clause 8.2.10 and also described in clause of 7.2.3.2 of TS 23.316 [25], with the difference that the AGF-CP acts on behalf of the FN-RG as an endpoint for N1 NAS signaling.

8.1.13.1 FN-RG Configuration Update procedure for Access and Mobility Management related parameters

This procedure can be further elaborated below based on clause 7.2.3.2 of TS 23.316 [25], which is in turn based on clause 4.2.4.2 of TS 23.502 [29]:

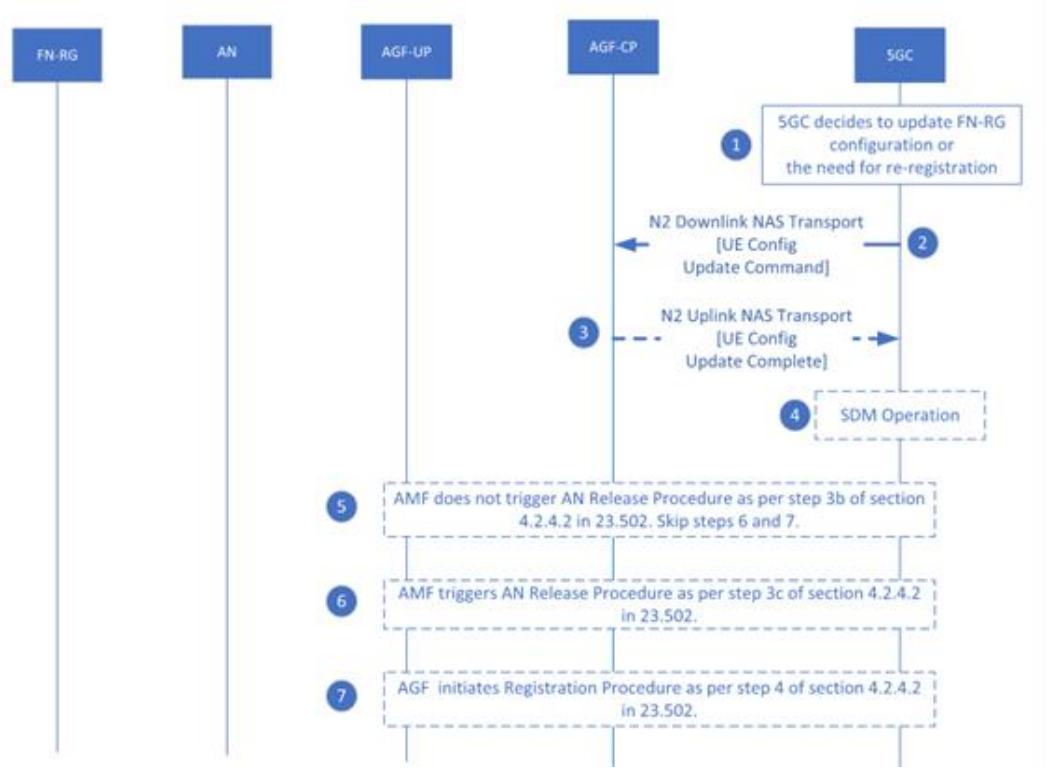

Figure 32: FN-RG Configuration Update Procedure for access and mobility management related parameters via W-5GAN

1. The 5GC determines the need for FN-RG configuration update or re-registration procedure as per step 0 of clause 4.2.4.2 in TS 23.502 [29]. One of the triggers for initiating this procedure is the reception of subscriber data update notification from the UDM and the RG-LWAC parameter can be updated through this procedure.

   If the FN-RG state stored in the AGF-CP is CM-IDLE, the 5GC waits until this changes to CM-CONNECTED state as Network Triggered Service Request is not applicable in this scenario.

2. The 5GC sends a UE Configuration Update command in an N2 Downlink NAS Transport message to the FN-RG which terminates at the AGF-CP with one or more parameters as per step 1 of clause 4.2.4.2 in TS 23.502 [29].

   Note: Refer to subclause 8.2.19 in TS 24.501 [11] for more details on IEs (Information Elements) for the message “Configuration Update Command” and subclause 9.2.5.2 of TS 38.413 [16] for IEs on “Downlink NAS Transport” message.

3. If applicable, the AGF-CP sends an acknowledgement on behalf of the FN-RG for the UE Configuration Update Indication via the UE Configuration Update Complete in an N2 Uplink NAS Transport message as per step 2a of clause 4.2.4.2 in TS 23.502 [29].

4. The 5GC may also perform an SDM operation to indicate to the UDM that the AGF-CP (on behalf of FN-RG) has received the subscription change indication as per step 2b of clause 4.2.4.2 in TS 23.502 [29].
5. If the existing connectivity to the network slices is not affected with the new parameters sent to the AGF-CP, the 5GC does not release the NAS signaling connection for the AGF-CP after receiving the acknowledgement in step 3 above and no immediate registration is required, as per step 3b of clause 4.2.4.2 in TS 23.502 [29].
6. If the existing connectivity to the network slices is affected due to the update with new parameters, the 5GC in its UE Configuration Update Command message includes the new network slice information as per step 3c of clause 4.2.4.2 in TS 23.502 [29].

   If the 5GC cannot provide the new network slice information, it sends an indication to the AGF-CP to initiate the registration procedure. After receiving the acknowledgement in step 3 above, the 5GC releases the NAS signaling connection for the AGF-CP as per step 3c of clause 4.2.4.2 in TS 23.502 [29].
7. The AGF-CP, on behalf of the FN-RG initiates the registration procedure after it enters the CM-IDLE state as per step 4 of clause 4.2.4.2 in TS 23.502 [29].

8.1.13.2 FN-RG Configuration Update procedure for transparent FN-RG Policy delivery

This procedure is initiated by the 5GC (or PCF) to change or provide new FN-RG policies in the AGF-CP. This is as per clause 7.2.3.2 in TS 23.316 [25], which is in turn based on clause 4.2.4.3 in TS 23.502 [29]:

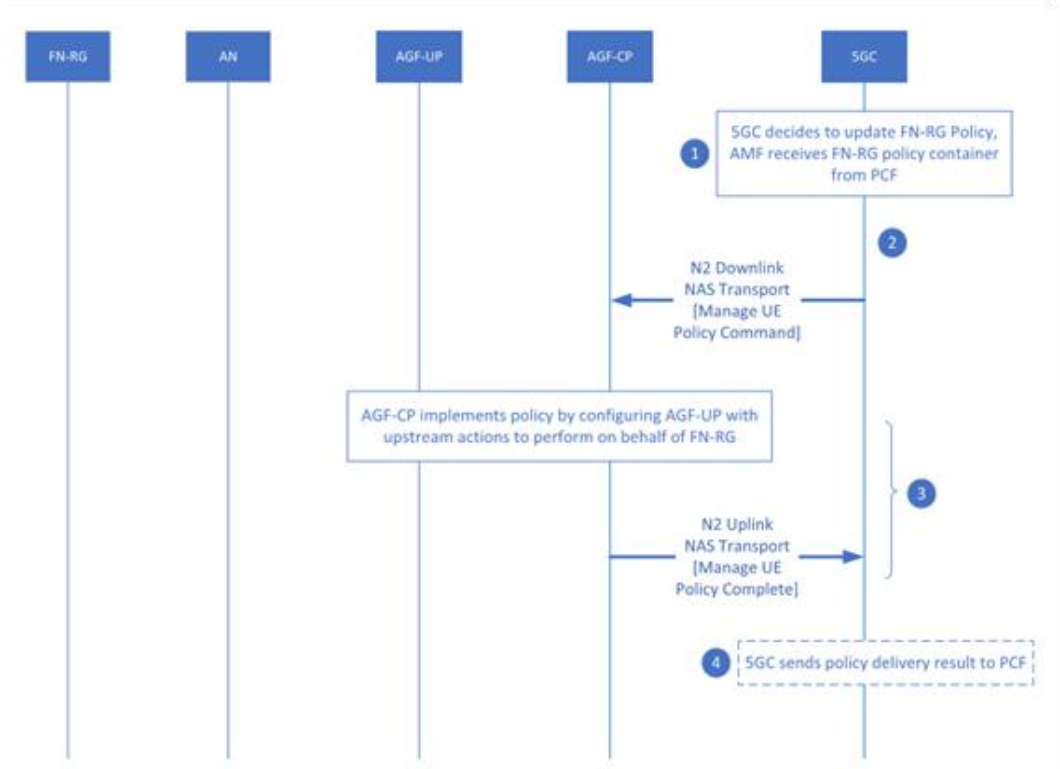

Figure 33: FN-RG Configuration Update Procedure for transparent UE policy delivery via W-5GAN

1. The 5GC (or PCF) decides to update the FN-RG policies based on the triggering conditions as per step 0 clause 4.2.4.3 of TS 23.502 [29]. The AMF (in the 5GC) receives the UE policy container from the policy function as per step 1 of clause 4.2.4.3 of TS 23.502 [29].

2. The AGF-CP receives the FN-RG policy from the 5GC in an N2 Downlink NAS Transport message as per step 3 of clause 4.2.4.3 of TS 23.502 [29] containing the Manage UE Policy Command.

   Note: The IE “Payload Container Type” is set to “UE Policy Container” as per TS 24.501 [11] subclause 8.2.11 and annex D.

3. The AGF-CP updates the policy provided by the 5GC for the FN-RG and sends the result to the 5GC in an N2 Uplink NAS Transport message as per step 4 of clause 4.2.4.3 of TS 23.502 [29] which contains the Manage UE Policy Complete message. In this issue of the specification, the AGF ignores the UE policy rules, but sends a positive result.

   Note: There is no signaling or message exchanges involved between the AGF and FN-RG for this procedure.

4. The AMF (in the 5GC) sends this response from the AGF-CP to the 5GC policy function (PCF) as per step 5 of clause 4.2.4.3 of TS 23.502 [29].

8.1.14 Support for Static IPv4 Addressing

To support an FN-RG pre-configured with an IP Address, AGF will need the following:

1. Configuration at Port/VLAN level to have IPv4 Address to match the SRC IP Address of the packets (ARP, IP Packets).
2. Line ID and/or Line ID Source for a Static Subscriber
   a. Can be locally configured for the IP Address mentioned in (1) to have a Line ID (Circuit ID and/or Remote ID)
   b. Can be configured for dynamic generation of GLI based on a pre-defined combination of any of the VLAN(s)/MAC Address/ PORT/IP Address/Hostname/etc.

Line ID and/or Line ID Source of the static subscriber must co-relate to a Line ID configured in the UDM for the service.

Notes:

- The dynamically generated Line ID should have at least one Network Supplied parameter like VLAN to ensure that the Line ID is secure.
- A single /32 IP Address is assigned by the 5GC during the PDU Session Establishment Procedure.

Procedure:

1. AGF will associate the SRC IPv4 Address of the first packet from the FN-RG with the configured or dynamically generated Line ID and generates the SUCI and SUPI.

2. AGF will initiate the Registration Procedure for the FN-RG.

3. AGF will initiate the PDU Session Setup Procedure using the NAS Signaling(ePCO) method to get the IPv4 Address assigned to the FN-RG in the 5GC. UDM should be already provisioned with the IP Address for the SUPI based on the Line ID for the FN-RG.

4. Based on the information available in UDM the 5GC will respond

   - with the same IP Address as the SRC IP Address of the packet which triggered the Registration and PDU Session Setup. AGF after comparing the SRC IP Address of the packet and the IP Address allocated by 5GC to be same, will provision the data path. (Success Case).

- with failure of authenticating the Line ID, AGF will clean up any user plane resources for the UE and flush the local 3GPP context. (Failure Case 1).
- with an IP Address which does not match the SRC IP Address of the packet, AGF will clean up the PDU Session State and UE Context by de-registering the FN-RG. (Failure Case 2).

5. A liveliness check based on ARP Ping or BFD or something similar can be used to update the FN-RG state to CM-IDLE or CM-CONNECTED.
6. Alternatively, an idle timer (no activity from the FN-RG) can also be used to update the FN-RG state to CM-IDLE.
7. Like other FN-RG models, a de-registration timer is started when the state is changed to CM-IDLE and triggers AN Release procedure on expiry of de-registration timer.

Notes:

- It is also possible to achieve a similar outcome by providing the same fixed IP address through PPP or DHCP signaling every time an FN-RG connects on the same Line-ID. For clarification, this section refers specifically to when an IP address is statically configured on the FN-RG, and there is no DHCP or PPP signaling.
- A change in the IP Address configured on the FN-RG can be detected via anti-spoof check based on MAC Address – IP Address mapping and Unicast RPF to avoid misuse of the resources. A detection of failure must trigger de-registration.

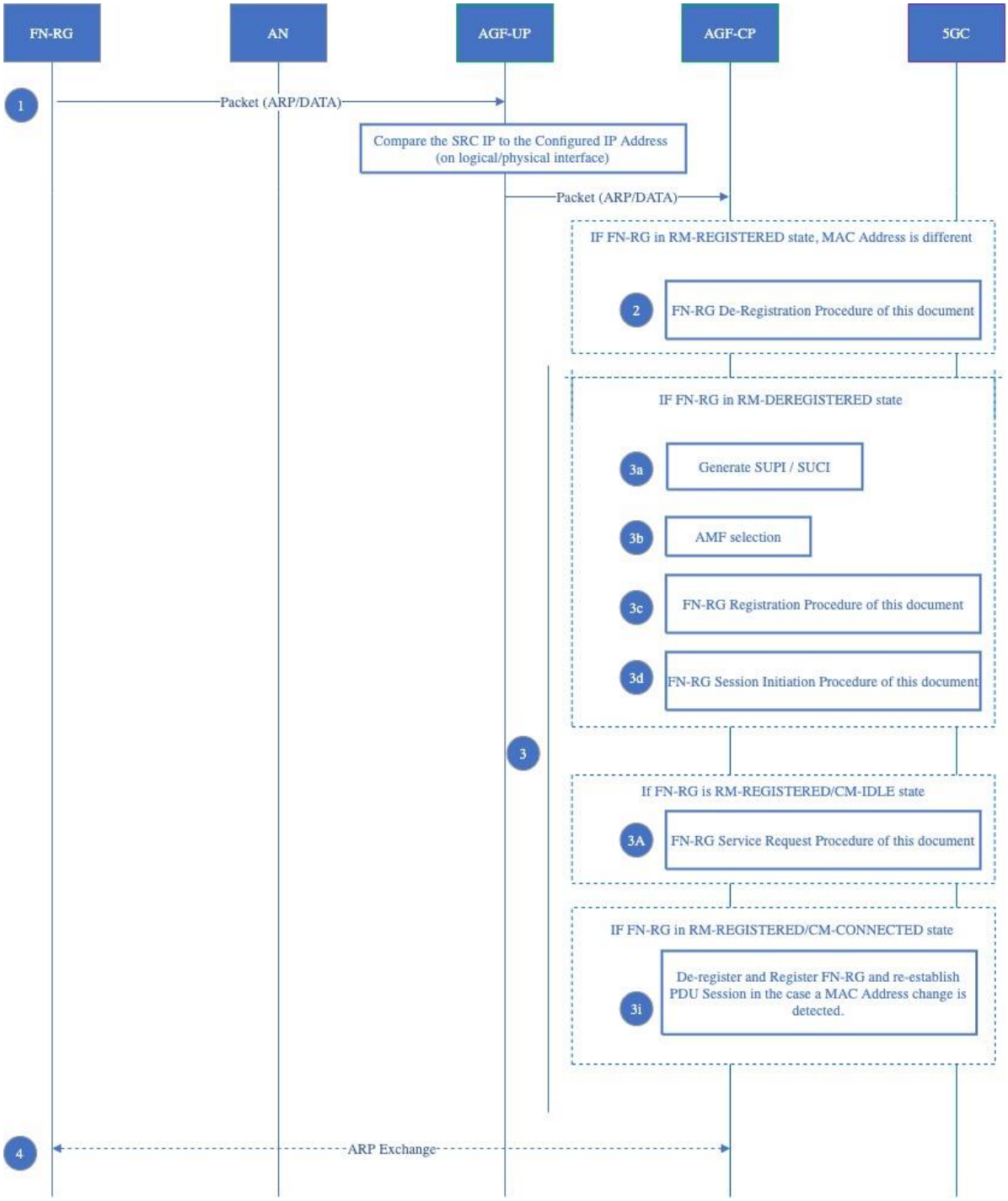

Figure 34: Call flow for static IPv4 assigned FN-RG

1. The first packet from a Statically Configured FN-RG could be an ARP or a Data Packet itself. Both these packets cannot carry the Circuit ID and/or Remote ID. The AN does not insert Circuit ID/ Remote ID in this case unlike where the FN-RG uses DHCP or PPP/PPPoE for IP Address allocation.

2. On receiving the packet, if the FN-RG is in the RM-REGISTERED state, the AGF- CP checks the FN-RG's MAC address with the information stored for Anti-Spoofing. The MAC Address should be

gleaned from the Ethernet header. If the gleaned information identifying the FN-RG is different compared to the FN-RG state on successful registration, the AGF interprets this as an equipment change and executes the AGF-CP initiated FN-RG Deregistration Procedure.

3. The AGF will then handle the IP session initiation according to the current registration and connection state:

   If the state is RM-DEREGISTERED:

   3a. The AGF stores the subscriber's information including the FN-RG customer equipment identifier, MAC Address, TCI, and port identification metadata.

   3b. The AGF-CP selects an AMF as per step 2 in TS 23.316 [23] subclause 7.2.1.3.

   3c. The FN-RG is registered into the 5GC based on the registration procedure described in section 8.1.6 (based on TS 23.316 [23], clause 7.2.1.3).

   3d. A PDU session is established.

   The AGF establishes a PDU session as defined in section 8.1.8 (based on TS 23.316 [23] clause 7.3.4). The formulation of PDU SESSION ESTABLISHMENT REQUEST by the AGF will adhere to the requirements in section 6.11 (FN-RG IP session initiation requirements).

   In case of Static IP Assignment, The PDU Session Type is IPv4. IPv6 and IPv4v6 are not applicable.

   The PDU session ID is allocated by the AGF.

   The 5GC, when formulating the reply to PDU SESSION ESTABLISHMENT REQUEST, considers the PDU session type requested by the AGF and the user's subscription data stored in UDM: the latter are authoritative.

   From the PDU SESSION ESTABLISHMENT ACCEPT received by the 5GC the AGF learns the type of PDU session that the subscriber is permitted to this information is in the Selected PDU Session Type field.

   If the state is RM-REGISTERED/CM-IDLE and the selected PDU session type is IPv4:

   3A. The AGF performs the Service Request Procedure for FN-RG. If there is no active PDU Session, AGF initiates a PDU Session Setup procedure.

   If the state is RM-REGISTERED/CM-CONNECTED and the selected PDU session type is IPv4:

   3i. The AGF continues to forward subscriber traffic until a change in MAC Address change is detected. On MAC Address change detection, AGF will block all the traffic by de-registration of the FN-RG. AGF will trigger new registration procedure followed by PDU Session Setup procedure.

4. The FN-RG will then typically resolve the MAC address of the default gateway with an ARP request (where the AGF proxies a reply with its own MAC address) as required in section 6.3.2.1 (L2/L3 Interworking).

Note: The use case where multiple IP Addresses are assigned to the same FN-RG Is for FFS.

8.2 For a 5G-RG

8.2.1 Registration Management Procedure for 5G-RG

Figure 35 shows the call flow for the registration management of a 5G-RG. It utilizes PPPoE to start 3GPP NAS registration with the 5GC. After the PPP LCP, the VSNCP Configuration Request is initiated by the 5G-RG and on a successful response from the AGF, the PPP VSNP channel is established. During Registration procedure the 3GPP NAS between the 5G-RG and the AGF is encapsulated in PPP VSNP. The AN parameters are sent by 5G-RG during registration procedure in PPP VSNP message as defined in TS 24.502 [12].

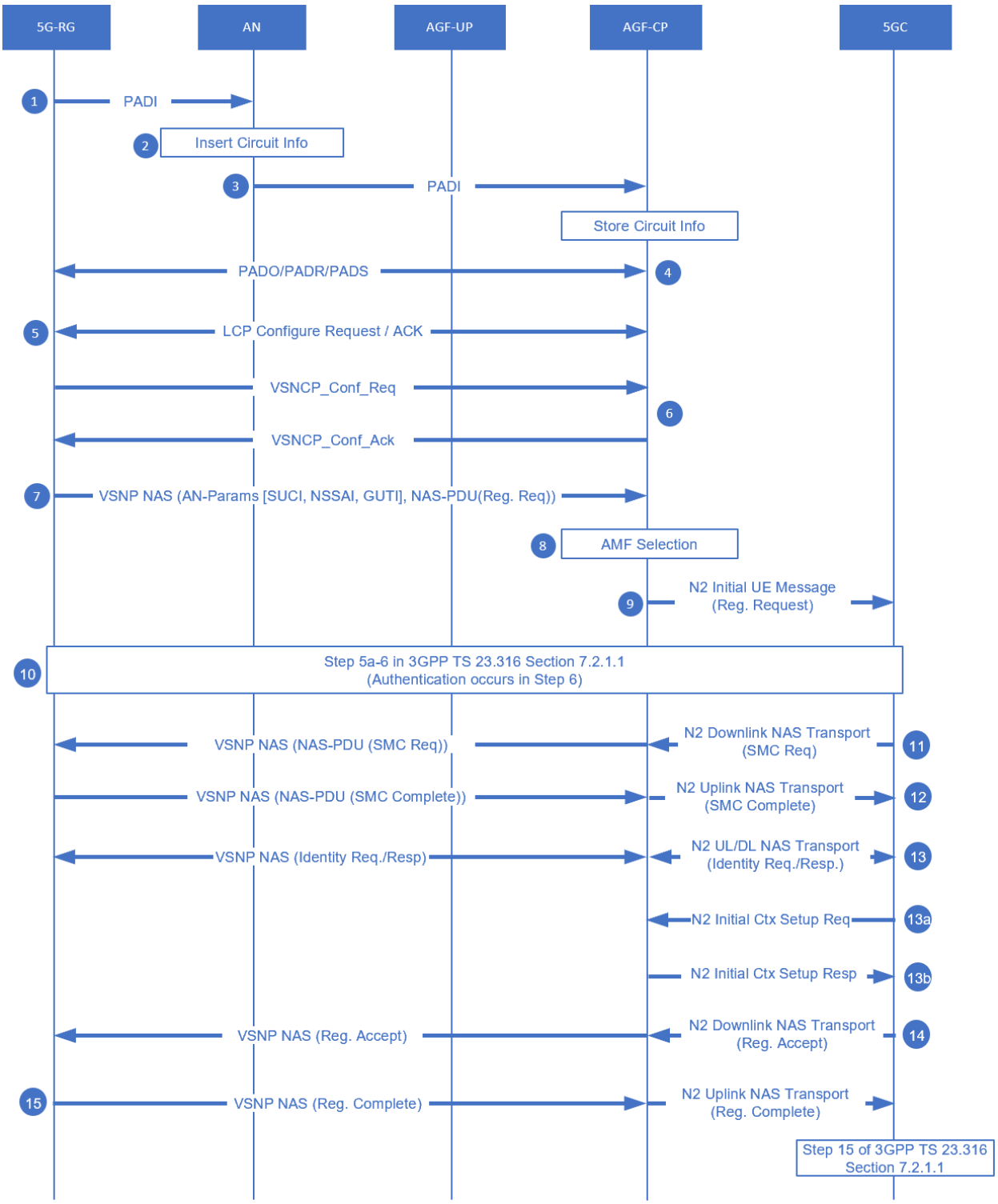

Figure 35: Call flow for the registration management procedure for a 5G RG

1. The 5G-RG starts a PPPoE session with a PADI message.
2. The AN receives the PPPoE PADI message and inserts PPPoE Tags into the PADI message. The PPPoE tags include PPPoE Circuit and Remote ID. The access node will insert vendor specific: 0x0de9 (IANA administered ADSL forum) option 0x01 “circuit-id” and option 0x02 “remote-id” information. This is required for authentication and serves as a location information for the 5GC.

3. The AN then forwards the entire message to the AGF-CP.
4. Once the AGF-CP receives the PADI message, the AGF-CP will store the subscriber's information based on both the Ethernet header and PPPoE tags. The 5G-RG will complete the PPPoE discovery process as outlined in section 5 in RFC 2516 [42]. After receiving the PADR message, the AGF-CP will allocate Session ID and send it to the 5G-RG via a PADS message. The Session ID will be used as the PPP encapsulation for the following LCP and VSNCP procedures between the 5G-RG and the AGF-CP to carry the 5G NAS signaling. The AGF-CP will store the Session ID into the 5G-RG context.
5. After the PPPoE discovery process completes, both the AGF-CP and 5G-RG establish the link layer with LCP packet message exchanges as described in section 5 of RFC 1661 [43].

   The LCP Configure-Request and Configure-Ack messages are exchanged between the 5G-RG and AGF-CP via the AN.

   The 5G-RG and AGF will not contain Authentication-Protocol (3) option in the LCP negotiations and, thus, no PPP authentication will be performed between the 5G-RG and AGF as described in Section 6.2 of RFC 1661 [43].

   For the 5G-RG, in addition to any other configuration options, the LCP 'configure-request' message must include the BBF defined Vendor Specific Option (VSO) using the ADSL forum IEEE administered OUI 0x256d as per RFC 2153 [39]:

   - RG type=5G-RG, this is to allow the AGF to recognize a 5G-RG and serve it accordingly. This is also to allow the 5G-RG to become aware of the PPP server capabilities and possibly downgrade to FN-RG upon receiving a Reject as response of the LCP Configuration-Request. If the 5G-RG cannot downgrade, LCP will fail to negotiate and stop at this stage.

   The AGF-CP will complete the LCP procedure by sending a Configure-Ack to the 5G-RG as specified in section 5.2 of RFC 1661 [43].
6. After LCP procedure, VSNCP procedures as per RFC 3772 [46] are used to open a VSNP encapsulated CP channel between the 5G-RG and the AGF.

   After this procedure, the vendor specific protocol channel is open for exchanging NAS and AS messages between 5G-RG and AGF-CP. Further NAS messages between the 5G-RG and the AMF, via the AGF-CP, must be inserted as a NAS TLV in the VSNP message as specified in section 9.7, where VSNP fragmentation will be used for NAS fragmentation.

   Further AS messages between the 5G-RG and the AGF-CP must be inserted as a AS TLV in the VSNP message as specified.
7. The 5G-RG will initiate the Registration procedure by initiating the Registration Request to the AGF-CP which includes:

   - A NAS-PDU field containing the NAS message (i.e., Registration Request) initiated by the 5G-RG; and
   - An AN-parameters field containing the access network parameters, GUTI, if available, selected PLMN, NSSAI, establishment cause, etc.

   Note: although PLMN selection is not supported for W-5GAN access, the 5G-RG still provides a selected PLMN ID in the AN parameters within the PPP VSNP message to the AGF.
8. The AGF-CP, on reception of the AN-parameters, MUST execute the AMF selection as per step 4 of TS 23.316 [25] clause 7.2.1.1.
9. The AGF-CP MUST forward the NAS message (Registration Request) to the selected AMF by sending an 'INITIAL UE MESSAGE' as specified in TS38.413 [16] Clause 8.6.

The AGF-CP MUST forward the Registration Request received from the 5G-RG within an N2 initial UE message (NAS message, Line ID based ULI, Establishment cause, UE context request, selected PLMN ID) as per step 4 of TS 23.316 [25] clause 7.2.1.1.

A unique RAN UE NGAP ID (identifier of RG level N2 interface, which is similar with RAN UE NGAP ID) will be allocated by the AGF-CP to be used for the 5G-RG and the AGF-CP must include this identity in the 'INITIAL UE MESSAGE'.

In addition, the AGF-CP will bind this RAN UE NGAP ID with the Session ID as received in Step 4 for transporting the NAS message between the 5G-RG and the AMF. Further NAS messages between the 5G-RG and the AMF will be forwarded with this binding.

10. After reception of the Registration Request, the 5GC may request for the identity of the 5G-RG in the form of SUCI, as per step 5 of TS 23.316 [25] clause 7.2.1.1.

    The AMF may also authenticate the 5G-RG (by invoking an AUSF) as per step 6 of TS 23.316 [25] clause 7.2.1.1. The AMF transfers the SUCI and the selected PLMN ID to the AUSF, that executes authentication of the 5G-RG.

11. The AMF sends a NAS Security Mode Command to 5G-RG via AGF-CP to activate NAS security. If the authentication was successful in Step 10 above, EAP-Success is sent in the EAP Container of the NAS Message for the authentication procedure in step 10 above is also encapsulated within this message as per step 7 of TS 23.316 [25] clause 7.2.1.1.
12. The 5G-RG completes authentication, creates a NAS security context and responds with an SMC complete message for the AMF, relayed via the AGF-CP.
13. The AMF may request PEI from the 5G-RG as per step 8, and performs step 9, involving the UDM as per step 9 of TS 23.316 [25] clause 7.2.1.1.

    The AMF sends a request for initial context information in N2 message as per step 10 of clause 7.2.1.1 of TS 23.316 [25]. This may include the RG Level Wireline Access Characteristics received from the UDM.

    Step12 from Figure 7.2.1.1 of TS 23.316 [25] follow where the 5GC is notified by the AGF-CP about the 5G-RG context creation.

14. The 5GC sends a NAS registration accept message to the AGF-CP as per step 13 of clause 7.2.1.1 of TS 23.316 [25]. This is conveyed to the 5G-RG via the newly established NAS channel in step 13 above.
15. The 5G-RG sends a NAS registration complete message via the AGF-CP to the 5GC, followed by step 15 in section 7.2.1.1 in TS 23.316 [25].

Note: For internal 5GC exchange of information, TS 23.316 [25] is the reference.

8.2.2 5G-RG Service Request Procedure via W-5GAN

In the general 3GPP case, the Service Request Procedure is initiated when there is no signaling connection between the UE, gNB and 5GC, but the UE is still registered in the 5GC. In W-5GAN access, this means that the AGF does not have any session information available about the 5G-RG stored in it, but the 5G-RG is registered in the 5GC. This implies that there is no initial VSNP connection channel or connectivity established between the 5G-RG and AGF when this procedure is initiated, and the 5G-RG appears as a new device for the AGF.

This procedure is initiated when:

- The 5G-RG is still registered in the 5GC, but the VSNP is not open. There is no pre-existing state associated with the RG in the AGF. The service request message from the 5G-RG triggers a VSNP response to open the channel.

- The Link has Flapped but the de-registration timer in the 5G-RG did not expire before connectivity was restored.

- The AGF is reset.

  The AGF performed a graceful AN release and N2 context release as well as closing the VSNP channel.

Note: A 5G-RG reset, or a link flap that exceeds the deregistration timer does not trigger the service request procedure as the 5G-RG will go through full registration and PDU session establishment.

This procedure is to be used by the 5G-RG

- In CM-IDLE state to request the re-establishment of the NAS signaling connection and re-establishment of UP for all or some PDU sessions associated to W-5GAN/non-3GPP access.

- In CM-CONNECTED state to request the re-establishment of UP for one or more PDU sessions associated to W-5GAN/non-3GPP access. Note the procedures described do not envision a use case for this scenario.

The procedure described below is initiated by the 5G-RG in CM-IDLE state and is as per clause 7.2.2.2 of TS 23.316 [25] with the following details/clarifications:

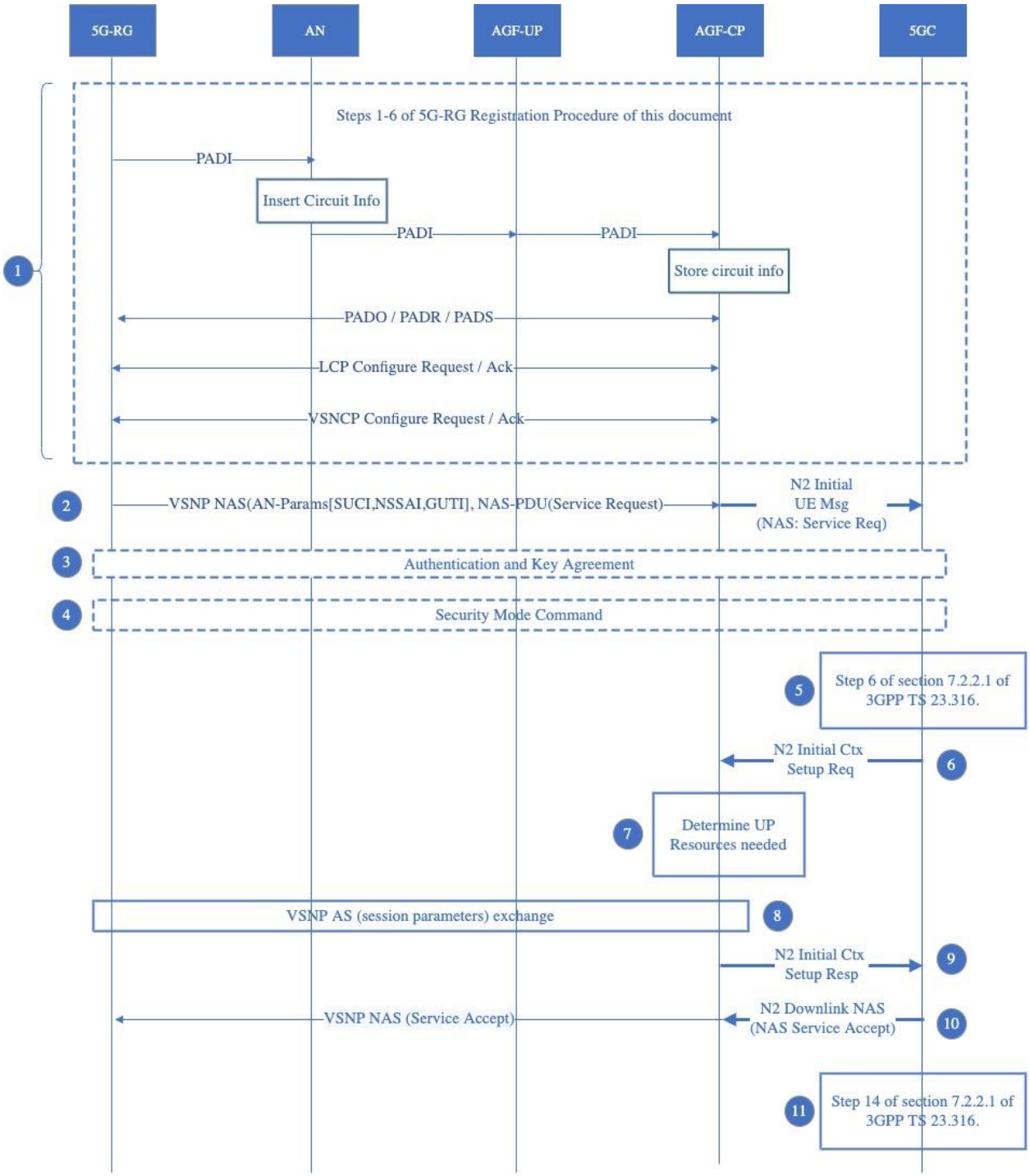

Figure 36: 5G-RG Triggered Service Request Procedure via W-5GAN

1. The 5G-RG connects to AGF-CP as per steps 1 to 6 of the 5G-RG registration procedure.
2. The 5G-RG sends the AN parameters and a NAS Service Request towards the 5GC via the AGF-CP in the PPP VSNP message. The AGF-CP forwards this Service Request to the 5GC within an N2 Initial UE message.
3. The 5GC initiates the NAS authentication procedure if the Service Request is not integrity protected as per step 5 of clause 7.2.2.1 in TS 23.316 [25].

4. The 5GC initiates the NAS Security Mode procedure as per step 7 of clause 7.1.1.1 in TS 23.316 [25].
5. Step 6 is executed in 5GC as per clause 7.2.2.1 in TS 23.316 [25].
6. The 5GC sends a N2 UE Initial Context Setup Request which contains the N2 SM information received from SMF(s), RG Level Wireless Access Characteristics, and other parameters to the 5G-RG as per step 7 of clause 7.2.2.1 in TS 23.316 [25].

   Note: This single message can setup the UP for several PDU sessions and some aspects of AS design are proposed based on this.

7. For every established PDU session, the AGF-CP determines which UP resources are required.
8. For every established PDU session, the AGF-CP and AGF-UP set up the UP resources via local configuration and/or AS exchange with the 5G-RG. This corresponds to step 11 of clause 7.2.2.1 in TS 23.316 [25].
9. After setting up the UP resources for all PDU sessions, the AGF-CP sends a N2 Initial Context Setup Response to the 5GC a per step 12 of clause 7.2.2.1 in TS 23.316 [25].
10. The 5GC sends a NAS Service Accept towards the message to the AGF-CP as per step 13 of clause 7.2.2.1 in TS 23.316 [25].
11. Further steps are executed in 5GC as per step 14 of clause 7.2.2.1 in TS 23.316 [25].

For the 5G-RG in CM-CONNECTED state and initiating the service request procedure as per clause 7.2.2.2 of TS 23.316 [25], the below clarifications are provided:

i. The service request from the 5G-RG in step 3 above consists of only the List of PDU Sessions To Be Activated and List of Allowed PDU sessions as per step 1 of clause 4.2.3.2 in TS 23.502 [29].

ii. This is followed by execution of steps 4 and 5 described above.

iii. The 5GC sends only the N2 SM information to the 5G-RG for step 6 described above, as per step 7 of clause 7.2.2.1 in TS 23.316 [25].

iv. Step 7 is executed as specified above where VSNP channel is established between 5G-RG and AGF-CP.

v. Steps 8 and 9 which are associated with UP resource setup also occur in this scenario.

vi. Steps 10-12 are executed for this scenario as specified above.

For 5G-RG in CM-CONNECTED state with network-initiated service request procedure, refer to clause 7.2.2.1 in TS 23.316 [25], which is in turn based on clause 4.2.3.3 of TS 23.502 [29].

8.2.3 5G-RG PDU Session Initiation/Establishment via W-5GAN

Figure 37 shows the call flow and message exchanges for the 5G-RG PDU Session Establishment Procedure via the W-5GAN.

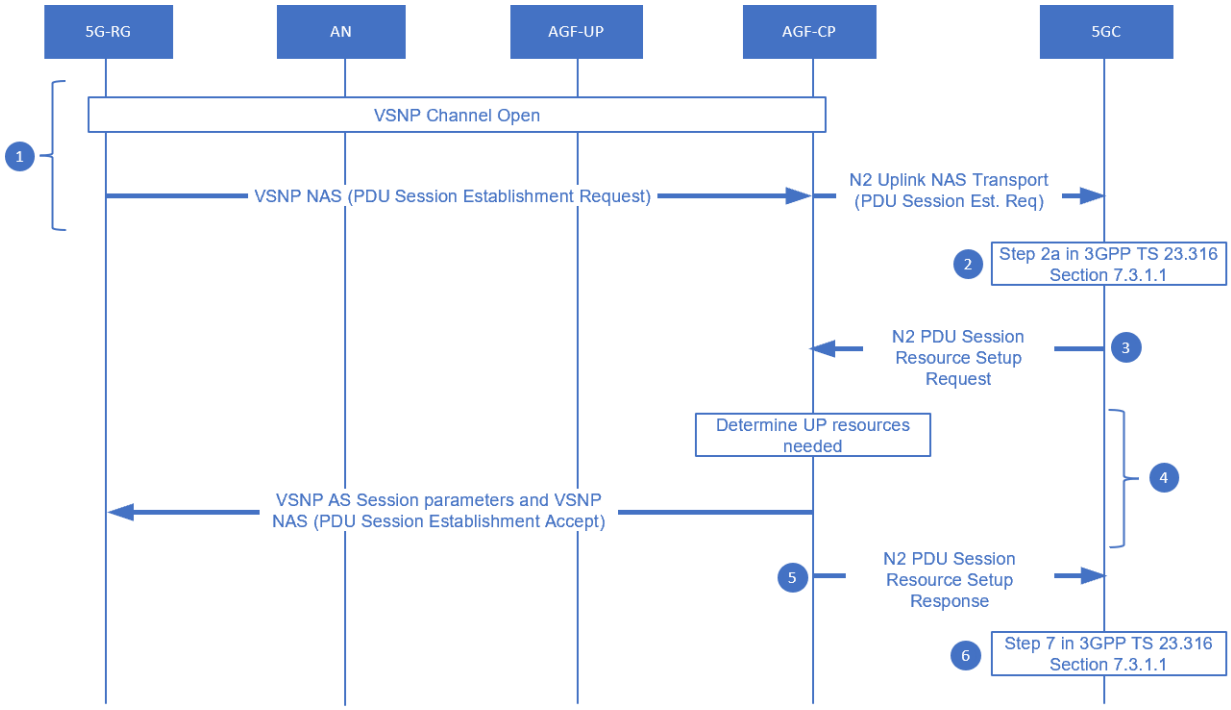

Figure 37: Call flow for 5G-RG Session Establishment via W-5GAN

1. For initiating PDU session establishment, it's a prerequisite that a VSNP channel is established and open between the 5G-RG and AGF-CP.

   The 5G-RG creates a PDU Session Establishment Request. This request first reaches the AGF-CP via the VSNP NAS channel as per step 1 of clause 7.3.1.1 in TS 23.316 [25].

   The AGF-CP forwards this message to the 5GC in uplink NAS message as per step 1 of clause 7.3.1.1 in TS 23.316 [25]. PCO is a part of this message.

2. On reception of the PDU Session Establishment Request, step 2a of clause 7.3.1.1 is executed in TS 23.316 [25].

3. The 5GC sends a N2 PDU Session Request message to the AGF-CP as in step 2b of clause 7.3.1.1 is executed in TS 23.316 [25]. Included in this message is an encapsulated PDU session accept message to be relayed to the 5G-RG upon completion of AN resource configuration.

4. The AGF-CP determines the UP resources for the PDU session based on the response from the 5GC as per step 3 of clause 7.3.1.1 is executed in TS 23.316 [25].

   The AGF-CP next sets up the UP resources in the AN for the 5G-RG as per step 4a of clause 7.3.1.1 executed in TS 23.316 [25]. Details are communicated to the 5G-RG via VSNP AS exchange.

   The AGF-CP can set up the UP resources with the 5G-RG via establishing a 5WE Session. After receiving N2 SM information from the SMF, the AGF-CP will generate AS session parameters and send them to the 5G-RG via VSNP AS message. The AS session parameters contains:

   - (a) the identity of the PDU Session associated with this 5WE Session
   - (b) QFI(s) associated with the 5WE Session and the default QFI,
   - (c) optionally an 802.1Q value and a DSCP value associated with each QFI,

- (d) the PDU Session user plane identification as a 5WE Session ID.

If 802.1Q PCP/DSCP value is included, the 5G-RG and AGF-UP will mark all traffic for this PDU Session according to the configuration of the marking/remarking for the specific 5QI/QFI.

- The AGF will always mark downstream frames with the indicated PCP value
- A 5G-RG will mark VLAN tagged frames with the indicated 802.1Q PCP value.
- A 5G-RG will use priority tagged frames to encode the indicated 802.1Q PCP value if the use of priority tagged frames is configured.
- If remarking of IPv4 and IPv6 packets is indicated by the RG-LWAC or local configuration the AGF will remark downstream frames with the indicated DSCP value
- If remarking of IPv4 and IPv6 packets is indicated to the 5G-RG by the AS session parameters TLV or local configuration, the 5G-RG will remark packets with the indicated DSCP value.

The AGF-CP sends the PDU Session Establishment Accept NAS IE received from the AMF encoded as a NAS TLV in a common SDU with an AS Session parameters TLV. This is based on Step 5 of clause 7.3.1.1 of TS 23.316 [25].

The AS session parameters are carried within the VSNP AS message as specified Section 5, with 5WE Session ID to use indicated in the discriminator portion of the session parameters information.

If the AGP-UP decides there is no suitable UP resources to be setup for the PDU Session, AGF-CP will directly sends a PDU Session Request Resource Setup Response to 5GC where the *PDU Session Resource Setup Unsuccessful Transfer* IE must be included containing a cause value as defined in TS38.413 [16].

5. The AGF-CP sends a PDU Session Request Resource Setup Response to the 5GC based on step 6 of clause 7.3.1.1 as executed in TS 23.316 [25]. The 5G-RG can send first uplink data to the UPF with the received AS parameters to encapsulate the data packet

6. This is followed by execution of step 7 of clause 7.3.1.1 in TS 23.316 [25] in 5GC. If the PDU session type is IPv4, IPv6 or IPv4/v6 and if there is no IP address/prefix included in the PDU Session Establishment Accept NAS IE, the 5G-RG will request the IP address/prefix via the established PDU Session using DHCP/DHCPv6 as specified in section 5.8.2 of TS23.501 [28]. The UPF can send first downlink data to the 5G-RG with the allocated IP address/prefix as Destination IP.

8.2.4 ACS Discovery

The 5G-RG can perform ACS Discovery as specified in clause 7.3.1.2 of TS 23.316 [25] and the ACS Discovery mechanism specified in clause 9.6.2 of TS 23.316 [25] is applicable.

As per clause 9.6.2 of TS 23.316 [25], the ACS information may be provided to the RG:

- Via DHCP interaction

  The RG sends a DHCPv4 Request, requesting for ACS information, and receives the same from the DHCP server.

- Via PCO during PDU session establishment procedure as in step 1 of section 8.2.3.

In case the SMF is to provide ACS information to the RG (via PCO or DHCP), it gets the ACS information from SMF subscription data. A DHCP server external to the SMF may also provide ACS information.

8.2.5 Deregistration Procedure for 5G-RG

Figure 38 shows the call flow for the deregistration of a 5G-RG from the 5GC. The deregistration procedure can either be 5G-RG initiated or 5GC-initated.

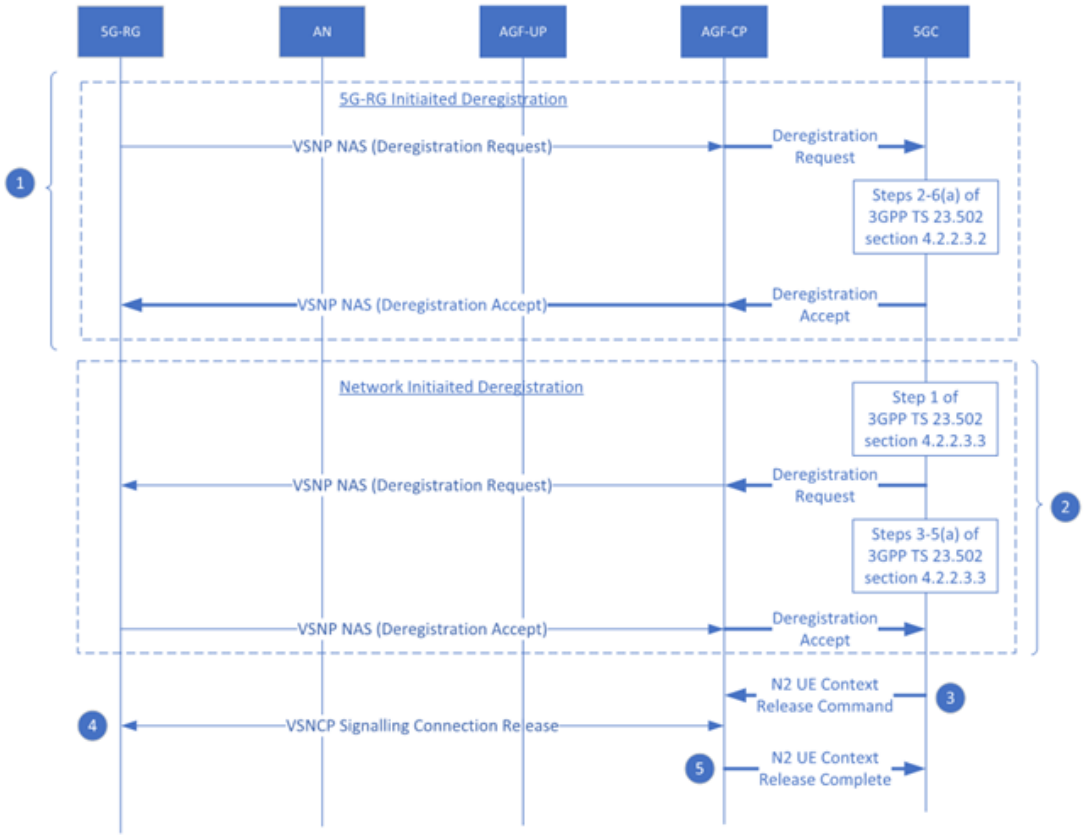

Figure 38: Call flow for the deregistration procedure for a 5G RG

1. The deregistration procedure for the 5G-RG from the 5GC network can be initiated by the 5G-RG itself and is specified in step (1a) of clause 7.2.1.2 in TS 23.316 [25], which is in turn based on UE-initiated deregistration procedure in TS 23.502 [29], clause 4.2.2.3.2.

   The 5G-RG sends a deregistration request towards the 5GC via the AGF-CP. This is followed by session release and policy termination mechanisms in 5GC. The 5GC then sends a deregistration accept message towards the 5G-RG via the AGF-CP.

2. The 5GC can also initiate the deregistration procedure towards the 5G-RG which is specified as Network-Initiated Deregistration in step (1b) of clause 7.2.1.2 in TS 23.316 [25], which is in turn based on clause 4.2.2.3.3 of TS 23.502 [29].

   A deregistration notification is first received from the UDM which triggers the AMF to send a deregistration request to the 5G-RG. This is followed by some message exchanges with the UDM, session release and policy termination.

   The 5G-RG sends a deregistration accept message to the 5GC via the AGF-CP.

3. The 5GC next sends a N2 UE Context Release Command to the AGF-CP as in step 2 of clause 7.2.1.2 in TS 23.316 [25].

4. The AGF-CP releases the signaling connection with the 5G-RG as in step 3 of clause 7.2.1.2 in TS 23.316 [25] and in the LCP procedures section of NAS and AS Transport and Information Elements in this document.

5. After the signaling connection is released with the 5G-RG, the AGF-CP sends a N2 UE Context Release Command message to the 5GC as in step 4 of clause 7.2.1.2 in TS 23.316 [25].

Note: The cause for the 5G-RG to initiate the deregistration procedure (or why the 5G-RG initiates this procedure) is for FFS and is described here for completeness. It implies a very graceful shutdown of connectivity for a fully functioning system that is normally just left on.

Note: A network-initiated deregistration is due to the loss of connectivity (and deregistration timer expiry) or business-related procedure where the subscriber is deactivated by UDM action (e.g., if the subscriber fails to pay their bills).

8.2.6 5G-RG or Network Requested PDU Session Modification via W-5GAN

The PDU session modification procedure for the 5G-RG, described in Figure 39, is as per clause 7.3 of TS 23.316 [25] with the following clarifications:

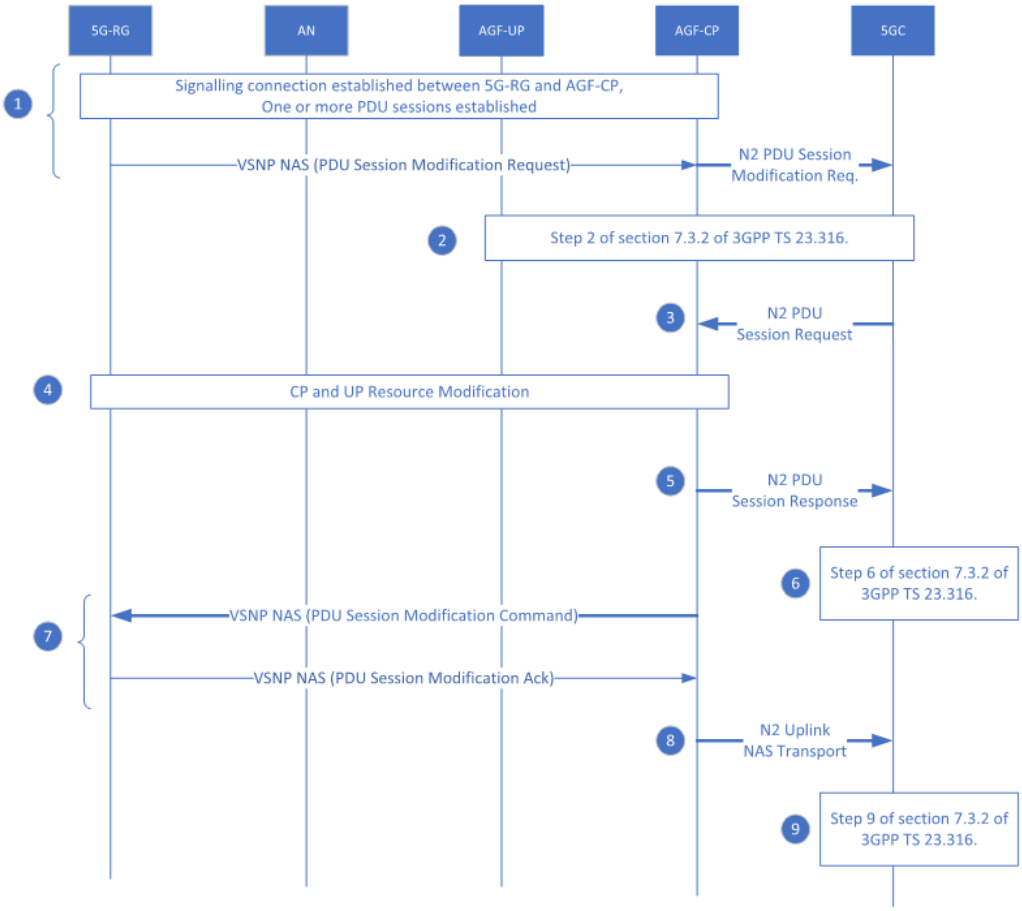

Figure 39: 5G-RG or Network Requested PDU Session Modification via W-5GAN

1. For initiating this procedure, it is a prerequisite that connectivity exists between the 5G-RG and AGF-CP and has at least one PDU session established.

   The 5G-RG creates a PDU Session Modification Request and sends it to 5GC via the AGF-CP as per step 1 of clause 7.3.2 in TS 23.316 [25].

2. This is followed by execution of step 2 of clause 7.3.2 in TS 23.316 [25].
3. The 5GC sends a N2 PDU Session Resource Modify Request to the AGF-CP as per step 3 of clause 7.3.2 in TS 23.316 [25].
4. The AGF-CP initiates the resource modification procedure for the CP and UP resources as per step 4 of clause 7.3.2 in TS 23.316 [25]. If there was any QoS flow added or removed, the AGF sends AS TLV updates to the 5G-RG with an updated set of QFI to PCP/DSCP mapping information.
5. The AGF-CP sends a N2 PDU Session Resource Modify Response towards 5GC as per step 5 of clause 7.3.2 in TS 23.316 [25].
6. The 5GC executes step 6 of clause 7.3.2 in TS 23.316 [25].
7. The AGF-CP sends the PDU Session Modification Command to 5G-RG and receives the PDU Session Modification Ack from the 5G-RG as per step 7 of clause 7.3.2 in TS 23.316 [25].
8. The AGF-CP forwards the PDU Session Modification Ack in an Uplink NAS Transport Message towards the 5GC as per step of clause 7.3.2 in TS 23.316 [25].
9. This is followed by execution of step 9 of clause 7.3.2 in TS 23.316 [25] in 5GC.

8.2.7 5G-RG or Network Requested PDU Session Release via W-5GAN

The PDU session release procedure for the 5G-RG, described in Figure 40, is as per clause 7.3.3 of TS 23.316 [25] with the following clarifications:

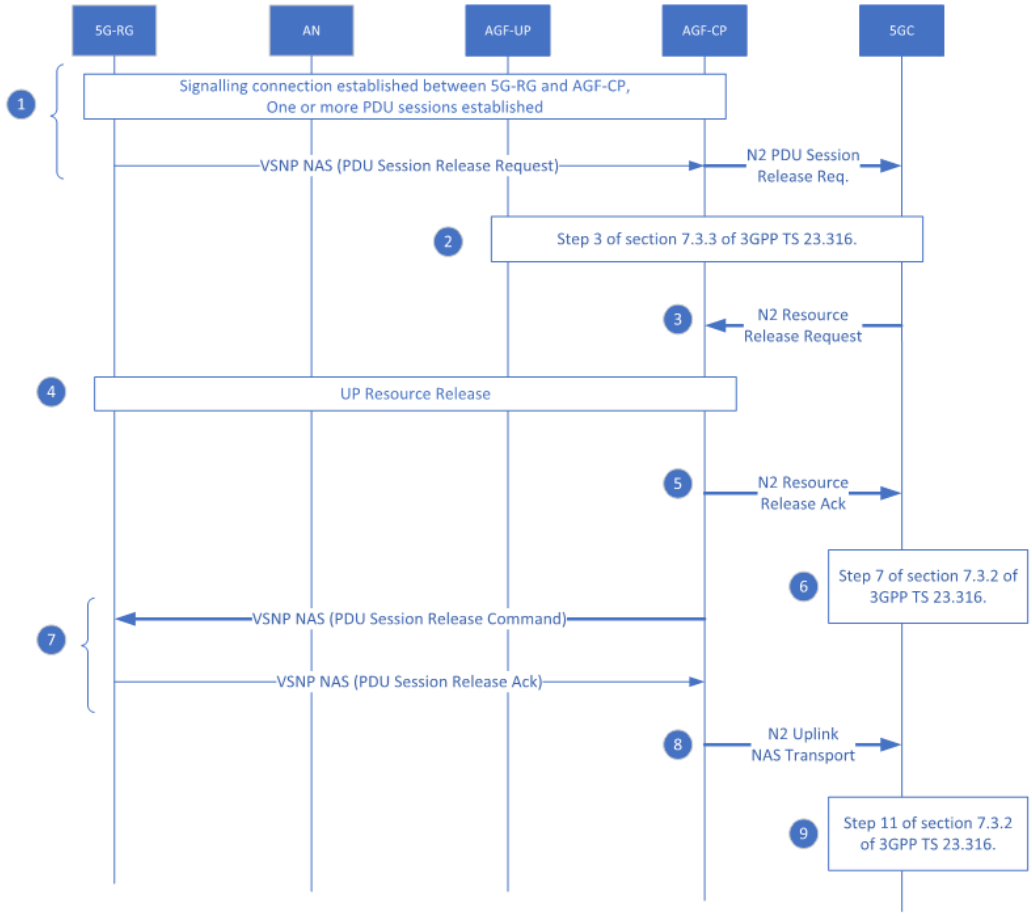

Figure 40: 5G-RG or Network Requested PDU Session Release via W-5GAN

1. For initiating this procedure, it is a prerequisite that connectivity exists between the 5G-RG and AGF-CP and has at least one PDU session established as per step 1 of clause 7.3.3 in TS 23.316 [25].

   The 5G-RG creates a PDU Session Release Request for the 5GC, which is forwarded by the AGF-CP as per step 2 of clause 7.3.3 in TS 23.316 [25].

2. The 5GC executes step 3 as in clause 7.3.3 in TS 23.316 [25].
3. The AGF-CP receives a N2 Resource Release Request from the 5GC as per step 4 of clause 7.3.3 in TS 23.316 [25].
4. Upon receiving the N2 Release Request message, the AGF-CP triggers the release of the corresponding UP resources and CP resources as per step 5 of clause 7.3.3 in TS 23.316 [25].

   This release process is purely a local action where the resources are entirely state and scheduler appearances.

5. The AGF-CP sends a N2 Release Ack towards the 5GC as per step 6 of clause 7.3.3 in TS 23.316 [25].
6. Step 7 is executed in 5GC as per clause 7.3.3 in TS 23.316 [25].
7. The AGF-CP sends a PDU Session Release Command towards the 5G-RG in a NAS message as per step 8 of clause 7.3.3 in TS 23.316 [25].

The 5G-RG responds towards the AGF-CP with a PDU Session Release Ack in a NAS message as per step 9 of clause 7.3.3 in TS 23.316 [25].

8. The AGF-CP forwards the PDU Session Release Ack in an Uplink NAS Transport Message towards the 5GC as per step 10 of clause 7.3.3 in TS 23.316 [25].
9. Step 11 is executed in 5GC as per clause 7.3.3 in TS 23.316 [25].

8.2.8 5G-RG AN Release via W-5GAN

The AN Release Procedure for the 5G-RG is used to release the NG-AP signaling connection and the associated N3 user plane connections between the W-5GAN and the 5GC. This procedure moves the 5G-RG from CM-CONNECTED to CM-IDLE in 5GC, and the 5G-RG related context information is deleted in the AGF-CP:

It is described in Figure 41 and is as per clause 7.2.5 of TS 23.316 [25] with the following clarifications:

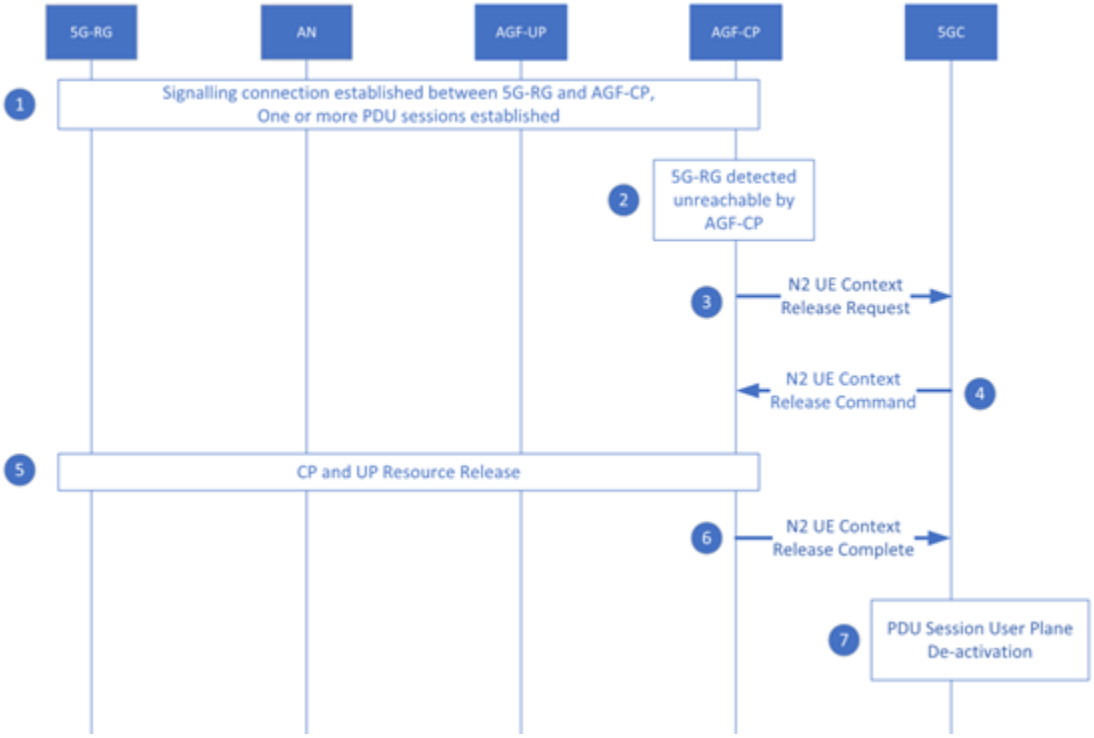

Figure 41: 5G-RG AN Release in AGF

1. It is a prerequisite that the 5G-RG is registered into the 5GC and may have one or more PDU sessions established as per step 1 of clause 7.2.5.2 of TS 23.316 [25].
2. The AGF-CP detects that the 5G-RG is unreachable, which serves as the trigger for initiating this procedure as per step 2 of clause 7.2.5.2 of TS 23.316 [25]. One way to check whether the 5G-RG is reachable or not is via the liveliness check by the LCP protocol using the LCP-ECHO message.
3. The AGF-CP sends a N2 UE Context Release Request to the 5GC as per step 3 in clause 7.2.5.2 of TS 23.316 [25].
4. The AGF-CP receives a N2 UE Context Release Command from the 5GC as per step 4 in clause 7.2.5.2 of TS 23.316 [25].

5. The AGF-CP initiates the release of CP and UP resources between the 5G-RG and AGF-CP as per step 5 of clause 7.2.5.2 of TS 23.316 [25]. The AGF may attempt to communicate the termination of both PDU sessions and the control connection to the 5G-RG via terminating the PPP link via LCP procedures and issuing a PADT message to the 5G-RG in addition to obligatory release and clean up of all session state for the 5G-RG local to the AGF. This would include 5WE session state, SDF filters and other artifacts of the active PDU sessions.

   Note: The communication of a cause code is FFS.

6. The AGF-CP next sends a N2 UE Context Release Complete to the 5GC as per step 6 of clause 7.2.5.2 in TS 23.316 [25].
7. This is followed by PDU session user plane deactivation in the 5GC as per step 7 of clause 7.2.5.2 in TS 23.316 [25].

8.2.9 CN-initiated selective deactivation of UP connection of an existing PDU session associated with W-5GAN access

The procedure described in TS 23.502 [29] clause 4.3.7 is applicable here for the scenario of W-5GAN access for the 5G-RG and FN-RG in the CM-CONNECTED state with the following clarifications:

1. NG-RAN is replaced by AGF.
2. The release of the user plane resources between the 5G-RG/FN-RG and AGF-CP is based on the procedures local to the AGF and 5G-RG.

8.2.10 5G-RG Configuration Update Procedure via W-5GAN

The 5G-RG Configuration Update procedure is used to update the 5G-RG configuration as per clause 7.2.3.1 in TS 23.316 [25] which includes:

- Access and Mobility Management related parameters like Configured NSSAI and its mapping to Subscribed S-NSSAIs, Allowed NSSAI and its mapping to Subscribed S-NSSAIs.

  When 5GC wants to change the 5G-RG configuration for access and mobility management related parameters, it initiates the procedure described in section 8.2.10.1 (5G-RG Configuration Update procedure for Access and Mobility Management related parameters).

- 5G-RG policy provided by PCF.

  When the PCF wants to update new UE policies in the 5G-RG, it initiates the procedure described in section 8.2.10.2 (5G-RG Configuration Update procedure for transparent Policy delivery).

Note: This procedure is transparent to the AGF, that is, it does not put any requirements on the AGF. It is included in this document so that the procedure descriptions have a common repository.

8.2.10.1 5G-RG Configuration Update procedure for Access and Mobility Management related parameters

This procedure can be further elaborated below based on clause 7.2.3.1 of TS 23.316 [25], which is in turn based on clause 4.2.4.2 of TS 23.502 [29]:

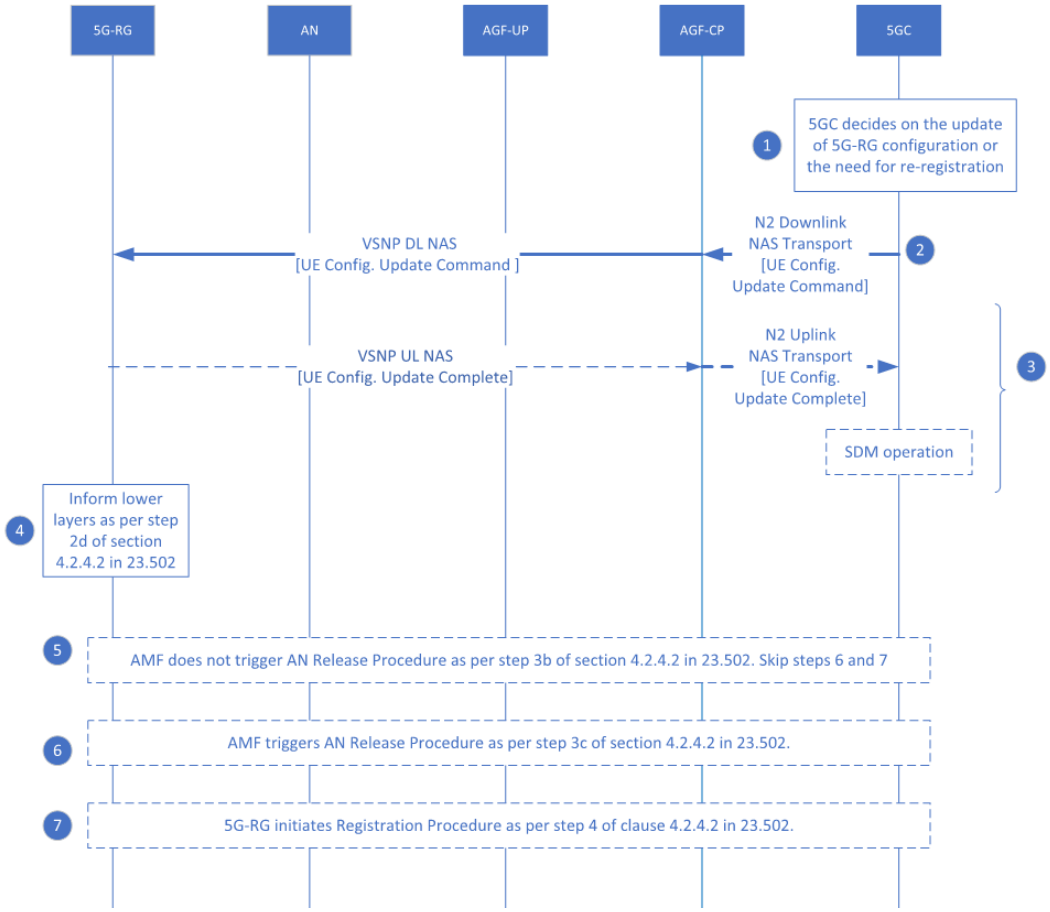

Figure 42: 5G-RG Configuration Update Procedure for access and mobility management related parameters via W-5GAN

1. The 5GC determines the need for 5G-RG configuration update or the re-registration procedure as per step 0 of clause 4.2.4.2 in TS 23.502 [29].

   If the 5G-RG is in CM-IDLE state, the 5GC waits until the 5G-RG is in CM-CONNECTED state as Network Triggered Service Request is not applicable in this scenario.

2. The 5GC sends a NAS Configuration Update Command to the AGF-CP in an N2 Downlink NAS Transport message with one or more 5G-RG configuration parameters as per step 1 of clause 4.2.4.2 in TS 23.502 [29]. The AGF-CP relays this message to the 5G-RG in the VSNP channel established between the 5G-RG and AGF-CP.

   Note: Refer to sub-clause 8.2.19 in TS 24.501 [11] for more details on IEs (Information Elements) for the message “Configuration Update Command” and sub-clause 9.2.5.2 of TS 38.413 [16] for IEs on “Downlink NAS Transport” message.

3. If applicable, the 5G-RG sends an acknowledgement for the UE Configuration Update Indication (if set in the message in step 2 above) via the Configuration Update Complete message as per step 2a of clause 4.2.4.2 in TS 23.502 [29]. This NAS message is sent to the AGF-CP through the established VSNP channel and then relayed to the 5GC in an N2 Uplink NAS Transport message.

   The 5GC may also perform an SDM operation to indicate to the UDM that the 5G-RG has received the subscription change indication as per step 2b of clause 4.2.4.2 in TS 23.502 [29].

   Step 2c of clause 4.2.4.2 in TS 23.502 [29] is not applicable here

4. If the 5G-RG is configured with a new 5G-GUTI above and registered to both wireless and 3GPP access, it informs the 3GPP access' lower layers about the new configuration update information as per step 2d of clause 4.2.4.2 in TS 23.502 [29].
5. Step 3a of clause 4.2.4.2 in TS 23.502 [29] is not applicable here.

   If the existing connectivity to the network slices is not affected with the new parameters sent to the 5G-RG, the 5GC does not release the NAS signaling connection for the 5G-RG after receiving the acknowledgement in step 3 above and no immediate registration is required, as per step 3b of clause 4.2.4.2 in TS 23.502 [29]. The steps 6 and 7 described below are skipped.
6. If the existing connectivity to the network slices is affected due to the update with new parameters, the 5GC in its UE Configuration Update Command message includes the new network slice information as per step 3c of clause 4.2.4.2 in TS 23.502 [29].

   If the 5GC cannot provide the new network slice information, it sends an indication to the 5G-RG to initiate the registration procedure. After receiving the acknowledgement in step 3 above, the 5GC releases the NAS signaling connection for the 5G-RG as per step 3c of clause 4.2.4.2 in TS 23.502 [29].
7. Followed by step 6 above, the 5G-RG initiates the registration procedure after it enters the CM-IDLE state as per step 4 of clause 4.2.4.2 in TS 23.502 [29].

8.2.10.2 5G-RG Configuration Update procedure for transparent Policy delivery

This procedure is initiated by the 5GC (i.e., PCF) to change or provide new 5G-RG policies in the 5G-RG. This is as per clause 7.2.3.1 in TS 23.316 [25], which is in turn based on clause 4.2.4.3 in TS 23.502 [29]:

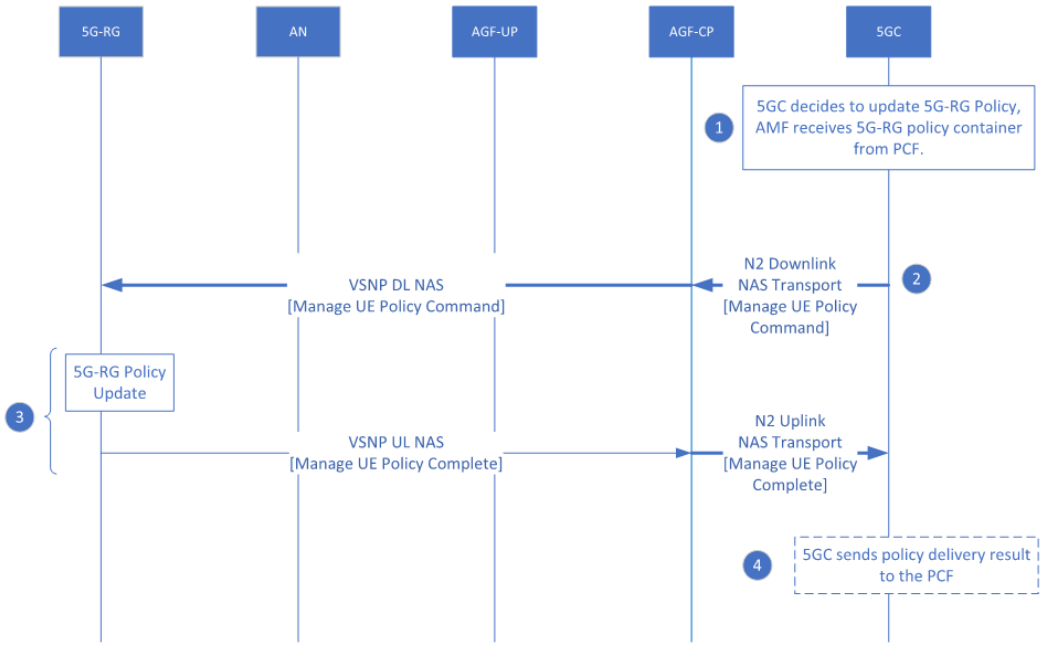

Figure 43: 5G-RG Configuration Update Procedure for transparent UE policy delivery via W-5GAN

1. The 5GC (or PCF) decides to update the 5G-RG policies based on the triggering conditions as per step 0 of clause 4.2.4.3 of TS 23.502 [29].

The AMF (in 5GC) receives the UE policy container from the policy function (PCF) as per step 1 of clause 4.2.4.3 of TS 23.502 [29].

2. The 5GC sends the policy container in the Manage UE Policy Command message to the AGF-CP in an N2 Downlink NAS Transport message, and the AGF-CP relays this NAS message to the 5G-RG in the established VSNP channel as per step 3 of clause 4.2.4.3 of TS 23.502 [29].

   Note: The IE “Payload Container Type” is set to “UE Policy Container” as per TS 24.501 [11] subclause 8.2.11 and annex D.

3. The 5G-RG updates its policy provided by the 5GC and sends the result to the AGF-CP in a NAS message as Manage UE Policy Complete in the established VSNP channel.

   The AGF-CP relays this message to the 5GC in an N2 Uplink NAS Transport message per step 4 of clause 4.2.4.3 of TS 23.502 [29].

4. The AMF (in 5GC) may send this response from the 5G-RG to the 5GC policy function (PCF) as per step 5 of clause 4.2.4.3 of TS 23.502 [29].

9 Annex: Requirements on the 3GPP core

The following annex is a normative text addressed at the 5G core. The requirements contained here have been or are to be communicated to 3GPP. Those requirements are in addition, and/or overriding, of 3GPP requirements in order to support RG-based customers.

9.1 Framed Route:

In case an UPF has to serve wireline users, it must support framed routing. Moreover, the support of framed routing is mandatory for a combined AGF/UPF.

1. UPF requirement-1: A UPF used to service an FN-RG or a 5G-RG MUST support framed routing.
2. UPF requirement-2: A UPF used to service an FN-RG or a 5G-RG MUST indicate to SMF the support of framed routing by setting the FRRT flag in the UP Function Features IE, as documented in TS 29.244 [17].

10 Appendices

10.1 NAS Timers and WWC

The following is a non-normative overview of NAS timers and their relevance to FN-RG and 5G-RG support. All timers used by a 5G NAS stack are referenced in TS24.501 [11]. Note that where appropriate the requirements in section 0 supersede the “action upon expiry” described in the following tables.

1) Older timers imported into TS24.501 [11]

Timer	Initiation Cause	Duration	Action upon Expiry	Comments
T3245	A PLMN added to the forbidden list	12h to 24h	Erase the forbidden PLMN list	
T3247	Registration rejection with some form of “not allowed” cause	Random value range 30m to 60m	If still needed, retry registration	
T3324				Applies to MICO mode, not relevant for WWC
T3346	NAS request rejected with a T3345 congestion back off timer value	Communicated in NAS message	If still needed retry registration	
T3396	Session management request rejected with a T3396 DNN congested timer value	Communicated via NAS message	NAS communication for that DNN may resume	
Back-off	Back off indicated instead of T3396	Communicated via NAS message	Retry any PDU session management messages for this DNN	Can be considered to be interchangeable with T3396
T3444				Applies to UE configuration for eCall. Not applicable to WWC

T3445				Applies to UE configuration for eCall. Not applicable to WWC
T3447				Relates to “service gap”. Not applicable to WWC
T3448				CIoT related. Not applicable to WWC

2) Mobility Management Timers

Timer	Initiation Cause	Duration	Action upon Expiry	Comments
T3502	5 registration attempts rejected	12m	Retry registration if needed	
T3510	Registration request sent	15s	Retry registration	Normal NAS retry
T3511	Registration request retried after lower layer failure	10s	Retry registration	If request rejected by some lower layer error
T3512	UE enters IDLE state when periodic re-registration is required	54m	Update registration	Not applicable to WWC
T3513	Paging initiated	6s		Not applicable to WWC
T3516	Registration or service request sent	30s		For WB-N1 IoT mode. Not applicable to WWC
T3517	Service request sent	15s	Service request retry	Normal NAS retry
T3519	Transmission of identity response or registration/deregistration with a new SUCI	60s	Delete stored SUCI	Applicable but should not affect FN-RG interaction
T3520	Sending Authentication failure or Authentication response	15s		Related to EAP and 5G-AKA processing. Not applicable to FN-RG
T3521	Deregistration indicated for reasons other than a switch off.	15s	Retry	Normal NAS retry
T3522	Deregistration initiated	6s	Retry	Normal NAS retry
T3525	T3517 expired and service requests >= 5	60s	Retry service request	Applicability is FFS
T3540	Deregistration request	10s	Release NAS channel	

T3550	Registration accept sent	6s	Retry	Normal NAS retry
T3555	Configuration update sent	6s	Retry	Normal NAS retry
T3560	Authentication request or security mode sent	6s	Retry	Normal NAS retry
T3565	Notification sent	6s	Retry	Normal NAS retry
T3570	Identity Response sent	6s	Retry	Normal NAS retry

3) NAS Session Management Timers

Timer	Initiation Cause	Duration	Action upon Expiry	Comments
T3580	PDU Session Establish Sent	16s	Retry	Normal NAS Retry
T3581	PDU Session Modify Sent	16s	Retry	Normal NAS Retry
T3582	PDU Session Release Sent	16s	Retry	Normal NAS Retry
T3583	UE creates or updates a derived QoS rule	60s	Delete QoS rule	For aging out of QoS rules generated by RQI processing. Not currently applicable to FN-RGs
T3584	Session rejected with cause code of 67	Communicated in NAS message	Retry	Usually “reject due to insufficient resources” for slice and DNN
T3585	Session rejected with cause code of 69	Communicated in NAS message	Retry	Usually “reject due to insufficient resources” for slice
T3590	PDU Session Authentication Sent	15s	Retry	Normal NAS Retry
T3591	PDU Session Modification Sent	16s	Retry	Normal NAS Retry
T3592	PDU Session Release Sent	16s	Retry	Normal NAS Retry
T3593	Receipt of PDU Session modification complete with cause code of #39	60s	Rip PDU session state	Used as part of SSC mode 3 re-homing of sessions in a different UPF. SSC mode 3 must not be used with FN-RG support so is not applicable to an AGF.

End of Broadband Forum Working Text TR-456