Technical Report

TR-470

5G Wireless Wireline Convergence Architecture

Issue: 2

Issue Date: March 2022

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 Editor	Changes
01	25 August 2020	25 August 2020	Bouchat Christele, Nokia	Original
02	1 March 2022	1 March 2022	Bouchat Christele, Nokia Manuel Paul, Deutsche Telekom	• Multiple IP session support for FN-RGs • Additional authentication in the form of PAP/CHAP support for FN-RGs • Extensions to RG-LWAC • Use cases, clarification and guidance

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

Editors: Christele Bouchat, Nokia
Manuel Paul, Deutsche Telekom

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 5G Wireless Wireline 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 and beyond, including network functions for adapting wireline access onto the 5G Core.

It enables several deployment scenarios, which are described in this document, to support different network environments, starting points and priorities, with different cases in terms of Residential Gateway (RG) type, access networks and interfacing model with the 5G Core. As part of these scenarios, devices supporting 3GPP procedures, connected to the RG via the Wi-Fi in the LAN and/or over the RAN, may also access the 5G core network.

In addition, this document defines information elements that are common to multiple BBF specified functions in the 5G WWC architecture. It also covers relevant QoS aspects.

1 Purpose and Scope

1.1 Purpose

The advent of 5G is seen by operators as an opportunity to converge the fixed and mobile side of their networks beyond structural convergence, where fixed and mobile functions coexist over a shared infrastructure (e.g., Cloud CO). In particular, functional convergence provides a single control plane for wireline and wireless sessions. Motives for convergence are varied but include:

- Offering their customers a seamless, access-independent service experience
- Enabling multi-access connectivity
- Streamlining the set of network functions required to operate their network
- Achieving common technology, on-boarding, training and services between fixed and mobile divisions
- Enabling common subscriber management
- Extending the geographical reach of their 5G core networks
- Extending the service offering of their fixed access

This is in addition to the new service capabilities enabled by the 5G Core (5GC).

Wireless-Wireline Convergence (WWC) requires a substantial architecture and operation transformation, as some assets become shared, instead of being dedicated per access type. This transformation has to account for the large installed base of wireline subscribers, as a result, broadband line migration is a major aspect of 5G WWC Architecture.

The Broadband Forum worked in cooperation with 3GPP to define how fixed access can integrate with the 5G core. The key concerns raised by operators and embodied in the work are:

1. The fact that no two operators will have the same starting point in the journey to 5G.
2. The need to eliminate as many dependencies as possible so that transformation steps can be implemented without major coordination between network domains.
3. The need for deployment flexibility in how 5G components are introduced into the network.

This document serves as a guide to the WWC architecture jointly defined by 3GPP and BBF. In addition, it defines certain information elements that are common to multiple BBF specified functions in the architecture.

1.2 Scope

This document describes the 5G WWC architecture. It is a companion of the following BBF suite of documents:

- TR-456 "AGF Functional Requirements"
- WT-457 "FMIF Functional Requirements" – BBF work in progress
- WT-458 "CUPS for AGF" – BBF work in progress
- TR-124 "Functional Requirements for Broadband Residential Gateway Devices" Issue 6 and beyond
- TR-181 "Device Data Model for TR-069" Issue 2 Amendment 13, and subsequent amendments,

as well as the 3GPP documents TS 23.501 and TS 23.316.

BBF 5G WWC specification work results in different phases of deliverables. This is the second issue of the document and adds:

- Multiple IP session support for FN-RGs
- Additional authentication in the form of PAP/CHAP support for FN-RGs
- Extensions to RG-LWAC
- Use cases, clarification and guidance

to the architecture described in TR-470 Issue 1.

Certain topics are in scope of the WWC work but to date are not or only partially covered, such as: multicast-based IPTV, wholesale scenarios, hybrid access, support for 3GPP procedures in the home, control-user plane separation, VLAN delineation use case (as alternative to 5WE), lawful intercept and FMIF. These topics are expected to be covered in future issues of this document.

In this document, it is assumed that the AGF and 5G Core are operated by the same network operator, while the rest of the wireline access network may be operated by a 3rd party access wholesale operator. Other wholesale scenarios, including AGF and 5GC operated by different operators, are for further study.

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 [RFC2119] [1] [RFC8174] [2] when, and only when, they appear in all capitals, as shown here.

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] RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[2] RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words	IETF	2017
[3] TR-069 Amendment 6	CPE WAN Management Protocol	BBF	2018
[4] TR-369 Amendment1	User Service Platform (USP) Protocol	BBF	2020
[5] TR-101 Issue2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[6] TR-181 Issue 2 Amendment 14	Device Data Model for TR-069	BBF	2020
[7] TR-124 Issue 7	Functional Requirements for Broadband Residential Gateway Devices	BBF	2021
[8] TR-131	ACS Northbound Interface Requirements	BBF	2015
[9] TR-134 Corr1	Broadband Policy Control Framework	BBF	2013
[10] TR-146	Subscriber Sessions	BBF	2013
[11] TR-177 corrigendum1	IPv6 in the context of TR-101	BBF	2017
[12] TR-178 Issue2	Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2017
[13] TR-187 Issue 2	IPv6 for PPP Broadband Access	BBF	2013
[14] TR-348	Hybrid Access Broadband Network Architecture	BBF	2016
[15] TR-378	Nodal Requirements for Hybrid Access Broadband Networks	BBF	2019
[16] TR-456	AGF Functional Requirements	BBF	2022

[17] WT-457	FMIF Functional Requirements (currently under specification)	BBF	Not published yet
[18] WT-458	CUPS for AGF (currently under specification)	BBF	Not published yet
[19] TR-459	CUPS for disaggregated BNG	BBF	2020
[20] TS 23.316	Wireless and wireline convergence access support for the 5G System	3GPP	For R16
[21] TS 23.003	Numbering, addressing and identification	3GPP	For R16
[22] TS 23.214	Architecture enhancements for control and user plane separation of EPC nodes	3GPP	For R16
[23] TS 23.401	Technical Specification Group Services and System Aspects; GPRS enhancements for E-UTRAN access	3GPP	For R15
[24] TS 23.501	System architecture for the 5G System (5GS)	3GPP	For R16
[25] TS 23.502	Procedures for the 5G System (5GS)	3GPP	For R16
[26] TS 23.503	Policy and charging control framework for the 5G System (5GS); Stage 2	3GPP	For R16
[27] TS 24.501	Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage3	3GPP	For R16
[28] TS 24.526	User Equipment (UE) policies for 5G System (5GS); Stage 3	3GPP	For R15
[29] TS 29.413	Application of the NG Application Protocol (NGAP) to non-3GPP access	3GPP	For R16
[30] TS 29.502	5G System; Session Management Services; Stage 3	3GPP	For R16
[31] TS 29.510	5G System; Network function repository services; Stage 3	3GPP	For R16
[32] TS 33.501	Security architecture and procedures for 5G system	3GPP	For R16
[33] TS 36.300	Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage2	3GPP	For R15
[34] TS 38.413	NG-RAN; NG Application Protocol (NGAP)	3GPP	For R16
[35] RFC 1334	PPP Authentication	IETF	1992
[36] RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)	IETF	1996
[37] RFC 7542	The Network Access Identifier	IETF	2015
[38] RFC 8822	5G Wireless Wireline Convergence User Plane Encapsulation (5WE), IETF, April 2021	IETF	2021
[39] ITU-T G.984.3	Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification	ITU-T	2014
[40] ITU-T G.987.3	10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification	ITU-T	2014
[41] ENISA	ENISA Threat Landscape Report 2018	ENISA	2018

2.3 Definitions

The following terminology is used throughout this Technical Report.

5G-RG	A RG acting in a role of a 3GPP UE towards the 5GC and exchanges N1 signalling with the 5GC.
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.
FN-RG	A RG connecting a home LAN to the WAN, which does not exchange N1 signalling with the 5GC.
Hybrid Access	Access that utilizes both wireline access networks and wireless access networks. From the perspective of a RG, 5G-RG or UE. This can either be exclusive or simultaneous access.
IP and PDU sessions	Where used, the term IP session refers to the BBF concept of an IP session as documented in TR-146 [10]. Where used, the term PDU session refers to the 3GPP concept as defined in TS 23.501 [24]. 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 [10], 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.
N1	Reference point between the 5G-RG and the AMF and between the W-AGF 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.
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 Network	Access network conforming with TR-101 [5]/TR-178 [12], that can be for example optical fiber. 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, we only consider NG-RAN as specified by 3GPP.

Definitions of 3GPP concepts: the following definitions summarize 3GPP definitions. In case of inconsistency between the text in the following and the 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 [24]).
Network Slice	A logical network that provides specific network capabilities and network characteristics (definition from TS 23.501 [24]).
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 [24]).
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 [24].
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 [24].
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 [24]).
Requested NSSAI	An NSSAI provided by the UE to the Serving PLMN during registration. The Requested NSSAI is defined in TS 23.501 [24].
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 [24] and the format of S-NSSAI is defined in TS 23.003 [21].
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 [20] and [25].

Session Management Function (SMF)	The SMF is a 5GC control plane function. For detailed specification of SMF refers to 3GPP documents [20], [24], [25] and [26]. 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 and QoS enforcement, including traffic usage report control.
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 [26]. The specification for supporting W-5GAN are described in this document and in [20].
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 [24] and the format of the GUAMI is defined in TS 23.003 [21].

2.4 Abbreviations

This Technical Report uses the following abbreviations:

5WE	5G Wireless Wireline Convergence User Plane Encapsulation
5GC	5G Core Network
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 Bit Rate
AMF	Access and Mobility Management Function
AN	Access Network
API	Application Programming Interface
AS	Access Stratum
ATSSS	Access Traffic Steering, Switching and Splitting
ATSSS LL	ATSSS Low Layer
AUSF	Authentication Server Function
AVP	Attribute Value Pair
BBF	Broadband Forum
BPCF	Broadband Policy Control Function
BNG	Broadband Network Gateway
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DL	DownLink
DN	Data Network
DNN	Data Network Name
DSCP	Differentiated Services Code Point
EAP	Extensible authentication Protocol
ES	End System
FMC	Fixed Mobile Convergence
FN-RG	Fixed Network Residential Gateway
FFS	For Further Study
GBR	Guaranteed Bit Rate
GLI	Global Line Identifier
GTP-U	GPRS Tunneling Protocol User Plane
GW	Gateway
IMSI	International Mobile Subscriber Identity
L2TP	Layer two Tunneling Protocol
LAC	Location Area Code
LCP	Link Control Protocol
LNS	Local Network Services
LTE	Long Term Evolution
MCC	Mobile Country Code
MFBR	Maximum Flow Bit Rate
MNC	Mobile Network Code
MPTCP	Multi Path TCP
MSBN	Multi-Service Broadband Network
MS-BNG	Multi-Service BNG
N3IWF	Non-3GPP Interworking Function
NAS	Non Access Stratum
NAT	Network Address Translation
NEF	Network Exposure Function
NFV	Network Function Virtualization

NFVI	NFV Infrastructure
NGAP	Next Generation Application Protocol
NG-RAN	Next Generation Radio Access Network
NID	Network Interface Device
OAM	Operations, Administration and Management
OLT	Optical Line Termination
ONT	Optical Network Termination
OSS	Operations Support Systems
PCP	Priority Code Point
PCF	Policy Control Function
PCO	Protocol Configuration Options
PLMN	Public Land Mobile Network
PMF	Performance Measurement Function
PON	Passive Optical Networking
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PSA	PDU Session Anchor
QFI	QoS Flow Identifier
RAN	Radio Access Network
RG	Residential Gateway
RG-LWAC	RG-Level Wireline Access Characteristics
RQA	Reflective QoS Attribute
RQI	Reflective QoS Indicator
RS	Router Solicitation
SDN	Software-Defined Networking
SMF	Session Management Function
SOHO	Small Office Home Office
STB	Set Top Box
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TC	Traffic Control
TCP	Transmission Control Protocol
TD	Traffic Descriptor
TLS	Transport Layer Security
TLV	Type, Length, Value
UDM	Unified Data Management
UDR	User Data Repository
UE	User Equipment
UL	Up Link
ULI	User Location Information
UNI	User Network Interface
UPF	User Plane Function
URSP	UE Route Selection Policy
USP	User Services Platform
VSNP	Vendor Specific Network Protocol
W-AGF	Wireline Access Gateway Function
WWC	Wireless Wireline Convergence

3 Inventory of Functions and Relevant Specifications

Figure 1 illustrates the set of functions and interfaces that realizes the use cases targeted by the BBF and 3GPP Rel-16 WWC work. Included are scenarios where LTE is supported by EPC interworking and the E-UTRAN presents an S1 interface, and where LTE interworking is supported in the NG-RAN and presents as N1/N2/N3 to the 5G System.

Note that this is a functional representation and does not necessarily represent implementation choices with respect to function co-location.

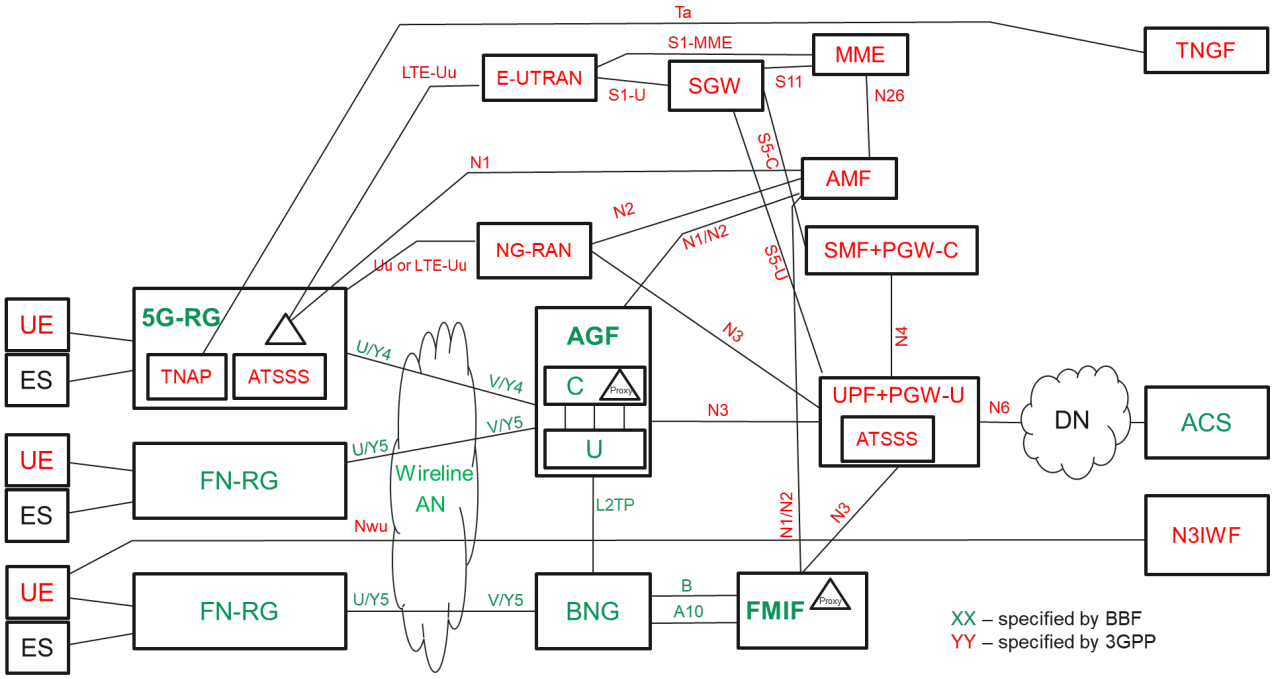

Figure 1: Architectural overview of WWC showing different functions

The functions (listed in alphabetical order) are:

5G-RG 5G Residential Gateway. A 5G-RG is an RG that has been augmented with 5G capabilities such as QoS handling, a NAS stack, and possibly additional capabilities such as multi access PDU with ATSSS, etc. The 5G-RG has the 5G specific requirements described in the '5G-WWC' requirements of BBF TR-124i6 and subsequent amendments [7]. A 5G-RG supports FN-RG WAN requirements in case it cannot operate as a 5G-RG due to lack of 5G WWC support on the network side.

5GC 5G Core. The 5G Core hosts all of the non-access functions of the 5G System. The documents TS 23.501 [24], TS 23.502 [25] and TS 23.503 [26] provide a stage 2 description of the 5G System. TS 23.316 [20] describes the specific 5GC requirements to support the architecture discussed here.

ACS Auto Configuration Server. An auto configuration server provides management of the FN-RG and 5G-RG devices using the BBF TR-069 [3]/369 [4] protocol. BBF TR-069 and TR-369 are where the ACS is specified. BBF TR-181 [6] provides the data models.

AGF Access Gateway Function. The AGF is a function that connects wireline AN to the 5GC. AGF can support both 5G-RGs (direct mode) and FN-RG(s) (adaptive mode). For the latter, the AGF provides NAS functions among others (N1 interface) for the FN-RGs. The AGF is specified in BBF TR-456 [16]. The AGF is separated into its control plane part AGF-c and its user plane part: AGF-u.

AMF Access and Mobility Management Function. The functionality of the AMF is described in detail in clause 6.2.1 in TS 23.501 [24]. Some of the functionalities offered by the AMF include registration, connection, reachability management etc.

ATSSS Access Traffic Steering Switching Splitting. The support for the ATSSS mechanism is described in detail in clause 5.32 in TS 23.501 [24]. This feature can be supported over any type of access network and enables a multi-access (MA) PDU connectivity service.

BNG Broadband Network Gateway. A legacy wireline access IP edge. First specified in BBF TR-101 [5], it has accreted additional functionality in BBF TR's 177 [11], 178 [12], 187 [13], etc.

DN Data Network. This network function is described in clause 4.2.2 in TS 23.501 and consists of operator services, internet access or 3rd party services.

ES End System. A networked device in the home supported by the FN-RG or 5G-RG that does not use 3GPP 5G procedures.

E-UTRAN Evolved Universal Terrestrial Radio Access Network. The E-UTRAN provides 4G radio access. It is described in TS36.300 [33].

FMIF Fixed Mobile Interworking Function. A function that interworks subscriber traffic received from the BBF A10 interface and adapts it to the 5G Core, see WT-457 (currently under specification) [17].

FN-RG Fixed Network-Residential Gateway. AN FN-RG is a residential gateway that connects the home LAN to the WAN without making use of 5G NAS. There is no active N1 interface from an FN-RG. The capabilities implemented in an FN-RG will follow the TR-124 (any issue) specifications, supporting a combination of selected 'a la carte' device profiles.

MME Mobile Management Entity. The MME is the mobility management control point for the LTE architecture. It is described in 3GPP TS23.401 [23].

N3IWF Non-3GPP access Interworking Function. The functionality of the N3IWF is described in detail in clause 6.2.9 in TS 23.501 [24]. Some of the functionalities offered by the N3IWF include support of IPsec tunnel establishment with the UE, termination of the N2 and N3 interfaces to 5GC control and user plane, handling of N2 signaling from SMF, etc.

NGRAN Next Generation Radio Access Network. An access network comprised of NG-RAN and/or non-3GPP AN connecting to the 5G core network as per clause 3.1 in TS 23.501 [24].

PGW PDN Gateway The PDN GW is the gateway which terminates the SGi interface towards the PDN. It is described in TS23.401 [23].

SGW Serving Gateway. The Serving GW is the gateway which terminates the interface towards E-UTRAN. It is described in TS23.401 [23].

SMF Session Management Function. The functionality of the SMF is described in detail in clause 6.2.2 in TS 23.501 [24]. Some of the functionalities offered by the SMF include session management, UE IP address allocation and management, DHCPv4 and DHCPv6 functions, responding to ARP requests, selection and control of UP functions, etc.

TNAP Trusted Network Access Point. The TNAP provides the 5G-RG end of support for devices using 3GPP procedures in the home and trusted access to the 5GC. TNAP procedures are described in TS 23.502 [25] clause 4.12a.

TNGF Trusted Network Gateway Function. The TNGF provides the network end of support for devices using 3GPP procedures in the home and trusted access to the 5GC. The TNGF is described in TS 23.501 [24] clause 6.2.9A, and procedures described in TS 23.502 [25] clause 4.12a.

UE (meant as a 5G UE in Figure 1): 5G-capable User Equipment. A networked device that uses 3GPP 5G procedures.

UPF User Plane Function. The functionality of the UPF is described in detail in clause 6.2.3 in TS 23.501 [24]. Some of the functionalities offered by the UPF include: allocation of a UE IP address in response to SMF request, external PDU session point of interconnect to DN, user plane policy rule enforcement, transport level marking in upstream and downstream traffic accounting. The UPF can be combined with AGF (co-located AGF-UPF).

The set of interfaces relevant to this set of functions are:

A10 The A10 is a BBF reference point for an IP handoff between a BBF specified network and the WAN. It may support a number of technologies such as MPLS, L2TP, Ethernet, TDM etc. Given the variety of potential interfaces in the industry, it has not been formally specified. The most thorough description available is in TR-178 [12] and TR-459 [19].

AGF-C to AGF-U CUPS interfaces described in WT-458 (currently under specification) [18].

B BNG to AAA interface. Defined in TR-134corr1 [9].

L2TP between a BNG acting as a LAC and an AGF. It is described in TR-456 [16].

LTE-Uu 4G Radio interface between E-UTRAN and UE as described in TR 36.300 [33].
N1 Reference point between UE and the AMF, as described in TS 23.501 [24] clause 4.2.7.
N2 Reference point between the (R)AN and the AMF as described in TS 23.501 [24] clause 4.2.7.
N3 Reference point between (R)AN and the UPF as described in TS 23.501 [24] clause 4.2.7.
N4 Reference point between the SMF and the UPF as described in TS 23.501 [24] clause 4.2.7.
N6 Reference point between the UPF and a data network as described in TS 23.501 [24] clause 4.2.7.
N26 Reference point between the MME and 5GS AMF in order to enable interworking between EPC and the NG core as described in TS 23.501 [24] clause 4.3.1.
Nwu Tunneled interface between a UE and an N3IWF as described in clause 4.2.8.3 of TS 23.501 [24].
S1-MME Reference point for the control plane protocol between E-UTRAN and MME. It is described in TS 23.401 [23].
S1-U Interface between the E-TRAN and the S-GW. It is described in TS 23.401 [23].
S5-U User plane interface between the S-GW and the P-GW. It is described in TS 23.214 [22].
S5-C Control plane interface between the S-GW and the P-GW. It is described in TS 23.214 [22][22].
S11 Reference point providing control plane between MME and Serving GW. It is described in TS 23.401 [23].
Ta Tunneled interface between a TNAP and a TNGF as described in clause 4.2.8.3 in TS 23.501 [24].
Uu Radio interface between RAN and UE as described in TR 21.905. In general, Uu refers to the radio interface between the UE and gNodeB.
U/Y4 The U/Y4 (BBF/3GPP) interface is the interface between a wireline access network and a 5G-RG. The Ethernet aspects are specified in TR-101 [5] and TR-178 [12]. The 5G aspects are specified in TR-456 [10].
U/Y5 The U/Y5 (BBF/3GPP) interface is the interface between a wireline access network and an FN-RG. The Ethernet and IP aspects are specified in TR-101 [5], 177 [11], 178 [12] and 187 [13].
V/Y4 The V/Y4(BBF/3GPP) interface is the interface between an AGF and a wireline access network supporting a 5G-RG. The Ethernet aspects are specified in TR-101 [5] and TR-178 [12]. The 5G aspects are specified in TR-456 [16].
V/Y5 The V/Y5 (BBF/3GPP) interface is the interface between an AGF and a wireline access network supporting an FN-RG. The Ethernet and IP aspects are specified in TR-101 [5], 177 [11], 178 [12] and 187 [13].

4 Deployment Scenarios

The BBF work on 5G Fixed Mobile Convergence enables several scenarios to support different network environments, starting points and priorities.

The deployment scenarios described in this document support different network environments, starting points and priorities, with different cases in terms of Residential Gateway (RG) type, access networks and interfacing model with the 5G Core. As part of these scenarios, devices supporting 3GPP procedures, connected to the RG via the Wi-Fi in the LAN and/or over the RAN, may also access the 5G core network.

The set of scenarios, as shown in Figure 2, allow deployments to pick and choose based on their local requirements and conditions.
While possible in theory, there is no need to implement multiple or all scenarios in parallel at once

Figure 2 represents six scenarios, with different Residential Gateway (RG) types, access networks and interfacing models with the 5G Core. As part of these scenarios, devices supporting 3GPP procedures (UE), connected to the RG via the Wi-Fi in the LAN and/or over the NG-RAN, may also access the 5G core network.

In all cases the operator is assumed to operate both the fixed and wireless 5G assets used for service delivery. As such the BBF considers roaming to be out of scope for a 5G-RG subscription for either access type.

The architecture supports two classes of CPE types: 5G-RGs which have been enhanced to support the 5G control plane and communicate with the 5G-Core directly and fixed network RGs (FN-RGs) which are RGs that might already have been deployed and do not support 3GPP procedures. 5G-RGs can have wireline only, wireless only (Fixed Wireless Access) or both types of WAN interfaces. A 5G capable RG is an RG that can support either mode of operation: 5G-RG and FN-RG. This enables the RG to fall back to FN-RG mode, in case the network does not support 5G WWC.

The architecture includes a network function for adapting wireline access onto the 5G core, the Access Gateway Function (AGF), specified in TR-456. It includes also a Fixed Mobile Interworking Function (FMIF) that is to be specified in future BBF work [17].

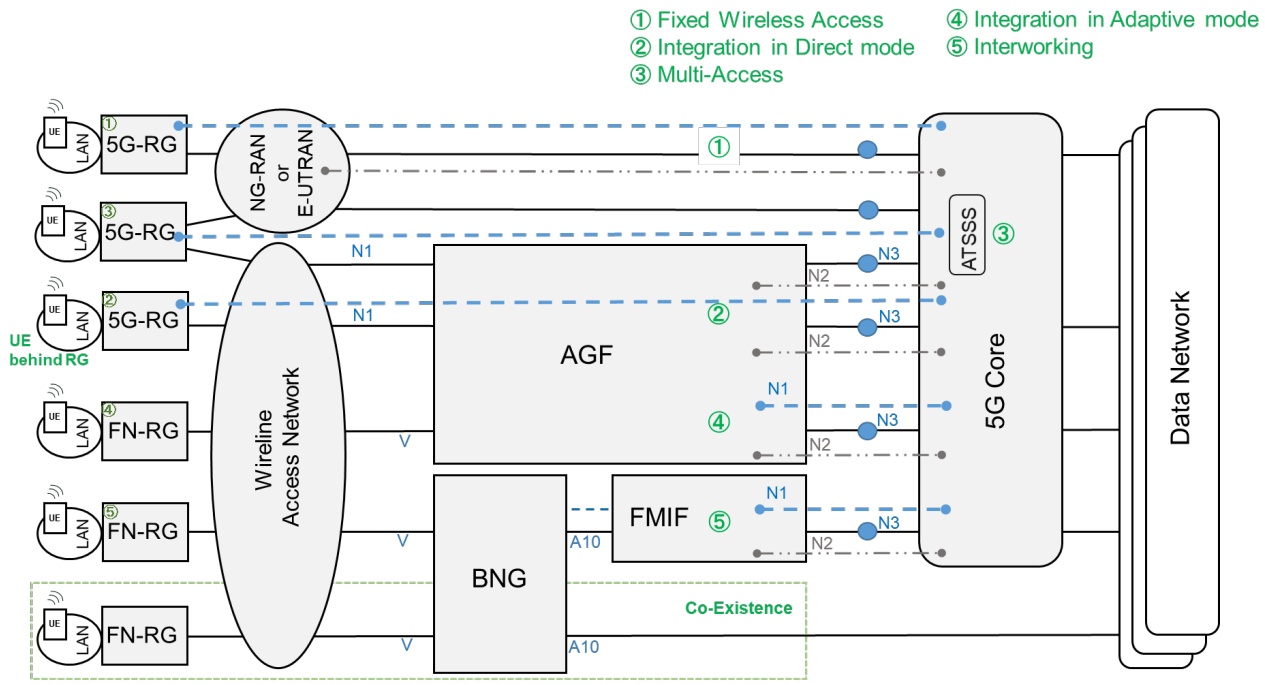

Figure 2: Different deployment scenarios for connecting RGs to the Data Network

1. Fixed Wireless Access (5G-RG) – The 5G-RG is connected over the NG-RAN or E-UTRAN.
2. Integration in Direct Mode (5G-RG). The RG is connected over the wireline access network. An Access Gateway Function (AGF) mediates between the wireline access network (aggregated at layer 2) and the 5G core network, based on N2 and N3 interfaces. The 5G-RG is able to authenticate, register and signal directly with the 5G core network based on the N1 interface. For this reason, the AGF is said to integrate with the 5G system in “direct mode”. Specific transport requirements between 5G-RG and AGF for NAS signaling and PDU session multiplexing are related to this scenario.
3. Multi-access (5G-RG) - The 5G-RG is connected over both the wireline access network (direct mode) and the NG-RAN or E-UTRAN. The 5G-RG may be connected over one of the access networks at one time (active-standby), both access networks in “steering” (flow-based load spreading) or “splitting” (per packet-based or per-flow-based load spreading, see clause 5.32 of TS 23.501 [24]).
4. Integration in Adaptive Mode (FN-RG) – Similar to (2), the RG is connected over the wireline access network and the AGF mediates with the 5G core network based on N2 and N3 interfaces. However, the FN-RG does not support N1, so the AGF acts as an end point of the N1 interface on behalf of the FN-RG. The AGF is said to integrate with the 5G system in “adaptive mode”. A given AGF instance could aggregate simultaneously CPEs in direct mode (5G-RG) and adaptive mode (FN-RG). AGF requirements are specified in TR-456.
5. Interworking (FN-RG) – The IP session is managed by a BNG. Services that are based on the 5G core network are passed to the 5G core via a Fixed Mobile Interworking Function (FMIF). The FMIF supports N2 and N3 interfaces to the 5G core network. Since the FN-RG does not support the N1 interface, the FMIF acts as end point of the N1 interface on behalf of the FN-RG.

Co-existence - Model that can be supported in parallel to WWC deployment scenarios. This is not a converged session model, as these sessions are not part of the 5G core network. However, co-existence is required to allow services that are not supported by the 5G core network to be available in a converged service provider network. Co-existing subscriber sessions are managed by the BNG or specialized platforms for voice or IPTV and may uniquely serve FN-RGs or 5G-RGs that can also support non-5G services. When the wireline access network is shared between converged sessions (models (2), (3), (4)) and co-existing sessions. Note that in this issue of the document, a RG is connected to a single AGF but can be served by multiple UPF.

After selecting the suitable deployment of scenario, an operator deploying WWC performs a series of steps:

- Deploy the 5G core and services.
- Populate User Data Management (UDM) with line ID-based identifiers, as defined in TS 23.501 [24], for the subscribers to be transitioned, and subscription information for the 5GC instantiation of their wireline service profile.
- Deploy the preferred interworking solution. This can be any combination of standalone AGF (connected via the access, in direct-mode only, or adaptive-mode only or both), or UPF integrated AGF, or BNG integrated AGF, or AN integrated AGF. As 5G-RGs are rolled out, the 5G Core Unified Data Management and Authentication Server Function are updated to include the 5G-RG credentials.
- Customer self-installation of 5G CPE at this point does not require coordination with any network changes. Similarly, the customer may back out the install and still receive service if any issues arise.

4.1 Fixed Wireless Access (5G FWA)

In this scenario, the 5G core network is used to provide fixed broadband services. The residential gateway is a fixed wireless device obtaining access via wireless access network.
For many operators, 5G is the next logical evolution step for their existing Fixed Wireless Access solution. It is also of interest to many operators that have limited last mile access through fiber and copper; and are interested in using FWA to broaden their offer and reach to end-customers. Moreover, operators have shown great interest in Fixed Wireless Access as an enterprise business critical solution and as a disaster recovery mechanism. It provides a backup plan when broadband wireline access fails or is disrupted. In disaster scenarios, deployment of wireless CPE in devastated zones may offer a rapid and economic solution to the restoration of service.

Traditional Broadband Network Gateway (BNG) and mobile core both deliver IP services to the end user. However, the services provided, and the protocols used for service delivery are quite different. For example, IPTV multicast historically is not a service offered over radio access networks to address these issues and offer the same fixed broadband service over 5G wireless, the BBF has, in close collaboration with 3GPP, defined the 5G-based Fixed Wireless Access solution within 3GPP Release 16. The BBF defined FWA architecture provides key broadband services offered on wireline today, including the following:

- High Speed Internet Service
- VoIP
- IPTV through IP multicast

A 5G-RG is connected to the 5GC utilizing a NG-RAN as illustrated in Figure 3. The broadband services offered by a 5G-RG over wireless compared to wireline have minor differences covered in the sections below.

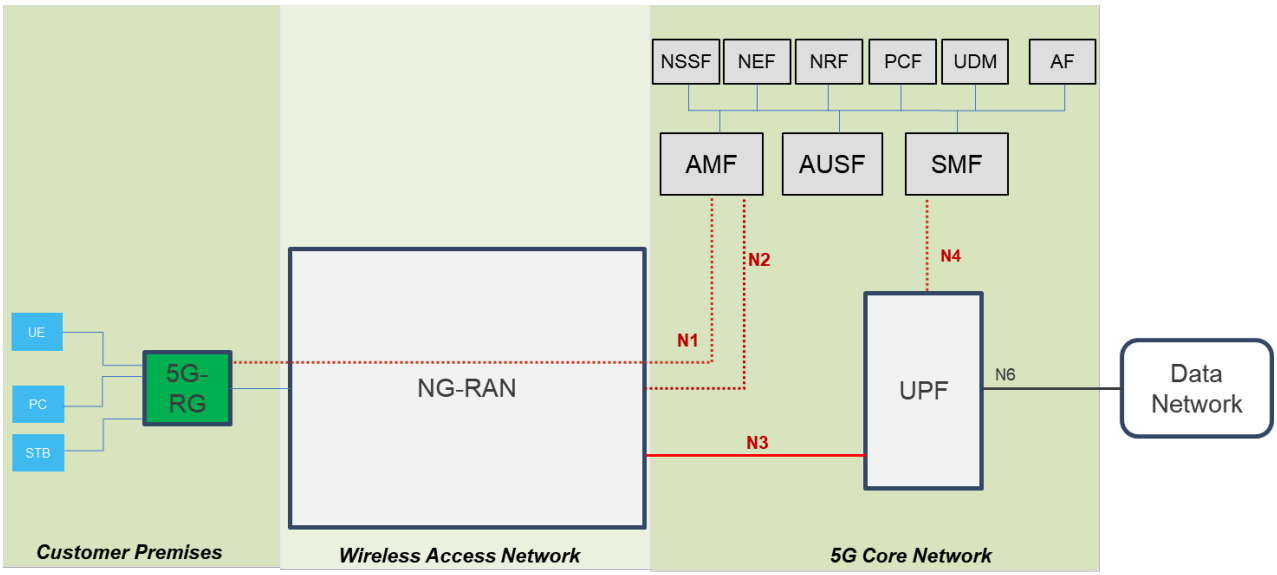

Figure 3: FWA offering fixed services and connecting to 5GC through RAN

4.1.1 Authentication and IP Address Assignment Procedures

The 5G-RG follows 3GPP authentication procedures based on IMSI credential procedure documented in TS 23.501 [24].

Similar to wireline IP address and/or prefix request, the 5G-RG will perform a session management request for at least one PDU session, as documented in TS 23.502 Clause 4.3 [25].
Each PDU session can support up to one IPv4 WAN address and optional set of IPv4 routed ranges (framed routes), one IPv6 WAN address, one IPv6 LAN prefix and one IPv6 LAN delegated prefix (typically /56).

Note that since every PDU sessions consumes an IP address, careful planning of address pools must be defined in the case of multiple sessions per subscriber.

4.1.2 5G-RG Security and privacy

In case of FWA compared to wireline, the 5G-RG fulfills the security and privacy requirements defined for accessing via 3GPP RAN where the 5G-RG takes the role of the UE. For example, for slice privacy as defined in TS 23.501 clause 5.15.9, relies upon user plane data confidentially and integrity protection as defined in TS 23.501 clause 5.10.3. Hence the requirements for 5G-RG accessing via wireless access and via 3GPP RAN may differ from that for wireline access as specified addressed in BBF TR-124 [7].

4.1.3 IPTV multicast specificities for FWA

IPTV services are provided through Set Top Boxes (STB) that are connected to the 5G-RG. The 5G-RG can use an already established PDU session or request a dedicated PDU session for IPTV. In the 5G architecture the UPF also acts as the multicast replication router. The call flow procedure is described in TS 23.316, clause 4.9.1 and shown as follow:

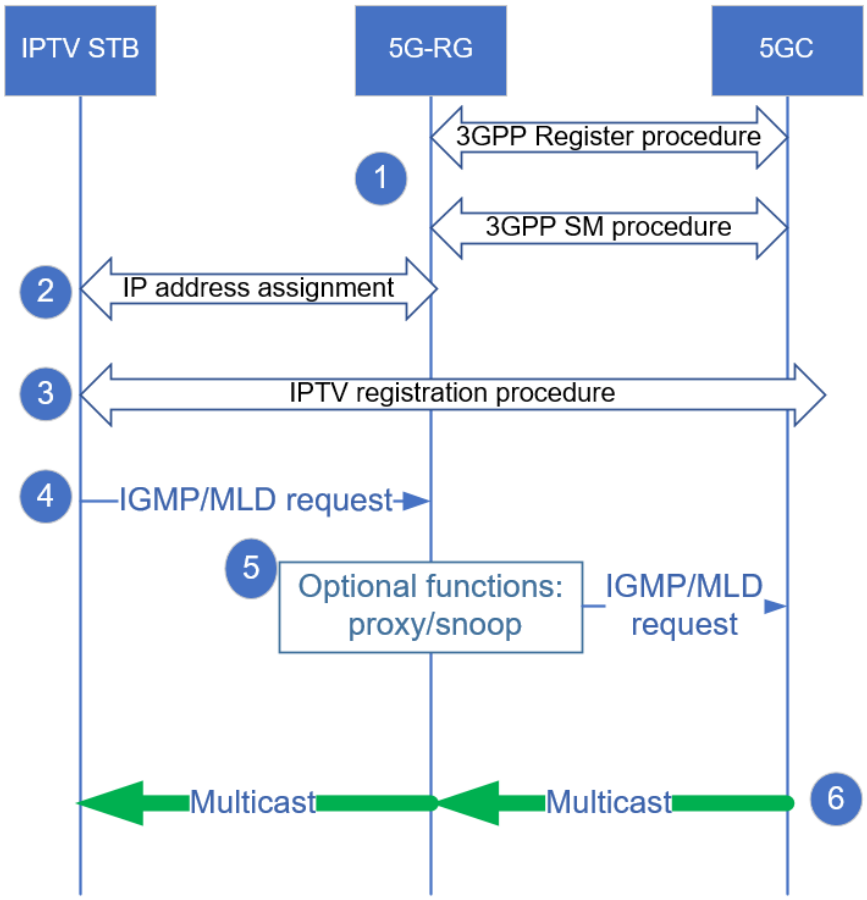

Figure 4: Call flow procedure for an IPTV STB in 5G FWA

Step 1: 5G-RG performs registration and session management procedure as specified in TS 23.502.
Step 2: The IPTV STB request an IP address and/or prefix from the 5G-RG.
Step 3: The IPTV STB performs additional registration processes as specified in clause 7.7.1 of TS 23.316 [20].
Step 4: The end user performs a channel request, and the STB performs an IGMP/MLD request to the 5GC.
Step 5: If there are multiple STBs, the 5G-RG can perform IGMP/MLD proxy/snooping functions. The 5G-RG will proxy the IGMP/MLD request to utilize the source IP of the 5G-RG. In the case of IPv4, the PDU session is assigned an IPv4 address. In the case of IPv6, the link local address of the WAN interface is assigned. The 5GC will then send at most a single (S,G) multicast group to the 5G-RG. The 5G-RG is expected to be the replicator to replicate the multicast (S,G) for multiple STBs requesting the same (S,G). In the case where the 5G-RG does not perform proxy, it bridges IGMP/MLD requests from the STB. Each STB will require its own separate PDU session.
Step 6: The 5GC will then send multicast traffic over each PDU session for which there has been a 5G-RG originated an (S,G) request. In the case where the 5G-RG requested the same (S,G) over each of 'N' PDU sessions, the 5GC is expected to send a copy of the traffic for the same (S,G) 'N' times, one on each PDU session.

4.1.4 5G QoS and filter policies

Overall, 3GPP QoS described in clause 5.7 of TS 23.501 is not an exact match of wireline QoS described in TR-178. In wireline, it is possible to guarantee a minimum bandwidth per application (IP flow) and at the same time allow any application to utilize remaining bandwidth up to the maximum bandwidth allocated for

the subscription. 5G QoS as specified by 3GPP offers a finer granularity in terms of the priority of the flows and gives the ability to reserve bandwidth. However, it is not possible to reserve a minimum bandwidth per application qualified as 'non GBR' within a single PDU session (typically data traffic). It is possible to separate each application into individual PDU sessions and rate limit each by session-AMBR, but deployments usually consider "access to Internet" as one application. The Session-AMBR limits the aggregate bit rate to be provided access all traffic Non-GBR for the specific PDU session.

In addition, wireless does not provide an aggregate subscription rate. The subscription rate is the sum of all MFBR (the Maximum Flow Bit Rate for a specific GBR flow) and UE-AMBR (limit of the aggregate bit rate to be provided across all traffic Non-GBR of a UE) where it is not possible for MFBR to utilize unused UE-AMBR bandwidth or vice versa. Therefore, the UE-AMBR would be the best representation of the overall subscription bandwidth. In conclusion, the engineering practices for FWA need to be adapted to offer the same Quality of Experience (QoE) as for traditional wireline services.

4.2 Coexistence between WWC and Traditional TR-178 Architecture

Coexistence allows sharing of the wireline access network between 5G WWC services offered via 5G core and non-converged services offered via the traditional fixed network core, as shown in Figure 2.

This sharing of common network infrastructure also supports multiple actors, and addresses regulatory requirements imposed in many Countries. In this case, traffic segregation mechanisms in the wireline access network are used to deliver the broadband services offered by different Operators using the same network with an appropriate level of isolation. Wholesale services, spanning from Layer 2 (such as bitstreaming) to Layer 3 services (such as L2TP), rely on these mechanisms.

Coexistence does not prevent a single Operator, benefiting from the use of a L2 service (retail or wholesale whatever it be), from sharing a common broadcast domain in the access network between the traditional BNG platform and the new gateway function (AGF) that offers 5G WWC services. This enables a CPE migration strategy that some operators find desirable but requires some specific CPE behaviors to be enabled. This is advantageous as it does not require any change in the network configurations for delivering wholesale services and might not require the re-provisioning of the access network nodes, which would typically require a high operational effort for the AN Operator.

Other motivations for the coexistence are listed in the following:

1. It supports existing regulatory requirements.
2. It supports existing wholesale requirements.
3. Services delivered side by side with the Internet and corporate access, such as access node delivered linear IPTV, could be left in place or re-engineered to be delivered via the 5GC, according to operator's business imperative and investment timetable.

There are a few consequences to the co-existence requirement. The AGF may be deployed as a platform connected to the FN-RGs and 5G-RGs via an unmodified Layer 2 aggregation network transiting an existing and unmodified Layer 2 aggregation network. This adds specific requirements to the protocol design:

1. Part of the protocol exchange needs to be recognized by access nodes such that they will insert additional metadata in the exchanged message for consumption by the AGF/FMIF.
   This includes the line ID for the specific subscriber and could include details of the DSL line physical characteristics (the objective is to leverage existing practice as much as possible and avoid requiring additional data-fill in operational systems).
2. An AGF connected to the aggregation network will not have direct visibility of DSL or PON failures, e.g., via session liveliness check mechanisms. Hence additional procedures will be required such that an AGF will have knowledge of the availability of connectivity to the CPE.
3. Many access nodes implement enhanced QoS, security features, and other proprietary "value-adds" that operators depend upon. The design of the User Plane encapsulation for 5G needs to be recognized by deployed equipment such that these dependencies in service design are not disrupted.

Some operators may have deployed VLAN delineated service connectivity and service specific platforms for the subscriptions as described in TR-178 [12]. Other deployments may see protocol multiplexing used with an untagged UNI to provide per-service connectivity and platform access models. Examples of services deployed in this manner could include voice, IPTV and internet access.

It is possible to combine 5G services with legacy service delivery down to the granularity of individual RG in these deployment models. An example would be the use of PPPoE(CP) and 5WE(UP) for 5G services multiplexed with IPoE delivery of IPTV and/or other services. In the IPoE case, AN delivered multicast for legacy IPTV implementations can be combined with transparent relay of 5G traffic to the AGF. A legacy AN can map IPoE traffic to the IPTV system VLAN, and 5G traffic to the AGF using the 5G-VLAN on the basis of Ethertype. Operators can offer 5G-specific service to the subscribers together with the replacement/upgrade of BNG. Consequently, some service/traffic requested by the FN-RG or 5G-RG accessing to the 5GC is transported through the AGF (adaptive mode), and some traffic can be forwarded to the BNG or other service platform by the AN. This model provides operators with the ability to choose what services they migrate to 5GC and when.

Coexistence does not preclude vendors integrating AGF functionality into DSLAMs and BNGs. The Broadband Forum's work on Control User Plane Separation (CUPS) for WWC will facilitate this class of implementation as access equipment only needs to implement the user plane functionality. Coexistence simply means WWC can be retrofitted to existing deployments.

4.3 Integration of Wireline Access with 5GC based on AGF

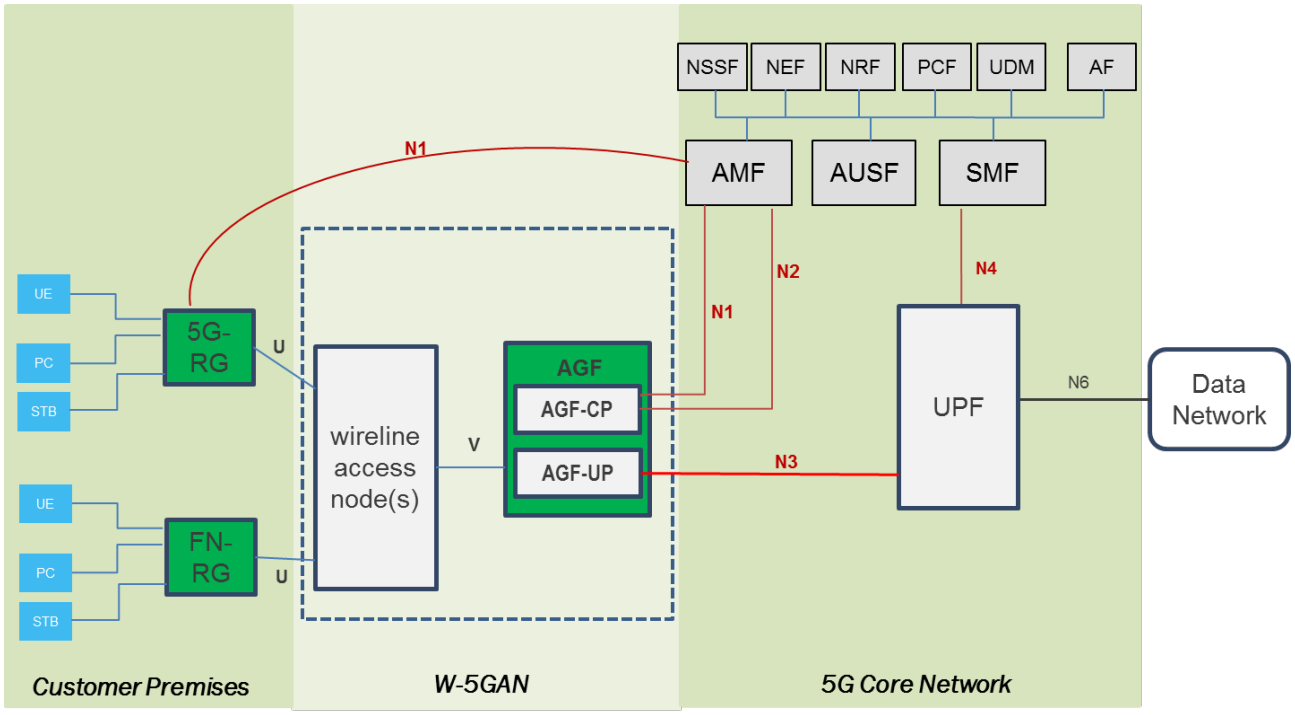

Figure 5: Integration with 5G-RGs and FN-RGs connecting to the 5G core through AGF

Figure 5 pictures an FN-RG and a 5G-RG connected to the 5G core through the Access Gateway Function (AGF).

The FN-RG may include an integrated network termination such as: Optical Network Units (ONUs) for optical access, Digital Subscriber Line (DSL) modems for twisted-pair access, and Cable Modems (CMs) for coaxial access.

W-5GAN comprises of wireline access nodes and a mediation function for 5G convergence, i.e., the AGF. Examples of wireline access nodes that could be part of the W-5GAN include: Optical Line Terminals (OLTs) in support of fiber access networks, Digital Subscriber Line Access Multiplexers (DSLAMs) in support of twisted-pair access networks, and Cable Modem Termination Systems (CMTSs) in support of coaxial access networks.

The AGF may be split into control plane, AGF-CP, and user plane, AGF-UP. The control plane and user plane separation of the AGF is work in progress by the BBF.

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

The interfaces of AGF towards the core form the border between access and core. They are the N1 (in the case of adaptive mode sessions) and N2 interfaces for the control plane and the N3 interface for the user plane. These are defined in 3GPP documents [27], [34], [29].

N1 is supported by 5G-RGs and carried over the W-5GAN. Note: the N1 messages between the 5G-RGs and the AMF are transported through the wireline access nodes and AGF. For an FN-RG, the AGF supports the N1 interface and generates the NAS signaling to the AMF on behalf of the FN-RG.

On interface of the AGF towards the wireline access node, the V reference point as defined in [12] connects the wireline access nodes to the AGF.

4.4 Hybrid Access

Hybrid access refers to a scenario where a 5G-RG connects to the 5GC via both 3GPP access and non-3GPP access simultaneously. It can not only increase the bandwidth that the 5GC provides by distributing traffic across the two access networks, but also offer service continuity in a failure scenario. 3GPP access is intended as NG-RAN (5G). A single, converged core network is used to manage both wireless and wireline sessions. This differs from prior BBF specifications related to hybrid access (TR-348 [14] and TR-378 [15]).

Figure 6 shows the architecture of hybrid access for 5G-RG.

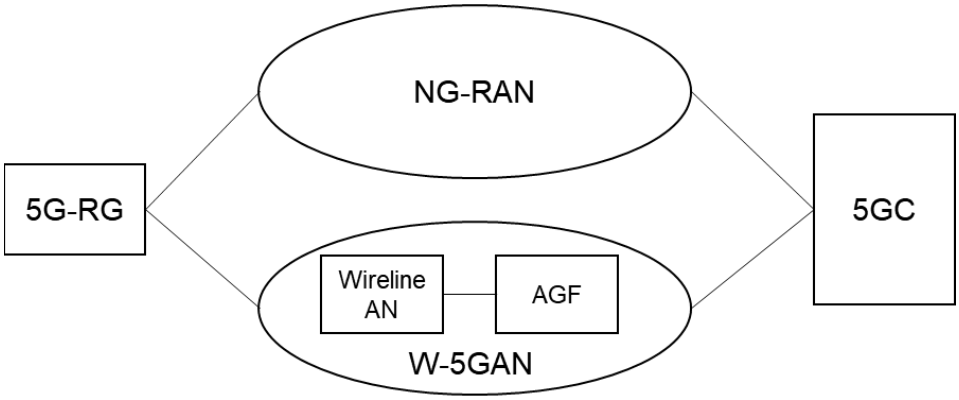

Figure 6: High level view of Hybrid Access for a 5G-RG

Note: Hybrid access with FN-RG is FFS.

There are two PDU session models to support hybrid access for 5G-RG, resulting in different benefits: Single-Access PDU sessions and Multi-Access PDU sessions. For both cases, the radio access can be either NG-RAN or E-UTRAN.

4.4.1 Hybrid Access based on Single-Access PDU Sessions

This model is based on a single-access PDU session that provides a PDU connectivity service which can use only a single access at a given time, i.e., either 3GPP access or wireline non-3GPP access. These sessions can be handed over between the two access types while preserving the session/service continuity. This means a single N3/N9 tunnel between PDU session anchor and either the AGF or the 3GPP access and the ability to move the tunnel between these access networks.

It should be noted that the Single Access PDU session enables the 5G-RG to move all PDU sessions between the available access, e.g., from 3GPP to Non-3GPP, based upon handover procedures triggered by the 5G-RG, and defined in clause 7.6 of TS 23.316 [20] as well as in TS 23.502 [25] clause 4.9.2.2, for 3GPP to Non-3GPP transition for a single-access PDU session (where “UE” is replaced by “5G-RG” and “N3IWF” by “W-5GAN”). This is a behavior equivalent to the Active-Standby or Priority-based ATSSS steering modes described in TS 23.501 [24] clause 5.32.8 "ATSSS Rules". However, for single-access PDU session the whole PDU is moved while for Multi-Access PDU in Priority-mode only part of traffic may be moved.

The following figure, Figure 7, shows an example of procedure where the 5G-RG triggers a handover from wireless access to wireline access.

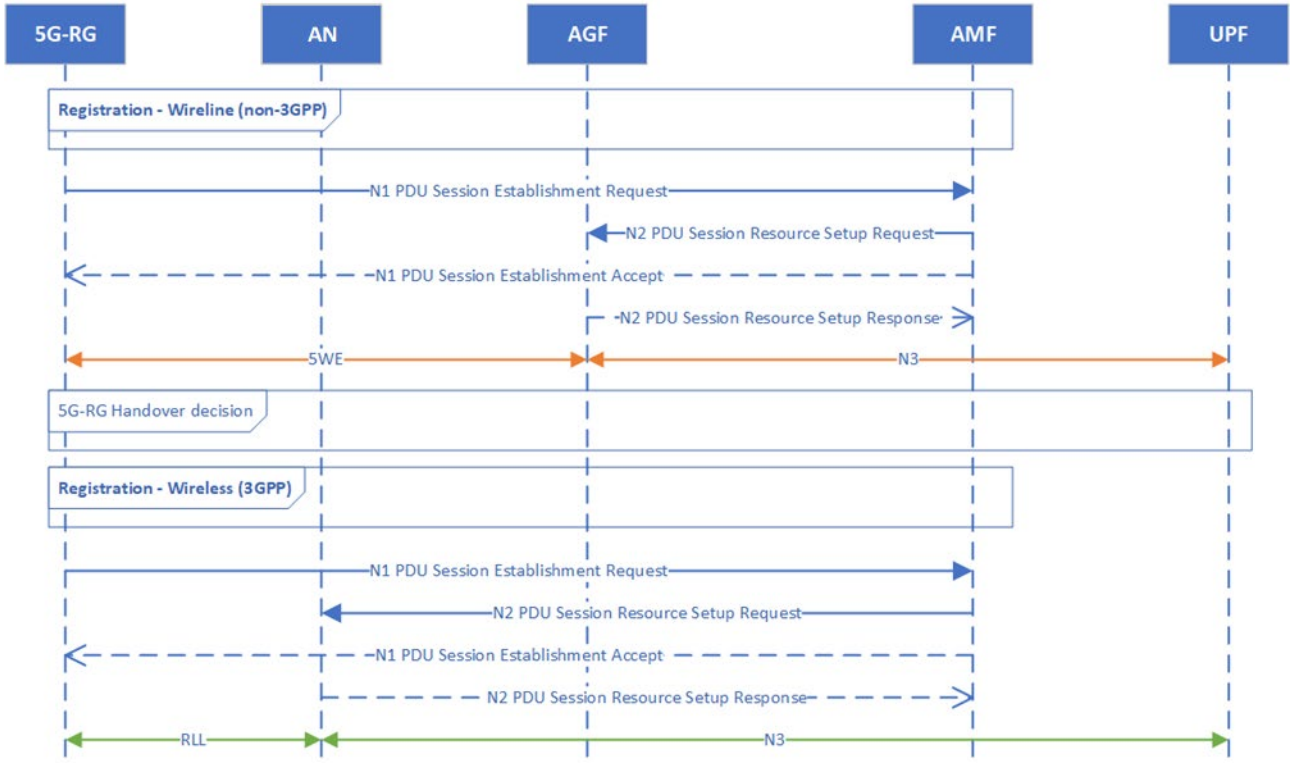

Figure 7: Procedure for 5G-RG with hybrid-access on Single-Access PDU sessions, including handover

Single-access PDU sessions can be used also for hybrid access with E-UTRAN access, using EPC interworking architecture. The mobility between EPS and W-5GAN is described in clause 4.11.3 of TS 23.502 [25] (where “UE” is replaced by “5G-RG” and “N3IWF” by “W-5GAN”).

4.4.2 Hybrid Access based on Multi-Access PDU Sessions

A Multi-Access PDU (MA PDU) session provides PDU connectivity service which can use one access at a time or simultaneously both 3GPP access and non-3GPP access. In this latter case, the PDU session is simultaneously associated with two independent N3/N9 tunnels between the PDU session anchor (i.e., the UPF where PDU session is terminated) and RAN/AGF. The multi-access PDU session from the 5G-RG uses the same SMF and same UPF. In the case of co-located UPF with AGF, that means that the combined UPF needs to be able to support the 3GPP access PDU sessions and other hybrid access requirements.

Hybrid access based on MA PDU sessions is supported with either NG-RAN access (including operator-controlled traffic steering) or E-UTRAN access, using EPC interworking (as described in TS 23.316 [20] clause 4.12.3).

The MA PDU session requires the support of the associated ATSSS (Access Traffic Steering, Switching, Splitting) features in the 5G-RG, UPF, SMF, AMF and PCF. This section intends to provide a highlight of the MA PDU and ATSSS feature. For detailed specification, refer to TS 23.316 [20] clause 4.12, TS 23.501 [24], clause 5.32, TS 23.502 [25] clause 4.22 and TS 23.503 [26] clause 6.1.3.20, clause 6.2.2.7 and clause 6.3.

The MA PDU session and ATSSS feature enables the dynamic addition and removal of one of the two accesses and when both are present to steer, to switch and to split the traffic within a single MA PDU session between the 2 accesses. The steering modes supported are:

- Active-Standby: It is used to steer the Data Flow traffic from the Active access to the Standby access when Active access becomes unavailable.
- Smallest Delay: It is used to steer the Data Flow traffic to the access that is determined to have the smallest Round-Trip Time (RTT). The measurements may be obtained by the UE and UPF to determine the RTT over 3GPP access and over non-3GPP access via specific 3GPP measurement protocols.
- Load-Balancing: It is used to split Data Flow traffic across both accesses based on a defined percentage (e.g., X% on 3GPP and 100-X% on Non-3GPP Access). If one access becomes unavailable, all traffic is switched to the other available access.
- Priority-based: It is used to steer all the traffic of a Data Flow to the high priority access, until this access is determined to be congested.

Figure 8 represents the ATSSS architecture enabling the MA PDU session support. The ATSSS feature makes use of the MPTCP protocol for TCP traffic and ATSSS-LL (ATSSS Low Layer) functionality defined by 3GPP for all kinds of traffic, such as UDP, Ethernet and TCP traffic.

- The PCF sends the ATSSS policy to the SMF.
- The SMF generates the ATSSS rules which are sent to the 5G-RG via N1 NAS protocol to control the ATSSS function in the 5G-RG.
- The 5G-RG steers, switches and splits the upstream traffic matching the traffic descriptors filter included in the ATSSS rules.
- The SMF generates N4 rules which are sent to the UPF to steer, switch and split the traffic in the downlink toward the appropriate N3 GTP tunnel interface [29].

Whether to use the ATSSS capability and which of the ATSSS capabilities is used is decided by the PCF at the establishment of a MA PDU session based on the UE capability provided to the network and the UPF capabilities available. The following requirements apply to a 5G-RG and UPF:

- The MA PDU Session of type Ethernet can only use ATSSS-LL functionality.
- If the MPTCP functionality is not supported, the ATSSS-LL functionality is mandatory for an MA PDU Session of type IP.
- If the MPTCP functionality is supported, the ATSSS-LL functionality with Active-Standby Steering Mode is mandatory for an MA PDU Session of type IP to support non-TCP traffic.

The implementation in 5G-RG and UPF may support all operation modes. The 5G-RG always indicates all supported operation modes.

The AGF is not impacted by support of MA PDU sessions since its components interact separately with each PDU session as they would on single access.

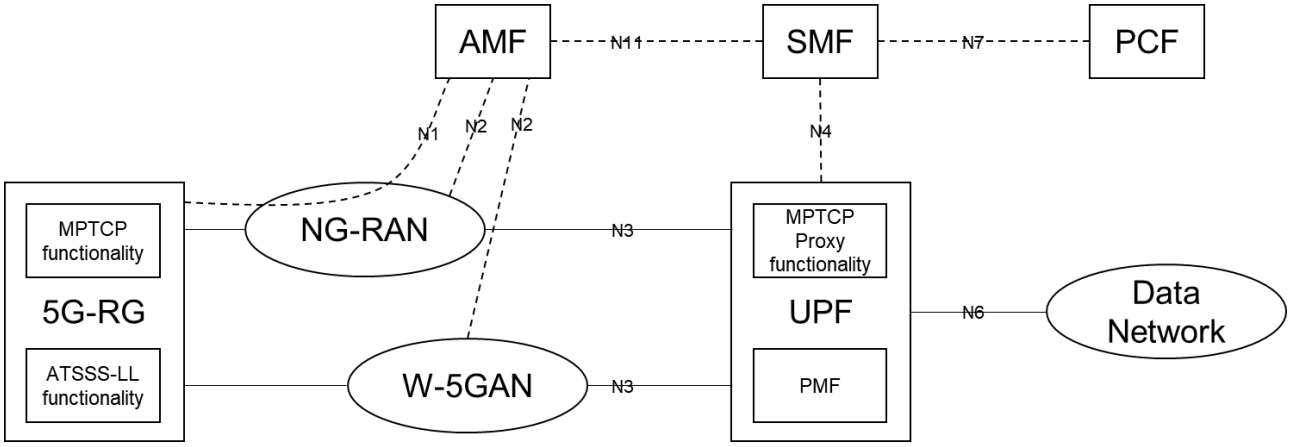

Figure 8: Architecture for ATSSS support

4.4.3 Impact of Hybrid Access on WWC Functions

It is expected that hybrid access has no impact on AGF, except in the case of collocated AGF-UPF, as the UPF terminates all sessions for the same 5G-RG. When wireless access is NG-RAN, the collocated UPF needs to support N3 from the NG-RAN. When wireless access is E-UTRAN, the collocated UPF/P-GW needs to support S5 interface from SGW (including LTE EPS interworking).

The collocated UPF supports the proper procedures and features depending on the hybrid use cases listed in the previous sections (e.g., handover, ATSSS, …).

All hybrid access use cases have dependency on 5G-RG access interfaces, procedures and features. A 5G-RG may be capable of both single-access PDU and multi-access PDU sessions, but subscriptions may allow only a specific mode. For example, a specific (DNN, S-NSSAI) could be associated to using exclusively single-access PDU session mode.

5 Architectural Aspects

5.1 Overview of 5G-RG Procedures

A 5G-RG is an RG that has been augmented with 5G mechanisms, in particular a control plane which can interact directly with the 5GC. That interaction is referred to as Non-Access Stratum (NAS) communication. NAS implements common channel signaling that performs life cycle management for all user plane sessions, known as Protocol data Unit (PDU) sessions. A PDU session implements connectivity to the core network at the granularity of a session per data network per slice. As such, an RG has a separate IP address/prefix for each PDU session. The operator rationale for multiple PDU sessions is described in this document. Subscription information and connectivity policies (known as UE Route Selection Policy (URSP)) are all disseminated via NAS. The NAS is authenticated, ciphered and integrity protected.

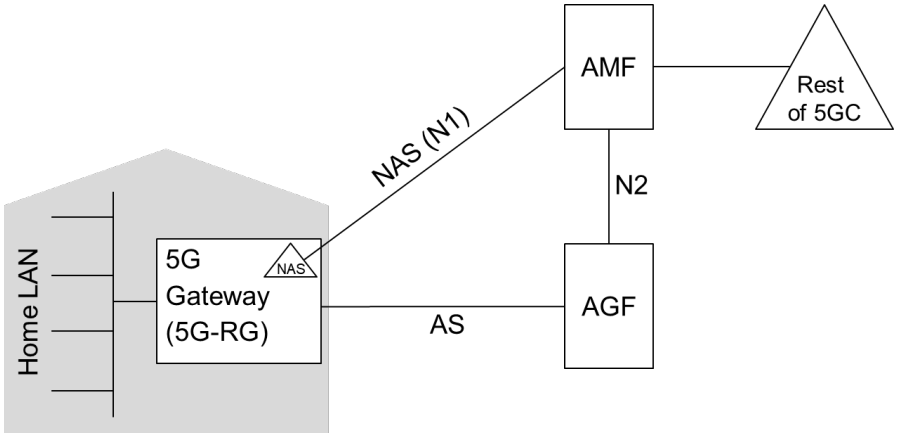

Figure 9: 5G-RG Control Connectivity

NAS communication is between the 5G-RG and an Access Management Function (AMF) in the 5G Core which also relay messages exchanged between the Session management Function (SMF) and the 5G-RG. The connectivity is achieved via the AGF which simply relays NAS packets between the 5G-RG and the AMF. This is known as the N1 interface. The AMF also communicates directly with the AGF over the N2 interface to control the network side of PDU session life cycle management. Finally, there is a control path for Access Stratum (AS) information between the AGF and the 5G-RG for the exchange of access specific subscription and PDU session configuration. The set of procedures for registration and PDU session life cycle management are described in the 5G-RG part of the Procedures and Call flows section in TR-456 [16].

5.1.1 Signaling and User plane Transport between 5G-RG and AGF

A 5G-RG is connected to an AGF via a VLAN delineated Ethernet circuit that is used for both NAS and AS signaling and 5WE encapsulated PDU sessions, 5WE is defined in BBF TR-456 [16] and IETF RFC 8822 [38].

This VLAN is called "5G VLAN", as represented on Figure 10. It shows a 5G-RG connecting to an AGF via a VLAN delineated access circuit known as the 5G VLAN. All control plane and user plane traffic is multiplexed within the 5G VLAN. Control plane traffic (NAS and AS) is encapsulated in PPPoE (and uses PPP/PPPoE procedures for control connection establishment) and user plane traffic is encapsulated in a 5WE header. User plane connection establishment is achieved via control plane exchange.

In Figure 10, we see an Ethernet circuit between the AGF and a 5G-RG while the 5G VLAN is only between the AGF and the AN. The VLAN ID of the 5G VLAN may be locally configured at the 5G-RG, otherwise it

defaults to zero (untagged or priority tagged). 5WE supports the IPv4, IPv6 and Ethernet PDU session types. The unstructured session type is FFS.

Control plane traffic is marked as high priority in order to not be affected if the user plane encounters congestion.

For user plane traffic, the 5WE Session ID is assigned by AGF and has a 1:1 correspondence with the PDU Session ID. QFI and RQI information is encoded in the 5WE header. The QoS markings for user plane traffic are derived from QFI to DSCP/PCP mapping information disseminated to the AGF and 5G-RG via the RG-LWAC data object and AS signaling respectively.

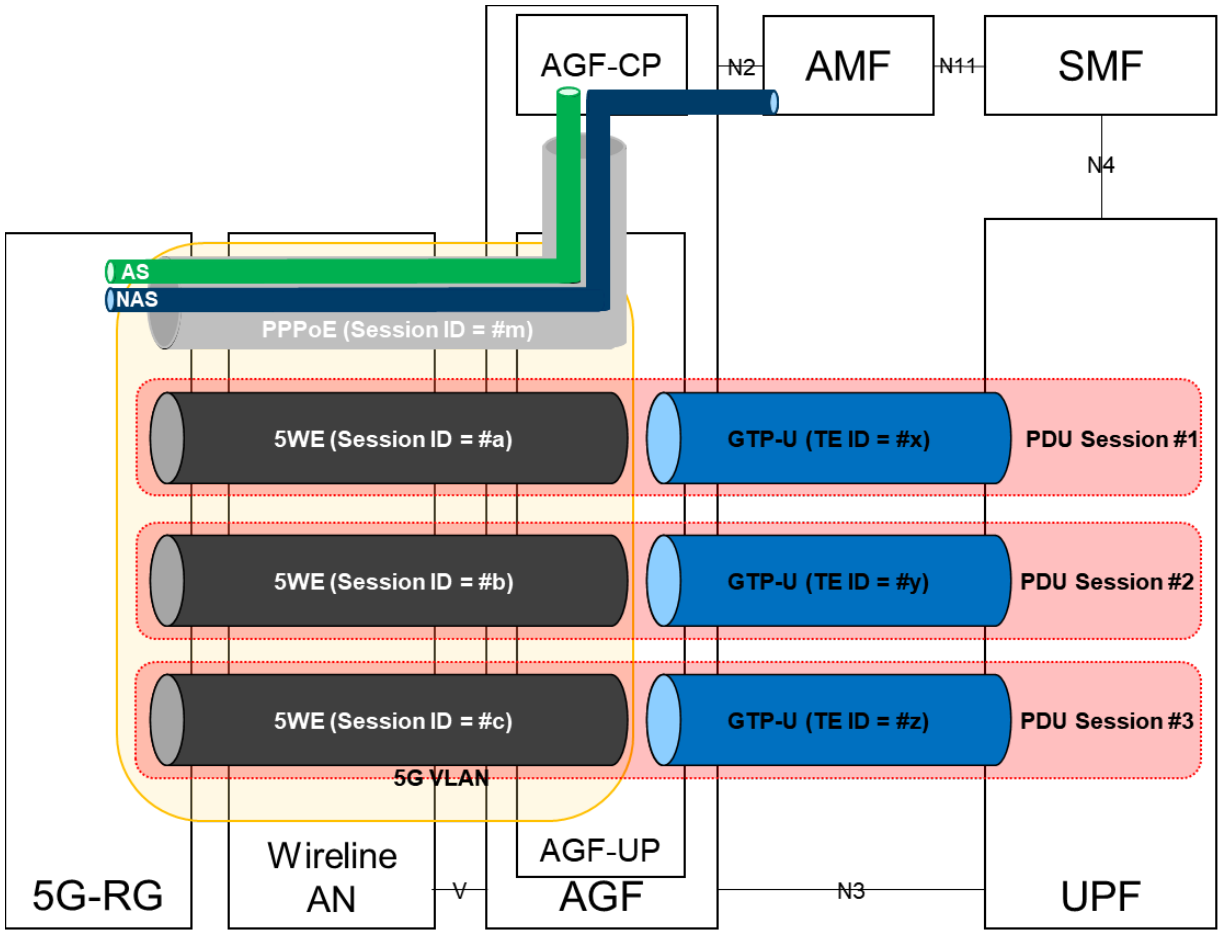

Figure 10: 5G-RG with a '5G VLAN' as VLAN delineation

The VLAN ID used for signaling and 5WE-based sessions is known a priori by the 5G-RG either by local configuration or defaulting to an untagged or priority tagged UNI.

5.1.2 Registration Process

Registration of a 5G-RG is a pre-requisite to PDU Session lifecycle management. Registration is the process of authentication of and establishment of a signaling path between a 5G-RG and the 5G Core via the AGF. Note that PPPoE is used for NAS signaling transport.

The registration process occurs in a series of phases:
- PPPoE session initiation
- PPPoE Link configuration
- PPPoE Authentication
- Establishment of the PPPoE VSNP, NAS, and AS connection

- Establishment of NAS ciphering
- An optional check of the 5G-RG's permanent equipment identifier
- Registration complete.

5.1.3 Registration and Connection Management States

The separation of registration and connection states is an artifact of mobility management in the radio access world. As a bit of background, user equipment (UE) can be continuously registered for service with the network but is only intermittently connected, which assists in both network scale and UE battery life.

The location of a registered UE is tracked at a coarse granularity by the network using low level exchange; broadcast of tracking area identifiers by the network which allows a UE to determine when it has changed tracking areas and update its coarse location information with the network. When the network needs to communicate with a UE that is not connected, for the purposes of an incoming call, notification, or emergency broadcast, it pages the UE within the last known tracking area. Upon receipt of the page, the UE will then connect to the network.

For wireline access, location tracking and paging are not relevant concepts. Hence the use of registration and connection states has been slightly modified. Whereas for a UE, not being connected is a normal artifact of fault free operation; for a registered wireline attached 5G-RG, not being connected corresponds to a fault condition.

Connection Management States are maintained at NAS layer in both 5G-RG and AMF: this state is about whether 5G-RG and AMF consider themselves able to transfer NAS signaling messages to the peer. N1 signaling between 5G-RG and AMF can be ensured by the combination of:

- Access signaling between 5G-RG and AGF.
- N2-AP signaling between AGF and AMF.

In the wireline network, access signaling is transported over a PPP link layer that, in case of failure, can be resumed only by 5G-RG. The failure can be caused by a loss of connectivity in the wireline access and/or in the transport network, or by a fault on 5G-RG (loss of power, reboot, etc.). In the former case, it can be detected by both 5G-RG and AGF, typically in different moments; in the latter case, it can be detected only by AGF.

The PPP link layer between 5G-RG and AGF is monitored by the AGF with periodic liveliness checks (LCP echo requests). Upon detecting a fault (either due to a loss of connectivity on the link or to a 5G-RG failure), the AGF starts the "AN Release" procedure towards the AMF, as documented in TS 23.316 clause 7.2.5.2 and TR-456 section "5G-RG AN Release via W-5GAN". When this procedure is completed, the AGF flushes the 5G-RG context. Corresponding procedures occurring in 5GC are documented in TS 23.501 clause 5.5.1 ("Registration Management for non-3GPP access") and TS 23.502 clause 4.2.2.3.3 ("Network-initiated Deregistration procedure").

Note: The AGF might hide frequent losses of connectivity in the access network (flapping) to 5GC. That can be achieved by informing AMF about the loss of connectivity with a certain delay from detection. This AGF feature is implementation dependent.

The PPP link layer between 5G-RG and AGF is also monitored by 5G-RG with periodic liveliness checks (LCP echo requests). Upon detecting a loss of connectivity on the link, the 5G-RG enters the CM-IDLE state and starts the non-3GPP Deregistration timer, using the default value or the value received by the AMF in the AS Registration Accept message as documented in TS 24.501 clause 8.2.7.17. When this timer expires, the 5G-RG enters the RM-DEREGISTERED state and releases its local 3GPP context.

While in RM-DEREGISTERED state or in (RM-REGISTERED, CM-IDLE) state, the 5G-RG tries to establish the PPP link with the AGF.

Whenever the PPP link is established,

a. if the 5G-RG was in RM-DEGISTERED state, the 5G-RG starts a NAS initial Registration procedure, as documented in TS 23.316 Clause 7.2.1.1 and TR-456 Section “Registration Management Procedure for 5G-RG”.

b. if the 5G-RG was in (RM-REGISTERED, CM-IDLE) state, the 5G-RG starts a NAS Service Request procedure, as documented int TS 23.316 Clause 7.2.2.1 and TR-456 Section “5G-RG Service Request Procedure via W-5GAN”, avoiding a new Registration on 5GC.

Notice that the de-registration timers held by 5G-RG and AMF may start at different instants and may lapse at different times (see clause 5.5.1 of TS 23.501 for details). Consequently, they typically expire in different instants with respect to a fault event and reset in different instants with respect to a recovery event.

Therefore, after a failure recovery over the PPP link, it might happen that the AMF de-registration timer has expired, while the 5G-RG considered itself registered. Consequently, the AMF might receive a Service Request from a 5G-RG. In this case, the AMF responds with a NAS Service Reject; upon receiving it, 5G-RG releases its local 3GPP context and then starts a new Registration procedure as documented in TS 23.316 clause 7.2.1.1.

On the other hand, after a failure recovery of the PPP link, it might happen that the 5G-RG de-registration timer has expired, while the AMF considered the 5G-RG still registered. Consequently, the AMF might receive a Registration Request from a 5G-RG which was considered registered. In this case, the AMF follows the procedure documented in TS 24.501 clause 5.5.1.2.8 (“Abnormal cases on the network side”), as a result, the 5G-RG’s old registration is overwritten by the new attempt.

5.1.4 TR-069/369 Support

For 5G, the TR-069/369 ([3],[4]) configuration received from an ACS will be applicable for connectivity to all data networks and slices, and access to an ACS will only be via a single PDU session. This may be a dedicated PDU session, or a shared PDU session that provides access to other services. This imposes an additional step in establishing ACS connectivity, as the 5G-RG needs to know in which DNN the ACS can be found.

The result is that, during the registration time, the 5G-RG receives an indication of the DNN and the S-NSSAI to use to reach the network hosting the ACS. At session establishment time, the 5G-RG can require, via PCO or via DHCP, the coordinates to reach the ACS once connected to the DNN.

5.1.5 PDU Session Life Cycle Management

The establishment of a PDU session is initiated by the 5G-RG. This is done consistent with the subscription information received from the AMF at registration time.

At a high level, the session is requested, the network is configured, the access is configured, and setup is confirmed.

The 5G-RG requests session establishment via the NAS channel. The AGF will communicate access specific configuration to the 5G-RG via an AS message. This will include the identifiers (5WE session ID) to use in the user plane to identify the session, and the valid QFI values for the session (including the default value) and whether the information mapping QFI to DSCP/PCP marking that overrides the previous configuration is included.

Upon communication of the access specific session parameters and the PDU session established accept message (NAS) to the 5G-RG, a confirmation is sent by the 5G-RG via an AS ACK message.
At any point during the session lifetime, a 5G-RG may modify the session or release the session. The network may also release the session. This is typically in response to business issues such as non-payment.

5.1.6 5G Behavior and Fall Back

A 5G capable RG implements 5G procedures and is identified as operating in a 5G-RG mode. A 5G capable RG typically also implements a non-5G set of capabilities (identified as FN-RG capabilities) allowing it to support a non-5G mode of operation (identified as an FN-RG mode of operation in BBF WWC specifications). Therefore, a 5G capable RG can be deployed in advance of deployment of a reachable AGF and 5G Core and may obtain service from existing BNGs.

LCP is used to negotiate whether the PPPoE session is used for 5G procedures or is attempting to initiate a PPPoE based legacy IP session, as explained in the section ‘LCP procedures’ in TR-456. A 5G capable RG that has an LCP request for 5G control channel connectivity rejected (indicating lack of 5G support) and implements FN-RG capabilities, will be able to fall back to the FN-RG mode of operation.

5.2 End-to-end QoS

The overall WWC system can be considered to be three hierarchical QoS domains. The service layer, the 5G System layer and the Wireline transport layer. For the purposes of this discussion, NG RAN access is considered to be part of the 5G system as the radio layer is specified by 3GPP and will not be further expounded upon in this recommendation.

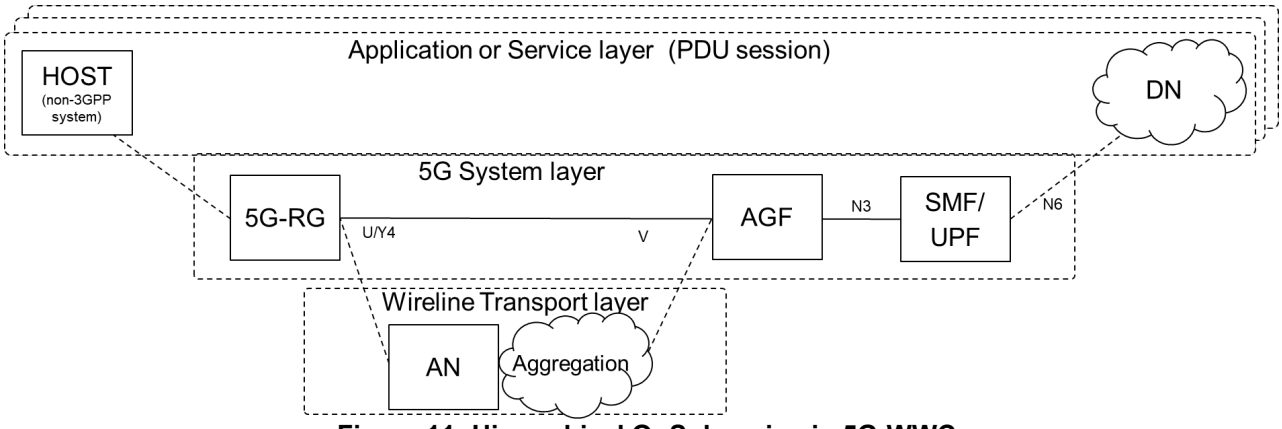

Figure 11: Hierarchical QoS domains in 5G-WWC

The 5G system is nominally transparent to service layer (PDU session) traffic other than applying specific QoS treatments to identified QoS flows. QoS rules are applied at the ingress to the 5G system to classify

traffic onto 5G QoS flows, and the results of this classification is conveyed per packet over the user plane within the boundaries of the 5G system by QoS Flow Identification metadata appended to each packet. QoS markings in the service layer packets and frames is not normally modified by the 5G System.

The ingress points to the 5G System for wireline access are:
- The 5G-RG for traffic originating from non-3GPP and 3GPP systems at the premises
- The AGF in the case of an FN-RG, for traffic originating from non-3GPP systems at the premises
- The UPF for traffic originating in a data network (DN) for forwarding to a 5G-RG or FN-RG.

The application layer extends beyond the boundaries of the 5G System and is not necessarily homogenous in terms of the QoS treatment, each QoS domain instance may not be contiguous end-to-end, but with the boundaries instantiated at the ingress points to the 5G System. The set of end systems at the premises served by a PDU session and a DN collectively can be considered to be a unique QoS domain, or concatenation of QoS domains at the service layer.

Examples of this would be business services for enterprise access whereby the IP packet QoS markings are preserved from non-3GPP device in the home to the serving end point in the DN. Internet access may require treating marking as untrusted and addressing this via ‘bleaching’ or reclassifying and remarking traffic at the ingress to the 5G system.

Application or service layer QoS is indicated by DSCP marking (IPv4 and IPv6) and by PCP (Ethernet). There are some best practices to consider for QoS rules:

1) Received DSCP can be used to map to 5QI for scenarios where there is a need for homogenous QoS treatment for a given IP flow in both the 5G System QoS domain and the non-3GPP service QoS domains in the premises network and the DN.
2) In deployments where the access equipment snoops the received DSCP and maps to traffic class, the QoS flow mapping to 5QI to traffic class should be configured such that traffic class quotas are not inadvertently exceeded. This can be achieved by operational practice, or where explicit preservation of DSCP by the 5G system is not required, by remarking.

And there are scenarios where on a UNI the DSCP is honored, and priority tagged frames not accepted, so the use of upstream indication of QoS requirements may be mutually exclusive.

Application layer traffic can leverage 5G QoS mechanisms (for some background information on QoS in 5G architecture, see clause 5.7 “QoS Model” in TS 23.501 [32]). In particular, data packets in the downstream and the upstream are mapped to QoS flows based on policy rules. In a PDU session, the QoS flow is used for QoS differentiation in the 5G System. A QoS Flow Identifier (QFI) is used to identify a QoS Flow in the wireless and wireline converged 5G System. The QFI is communicated in the GTP-U encapsulation on the N3 and N9 interfaces between the UPFs and the AGF and it is communicated in the 5WE [38] header between the AGF and the 5G-RG. At the PDU session resource establishment point in the NGAP control N2 flows, the mapping from user plane QFI to other 5GS QoS parameters (e.g., 5QI) and then to the Wireline transport layer Ethernet packet markings for the specific PDU session is determined.

This may use:
- NGAP signaling information for the mapping of QFI to 5QI or Pre-defined QoS parameters for standardized or pre-configured 5QI.
- RG-LWAC information for the mapping of specific values of 5QI to Ethernet PCP as well as IP DSCP and indication as to applicability for upstream and/or downstream marking/remarking.

The marking/remarking controls are locally configured and may be overridden by RG-LWAC information communicated to the AGF or FMIF at registration time. The upstream marking control information is further disseminated by an AGF to the 5G-RG at session establishment time. The controls are encoded as 3 bits:

- P-bit indicates that priority tagging MUST be used for Ethernet frames communicated in the upstream direction. (VLAN tagging is always assumed to be used by the AGF in the downstream direction, this PCP can always be marked in downstream frames)

- U-bit indicates that DSCP remarking of IP packets is to be performed by the 5G-RG for packets sent upstream. This is performed by an AGF in the case of an FN-RG.
- D-bit indicates that DSCP remarking of IP packets is to be performed by the AGF for packets sent downstream.

The bit tuples and their corresponding use cases for a 5G-RG are:

- PUD=110: The IP DSCP values received from the home LAN are considered untrusted and is remarked by the 5G-RG. Priority tagging is used to communicate upstream differentiated QoS requirements in the access network. The AGF communicates differentiated QoS by PCP marking of downstream frames.
- PUD=100: The IP DSCP values received from the home LAN are trusted and are to be preserved across the 5G system and presented on the N6 interface. Priority tagging is used to communicate upstream differentiated QoS requirements in the access network. The AGF communicates differentiated QoS by PCP marking of downstream frames.
- PUD=011: The IP DSCP value is used by access network equipment, therefore is set to correspond to the requirements of the 5G system. In some deployments this configuration precludes the use of priority tagging. AGF communicates differentiated QoS requirements by marking PCP and DSCP on downstream packets. For some deployments, a single, default PCP may be used.
- Other configurations of the PUD bit tuple are not precluded, however there are no use cases currently under consideration.

Wireline access typically has a static resource allocation for a pre-provisioned access circuit that is shared by a subscriber's set of PDU sessions. The resource allocation is expressed as a traffic contract with a number of traffic classes and associated bandwidth parameters. Therefore, the AGF needs to ensure that requested PDU session resources can be satisfied within the context of the traffic contract, and the QFIs are mapped to the appropriate traffic class (identified by PCP value) that corresponds to the 5QI value of the relevant QoS flow to receive the proper QoS treatment.

5G WWC takes the 5G QoS Parameters as defined in clause 5.7.2 in TS 23.501 [24] as basis, typically supports:

- **5QI** (5G QoS Identifier) is a scalar that is used as a reference to 5G QoS characteristics, i.e., wireline access node-specific parameters that control QoS forwarding treatment for the QoS Flow in 5G WWC.

- **ARP** (Allocation and Retention Priority) allows deciding whether a QoS Flow establishment/Modification may be accepted or needs to be rejected in the case of resource limitation.

- **Session-AMBR** (Aggregated Maximum Bit Rate) represents the aggregated bit rates at the PDU Session level (in the upstream and the downstream) for all Non-GBR QoS flows. The downstream value is enforced by the UPF anchoring the session and the upstream value is enforced by the 5G-RG. Session-AMBR limits the sum of Non-GBR QoS flows for a specific PDU session.

- **FBR** (Flow Bit Rates) including GFBR (Guaranteed Flow Bit Rate, UL and DL) and MFBR (Maximum Flow Bit Rate, UL and DL) are only valid for GBR QoS Flow. GFBR guarantees the minimum and MFBR limits the maximum of the bit rate for a GBR QoS flow.

- **RQA** (Reflective QoS Attribute) is an optional parameter which indicates that certain traffic carried on this QoS Flow is subject to Reflective QoS. Reflective QoS identifies scenarios where the upstream response to an IP 5 tuple identified flow will use the QFI of the downstream message and not the default QFI for the PDU session. RQI indicates the activation of the reflective QoS towards the 5G-RG for the transferred packet. It is used only in the downlink direction. If Reflective QoS Activation has not been configured for the involved QoS flow, the RQI shall be ignored by the NG-RAN node. RQI is communicated in the GTP-U header across the N3 and N9 interfaces, and in the 5WE header across the V interface.

Note that the Notification control, UE-AMBR, Maximum Packet Loss Rate as defined in Clause 5.7.2 in TS 23.501 are not supported for wireline access.

Wireline access specific 5G QoS characteristics are defined as RG-LWAC (RG-Level Wireline Access Characteristics), which is per subscription characteristics that describe the wireline access resource model for both upstream and downstream traffic. The RG-LWAC information is communicated to the AGF or FMIF during the N2/NGAP Initial UE Context procedure (that itself is part of the RG registration or Service Request procedure and can be updated during the session).

Note: at the time of publication of this document, N2 specifications do not cover the in-session modification of RG-LWAC.

It contains:

- the bandwidth profile information for up to eight traffic classes (identified by Ethernet PCP). The RG-LWAC object that is communicated to the AGF or FMIF contains the traffic contract description and the relevant aspects of which are communicated to the 5G-RG via the AS subscription parameters TLV. The RG-LWAC is uniquely applicable to the wireline access network and is only relevant to the AGF or FMIF. The descriptors as defined in RG-LWAC are used as the wireline specific 5G QoS mechanism for shaping, queuing and policing the QoS flow as specified in both TS 23.316 [20] and TR-456 [16].
- The mapping of specific values of 5QI to Ethernet PCP and DSCP marking as well as controls for the performance of marking/remarking by the 5G-RG and the AGF. This information may also be preconfigured in the AGF. This packet marking provides indication of required packet/frame treatments at intermediate queuing points in the PDU session path.

NOTE: How the RG-LWAC is used for FMIF [17] is FFS.

5.2.1 5G-RG E2E QoS Aspects

5G-RG will receive QoS rules, the relevant traffic class descriptors, Session-AMBR, and the transport layer priority value for performing the 5G System QoS per QoS Flow which is identified by QFI.

- The QoS rules are PDU Session-specific and used to mapping the UL packets against a specific QFI. A QoS rule contains packet set filter (e.g., IP 5-tuple or received DSCP for IP type PDU session) and the corresponding QFI and may be:
    - explicitly provided to the 5G-RG by the SMF (i.e., explicitly signaled QoS rules using the PDU Session Establishment/Modification procedure),
    - implicitly derived by the 5G-RG by applying Reflective QoS (see clause 5.7.5 in TS 23.501).

- The traffic class mapping information for the wireline traffic contract containing UL Descriptor and UL TC Descriptor (part of the RG-LWAC) is provided to the 5G-RG via AS subscription parameters TLV during the establishment of the AS signaling connection between 5G-RG and AGF (e.g., at registration time).

- Session-AMBR for all Non-GBR QoS flow and/or GFBR/MFBR for GBR QoS flow are PDU Session-specific and provided to the 5G-RG in PDU Session Establishment/Modification procedure.

- Transport layer priority value is QFI specific within a PDU Session, which contains QFI to 802.1P PCP and DSCP value mapping pair information as well as control over the applicability of each for upstream and downstream. The mapping between QFI and transport layer priority value may be:
    - explicitly provided to the 5G-RG by the AGF during the PDU Session Establishment/Modification procedure, or defaulting to values pre-configured in the 5G-RG, or

- implicitly derived by the 5G-RG via the received QFI and PCP/DSCP marked downstream traffic.

AGF will receive RG-LWAC, one or multiple QoS profiles and the corresponding QFIs and maintain an up-to-date list of QFI to PCP/DSCP mapping for performing the E2E QoS per QoS flow which is identified by QFI.

- The QoS profile(s) is PDU Session-specific and provided by the SMF during PDU Session Resource Setup/Modify Request via N2 interface. For Non-GBR QoS flow, 5QI and ARP are mandatory and RQA is optional. For GBR QoS flow, 5QI, ARP and GFBR/MFBR are mandatory.

AGF will ignore parameters that are wireless specific such as priority level, averaging window etc. if received.

- The QFI to PCP and or IP DSCP mapping is derived using both QFI with corresponding QoS profile (e.g., 5QI) relationship and the 5QI descriptor (5QI to PCP/DSCP mapping).
- DL Descriptor and DL TC Descriptor as indicated in RG-LWAC and/or AGF RG local configuration contains information of how the AGF perform both RG-level and Traffic class level shaping and queuing of downstream traffic. DL policing descriptor and DL TC policing descriptor may be provided as augments.
- UL Policing Descriptor and UL TC Policing Descriptor as indicated in RG-LWAC and/or AGF RG local configuration contains information of how the AGF perform both RG-level and Traffic class level policing of upstream traffic.

Use of Parameters for DL and UL traffic between 5G-RG and AGF

For DL traffic:

- AGF receives the DL User Plane traffic and obtains the QFI and RQI from the GTP-U header
- AGF performs the wireline-specific marking for the wireline access-specific resources based on the up-to-date list of QFI to PCP/DSCP mapping:
  - Mark the 5WE header by copying the QFI value and RQI from the GTP-U header
  - Mark the transport layer with the QFI corresponding 802.1P PCP value and apply any configured remarking of the IP DSCP value if the D-bit is set in the marking controls
- AGF shapes and queues the marked downstream traffic based on DL TC descriptor on the basis of the QFI value as indicated in the GTP-U header and DL descriptor
- AGF transmits the shaped and queued downstream traffic based on the protocol discriminator
  - in a single tunnel (5WE) between AGF and 5G-RG
- 5G-RG receives the downstream traffic.
- 5G-RG activates Reflective QoS mechanism for the RQI=1 marked QoS flow, i.e., creates a derived QoS rule including upstream packet set filter (e.g., IP 5-tuple), and the required QFI marking.

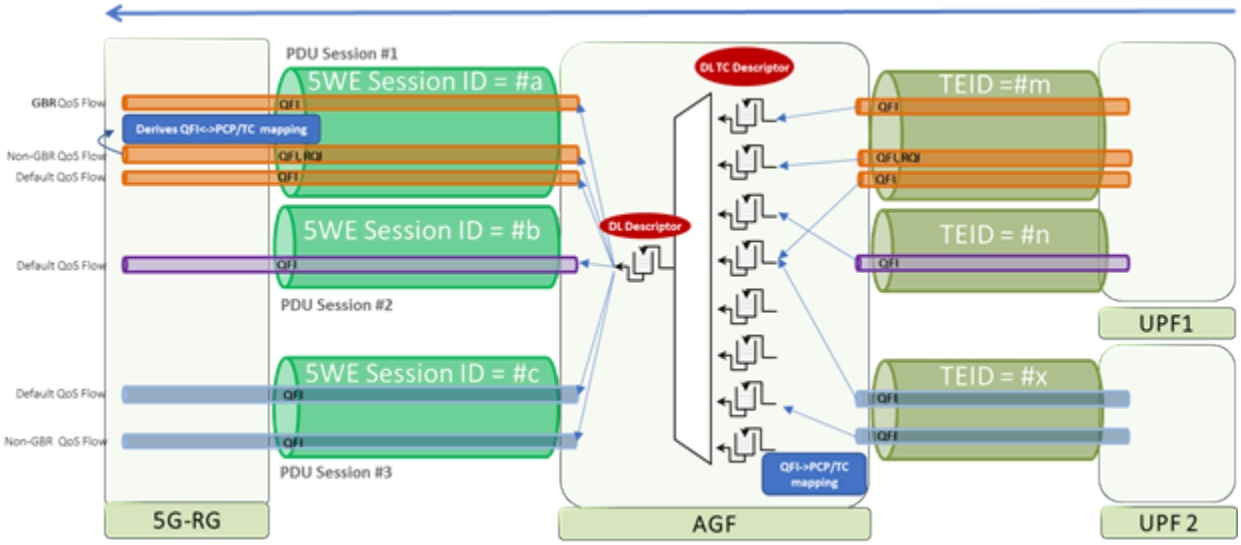

Figure 12: Example of downstream packet forwarding

For UL traffic:

- 5G-RG generates UL User Plane traffic based on the received/derived QoS rules.
- 5G-RG performs the wireline-specific marking for the wireline access-specific resources based on the QFI and the associated QoS rule
    - Mark the QFI in the 5WE header based on a QoS rule
    - Mark the indicated PCP value for VLAN tagged traffic, and if the use of priority tagged frames is configured (P bit set in the marking controls), the use of priority tagging to encode PCP information for untagged traffic.
    - If remarking of IP DSCP traffic is indicated for the QFI via the U bit in the marking controls, remark the upstream IP Packet DSCP value.
- 5G-RG performs Session-AMBR limiting of all non-GBR traffic rate, MFBR limiting of GBR traffic rate.
- 5G-RG shapes and queues the marked upstream traffic based on UL TC descriptor on the basis of QFI value as indicated in 5WE header and UL descriptor.
- 5G-RG transmits the shaped and queued upstream traffic based on the protocol discriminator,
    - in a single tunnel (5WE) per PDU Session between 5G-RG and AGF.
- AGF receives and aggregates the marked upstream traffic based on UL policing descriptor and UL TC policing descriptor on the basis of the TC mapping indicated for the QFI in the received 5WE header.
- AGF marks the aggregated upstream traffic:
    - Mark the GTP-U header by copying the QFI value indicated in 5WE header,
    - Mark the transport layer, i.e., UDP/IP encapsulating GTP-U with a DSCP value that is determined based on 5QI (and possibly ARP) of the associated QFI identified QoS flow and information configured by management.

Details and requirements for user plane aspects of QoS on the AGF are covered in the “QoS” section of TR-456 [16].

Requirements for user plane aspects of QoS on the 5G-RG are covered in the “5G-WWC.WAN.UP.QoS” section of TR-124i6 [7].

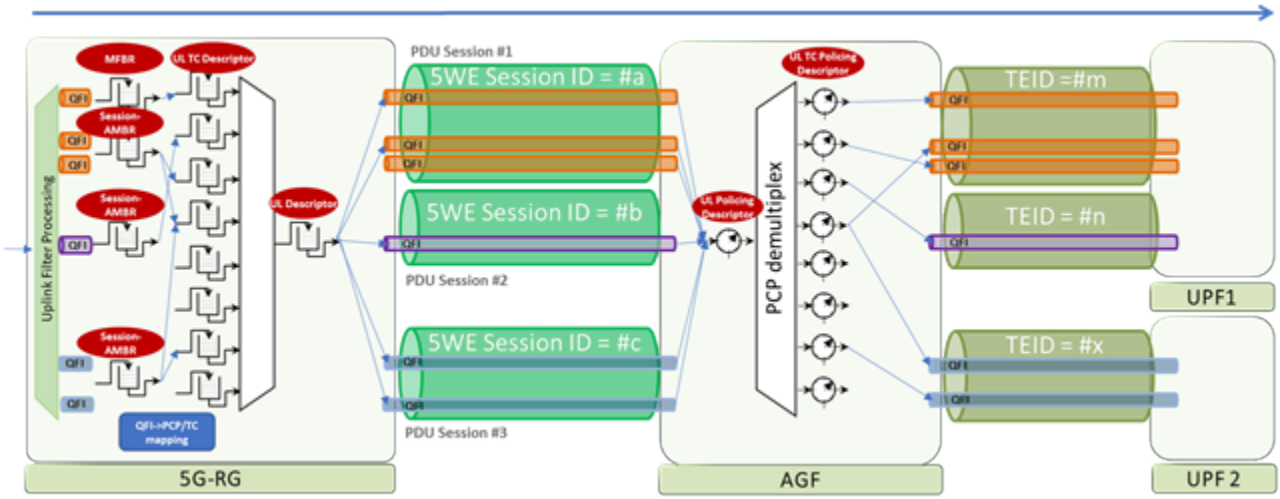

Figure 13: Example of upstream packet forwarding

5.2.2 FN-RG E2E QoS aspects

An AGF acting as a proxy UE on behalf of an FN-RG also is required to perform upstream QoS flow mapping for the purposes of:

- Conveying QFI metadata to remote UPFs (N3 connected) for the purposes of policing, and charging
- Establishing correct tunnel DSCP marking for N3 encapsulated packets and frames.
- Policing and charging at a co-located UPF that serves as an anchor for the PDU session.

Note that there is no mechanism, to date, to either communicate or support 5QI, ARP, and RQA or SDF filter information for an FN-RG.

5.2.3 ATSSS QoS aspects

ATSSS leverages a similar QoS model to the single access scenarios, but applied to the multi-access PDU sessions, as described in TS 23.501 clause 5.32 “Support for ATSSS”. ATSSS does not introduce new requirements to the mapping of 5G QoS onto wireline transport.

5.3 Accounting

5.3.1 Accounting in 5GS

In 5GS, subscriber accounting is done at the user plane (UPF).

In 5G WWC, the UPF may limit the aggregate bandwidth for all Non-GBR Flows for a single PDU Session, while the AGF, enforcing the QoS at RG level, may limit further the aggregate of traffic flowing towards the user. In case the RG supports multiple PDU sessions, the bandwidth shaping performed by the AGF in downstream direction might cause packets discards.

UPF accounting is controlled by SMF, which itself interacts with the Policy and Charging Function (PCF) and the Charging Function (CHF), as described in TS 23.503 [26].

5.3.2 Accounting Accuracy

Assuming no mistakes in configuring the bandwidth in the wireline access network to accommodate the shaping rate applied at the AGF level (either via the RG-LWAC parameters or via local configuration), the loss of packets that may result from the AGF policy enforcement has to be considered the main structural issue impacting the accounting accuracy.

There might be other forms of losses in the wireline access network: temporary fault conditions, congestion on some links, limited queues length along the path, flapping in the DSL bandwidth due to crosstalk phenomena, and so on. However, these losses are statistically less relevant, somewhat unavoidable and normally occurring also in deployments with traditional BNG.

The real new element introduced for wireline access by the adoption of the WWC is that the QoS is enforced on both the UPF and the AGF, while in the legacy scenario the QoS enforcement is performed by the BNG, which is also in charge of the accounting. Notice that this newness element is however well-established in the wireless architecture context, where both UPF and RAN perform QoS enforcement (even if RAN uses different mechanisms compared to AGF), while the UPF is the only element designated for the accounting.

The extension of the 5GS paradigm to the wireline access may cause problems with the accounting accuracy (with some packets being reported that have not been delivered to the user), as the UPF is not aware of possible losses occurred at the AGF level.

As far as there is a unique PDU session serving the RG, the downstream traffic can be correctly counted, as far as the shaping applied by the AGF is configured consistently with the shaping on the UPF. However, in case the RG handles multiple PDU sessions, the accounting accuracy cannot be guaranteed.

It is however important to point out that:

- For wireline users, normally operators do not tend to base their offers on volume.
- Most of the bandwidth consuming applications like video are TCP-based and more and more of them will be QUIC-based. These protocols allow the upper layers to quickly adapt to the experienced e2e bandwidth, avoiding the AGF performing heavy discards on traffic already counted or mirrored by the UPF.
- For wireless users, due to the nature of the Radio Access Network, operators are already used to this kind of inaccuracies.
- If the operator configures the network so that all the PDUs sessions opened by a wireline user are served by the same co-located AGF/UPF, accounting accuracy may be achieved.

Note 1: potential enhancements to address or mitigate further this accuracy issue is FFS.
Note 2: in 5GS, lawful interception is also performed at the UPF. For the same reasons explained above with regards to accounting, there might be differences between the traffic mirrored in the UPF and the traffic delivered to the target. Since the whole lawful interception subject is FFS, this problem will be addressed in a later phase.

5.4 Control and User Plane Separation

The AGF Control and User Plane Separation (CUPS) is described in BBF work in progress document WT-458 ‘CUPS for AGF’ [18]. AGF CUPS is a possible deployment option. AGF-CP refers to the AGF control plane and AGF-UP is referring to AGF user plane.

Some of the drivers for this work are: independent scaling of CP and UP, separate locations for CP and UP, more flexibility to locate and combine AGF functions.

BBF WT-458 defines the AGF CUPS solution and architecture utilizing the PFCP protocol. PFCP is also used in the BBF specification for dis-aggregated BNG TR-459 [19]. The base PFCP is specified by 3GPP and details are covered in TS 29.244.

The BBF is using the extensibility mechanism of PFCP. Defining new PFCP information elements for the AGF in BBF work in progress in document WT-458.

In the case of co-located UPF, the combined AGF-UP/UPF supports two control interfaces: one toward AGF-CP and N4 toward SMF.

5.5 Migration Aspects

This section describes the enablers built into the WWC architecture to support smooth migration paths. As operators already service fixed broadband subscribers, they look for efficient ways to transfer their end users and services to the converged 5G core. Migration must take into account external constraints, such as regulation or agreements with 3rd party access operators, while limiting impacts on existing end users and integrating with operator’s existing infrastructure and operations.

Each operator has their own starting point (e.g., RG models, access network characteristics, service offerings, …) and their end goal (e.g., limit convergence only for new 5G services or eventually migrate all subscribers and services to 5G core), as a result, the Broadband Forum does not mandate a specific

migration strategy. Instead 5G WWC specifications include a number of features for operators to build their own migration path.

The key enablers for migration include:

- **FN-RG support**: existing RGs that do not have 5G functionalities can be managed by the 5G core, by having the AGF act as a “proxy UE” (session in adaptive mode). The session between FN-RG and AGF can be either PPPoE or IPoE/DHCP.

- **Line-ID based state machine** where the key identifier for an end user is the network-based line-id, as already used by operators, with the access node inserting the identifier. The AGF state machine allows a move from FN-RG to 5G-RG, as well as fall back to FN-RG. The main benefit is the possibility to separate the lifecycles of RGs and network elements, where no synchronized operations on RG, BNG and AGF are required when introducing 5G-RG or AGF. In particular, an operator may not have control on the type of RG installed by the end user.

- **Dual mode RG** can support both 5G-RG and FN-RG modes, as specified in TR-124. They can operate in 5G-RG mode when they find an AGF supporting direct mode sessions, else they default to FN-RG mode (typically in the case where the RG only faces a BNG).

- **Support of existing Layer 2/VLAN network models** allow given VLANs to remain on the existing BNG/AAA infrastructure. For example, an RG can have a dedicated VLAN for IPTV (multicast) that is not terminated by the AGF. As a result, not all services need to be immediately supported by the 5G core.

- **Shared broadcast domain** for AGF and BNG, combined with the line-ID based state machine described in the Migration Consideration section of TR-456 and the RG own state machine, described in TR-124 (see use of PPPoE Service-Name tag in particular), enables the simultaneous co-existence of AGFs and BNGs.

- **Support of existing access model** including ethernet VLANs, tagged or untagged, and L2TP aggregation from a LAC in the access network, enables the AGF to process existing broadband lines, without the need to re-provision access lines. Attention must be paid on the following points though:
    - In this issue, 5G-RG support requires 1:1 VLAN. Operators using N:1 VLANs today (a.k.a. “shared VLANs”) must change the access node configuration to add a customer tag towards the AGF (no modification is needed on the U interface, toward the RG). Support of N:1 VLAN for 5G-RG is FFS. This does not apply to FN-RG as both 1:1 and N:1 VLAN models are supported.
    - 5G-RG uses 5WE protocol to transport PDU to/from AGF. It is expected that the Access Node will transparently forward 5WE frames, as 5WE repurposes PPPoE data encapsulation with the same Ethernet type but at the value of 2 in the version field.

- **Support of E-UTRAN (LTE)** as an option for hybrid access, so that the benefit of dual access with WWC is not conditioned to the general availability of 5G new radio.

- **Flexible “boxing”** leaves the flexibility to vendors and operators how the logical functions are implemented. In particular, an AGF could be based on an upgrade of an existing node (e.g., BNG or Access Node) or on a new standalone element. The AGF could also be combined with the UPF.

A number of the features above supporting migration are specified in a way that is configurable, so that the operator can decide which modes of operation are acceptable for the network and the RG.

The 5G WWC specifications do not detail specific migration actions, such as subscriber data management, when moving from wireline AAA (e.g., RADIUS server) to 5G Core (UDR), or IP address management (as each PDU session consumes an IPv4 address or IPv6 prefix).

Note that migration aspects may be extended in future phases, based on additional convergence use cases (e.g., multi-access).

5.6 Access Wholesale

Wholesale applied to 5G WWC means that 5G services are delivered based on a set of network components, typically access nodes, AGF and 5G core, that are owned and operated by at least two network operators. Currently 5G WWC supports the case where access nodes can be owned and operated by a different operator than the 5G operator.

There are two options specified for third party access network support: L2 bitstream and L2TP. Additional wholesale scenarios are FFS.

5.6.1 Ethernet wholesale

Ethernet wholesale, also known as L2 bitstream, is based on VLAN handoff between access provider and 5G operator. It is illustrated in Figure 14. The line-Id is inserted by the access node (3rd party access provider), which is unique within the access provider domain and known by the 5G operator. In case of FN-RG, the AGF adds an identifier for the access provider, as described in TR-456, so that the SUPI contains a line identifier that is globally unique.

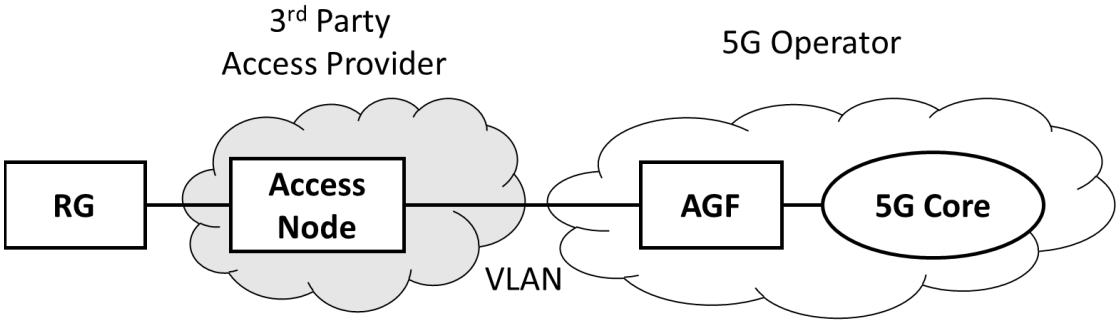

Figure 14: Access Wholesale based on Ethernet

5.6.2 L2TP Wholesale

Wholesale based on L2TP assumes that the RG initiates PPP to an L2TP access concentrator (LAC) in the access provider domain, as shown in Figure 15. The LAC selects an L2TP network server (LNS) within the 5G operator domain.

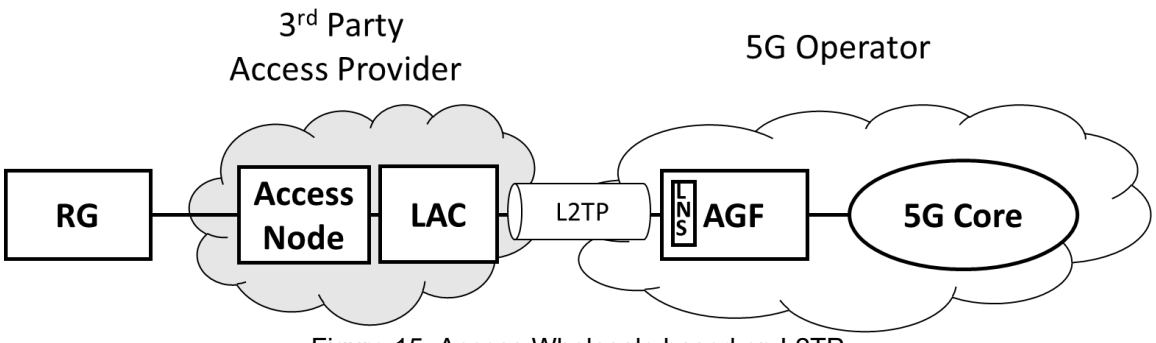

Figure 15: Access Wholesale based on L2TP

In general, the LNS host selection is based on a AAA interaction on the LAC and the 5G operator may influence the selection of an LNS that is part of an AGF, so that the session is passed to the 5G core. This assumes that the RG is an FN-RG that uses PPP towards the LAC and that the AGF terminates PPP over L2TP and processes the session in adaptive mode. Identically to the L2 bitstream use case, the AGF adds the line ID source that corresponds to the access provider, to create a globally unique identifier for the 5G core.

Note that support of L2TP wholesale for 5G-RG is FFS.
Note that L2TP can also be used by a 5G operator owning their access network, so this model can apply also in non-wholesale use cases.

5.7 Supervision of the connectivity in the wireline access network

In existing wireline deployments, there is not a uniform deployment of tools and capabilities for supervision of wireline access. Therefore, when interworking observed the FN-RG behaviour with the session and registration state machines for the 5GC, outages may manifest themselves as different behaviours in different deployment scenarios.
In the context of the variety of supervision tools used, a high-level summary of the possible scenarios and examples of supervision tools in a network where AGF is deployed would be:

- FN-RG to AGF connectivity is unsupervised;
- FN-RG to AGF connectivity is supervised by the AGF (typically via PPP LCP Echo Request, ICMP Ping, BFD);
- FN-RG to AGF connectivity is supervised by the FN-RG (typically via ARP-Ping or PPP LCP Echo Request);
- FN-RG to AGF connectivity is supervised by both the FN-RG and the AGF.
- FN-RG to AN physical layer connectivity is monitored by the AN and reported to the AGF (ANCP). AN to AGF is supervised.

The FN-RG to AGF connectivity may be unsupervised only in the case the FN-RG is attached via DHCP. If the FN-RG is attached via PPPoE, the liveliness check via LCP Echo Requests by the AGF is mandatory. However, the periodicity for this check is configurable. In some networks the interval may be configured to be quite large.

When an AGF does not supervise the wireline connectivity or it does it but with large periodicity, it might receive from an FN-RG an IP session initiation after a fault either occurred in the wireline access network or if it had a reset. It is also possible to envision an outage as simply an interruption in traffic that may be restored without AGF having detected the problem.

5.8 Connection Management state machine on AGF acting on behalf of FN-RG

When the AGF supervises wireline connectivity, the defined procedure to handle a detected outage (either due to a loss of connectivity or to an FN-RG fault) envisions that the AGF starts the AN Release procedure as documented in TS 23.316 clause 7.2.5.3 and TR-456 Section “FN-RG AN Release via W-5GAN”.

This procedure will cause:

- The AMF to send an N2 context release to the AGF.
- The AMF to enter the (CM-IDLE, RM-REGISTERED) state.
- The AMF to start the de-registration timer which, if allowed to expire, will result in a network initiated de-registration of the FN-RG.

Details about the above procedures are documented in TS 23.316 clause 7.2.5.3 ("FN-RG AN Release via W-5GAN”), TS 23.501 clause 5.5.1 (“Registration Management for non-3GPP access”) and TS 23.502 clause 4.2.2.3.3 (“Network-initiated Deregistration procedure”).

Upon receiving the N2 UE Context Release command from the AMF, the AGF will perform the following actions.

- The AGF to flush the FN-RG N2 context, keeping the N1 context and release the local scheduler appearances;
- The AGF to change state from (RM REGISTERED, CM-CONNECTED) to (RM-REGISTERED, CM-IDLE) (notice that the AGF acting on behalf of an FN-RG plays the role of a UE for the N1 interface, therefore it implements both the Registration and the Connection Management state machines);
- The AGF to start the 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 clause 8.2.7.17).

When this timer expires, the AGF enters the (RM-DEREGISTERED, CM-IDLE) state and flushes the local 3GPP N1 context.

If the wireline connectivity is restored prior to the expiry of the AGF Implicit Deregistration timer, the AGF will issue a Service Request on behalf of the FN-RG on the N1 interface to restore the set of PDU sessions active at the time of the outage, avoiding a new Registration on 5GC. Upon resuming the PDU sessions, the AGF will transition back to the (RM-REGISTERED, CM-CONNECTED) state.

If the wireline connectivity is restored after to the expiry of the AGF Implicit Deregistration timer, the AGF will start a NAS initial Registration procedure, as documented in TS 23.316 Clause 7.2.1.3 and TR-456 Section 8.1.10 “Registration Management Procedure for FN-RG”.

5.9 Co-ordination of Policies between ACS and PCF

This section explains how to co-ordinate via the OSS the policies configuration made by the PCF and the ACS on the UEs (5G-RG, FN-RG and AGF as proxy UE).

For the FN-RG case, in issue 1 of TR-456, the use of URSP policies by the AGF has not been specified and only one PDU session is supported. Therefore, a coordination of PCF and ACS for route selection policies is not needed. The ACS will configure the FN-RG for the legacy aspects. The URSP that the PCF might send to the proxy UE are not applied by the AGF. Therefore, for FN-RG, the following description concerns general ideas that may be studied to build further enhancements of this specification, whenever multiple PDU sessions and URSP might be reconsidered.

Figure 16 below represents the architectural view of 5G-RGs and FN-RGs connecting to the 5GC through an AGF, and adding the ACS, PCF, NEF, UDR and OSS elements.

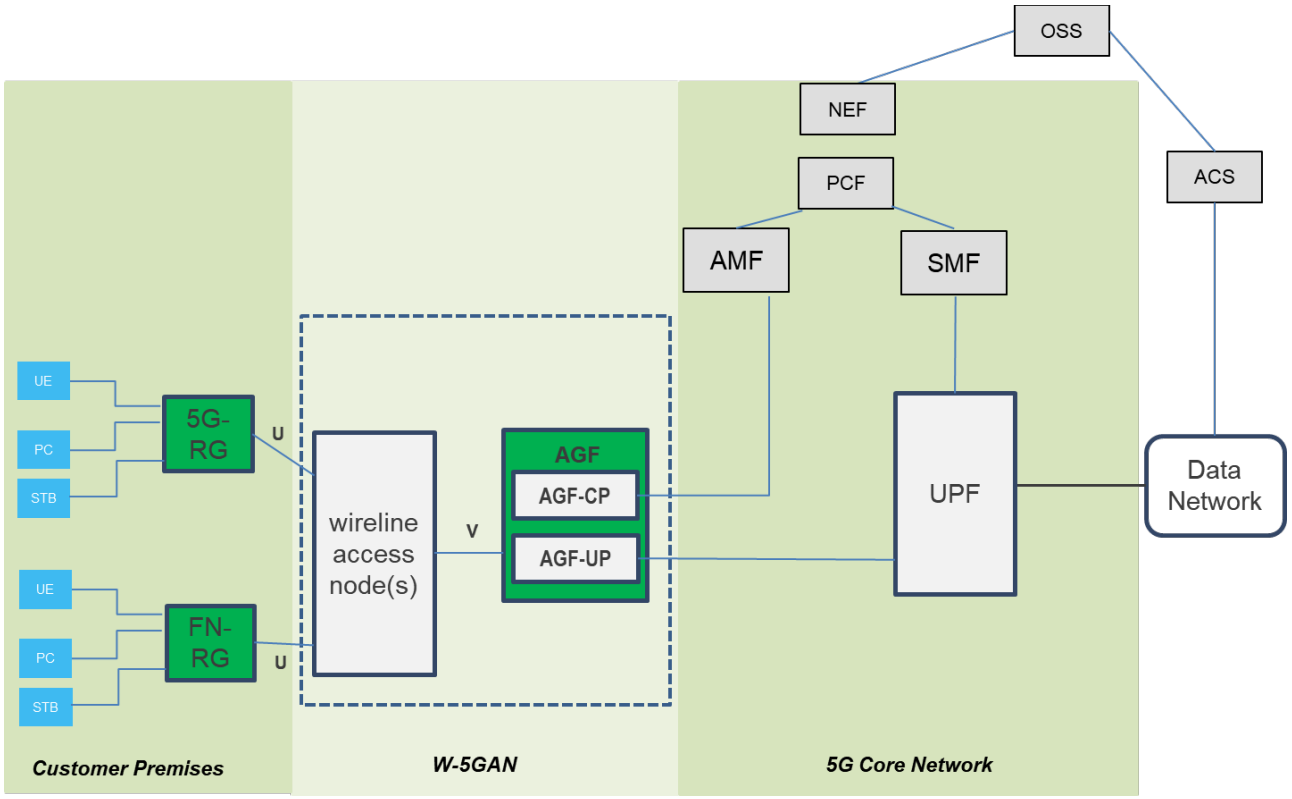

Figure 16: Interaction of ACS with PCF through the OSS

A 5G-RG behaves as a regular 3GPP UE (User Equipment, as a smartphone) i.e., it is able to exchange NAS/N1 signaling with the 5GC including:

- NAS to register to and establish signaling connectivity with the 5GC
- NAS to establish / modify /release data connectivity capabilities via the 5GC (called PDU Sessions)
- 5G-RG receiving URSP (UE Route Selection Policy) policies from the 5GC PCF (Policy Control Function) (via the AMF).

URSP are defined in TS 23.503 clause 6.6.2 and in TS 24.526 [28].

The N1/NAS for the FN-RG, which is not 5G capable, is terminated on AGF. The AGF exchanges NAS/N1 signaling with the 5GC on behalf of the FN-RG(s) they serve. This includes:

- NAS to register to and establish signaling connectivity with the 5GC
- NAS to establish / modify /release data connectivity capabilities via the 5GC (called PDU Sessions)
- AGF receiving URSP policies from the 5GC PCF (Policy Control Function) (via the AMF).

The PCF may send the URSP via NAS to the UE, which is the “AGF” since it is not requested to PCF to make differences between 5G-RG and FN-RG.

From the perspective of the 5GC, both the 5G-RG and the FN-RG are UE. The 5GC PCF determines and sends corresponding URSP policies to the 5G-RG or to the AGF in the case of FN-RGs.
The PCF gets policy related subscription information about a UE (or an RG) from the UDR. Current definition of this policy information is in TS 23.503.

Moreover, in a wireline network, an ACS using either CWMP (CPE WAN Management Protocol) protocol (BBF TR-069 latest issue [3]) or USP (User Services platform) protocol (TR-369, latest issue [4]), configures the RGs deployed in the customer premises by wireline operators. Both the 5G-RG and the FN-RG receive provisioning rules from the wireline ACS. The 5G-RG and the FN-RG use the user plane to exchange information with the ACS, possibly via an IP management address.

Requirements for the Northbound interface of the ACS are described in TR-131 (ACS Northbound interface requirements [8]). This northbound interface connects the ACS to an OSS (Operational Support System).

For 3GPP systems, it is the Network Exposure Function (NEF) that connects to the OSS to retrieve the ACS policies. The NEF exposes the information within the 5GS as URSP and the UDR becomes aware of this information. The UE policies can be delivered from the PCF to the RG interrogating the UDR.

The co-ordination of the policies in the PCF (wireless) and the ACS (wireline) happens at the OSS level.

The potential policy related co-ordination between ACS and PCF policies may correspond to the following example sets of policy information:

- Mapping from applications (e.g., internet / IMS Voice / IPTV) to data sessions: Data sessions relate to DNN, slice identifier S-NSSAI in 5GC. A priori, the mapping from applications (e.g., internet / IMS Voice / IPTV) to data sessions is configured once on the terminal.
- For FN-RGs, URSP policies that maps traffic multiplexing identifiers (e.g., S-tags) to 5GC PDU session level parameters (DNN, S-NSSAI).

In 5GC, the PCF provides the UE with URSP rules that contain a mapping from traffic filters to PDU Session parameters (DNN, S-NSSAI) where traffic filters may correspond to an application Id or to traffic related filters (e.g., IP “5 Tuple”).

TR-181 [6] object defines policies sent by an ACS that can associate an application (e.g., internet / IMS Voice / IPTV) with a L2 header (e.g., VLAN) to be used by the RG.

When there is only one IP session, additional configurations for mapping FN-RG IP sessions to VLANs by the ACS to the RG are not required.

In the case of multiple VLANs between the FN-RG and the AGF, ACS rules control how the RG sends upstream traffic and signaling requests (DHCP, PPPoE, RS) on the Line ID (or VLAN in case of a dedicated VLAN per IP session) corresponding to the target application (as defined in the TR-181 object model).

When the AGF handles signaling requests (DHCP, PPPoE, RS) received from the RG, the AGF will either default the DNN/S-NSSAI or infer it via PPPoE credentials (NAI) and URSP.

Coherency is required between the “application to Line ID” mapping defined in the ACS and the Line ID to (DNN, S-NSSAI) mapping used by the AGF, because improper configuration may lead to service deployment issues.

To ensure this coherency, the 5GC supports a mechanism described in clause 9.6.3 of TS 23.316 [20] where the ACS information may be configured by a 3rd party AF. The ACS information useful in this case is the mapping between the Line ID (or VLAN in case of one VLAN per IP session) used on the V (wireline) interface of the AGF and the PDU session subscription parameters (e.g., (DNN, S-NSSAI)).

5.10 RG management

The 5GC has been extended to support TR-069/369 for CPE management, including FN-RG and 5G-RG. This permits a significant suite of service capabilities to be easily ported to the converged core. Extensions to the BBF document ‘Functional Requirements for Broadband Residential Gateway Devices’ have been made for 5G-RGs in [7]. Extensions to the TR-069/369 data models explicitly for 5G remote management are included in BBF document TR-181[6].

5.11 Network slicing support

In case the text of this section conflicts with 3GPP Rel. 16 references, 3GPP references prevail.
The specification TS 23.501 [24] clause 5.15 defines the 5G Network Slice as a logical network that provides specific network capabilities and network characteristics; specifically, network slice is composed by the access network and the core network.

The network compliance with 3GPP specification supports at least one network slice instance including the Core Network Control Plane and User plane network Functions.
The selection of the set of Network Slice instances is triggered by the Registration procedure and it is supported for both 5G-RG and FN-RG.

The Network Slice is identified in the 5G-RG and in AGF by the S-NSSAI (Single Network Slice Selection Assistance Information).

The S-NSSAI is specified in TS 23.501 clause 5.15.2. It is comprised of:

- A Slice/Service Type (SST), which refers to the expected Network Slice behavior in terms of features and services.
- A Slice Differentiator (SD), which is an optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

The format of S-NSSAI is defined in TS 23.003 [21] clause 28.4.

The AMF plays the role of the control plane anchor point and entrance of slices: in fact, for a device that is connected simultaneously to more than one slice, the same Serving AMF must be used. Therefore, the AGF, handled by the 5G Core as the equivalent of an access node, is responsible for the AMF selection for both 5G-RG and FN-RG as described in the section below. The selected AMF is responsible to verify whether it is the effective serving AMF supporting the set of slices requested by the device. The procedure describing how the AMF checks whether it can serve the S-NSSAI(s) from the Requested NSSAI is defined in TS 23.501 clause 5.15.5.2 and in clause 4.6 of TS 24.501 [27].

The 5G-RG supports the NSSAI configuration and storage aspects defined in TS 23.501 clause 5.15.4. Since for wireline access network, there is no issue in adding the Requested NSSAI in clear text in the NAS protocol before the NAS security is established, the 5G-RG sends the Requested-NSSAI, if available, and it works in default in mode b) defined in TS 23.501 clause 5.15.9.

In case of an IPoE FN-RG, there is a separate subscription per PDU session supported, therefore only the defaults in UDM apply. The subscription will have a subscribed NSSAI which is also the default S-NSSAI and a default DNN within that S-NSSAI. The AGF will not include DNN or slice information in PDU SESSION ESTABLISHMENT REQUESTs. The default DNN and S-NSSAI will be determined by the AMF via a combination of subscription information and local policy.

In case of an PPPoE FN-RG, the subscription will have a set of subscribed NSSAI that is communicated to the AGF proxy UE termination as the set of allowed NSSAI, one or more default S-NSSAI as well as subscribed DNN per NSSAI. The identification of default values is not shared with the AGF.

Normal procedure would be that the default AMF for the AGF supports the set of subscribed NSSAI and if not, the registration will be redirected. When S-NSSAI is not indicated in PDU SESSION ESTABLISHMENT REQUESTs from the AGF, the AMF will use the subscription defaults combined with local policy to determine the appropriate S-NSSAI. The AGF however may indicate a specific S-NSSAI/DNN pair in PDU SESSION ESTABLISHMENT REQUEST, mapping the NAI realm information received from the FN-RG during the PPP authentication phase onto S-NSSAI/DNN information via URSP rules communicated to the AGF proxy NAS termination at registration time.

This means PPPoE based FN-RG may access different S-NSSAI/DNN of the 5GS, indicating the intended DNN and S-NSSAI via the NAI information used in the PPP authentication, which on turn may be configured remotely via TR-069. The AGF will proceed with access to the requested S-NSSAI/DNN if and only if the

subscription includes the S-NSSAI/DNN pair is in the allowed set (which may include default selections), communicated to it at registration time.

5.12 Managing and using AMF connections

5.12.1 Managing N2 connections

AMF is the anchor point of all 5GC control plane interactions; it is connected to AGF via N2 interface, which leverages the NGAP protocol.

The AGF is responsible for establishing and maintaining connections to all AMF nodes that are candidates for serving any RG served by the AGF. For managing the AMF connections, the AGF supports the relevant functions that are equivalent to signaling aspects in the wireless access nodes, to ensure that the W-5GAN access can be natively integrated to the 5GC of a network operator. This ensures that not only the 5G functionality, but the same design, deployment and operation principles can be applied for wireline related network slices and network functions.

The AGF supports the following major functions, defined in detail in TS 23.501, TS 38.413 and TS 29.303 clause 7.2. “Procedure for AMF Discovery by 5G-AN” including:

- Discover the AMF nodes it can connect to. For this, the AMF may use the DNS method defined in clause 4 of TS 29.303, or may use O&M configuration.
- Establish SCTP connections with redundant paths to each AMFs and monitor them for transport layer connectivity.
- Establish and update/reset N2 application layer connection to each AMF as per the interface management procedures defined in clause 8.7 of TS 38.413 and clause 5 of TS 29.413. The AGF learns and stores information about AMF capacity, supported network slices, overload situation etc.

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

5.12.2 Using N2 connections to serve RGs

The AGF makes use of the N2 connections and the AMF information learnt during interface management procedures for:

- Connecting the RG to an AMF and establishing UE context for the RG related signaling. This will involve AMF selection (as detailed below) and, optionally, rerouting the NAS request to another AMF.
- Moving the RG related context to another AMF (at any time) for load rebalancing purpose, if requested by AMF.
- Reselecting the AMF / reconnecting the RG to another AMF, if connectivity to the original AMF was lost. For this, the AGF uses AMF set information and/or backup AMF.
- Support NGAP UE-TNLA-binding (TNLA = SCTP association) as described in TS23.501 clause 5.21: while an RG is in CM-Connected state, the AGF maintains the same NGAP UE-TNLA-binding (i.e., use the same TNL association and same NGAP association for the UE) unless explicitly changed or released by the AMF.

Whenever a new AMF is to be selected for an RG, the AGF takes into consideration:

- Network slices served by the AMFs it has connection to – in comparison with the slices requested by the 5G-RG or with the slice allowed to the FN-RG according to subscription.
- The relative capacity, overload and operational status of the AMFs, to provide proper load balancing.

5.12.3 AMF selection

Generally speaking, the AMF, that directly or indirectly serves an RG, is selected by the AGF. This selection occurs differently for 5G-RG and FN-RG.
An RG is served by a unique AMF regardless of the number of slices this RG may need to use.
For 5G-RG the following applies:

- The selection of the AMF is performed by AGF as specified in TS 23.501 [24] clause 5.15.5.2 and clause 6.3.5 where 5G-RG replaces UE and AGF replaces 5G-AN, by making use of the Requested NSSAI and the GUAMI:
  - The Requested NSSAI represents the set of slices that the 5G-RG requests to be connected to.
  - The GUAMI is used to uniquely identify an AMF or a set of AMF within a 5GC network. The AGF, as a 5G AN, supports TS 23.501 clause 5.19 and clause 5.21.1
- The AMF selected by the AGF, upon receiving the Registration request, determines whether itself can serve the 5G-RG or whether the request needs to be redirected to another AMF. The source AMF may ask the AGF to redirect the 5G-RG to another AMF (case B of TS 23.502 clause 4.2.2.2.3).

For FN-RG the following applies:

- In this issue of the specification, the AGF selects the AMF on the basis of local information from a set of default AMFs, as specified in TS 23.501 clause 5.15.2.1.
- The selected AMF may redirect AGF towards a different Serving AMF on the basis of the procedure defined in TS 23.501 [24] clause 5.15 and TS 23.502 [25] Clause 4.2.2.2.3, taking into consideration the FN-RG subscription information.

5.13 Combined AGF/UPF

AGF is defined as a logical function. Implementing AGF and UPF as separate nodes means the duplication of equipment resources for the data planes. The duplication of data planes can result in implementation complexity and additional latency, which could prevent the support of demanding applications, such as augmented reality/ virtual reality.

5G WWC supports the option to deploy an AGF and an UPF as a combined implementation. In addition to avoiding the duplication of data planes, this configuration may improve accounting accuracy limited to those PDU sessions that are served by the co-located UPF. See section “Accounting accuracy” for a discussion of the related issues.

The combined AGF/UPF supports the following external interfaces: N1, N2, N3 (to external UPFs), N4, N6, N9 and V interfaces.

The internal N3 interface and whether any kind of tunneling is needed are left for implementation.

The combination of UPF with AGF can be applied on a per PDU session basis. While some sessions can benefit from the data plane optimization, other sessions may require a UPF with specific properties not supported by the combined AGF/UPF. Therefore, the combined AGF/UPF still offers an external N3 interface on AGF for sessions that do not use UPF co-location or require capabilities not available in the co-located/combined implementation.

The figure below shows an example of combined AGF/UPF, with multiple sessions for a given 5G-RG (note that combined AGF/UPF can also apply to FN-RG). In this example, the PDU session #1 is handled by the collocated UPF and then relayed over N9 to a second UPF (it may be because a specific service is delivered by this UPF). The collocated UPF also handles the PDU session #2 providing DNN connectivity over N6. The PDU session #3 is processed by an external UPF over N3 interface. The PDU session #4 is associated with

a 3GPP access: the combined AGF/UPF terminates N3 from gNodeB – which enables hybrid access, as defined in section 'Hybrid Access'.

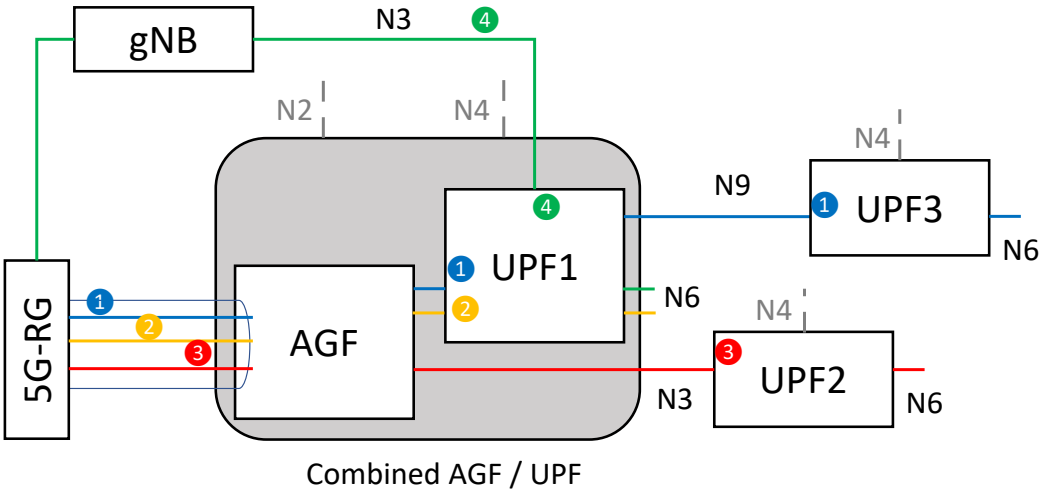

Figure 17: Example of combined AGF/UPF

UPF selection is provided by the SMF. Hence the SMF decides if a PDU session uses the co-located UPF. Clause 6.3.3.3 (UPF Selection) of TS 23.501 [24] specifies that the SMF may consider identifiers provided by the AGF, related to N3 termination, in order to select the UPF. The AGF provides this information to the AMF in N2 messages, as described for procedures in TS23.316 [20] clauses 7.3.1 and 7.3.4. WAgfInfo is the attribute used to provide this information, it is defined in clause 6.1.6.2.51 of TS 29.510 [31]. WAgfInfo contains a list of endpoint addresses, prefixes or Fully Qualified Domain Name (FQDN) of the N3 terminations. The AMF relays this attribute to the SMF during PDU session establishment request.
In the case of 5G-RG, the AGF does not have visibility if the messages relayed to AMF on N2 are related to PDU session establishment requests. Therefore, an AGF that supports a co-located UPF adds the WAgfInfo to all N2 messages sent to the AMF (in case of wireline access, as N2 message frequency is limited, because there are no periodic registrations and Service Requests are rare - this is not considered a significant overhead). The AMF relays the WAgfinfo attribute to the SMF only in the Create Session Management (SM) Context Request, as specified in clause 5.2.2.2 of TS 29.502 [30]. The SMF then selects the UPF instance based on its local configuration or with the assistance of NRF (Network Repository Function. UPF can be registered optionally in NRF with UpfInfo that contains WAgfInfo (it is set it to the same value as what is used to identify the N3 interface of its AGF part), as described in TS 29.510 clause 6.1.6.2.13. Using the Nnrf interface can be useful in virtualized environments where AGF+UPF instances can be managed dynamically.

If SMF selects the co-located UPF, the AGF receives the UPF information from the SMF (via AMF) that matches the co-located UPF and then uses the internal N3 interface.

In the hybrid access scenario, and assuming the wireline session is terminated on the co-located UPF (combined AGF/UPF), the SMF selects the same UPF instance for the radio access session. In that case, the UPF supports N3 interface to the NG-RAN. If the 3GPP access is E-UTRAN with EPC interworking, then the co-located UPF includes PGW-u support, aggregating access traffic over S5 interface (instead of N3). Hybrid access can also be supported via a non-local UPF, based on the external N3 interface on AGF.

In case of CUPS implementation of AGF, the UPF is co-located with AGF-UP. In particular, the AGF identifier parameter (WAgfInfo) is specific to the AGF-U instance used for this PDU session. The combined AGF-UP/UPF supports both AGF-CP/AGF-UP interface and N4.

Note: AGF CUPS is FFS.

UPF co-location still works with slicing. For example, the AGF and collocated UPF can support a convergence slice for which the collocated UPF can also support wireless access for 5G-RG. In the case of hybrid access, 5G-RG, AMF, SMF, NG RAN, AGF and UPF(s) shall be in the same slice (all shall support the S-NSSAI of the PDU session).

Functional requirements related to the combined AGF/UPF are specified in TR-456 [16], in section "Combined AGF/UPF".

5.14 Additional Authentication

PPPoE operators may require the ongoing support of PAP/CHAP credentials to facilitate the transformation of their networks to the 5G system. One objective being to decommission existing RADIUS infrastructure as part of the transformation process.

To achieve this WWC introduces the concept of "additional authentication". This is to specifically distinguish this from the 3GPP concepts of "primary" and "secondary" authentication. Primary being the authentication of the subscriber to the 5G System, and secondary being the authentication of the subscriber to the operator of a specific DNN.

Additional authentication allows the 5G system operator to perform additional PAP/CHAP authentication of FN-RG subscriber IP session initiation when the subscriber has already have had primary authentication performed via GLI based SUCI. This may be combined with NAI based session steering to allow per session credentials.

This capability is achieved by the porting of PAP/CHAP credential information from RADIUS into the RG-LWAC data structure as one or more Additional Authentication Credential Instance TLVs. This permits an AGF or FMIF to evaluate the results of CHAP challenges, and/or validate PAP passwords directly.

It should be noted that this does involve the communication of shared secrets unencrypted within the 5G system, but the validity of such credentials is scoped to that of the subscription authenticated by the primary authentication mechanisms (GLI based SUCI). Operators may weigh the merits of decommissioning existing RADIUS infrastructure accordingly.

5.15 MTU Handling

For the purposes of this discussion these terms are used:

- 5G-System-MTU refers to the path MTU of the network from 5G-RG to UPF.
- transport MTU refers to the MTU available net of GTP tunnel overhead on the N3 and N9 interfaces.
- wireline access MTU refers to the MTU of the Y4 and Y5 interfaces.

Wireline differs from mobile networks in that there is a much more constrained MTU in the access. Mobile networks have a much higher MTU limit for the RLC layer and a layer 2 fragmentation mechanism. This means the 5G-System-MTU for wireless access typically is only constrained by the transport MTU.

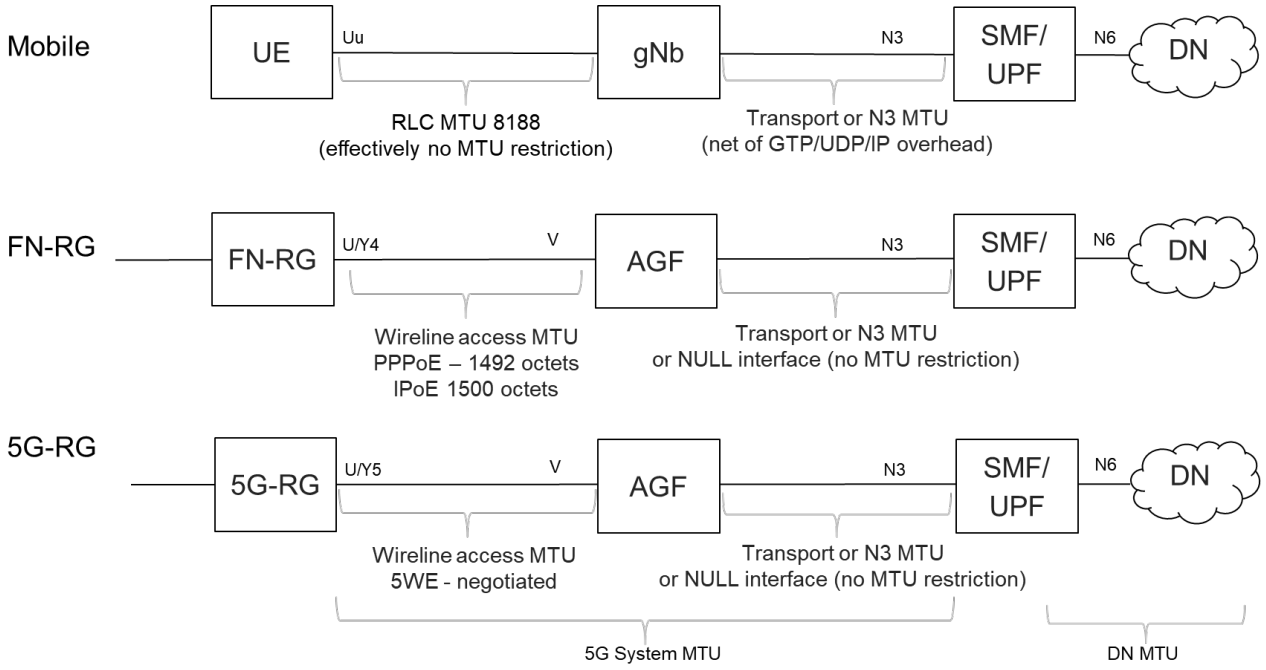

Figure 18: the MTU landscape

In addition, whereas mobile networks seek to have a homogenous ‘transport MTU’ within the 5G system to simplify procedures such as handoff from base station to base station, wireline sees heterogeneous wireline access MTU values dependent on the access protocol suites used (IpoE, PPPoE, 5WE) as mobility is not a consideration. The overall 5G-System MTU for wireline access is the minimum of the value of wireline access MTU and transport MTU, and this may produce a unique value per PDU session.

It is desirable but not Is achievable that the 5G-System-MTU is known at the DN ingress/egress points to the 5G system and to the non-3GPP hosts served by the Y4 and Y5 interfaces in order to minimize the number of places in the path that through the 5G System will be required to reject ‘too large’ packets.

There are a number of considerations that come to play:

- The 5G-System-MTU for a single access session served by a co-located AGF/UPF is not constrained by the transport MTU
- The 5G-System-MTU for a multi-access session is constrained by the transport MTU irrespective of the serving UPF
- 3GPP procedures do not exist to handle the case where the MTU of the wireline access is less than the transport MTU, this requires the AGF to be able to perform MTU processing for downstream traffic. Support of multi-access sessions may not be possible in this scenario and is FFS
- Operators typically have already operationalized the wireline access MTU that has resulted from their choice of the use of PPPoE or IPoE, and may be reluctant to embark on a network transformation that involves introducing new MTU constraints.
- The tools exist to disseminate the 5G-System-MTU in the home LAN and BBF specifications mandate their use
- Due to the lack of fragmentation/reassembly mechanisms at Ethernet layer, support for Ethernet PDU sessions by other than a co-located UPF will require an actual transport MTU larger than the PCO advertised Ethernet Maximum Frame Payload value.
  As an example, for a standard Ethernet Frame payload of 1500 bytes, the actual supported MTU needs to have the following additional allowances:

- 14 bytes for the MAC header
- 4 bytes for each tag control information instance. (so 8 bytes total to encapsulate a C and S tag).

Which for a MAC header and two tags results in an actual transport MTU of 1522 octets. It is incumbent on the operator to ensure the actual MTU that can be supported is in excess of the advertised value to include Ethernet header allowances.

Normal procedure is that the SMF disseminates the N3 transport MTU as part of PDU session establishment procedures. Considering that, a mismatch between the transport MTU and the wireline access MTU may cause issues, the following remedies can be put in place, assuming some capabilities on SMF:

- Case with wireline access MTU greater than transport N3 MTU and co-located AGF/UPF. When the SMF is performing single access PDU session establishment for a co-located AGF/UPF or FMIF/UPF. It may disseminate a value different than the transport N3 MTU, which is administratively configured to be greater than or equal to the MTU of the wireline access network. On the other hand, the co-located AGF/UPF or FMIF/UPF, the 5G-RG and the FN-RG are all able to adjust the MTU value to the actual value used in wireline access allowing for the actual access protocol suites used. This applies to both FN-RG and 5G-RG support and mitigates MTU issues for the case where the wireline access MTU is greater than the transport MTU.

  Note that a single access session that is using an MTU value larger or less than the transport MTU cannot be subsequently upgraded to a multi access session as this would require the ability to modify the session MTU, and this capability does not exist in 3GPP procedures.

- Case with transport N3 MTU greater than wireline access MTU. In the scenario where the MTU of the N3 transport network is larger than the value that can be supported for 5G-RG wireline access, MTU issues can be mitigated if the SMF and UPF are configured to both disseminate and use the MIN of the transport MTU and wireline access MTU for all PDU sessions that have a wireline access component, both single and multi-access. This would apply to both the co-located AGF/UPF case and when an N3 interface between them is exposed.

  Note that in an AGF/UPF/SMF deployment that supports both FN-RGs and 5G-RGs that do not have a common wireline access MTU, have a transport MTU greater than at least one of the wireline access MTU values, and have an exposed N3 interface, MTU issues can be mitigated but not completely eliminated.

Recommended practice is that the transport MTU is configured equal to the wireline access MTU to minimize the risk of misconfigurations.

Recommended practice is that a 5G-RG use RFC 4638 procedures to attempt negotiate the largest wireline access MTU possible such that it will be greater than the transport MTU and therefore minimize both constraints on PDU session establishment, and the number of points in the 5G system where there will be an MTU change not visible to the ingress points to the 5G system. Operators may choose as a matter of policy to then align the wireline access MTU with existing practice, or once the network is fully transformed, to raise the negotiated MTU value where the equipment supports it.

Note: The SMF capability described above with respect to MTU use and dissemination for a co-located AGF and UPF has been requested of 3GPP but has yet to be confirmed.

5.16 Framed routing

Framed routing is a typical premium service for SOHO customers that allows to support an IP network behind a CPE, such that a range of IP addresses or IPv6 prefixes is reachable over a single PDU session. The CPE itself is assigned a separate address, which is used on the WAN side. The mechanism by which

home network devices behind the CPE get an IP address extracted from the routed network is out of the scope of 3GPP specification, but legacy CPEs such as FN-RGs that already support it are expected to be compatible with a convergent core network.

The support of Framed routing by the 5GC is specified in TS 23.501 clause 5.6.14 [24].

In the WWC context, the CPE (FN-RG or 5G-RG) that has subscribed a Framed Routing service requests a PDU session with the usual procedures described in TR-456 [16]. The CPE is assigned a global IP address for the WAN, which may or may not belong to the framed route.

The SMF will provide the Framed Routing information to the UPF (acting as PDU Session Anchor) as an attribute of a Packet Detection Rule for DL traffic. The UPF will advertise the relevant IP routes to receive packets destined to the devices behind the CPE and will forward these packets over the PDU session to the CPE. Local routing on the CPE allows then packets to reach their destination within the home network. Framed routing is defined for PDU sessions of any IP type (IPv4, IPv6, IPv4v6).

Framed routing can be offered via a wireline or an FWA access. It can be also offered via a hybrid access, possibly based on MA-PDU session.

5.17 Ethernet PDU Session Support

Ethernet services are supported by the 5G system in the form of Ethernet PDU sessions. However, in the context of WWC there are a number of implications and restrictions to consider as Ethernet is both a service and a transport in the access:

An Ethernet Frame Payload MTU value is communicated to a 5G-RG during Ethernet PDU session initiation procedures. However, in the WWC case this MTU cannot be disseminated to non-3GPP devices attached to a 5G-RG so they will default to using the 802.1D 1500 octet as the frame payload size. Ethernet does not include fragmentation support, therefore for Ethernet services to work in a WWC 5G System context the Ethernet Frame Payload MTU supported by the 5G system needs to be a minimum of 1500 bytes.

Ethernet frames including MAC header and 802.1Q tag information in addition to the 1500 byte payload must be accommodated by any GTP tunneling that carries Ethernet traffic. This requires an N3 MTU for Ethernet PDU sessions of at least 1522 octets to include the MAC header and VLAN tag information, and a corresponding PPP MTU in the access for 5G-RGs using 5WE encapsulation.

Note that support of Ethernet PDU sessions by a co-located AGF/UPF that acts as the session anchor will reduce the MTU constraints to that of the wireline access MTU as there is no N3 interface MTU to adapt to.

The RG MAC address currently functions as the permanent equipment identifier (PEI) for FN-RGs. Supporting bridged FN-RGs will be problematic as there will not be a stable MAC address value present in all PDUs received from the FN-RG. Any policing of PEI or detecting RG change will not be able to produce a consistent result. As such, support for Ethernet PDU sessions for FN-RGs is FFS. For a 5G-RG, supporting multiple MAC addresses from the premises does not present problems, as all premises originated ethernet frames are encapsulated in the 5WE header which is transported using the 5G-RG MAC as the originating MAC address, so the 5G-RG MAC address is always the address presented to the AGF. A 5G-RG also uses an IMEI as the PEI.

6 Use Cases and Examples

The WWC Architecture in conjunction with the 5G Core offers a wide variety of access methods.

The principal concepts driving this flexibility are:

- Single (wireline only or wireless only) or multiple (wireline and wireless) access technologies.
- Single or multiple PDU sessions per subscriber.
- Steering of traffic between access technologies.
- Backwards compatibility with legacy gateways (FN-RG).
- Possibility to modify session parameters by either 5G-RG or 5G Core at any time.

6.1 Use Cases

The use cases described below largely concentrate on multiple PDU sessions since a single PDU session represents the trivial case.

In addition, WWC will support 5G UEs behind the RG (for example, a 5G smartphone connected via Wi-Fi to the RG). The specifics vary depending on whether it is a 5G-RG or an FN-RG and are FFS.

6.1.1 FN-RG connected to a 5G core

What:
Backward compatibility support for existing customer equipment. The sum of AGF and 5G core will provide equivalent BNG functionality such that any existing residential gateway may connect to a 5G core without RG modification.
Why:
An operator may offer convergent services with a 5G core to customers provided with 5G-RGs, and, simultaneously, use the same core to continue to serve legacy customers equipped with FN-RGs. This allows the flexibility of supporting customers supplied with either 5G-RG or FN-RG equipment and removing the dependency of requiring 5G-RGs in order to rollout a 5G Core network.

How (basic mechanism):
1) The FN-RG establishes either a PPPoE or IPoE based IP session using the procedures detailed in TR-101 [5]. The IP session is mapped to a 5G-System DNN S-NSSAI based upon the defaults associated with the subscription. In the case of PPPoE, the DNN/S-NSSAI may be derived via URSP using NAI information included with validated additional authentication credentials.

2) The AGF operating in adaptive mode signals with the 5G core on behalf of the FN-RG. In particular, the N1 interface is initiated on the AGF.

3) IP addresses are provided to the RG as per existing procedures (a combination of IPCP, SLAAC and/or DHCPv4/v6 depending on the access protocol suite).

4) All 5G features are supported only between the AGF and 5G core. Between the FN-RG and the AGF, only features described in TR-101 are supported. As a consequence, not all 5G core benefits are available in this use case (in particular, no ATSSS support, reflective QoS or other capabilities)).

5) The session control including authorization and accounting functions are executed by the 5GC.

6) Primary AAA functions are executed by the 5GC and not by the legacy fixed network AAA platform on the basis of the GLI encoded SUCI constructed from the line ID identifying the subscriber access facility. Additional per IP session authentication may be performed for PPPoE based IP sessions using PAP/CHAP credential information delegated to the AGF or FMIF in RG-LWAC.

7) Although not all the 5G features are exploitable by an FN-RG, it might be possible to achieve convergence of the service platforms (e.g., IMS, gaming application servers, and so on).

An additional scenario is Multiple VLAN Delineated IP Sessions:

There are deployed models for FN-RGs that use multiple VLANs on the Y5/U interface. This deployment typically supported access to a different service via each VLAN. For example, voice on one, internet access on the next and video on another.

This model can be supported by the 5G system using the basic mechanism Each VLAN access circuit is configured with a unique line ID in the existing access network, so the individual line IDs (and associated IP sessions) can be modelled in the 5GC as a unique subscription. In the scenario whereby multiple VLAN circuits are identified by a common line ID, an AGF may augment the line ID information with a modifier such that a unique subscription per VLAN may be achieved. As such each IP session originating with the FN-RG can be associated with a unique DNN and S-NSSAI.

It should be noted that depending on how this model is deployed, migration of the deployed CPE to a 5G-RG may present additional challenges. The configuration of the access connectivity is different between the two scenarios and additional procedures and access provisioning may be required to enable the migration. In addition, it may not be possible for an AGF to correlate the VLAN based FN-RG subscriptions with the 5G-RG connectivity for the purposes of state reclamation.

6.1.2 5G-RG using a single access network and a single PDU session

What:
Simplest implementation of a residential gateway using 5G NAS and session transport. The access network may be wireline or wireless (FWA).
Why:
Via 5G NAS, the 5G-RG has access to 5G policy, QoS, and the ability to modify sessions without loss of service. Furthermore, operators gain a uniformly standardized ability to detect connection loss, modify RG behaviour during PDU session, and set access policy.
How:
1) The 5G-RG registers to the 5G core using the procedures detailed in TR-456,
2) The 5G-RG use the URSP policy information stored locally or the updated information received via NAS,
3) The 5G-RG creates a PDU session using the procedures detailed in TR-456,
4) The 5G-RG receives the IP address/prefix via 5G NAS signaling or requests IP address allocation using DHCP or DHCPv6 via the newly established PDU Session.

6.1.3 5G-RG using multiple access networks and multiple PDU sessions

What:
A more complex example of a residential gateway using 5G NAS and session transport, with a choice of wireless and wireline access networks and establishing multiple PDU sessions.
Why:
Using policy (URSP), an operator may specify which access network it prefers a 5G-RG to use. Multiple PDU sessions allow an operator to access different data networks or different services as well as segregate traffic for security or QoS purposes. Different PDUs can be associated with different DNNs and slices.
How:
1) The 5G-RG registers to the 5G core separately using the procedures detailed in TR-456 for fixed access and using the procedures detailed in TS23.316 clause 4.11 for cellular access (FWA).
2) The 5G-RG receives policy information via URSP. This information includes the mapping between flows and PDU sessions.
3) The 5G-RG establishes each PDU session using the procedures detailed in TR-456 by choosing the preferred access network from the URSP rules.
4) The 5G-RG receives the IP address/prefix via 5G NAS signalling or requests IP address allocation using DHCP or DHCPv6 via the newly established PDU Session.
5) All the 5G features are supported between the 5G-RG and 5G core. Additional PDU sessions are established by repeating steps 3 and 4.

6.1.4 5G-RG using multiple access networks and multiple PDU sessions with failover

What:
A more complex example of a residential gateway using 5G NAS and session transport, with a choice of access networks and establishing multiple PDU sessions. Upon failure of one access network, the PDU session may be transferred to a new access network.
Why:
Using policy (URSP), an operator may specify which access network it prefers a 5G-RG to use. Multiple PDU sessions allow an operator to segregate traffic for security or QoS purposes. Resilience is added by the ability to transfer a PDU session to another network during PDU session.
How:
1) The 5G-RG receives the IP address/prefix via 5G NAS signaling or requests IP address allocation using DHCP or DHCPv6 via the newly established PDU Session.
2) The 5G-RG use the URSP policy information stored locally or the updated information received via NAS.
3) The 5G-RG creates a PDU session using the procedures detailed in TR-456 by choosing the preferred access network from the URSP rules.
4) The 5G-RG receives the IP address/prefix via 5G NAS signaling or requests IP address allocation using DHCP or DHCPv6 via the newly established PDU Session.
5) Additional PDU sessions are established by repeating steps 3 and 4.
6) The 5G-RG detects a loss of connectivity on the current access network.
7) The 5G-RG modifies the PDU session to use the other registered access network, see clause 4.9 from TS 23.502.

6.1.5 5G-RG using multiple access networks and multi-Access PDU sessions using ATSSS

What:
A complex example showcasing all the features a 5G-RG is capable of. In addition to multiple access networks and multi access PDU sessions, ATSSS allows traffic to be seamlessly steered, switched, and split across multiple access networks.
Why:
Failover provides operators network resilience. ATSSS takes that concept further and allows the traffic to be split over multiple networks controlled by operator policy.
How:
1) The 5G-RG registers to the 5G core separately using the procedures detailed in TR-456 8.2.1 for fixed access and using the procedures detailed in TS23.316 4.11 for cellular access (FWA).
2) The 5G-RG use the URSP policy information stored locally or the updated information received via NAS.
3) The 5G-RG creates a MA PDU Session using the procedures detailed in TS23.502 choosing the multiple access network from the URSP rules.
4) The 5G-RG receives the IP address/prefix via 5G NAS signaling or requests IP address allocation using DHCP or DHCPv6 via the newly established PDU Session.
5) Additional PDU sessions are established by repeating steps 3 and 4.
6) ATSSS rules are applied to the MA PDU sessions and access networks to permit steering, switching and splitting.
7) The 5G-RG detects a loss of connectivity on the current access network.
8) ATSSS function seamlessly switches the traffic to an alternate access network.

6.1.6 5G capable UE behind FN-RG or 5G-RG

This section is giving an overview, more details and impact are FFS.

A 3GPP UE behind a 5G-RG accesses the 5G Core network over a Non-3GPP access network. The 3GPP UE is assumed to be 5G capable. The 5G-RG UE has registered and authenticated to the 5GC through the

W-5GAN which generates N2 and N3 connections. If a 5G-RG can support EAP-based authentication and support the Trusted Non-3GPP Access Point (TNAP) defined in clause 4.2.8.2 of TS 23.501, the W-5GAN can be considered as a Trusted Non-3GPP Access Network (TNAN) for 5G capable UE. Through discovering and connecting a Trusted Non-3GPP Gateway Function (TNGF) which uses NAS and PDU procedures to converge to the 5G Core network. The interface between TNAP and TNGF is defined in TS 23.316 as Ta interface

When the 5G capable UE initiates connection with TNGF, the 5G-RG can be triggered to find the right PSA/UPF to set up a PDU session to bear the control and user plane transport from a 5GC-capable UE. About the right PSA/UPF selection, considering the connection between PSA/UPF and TNGF is N6 interface, the TNGF can be considered as a “Data Network (DN)” for the 5G-RG. The "DN" (i.e., TNGF) can be stored in SMF as specified information used for PSA/UPF selection and re-selection. Local operator policies can also be considered to be the parameters for PSA/UPF selection. After the registration of a 5G capable UE to the 5G Core network, the NAS signaling and PDU messages of 5G capable UE are transported over a 5G-RG PDU session to the PSA/UPF. The architecture figure is shown below in Figure 19.

A “5GC capable UE device behind an RG (either 5G-RG or FN-RG)” can access 5GC services by connecting via Wi-Fi to an RG and exploiting an IP PDU connection that this RG has set with the 5GC. Through this PDU session, the UE accesses the 5GC via a N3IWF or via a TNGF (for 5G-RG only).
A single RG PDU session can be used to serve multiple UEs behind the RG. Please refer to clause 4.10 of TS 23.316 [20] for further details.

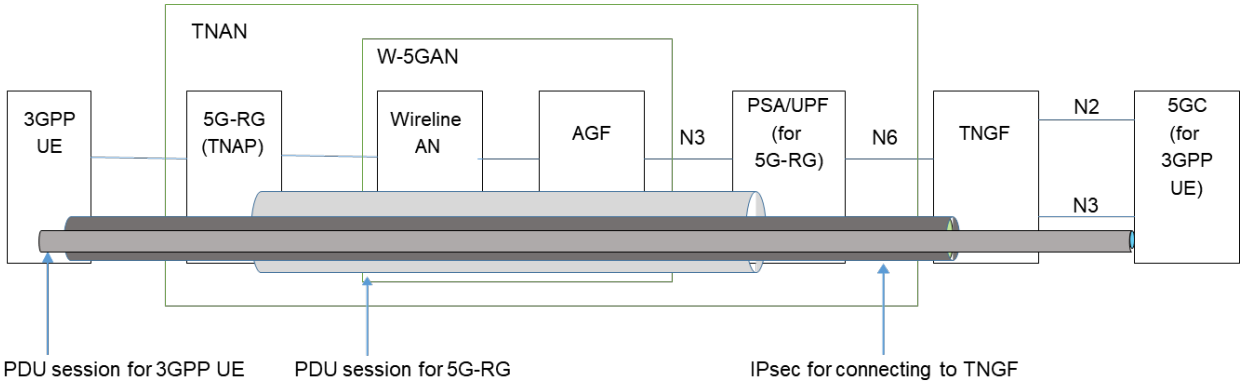

Figure 19: 5G UE behind a 5G-RG

6.1.7 Framed routing

The description of framed routing is to be found in section 5.16.

In case the AGF-UP is combined with the UPF, the combined AGF-UP/UPF indicates to SMF the support of framed routing by setting the FRRT flag in the UP Function Features Information Element.

Configuration of Framed Routing in the RG (FN-RG or 5G-RG) can be done via the ACS (TR-069 [3] or USP [4]). Dynamic provisioning of Framed Routing via NAS is not yet supported by 3GPP at this point of time and is FFS.

6.1.8 Coexistence of AN delivered IPTV and 5G services

When migrating to 5G, operators may conclude that the cost of transforming specific technically demanding services may result in unacceptable costs. As such they will conclude that they wish to continue with the

deployed service. Some service architectures are amenable to such an approach. An example is AN delivered multicast for IPTV.

Deployed access nodes have the ability to separate traffic on the basis of for example, Ethertype or VLAN tag, and direct the traffic on the V interface to different service platforms. Protocol multiplexing has been leveraged for some IPTV deployments for FN-RGs where internet traffic is carried via a PPPoE session and IPTV Multicast traffic (typically controlled by IGMP and augmented with fast channel change mechanisms) is carried via IPoE.

This “protocol multiplexing” as a mechanism to separate services is equally applicable to 5G WWC deployments. Support for NAS and 5WE to an unmodified access node leverages the same model to permit a 5G-RG to continue to consume IPTV services coexisting with 5G System delivered services.

6.2 Multiple PDU sessions use cases

Looking at a PDU session in abstract, it can be seen as a logical circuit between a 5G-RG and UPF with dedicated resources and QoS rules. This provides support for applications requiring:

- Separate IP or Ethernet sessions.
- Preferential data paths within the operator’s network through the use of dedicated UPF instances. For example, specific for VoIP or streaming media
- Traffic separation for security.
- Guaranteed bit rates for a given application.

6.2.1 VoIP

Operators providing a ‘carrier grade’ VoIP solution require a reliable solution capable of supporting emergency calls. A dedicated PDU for VoIP would provide the following benefits:

- Restricts access to operators’ customers only.
- Guaranteed bit rates are supported at a per service level allowing multi line services.
- A Network path can go directly from UPF to the voice platform simplifying the network architecture.
- An Operator can specify application specific QoS rules

Note that full integration with 5GS IMS voice systems is FFS.

6.2.2 Secure Device Management (TR-069/TR-369)

Security is of paramount concern for any device management system. An operator must have total confidence that they are the only entity capable of managing a device. Consequently, a dedicated PDU for device management offers Private network for device management at both CPE and platform ends.

6.2.3 Gaming (and other low latency applications)

The gaming community demands a network that supports both low latency and traffic prioritization. A dedicated PDU provides:

- Guaranteed bit rates for gaming traffic.
- Minimized latency via a dedicated UPF supporting local gaming servers and network breakout.

6.2.4 IoT

IoT is one of the fastest growing areas and is notorious for poor security. Placing IoT devices on a dedicated LAN network supporting by its own PDU session provides:

- IoT traffic separated from regular internet traffic.
- A UPF supporting IoT allows breakout to the internet with dedicated firewall rules.

6.2.5 Enhanced Work from Home

Multiple PDU session capability can provide a clear separation of interests that can be leveraged in a number of cases. A particular case of note would be providing an enhanced work from home environment for valued knowledge workers, as pictured in Figure 20.

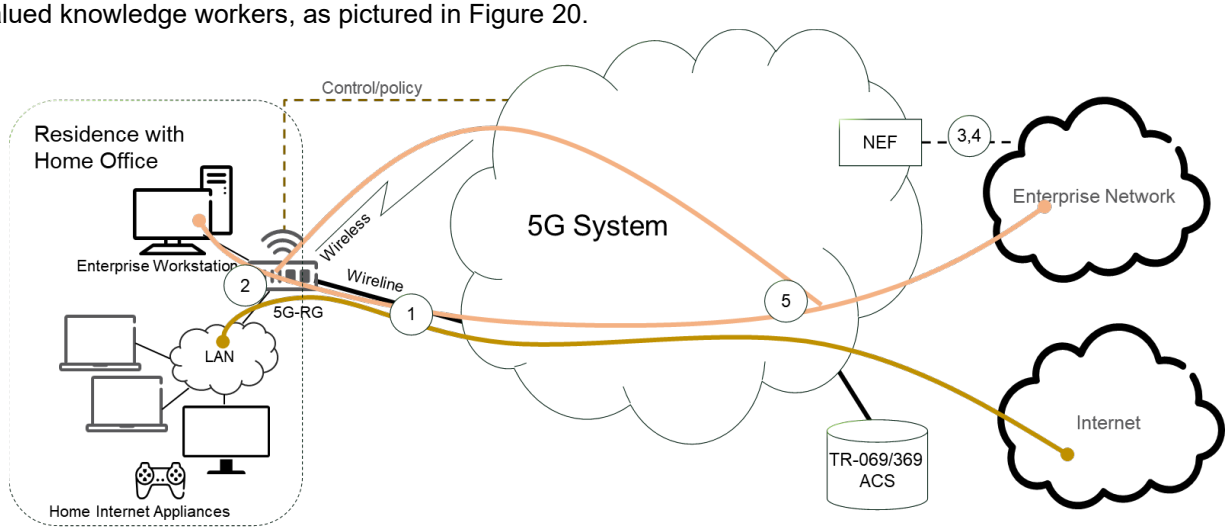

Figure 20: use case of enhanced work from home

The solution components are as follows:

1) A PDU session for normal residential internet access is multiplexed with a session directed to the enterprise VPN.
2) Traffic separation mechanisms in the home configured via TR-69/369 procedures (such as SSID, RG port or VLAN) are used to isolate traffic from an enterprise workstation from that of other internet appliances and map it to the 5G access. Enterprise traffic is isolated from the rest of the home LAN, and is only directed to the enterprise VPN, where additional security policies may be applied.
3) The enterprise facing Network Exposure Function (NEF) may be used to inject policy for enterprise VPN use, and direct charging for enterprise traffic, and any QoS enhancement consumed by the employee to the enterprise.
4) The enterprise facing NEF may also be used to extract information related to security from the 5G system such as the provenance of the CPE and location of access. This combination of trusted access and context information can be used to augment enterprise security practices such as ZTNA & SASE
5) Additional bandwidth and resiliency may be provided by the deployment of ATSSS capable CPE that uses both wireless and wireline access.

The initiation of the service is that the enterprise and the employee agree to add enterprise access to the employee 5G-RG subscription and coordinate this with the 5G provider. The 5G provider sets up the subscription changes and configures the 5G-RG to perform the necessary traffic separation. The changes are communicated to the 5G-RG which initiates connectivity to the enterprise. The enterprise is then able to use the NEF to direct charging, introduce QoS policies etc.

The employee gets a superior work environment without incurring additional personal costs. The enterprise only pays for the enhanced service components. The 5G communication service provider leverages several aspects of the 5G system in order to offer and meet the requirements of a more stringent SLA.

7 BBF specified Information Elements

7.1 Line ID

The format of the Line ID is generic, allowing different operators and access networks to use different encoding of the content. The Line ID has common information (Circuit ID and/or Remote ID), but it can be encoded in different formats:

- DHCPv4 option 82 (TR-101 issue 2 Annex B, original specification 2006 [5]);
- PPPoE Circuit and Remote ID AVP (TR-101 issue 2 Annex A/8.3, original specification 2006 [5]);
- DHCPv6 option 18 and/or option 37 (BBF TR-177 Issue 1 Corrigendum 1, original specification 2010 [11]);
- Line ID Option (LIO) in RS messaging (BBF TR-177 Issue 1 Corrigendum 1, original specification 2010 [11]).

7.2 Global Line Identifier (GLI)

An operator wide unique identifier of the line connecting the RG (For both 5G-RG and FN-RG) to the network is mandatory to achieve the usage with 5GC. Therefore, AGF needs to construct a unique identifier in the form of a GLI based on the Line ID.

The BBF specified GLI serves two roles in the 5G System:

1) It is used for construction of a SUCI and/or SUPI as a specialized subscription identifier for FN-RG support. Actual procedures are documented in TS 23.316.
2) It is used as the User Location Information (ULI).

The BBF specified GLI is required to be unique to the network operator that owns the AGF or FMIF and this operator is also assumed to be the 5GC operator and is subsequently referred to as simply the operator. As an operator may obtain access via wholesale arrangements with 3GPP access operators, the circuit-ID/remote-ID information may not be unique and duplicate values could occur within the operator's network. It is combining Line-ID with an operator administered "Line ID source identifier" to permit duplicates to be disambiguated.

As specified in Figure 21, the concatenation of Line ID source and Line ID is functionally equivalent with the GLI.

- Line ID source: this is AGF Operator/FMIF Operator administrated Source ID;
- Line ID: this is specified as above format;

Therefore, the GLI is unique within an operator's 5G system.

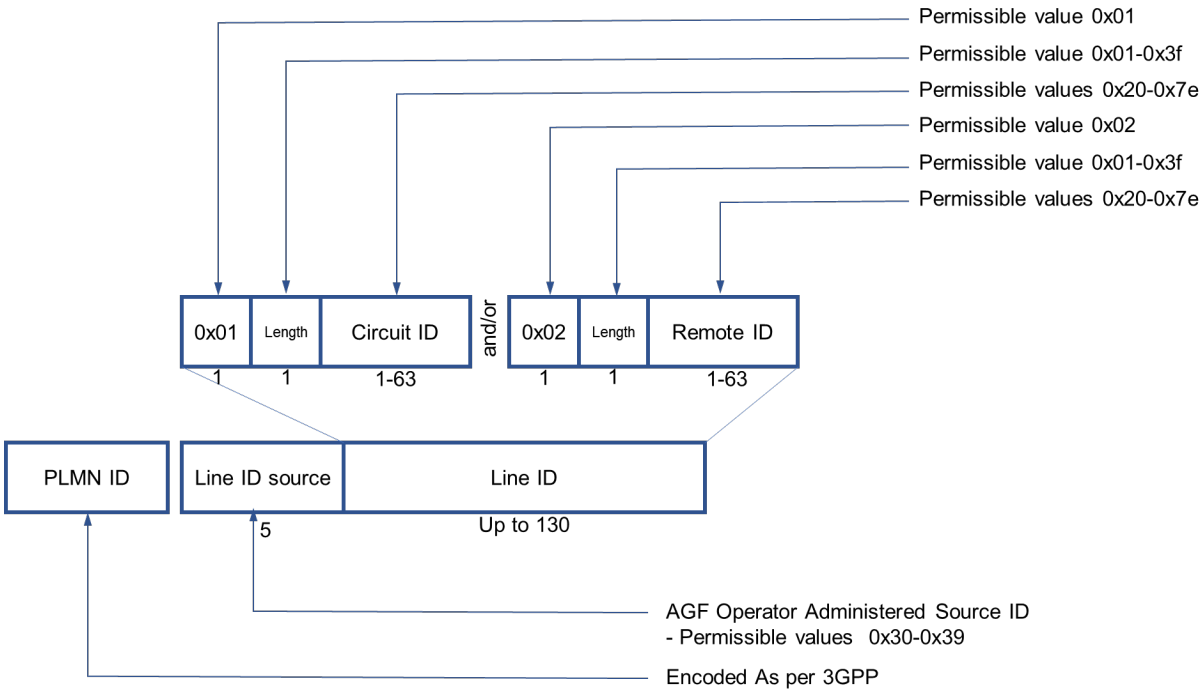

Figure 21: Global Line Identifier

Within this encoding the GLI may include the circuit ID, remote ID or both depending on existing operator practice. The possible arrangements of the GLI are as the following format shown in Figure 22.

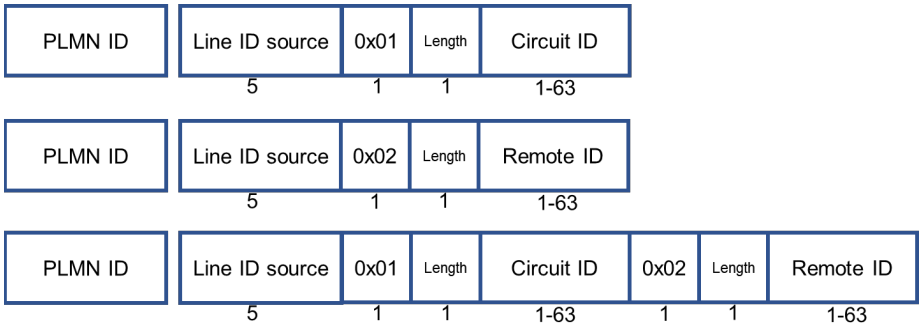

Figure 22: Possible formats of the Global Line Identifier

7.3 User Location Information (ULI)

The 3GPP specifies the User Location Information (ULI) to be used as the location information for both 5G-RG and FN-RG. As defined in clause 28 of TS 23.003, GLI is equivalent to the ULI. TS 23.003 [21] specifies the actual format of the ULI and clause 28.16 defines the GLI.

7.4 SUPI/SUCI for 5G-RG

The SUPI for an 5G-RG contains an IMSI, as described in clause 5.9.2 of TS 23.501 [24].

The SUCI provided by the 5G-RG to the network contains the concealed SUPI, as described in TS 33.501 [32] in clause 6.12.2 and TS 23.003 [21] in clause 2.2.B.

7.5 SUPI/SUCI for FN-RG

In case the text of this section conflicts with 3GPP references, 3GPP references apply.

The 3GPP specifies the SUCI and the SUPI encoding for FN-RG. The SUPI for FN-RG specified in TS 23.316, based on operator configuration, can either contain an IMSI or a GLI as defined in clause 7.2. The mapping between SUCI based on GLI and SUPI based on IMSI is defined in Table 8.6.1.1 in TS 23.316. When the SUPI is based on the GLI, it takes the NAI format username@realm as per 3GPP specification TS 23.316 in clause 4.7.3 and TS 23.003 in clause 2.2A and 28.16.2 where:

a. the username part is the GLI defined in section 7.2 encoded in Base64 as defined in RFC4648 section 4,
b. the realm part identifies the operator owning the subscription. If the operator owns a PLMN ID, the realm part is in the form: "5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org".

The SUCI provided by the AGF to the 5G Core Network is always built based on the GLI and it acts as a pseudonym of the SUPI. Therefore, the 5GC performs the mapping per operator configuration from the SUCI based on GLI to a SUPI.

The SUCI provided by the AGF to the 5G Core Network is defined in TS 23.316 [20] clause 4.7.3 and TS 23.003 [21] clause 2.2B: the SUCI is derived using the null encryption scheme defined in annex C of TS 33.501 [32].

The following provides information on the components of the SUCI for FN-RG:

- SUPI Type is set to 2, corresponding to GLI type
- Home Network Identifier corresponds to the realm part of SUPI in NAI format
- Routing Indicator consists of one decimal digit set to 0
- Protection Scheme Identifier is equal to 0x0, corresponding to NULL Scheme protection defined in TS 33.501 Annex C [32]
- Home Network Public Key Identifier is equal to 0, corresponding to NULL Scheme protection defined in TS 33.501 Annex C [32]

Scheme Output is formatted as a variable length of characters. It contains username part of the GLI defined in section 7.2 encoded in Base64 as defined in RFC4648 section 4.

7.6 RG-LWAC Encoding

The encoding of the RG-LWAC data structure is based upon type-length-value encoding with a 16-bit type field, a 16-bit length field, and a variable length value field. The length field contains the length of the value field in octets.

The generalized structure of the RG-LWAC is defined as shown in Figure 23.

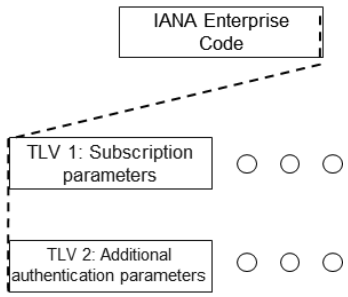

Figure 23: Generalized structure of RG-LWAC

The first field in the RG-LWAC identifies the owning authority of the subsequent data structure. The BBF encoding of the RG-LWAC is identified by the use of the IANA Enterprise code assigned to the BBF. This field is 32-bits in size and is set to 3561 decimal. Note that this also permits differentiation from CableLabs (whose IANA code is 4491) and provides the possibility of proprietary RG-LWAC encodings.

Subscription Parameters (SP) sub-TLV family

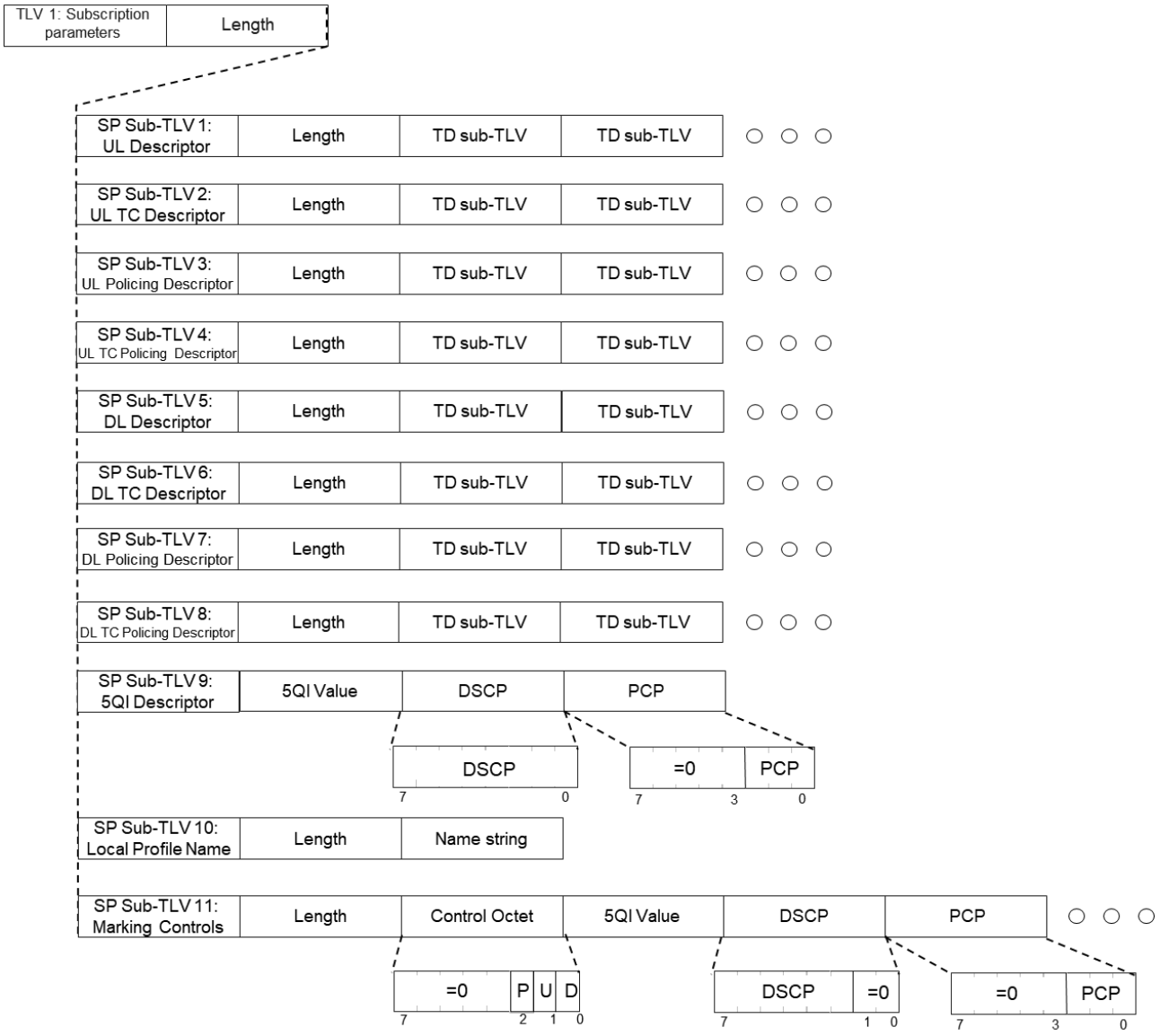

Figure 24: Subscription parameters TLV family

The subscription parameters TLV is composed of nine potential classes of sub-TLVs. This is the SP sub-TLV family of TLVs. The defined sub-TLVs are:

SP sub-TLV 1 (UL descriptor): This provides the aggregate upstream traffic parameters for the wireline subscription. This is communicated to a 5G-RG at registration time.

SP sub-TLV 2 (UL TC descriptor): This provides the upstream traffic parameters for an individual class and the mapping information for the class. This is communicated to a 5G-RG at registration time.

SP sub-TLV 3 (UL policing descriptor): This provides the aggregate upstream traffic parameters for policing the wireline subscription. If this TLV is not present, then any UL policing parameters are obtained from local configuration.

SP sub-TLV 4 (UL TC policing descriptor): This provides the upstream traffic parameters for policing identified traffic class. If this TLV is not present, then any UL traffic class policing parameters are obtained from local configuration.

SP sub-TLV 5 (DL descriptor): This provides the aggregate downstream traffic parameters for the wireline subscription. If this TLV is not present, then any aggregate DL parameters are obtained from local configuration.

SP sub-TLV 6 (DL TC descriptor): This provides the downstream traffic parameters and mapping/queuing information for the class. If this TLV is not present, then any per traffic class mapping/queuing DL parameters are obtained from local configuration.

SP sub-TLV 7 (DL policing descriptor): This provides the aggregate downstream traffic parameters for policing the wireline subscription. If not present, then any DL policing parameters are obtained from local configuration. It may be used in lieu of the DL descriptor sub-TLV.

SP sub-TLV 8 (DL TC policing descriptor): This provides the downstream traffic parameters for policing the identified traffic class. If not present, then any DL traffic class policing parameters are obtained from local configuration. It may be used in lieu of or to augment the parameters in the DL TC descriptor sub-TLV.

SP sub-TLV 9 (5QI descriptor): This provides the mapping to be used for 5QI to DSCP and PCP. 5QI, DSCP and PCP are all encoded in unsigned 8-bit fields. This TLV is documented for backwards compatibility reasons and is superseded by SP sub-TLV 11 (marking controls) as of issue 2 of this specification. An RG-LWAC data structure MUST NOT contain both SP sub-TLV 9 and SP sub-TLV 11.

SP sub-TLV 10 (Local profile name): This provides the name of a locally configured profile on the AGF. A profile name is encoded in printable ASCII (range 0x020 to 0x7e) and may be from 1 to 256 octets in length. The local profile name is used to reference a locally configured profile that configures some or all UL and DL subscription parameters.

SP Sub-TLV 11 (marking descriptor): This provides the indication of upstream and downstream applicability of DSCP and PCP information for both AGF and 5G-RG and a list of 5QI to DSCP/PCP tuples for the set of 5QI values that are valid for the subscription.

The control octet is an unsigned 8 bit integer which encodes 3 control flags:

- P bit – of significance only to the 5G-RG and indicates if the use of priority tagging of upstream traffic is permitted. (An AGF always performs downstream PCP marking).
- U-bit – of significance to a 5G-RG, an FMIF or an AGF in adaptive mode and indicates if remarking of the service IP DSCP for upstream traffic is required.
- D-bit – of significance only to an AGF or FMIF and indicates if remarking of IP DSCP for downstream traffic is required.

The control octet is followed by a series of zero or more 5QI to DSCP/PCP mapping tuples. Each tuple comprises 3 octets:

- 5QI – which encodes the 5QI value
- DSCP – the upper 6 bits of which encodes the DSCP value to be used in conjunction with the U and D marking control bits
- PCP – the lower 3 bits of which encodes the PCP value to be used in conjunction with the P marking control bit and for downstream PCP marking

The UL, UL TC, UL policing, UL TC policing, DL, DL TC, DL policing and DL TC policing descriptor SP sub-TLVs contain further sub-TLVs from the Traffic Descriptor (TD) sub-TLV family.

Traffic Descriptor (TD) sub-TLV family

The TD sub-TLV family has the defined elements as shown in Figure 25.

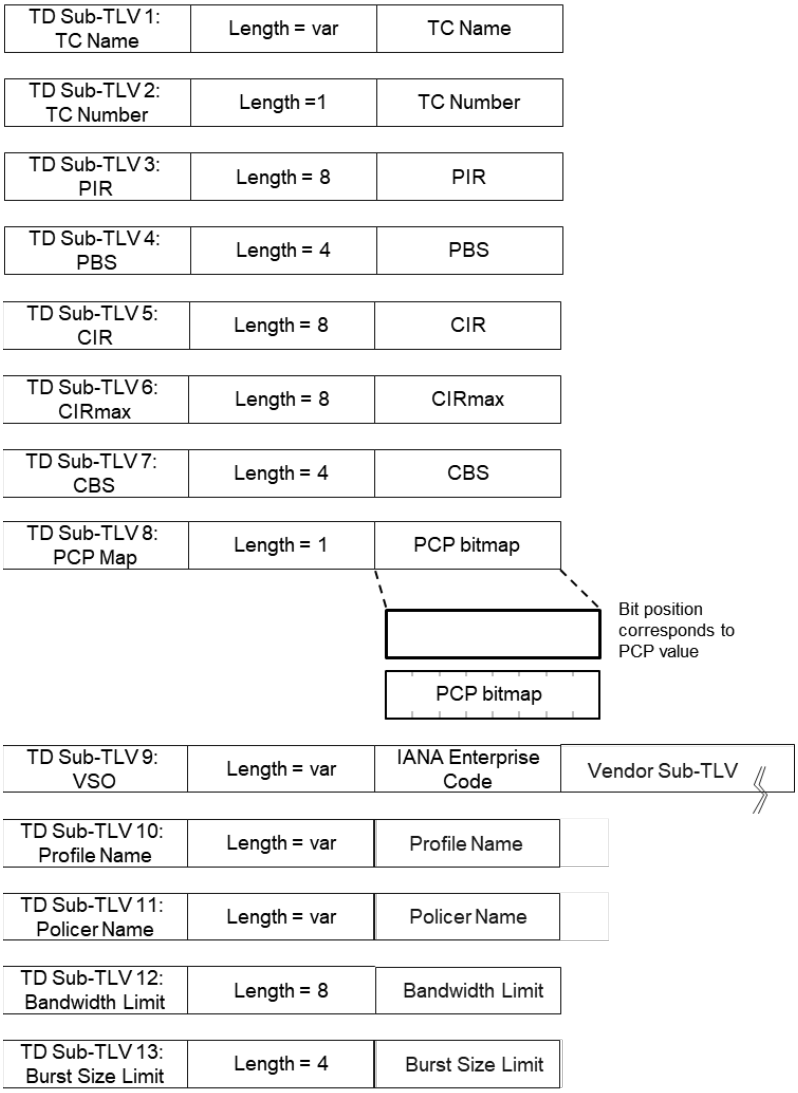

Figure 25: sub-TLV family for RG-LWAC Subscription Parameters

The sub-TLV type and length fields are encoded as unsigned 16-bit values. The length field contains the length of the value field expressed in octets.

The descriptions of the TD family of sub-TLVs are as follows:

TD Sub-TLV 1 (TC name):

Length is 16-bit unsigned value encoding the length of the TC Name field in octets. Note this can serve to identify a class, a queue, a scheduler etc. in a vendor implementation.

TC name is an ASCII character string from 1 to 64 octets in length.

TD Sub-TLV 2 (TC number):

Length is 16-bit unsigned value and is set to 1. This TLV may be used as an alternative identification to the TC name or in lieu of a TC name.

TC number is the traffic class number in the range 0...7.

TD Sub-TLV 3 (PIR)

Length is a 16-bit unsigned value and is set to 8.

PIR is the peak information rate in bits/sec encoded in a 64-bit unsigned integer.

TD Sub-TLV 4 (PBS)

Length is a 16-bit unsigned value and is set to 4.

PBS is the peak burst size in bytes encoded in a 32-bit unsigned integer.

TD Sub-TLV 5 (CIR)

Length is a 16-bit unsigned value and is set to 8.

CIR is the committed information rate in bits/sec encoded in a 64-bit unsigned integer.

TD Sub-TLV 6 (CIRmax)

Length is a 16-bit unsigned value and is set to 8.

CIRmax is the maximum committed burst rate in bits/sec encoded in a 64-bit unsigned integer.

TD Sub-TLV 7 (CBS)

Length is a 16-bit unsigned value and is set to 4.

CBS is the committed burst size in bytes encoded in a 32-bit unsigned integer.

TD Sub-TLV 8 (PCP map)

Length is a 16-bit unsigned value and is set to 1.

PCP bitmap is a bitmap of the PCP values that map to the traffic class and queue.

TD Sub-TLV 9 (Vendor specific option)

Length: is a 16-bit unsigned value and encodes the variable length value field in octets. It includes the IANA Enterprise Code field and the Vendor Sub-TLV that follows. The length is thus >= 9 octets.

IANA enterprise code: is a 32-bit unsigned integer that encodes the vendor's IANA Enterprise code (see: https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers)

Vendor Sub-TLV represents the value portion of the Sub-TLV. It is of Length minus 4 octets (to allow for the IANA code length). It is encoded as follows:

Type: 16-bit value representing the Vendor Type, such that the vendor manages its own type number space

Length: 16-bit value containing the length of the value field expressed in octets

Value: A variable length series of octets, the treatment of which is dependent on the vendor's definition of that attribute

The following diagram summarizes the Vendor Specific Option Sub-TLV format:

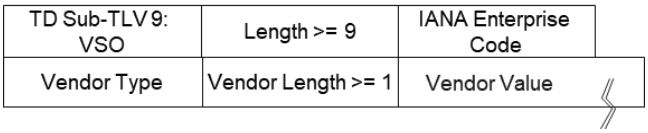

Figure 26: Vendor Specific Option Sub-TLV format

Note: Multiple instances of TD Sub-TLV 9 may be present in a SP sub-TLV.

TD Sub-TLV 10 (Profile Name):

Length is 16-bit unsigned value encoding the length of the Profile Name field in octets. This references the name of a locally configured profile or template, specifying configuration for a given Subscriber Parameters Sub-TLV. When used to configure a given Subscription Parameters Sub-TLV, its scope is limited to that Sub-TLV.

Profile name is an ASCII character string from 1 to 256 octets in length.

TD Sub-TLV 11 (Policer Name):

Length is 16-bit unsigned value encoding the length of the Policer Name field in octets. This serves to reference the name of a locally configured policer.

Policer name is an ASCII character string from 1 to 256 octets in length.

TD Sub-TLV 12 (Bandwidth Limit):

Length is a 16-bit unsigned value and is set to 8.

Bandwidth-limit is the rate limiter bandwidth in bits/sec encoded in a 64-bit unsigned integer.

TD Sub-TLV 13 (Burst Size Limit):

Length is a 16-bit unsigned value and is set to 4.

Burst Size Limit is the rate limiter burst size in bytes encoded in a 32-bit unsigned integer.

Notes:

1) The SP sub-TLVs 2,4,6 & 8 (TC descriptors and TC policing descriptors) contains one of TD sub-TLV 1 or TD sub-TLV 2 (to identify the TC the sub-TLV refers to) and at least one other TD sub-TLV.

2) Not all TD sub-TLVs are valid in all SP sub-TLVs. TC name, TC number and PCP map TLVs only apply to TC related TD sub-TLVs. The following table indicates validity:

TD sub-TLV→	1	2	3	4	5	6	7	8	9	10	11	12	13
SP sub-TLV 1 UL Descriptor	-	-	Y	Y	Y	Y	Y	-	Y	-	-	-	-
SP sub-TLV 2 UL TC Descriptor	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-
SP sub-TLV 3 UL Policing Descriptor	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y
SP sub-TLV 4 UL TC Policing Descriptor	Y	Y	-	-	-	-	-	-	Y	Y	Y	Y	Y
SP sub-TLV 5 DL Descriptor	-	-	Y	Y	Y	Y	Y	-	Y	Y	-	-	-
SP sub-TLV 6 DL TC Descriptor	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-
SP sub-TLV 7 DL Policing Descriptor	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y
SP sub-TLV 8 DL TC Policing Descriptor	Y	Y	-	-	-	-	-	-	Y	Y	Y	Y	Y
SP sub-TLV 9 5QI Descriptor	-	-	-	-	-	-	-	-	-	-	-	-	-

SP sub-TLV 10 Local Profile Name	-	-	-	-	-	-	-	-	-	-	-	-	-
SP sub-TLV 11 DL TC Policing Descriptor	Y	Y	-	-	-	-	-	-	Y	Y	Y	Y	Y

3) A PCP bit value may not appear in two different DL TC Descriptors or two different UL TC Descriptors. If it did appear in more than on TC descriptor in the same direction, it would mean that an individual PCP code point mapped to more than one traffic class.

Additional Authentication (AA) sub-TLV Family

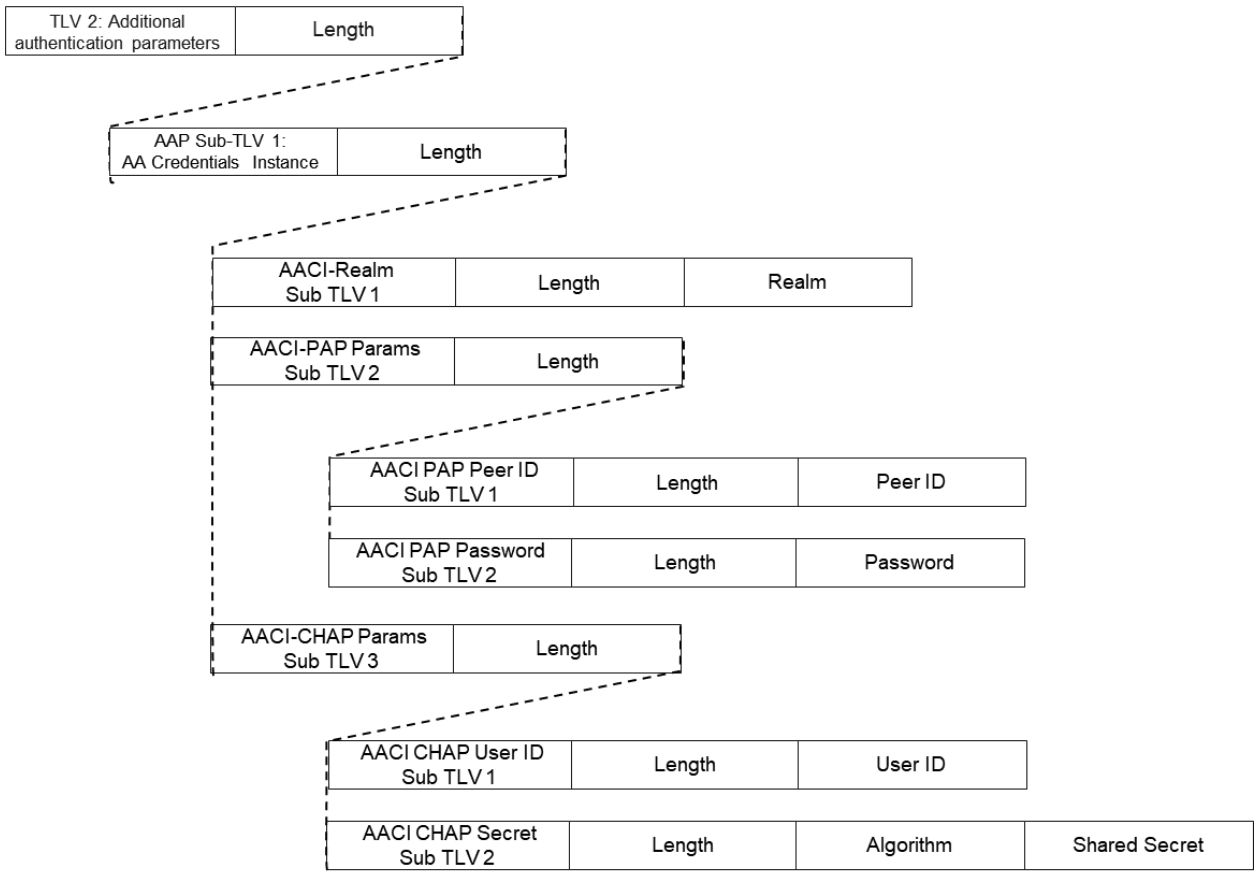

Figure 27: Additional Authentication Parameters sub-TLV family

The additional authentication parameters TLV is composed of one or more Additional authentication Credential Instance (AACI) TLVs.

Each AACI TLV comprises an optional AACI-Realm sub-TLV and one of an AACI-PAP TLV (sub-TLV 2) or an AACI-CHAP TLV (sub-TLV 3). The AACI TLV length field encodes the cumulative length of all sub-TLVs in octets. An additional authentication parameters TLV may only contain one AACI sub-tlv that does not encode a realm. The AACI TLV needs to be unique from the point of view of the realm information such that the presence or absence of an NAI realm will only resolve to a single AACI TLV.

NOTE: it is for further study as to whether an AACI TLV that ONLY contains a realm sub-TLV is appropriate to use as an unauthenticated default; any presented credentials with the specified NAI will be accepted.

An AACI-PAP TLV is comprised of an AACI-PAP Peer ID sub-TLV and an AACI-PAP Password sub-TLV.

An AACI-CHAP TLV is comprised of an AACI-CHAP User sub-TLV, and an AACI-CHAP Secret sub-TLV.

The encoding of the sub-TLVs is as follows:

AACI-Realm TLV (Sub-TLV 1)

Length is 16-bit unsigned value encoding the length of the Realm field in octets.
Realm is a variable length array corresponds to the NAI realm as specified in RFC 7542.

AACI-PAP Peer TLV (sub-TLV 1)

Length is 16-bit unsigned value encoding the length of the Peer-ID in octets
The Peer ID is a variable length array corresponds to the peer-ID in a PAP message as per RFC 1334 exclusive of NAI realm information as per RFC 7542.

AACI-PAP Password (sub-TLV 2)

Length is 16-bit unsigned value encoding the length of the password in octets.
Password is a variable length array that encodes the password as per RFC 1334.

AACI CHAP User ID (sub-TLV 1)

Length is 16-bit unsigned value encoding the CHAP user ID.
CHAP User ID is a variable length array corresponds to the name field in a CHAP response message as per RFC 1994 exclusive of NAI realm information as per RFC 7542.

AACI CHAP Secret (sub-TLV 2)

Length is the value in octets of the algorithm and secret fields (currently specified as 17 octets)
Algorithm is a fixed length field one octet in length and MUST be set to 5 (CHAP with MD5) as per RFC 1994
Secret is a variable length array that encodes the secret as per the algorithm field. In this case it is a 16 byte MD5 hash used for CHAP validation of challenges.

Error Handling

An AGF will discard information it does not recognize within an RG-LWAC structure while preserving and acting upon valid information. When there is conflicting information between two sub-TLVs, the first is retained, and any subsequent conflicting sub-TLVs are discarded.

The following is a non-exhaustive list of the errors that could occur parsing an RG-LWAC data structure.

- Unrecognized IANA Enterprise Code
- Unrecognized TLV identifier
- Unrecognized local profile name
- Unrecognized SP sub-TLV identifier
- Unrecognized TD sub-TLV identifier
- Malformed set of TD sub-TLVs
    - A TD sub-TLV did not contain either a TD name or TD number sub-TLV or did not contain at least one other TLV
- Invalid TD sub-TLV length
- Invalid PCP mapping
- Invalid TC number
- Duplicate TC number
- Duplicate TC name

How errors are reported is FFS.

Vendor Specific Option TD Sub-TLV 9 Usage

The VSO TD Sub-TLV may be used to support a vendor-specific capability or feature to augment the valid set of standard TD Sub-TLVs for a given UL or DL Subscription Parameters Sub-TLV. For example, TD Sub-TLVs 3 through 7 define a comprehensive, standard set of shaping-related attributes for the DL Descriptor Subscription Parameters Sub-TLV. If a vendor wishes to return an attribute to augment these standard TD Sub-TLVs for the DL Descriptor, the VSO TD Sub-TLV may be used for that purpose. However, using a VSO Sub-TLV to represent the same capability as an already defined standard TD Sub-TLV should be avoided. In the event both a standard TD and VSO TD Sub-TLV are returned such that the VSO Sub-TLV is equivalent in meaning to the standard TD Sub-TLV, the standard TD Sub-TLV should take precedence.

Profile Name TD Sub-TLV 10 Usage

The Profile Name TD Sub-TLV may be used to reference a locally configured profile that satisfies the configuration for a given UL or DL Subscription Parameters Sub-TLV. It may be used in lieu of the valid set of standard TD Sub-TLVs for a given UL or DL Subscription Parameters Sub-TLV, or it may be returned with one or more other valid TD Sub-TLVs. In the event of a conflict, a standard TD Sub-TLV returned in RG-LWAC should take precedence over local configuration referenced by the Profile Name TD Sub-TLV. In general, its semantics align with the Local Profile Name Subscription Parameters Sub-TLV, just at a more granular level.

RG-LWAC usage:

An AGF will have a locally configured default behavior.

The RG-LWAC is communicated to the AGF as part of the registration process for either a 5G-RG or FN-RG. An RG-LWAC may:

1) Completely define all traffic parameters for the traffic classes available for a given subscription,
2) Refer to a local profile that completely defines the traffic parameters for all the traffic classes available for a given subscription.
3) Provide a combination where a reference to a local profile provides the default parameters or a portion of the subscription, and any additional parameters that override or augment the defaults are communicated as SP & TD sub-TLVs in the RG-LWAC.
4) Provide some parameters and/or references to local profiles that override locally configured defaults.

For example, a subscriber is eligible to use three traffic classes in the access; classes gold, silver and bronze. This could be encoded in multiple ways. An RG-LWAC could:

1) Encode in the RG-LWAC structure using SP TLVs and TD sub-TLVs all traffic parameters associated with the overall subscription as well as complete traffic descriptors for the Gold, Silver and Bronze traffic classes.
2) Encode in the RG-LWAC structure the name of a local profile that provides all traffic parameters associated with the overall subscription as well as complete traffic descriptors for the Gold, Silver and Bronze traffic classes.
3) Encode in the RG-LWAC structure the name of a local profile that provides the default values for the overall subscription as well as complete default traffic descriptors for the Gold, Silver and Bronze traffic classes, and includes SP TLVs and TD sub-TLVs that selective override certain traffic parameters for the particular subscription.

As an example, the RG-LWAC contains the name of a local profile called ‘Gold/Silver/Bronze’, and a SP sub-TLV that redefines the DL PIR rate for the overall subscription, and an SP sub-TLV that redefines the DL TC PIR rate for the “Gold” traffic class.

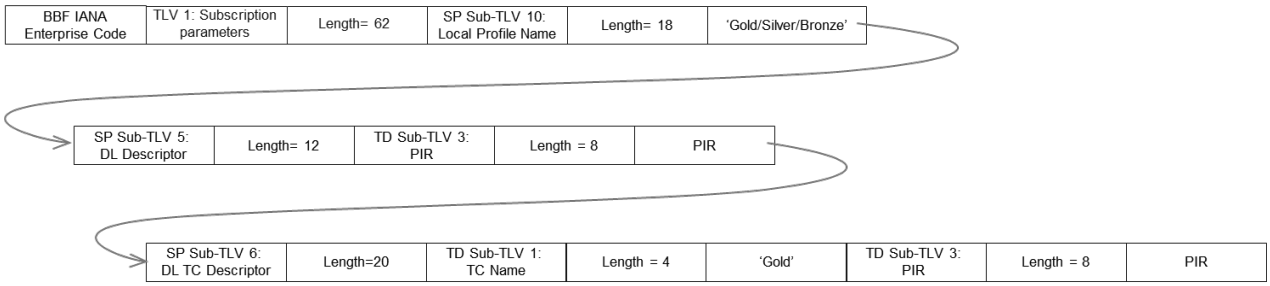

Figure 28: Example of a combination of local profile and selective overriding of parameters

Notes:

A TD sub-TLV that overrides parameters for a given traffic class contains the sub-TLVs that specify values for all parameters that are being overridden. Two TD sub-TLVs referring to the same set of parameters (e.g., with a common ttou class name) is an error and the second will be rejected by the AGF.

The DL parameters and UL policing parameters are consumed locally to configure downstream traffic management. The UL parameters are consumed locally to configure upstream policing of subscriber traffic, AND in the case of a 5G-RG are communicated to the 5G-RG using an AS subscription parameters message. Refer to the section in TR-456 on 5G-RG registration procedures.

As part of the 5G-RG registration process the AGF constructs an AS subscription parameters message (refer to TR-456 Annex) from the RG-LWAC information and communicates this to a 5G-RG.

RG-LWAC and mapping from QFI to traffic class:

An AGF will map downlink traffic to traffic class using the RG-LWAC information according to the following:

An AGF will have a mapping from 5QI to DSCP/PCP in order of preference via:

- The 5QI value in a received packet matching the 5QI in a 5QI descriptor SP sub-TLV (8, deprecated in this issue) in the RG-LWAC
  OR if SP sub-TLV 11 (marking descriptor) is present and a 5QI to DSCP/PCP mapping tuple is present for the 5QI value, then the PCP value is used, and the DSCP value is used IF the D bit is set in the marking controls
  OR RG-LWAC indicates information in a locally configured profile, which may be referenced by a local profile name SP sub-TLV (10).
  (these will be mutually exclusive)

The 5QI information in local configuration.

The AGF will map PCP to a traffic class. This is achieved by (in order of preference):

- The PCP value output from the 5QI mapping corresponding to a PCP value in a PCP map TD sub-TLV (8) contained in the DL TC Descriptor SP sub-TLV (6).
- Local configuration

Appendix I. Security in Fixed Access Networks

This section explores the notion of security in fixed access networks, in particular the threat models that the use of encryption may mitigate. The discussion focuses on deployment practices and the vulnerability of the different technologies when viewed in this context.

Terminology used:
Malicious Agent – a device or piece of software deployed by a malicious actor
Malicious Actor – the individual or organization deploying and operating malicious agents
Target – A broadband subscriber whose security is threatened by a malicious agent

The insertion of a malicious agent in either a wireless or wireline path have similar classes of challenges. However, the economics of such activity in terms of benefit to a malicious actor are radically different between the two. There are two aspects to this:

1. For radio, a malicious actor can choose the placement of a malicious agent where it is convenient for their purposes and the physical challenges of deploying such an agent can be significantly mitigated. In a wireline context the malicious actor is not presented with a choice and has significant economic penalty and additional risks of detection as a result.
2. For radio, a single malicious agent can address a significant and variable community of targets whereas any practical deployment of a wireline malicious agent can only address an invariant single target or the set of targets served by a single drop. Therefore, the potential economic upside to a malicious actor is very limited.

Given the number of threat vectors not addressed by encryption of only a portion of an end-to-end path, the economic and performance (hence Quality of Experience) penalty on wireline access of 5G-RG to AGF encryption is not justified.

I.1 Detailed Analysis

Threat Model:

This analysis focuses on a particular threat model, which is the insertion of a malicious agent in the path between a 5G-RG and an AGF or the attachment of a malicious agent to a DSL or PON access network as an NT/ONU. This may involve the insertion of physical equipment in the path, passive monitoring of the technology via intrusive or non-intrusive means, or the ability to manipulate access network connectivity and/or traffic patterns. The latter may be a consequence of the access technology, or as a result of compromising the control/management plane of the access network.

Such an agent would be able to:
- Passively or actively monitor subscriber traffic (loss of privacy)
- Impersonate the subscriber (theft of service)
- Perform a denial of service attack on one or more subscribers via the introduction of traffic that interfered with normal operation

The following discussion focuses upon a number of aspects:
- Ease of access to an insertion point for a malicious agent
- Ability to detect the presence of a malicious agent
- Cost to the malicious actor
- What a malicious agent can do.

General challenges with inserting a physical agent in the path:

The challenges with any attempt at physical insertion of a malicious agent at a point in the path between an RG and the AGF are:

Access:

The ability to get at the path. The path in general is implemented as equipment in a combination of secure facilities and outside plant. Outside plant may be overhead or buried cable, and in the case of FTTdp or Cable electrical equipment that is not in a secure enclosure such as a vault.

Targeting:

The ability to identify the component of outside plant serving the targeted subscriber. For example, identifying a particular copper pair in a binder group.

Concealment.

How to avoid detection of surveillance. This falls into two classes:

a) Concealment of the physical malicious agent: For example, a physical agent would not likely fit inside a NID and therefore would be visible to casual passers-by. Or the act of installing a physical agent in outside plant (e.g., at a pole mounted device) being difficult to do innocuously.
b) Concealment of breaking into the physical media: A malicious agent that broke into the access media may also be detectable, as may introduce a one hop latency in addition to modifying other observable characteristics of the path behavior such as the impedance model or other artifacts.

Powering:

Any malicious physical agent attached to outside plant would require the agent to have a self-contained power source which would imply a limited lifetime.

Harvesting:

The malicious agent would need connectivity to the malicious actor. This will require either connectivity or non-volatile storage. Depending on the connectivity cost, avoiding the cost of harvesting information of near-zero value (e.g., streamed video) will place additional requirements on a malicious agent. Technologies that could be considered for harvesting would include cellular or Wi-Fi (although Wi-Fi would have reach limitations).

Hardening:

If the malicious agent is to be deployed outdoors it will need to be environmentally hardened.

Cost:

The cost of the physical agent itself vs. the perceived value of the information harvested

Concealment of the physical malicious agent, Powering, Harvesting and Hardening can be considered to be equivalent challenges for a physical malicious agent for any access technology. However, there are significantly different deployment considerations for intercepting radio vs. wireline, as wireline requires proximity to the physical media.

Access Technology:

Within a broadband access network there are various classes of p2p, p2mp and mp2mp interfaces and/or a comparable set of overlaid network behaviors within the TR-101/156/167/301 architecture. The following is an overview of the physical connectivity.

Note, while it is easy to imagine a physical repeater inserted into the path that can monitor as well as insert traffic, in some cases this would be detectable. Commercial products also exist that passively monitor the path without having to physically break into the path exist for both DSL and PON technologies (however, these products are generally marketed only to Law Enforcement Agencies).

DSL Characteristics:

Overview:

DSL physical connectivity is physical p2p connectivity to the premises implemented with a copper twisted pair cable. The limited reach of DSL (inversely proportional to the data rates that can be achieved) means DSL is combined with an aggregation network which may also use DSL, PON or P2P fiber. A DSLAM or DPU may be deployed as hardened outside plant, in an environmentally conditioned and secure vault or a central office. The corresponding modem or network termination (NT) at the customer premises may be external to; or integrated into; the RG.

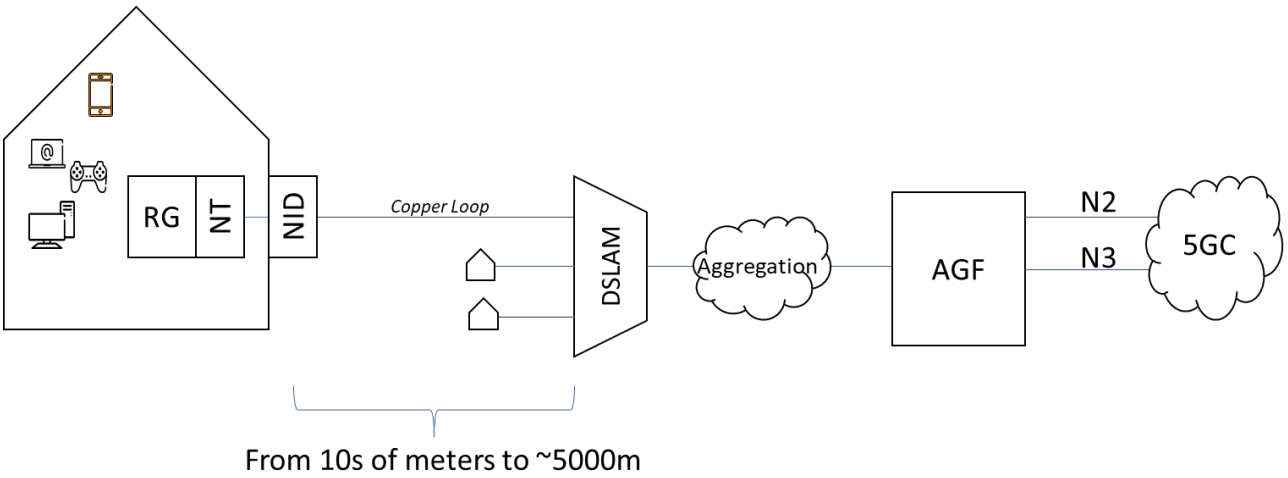

Figure 29: DSL access to 5GC Example

Access & Targeting:

The copper pair is exposed and accessible between the distribution point (where the pair is extracted from a cable bundle/binder group) and the subscriber premises. The cable bundle can range from a few to 100s of pairs, is typically hardened against environmental factors, may be routed in a duct, or overhead, and therefore not an easy target without significant resources at the disposal of the malicious actor including access to operator records on copper pair assignment.

The subscriber termination is deployed within the subscriber premises. This may be an operator installation or customer self-install. Many installations have a network interface device (NID) at the exterior of the premises that acts as a demarcation point between the carrier network and the premises network and allows a test set to be inserted for sectional fault. This is a location that provides both easy access and easy targeting (but poor concealment).

Concealment of breaking into the physical media:

Breaking into the media to insert a repeater will of course result in a disruption of service. It may also change the impedance model such that the DSL retrains at a different rate, which would be observable to the management systems.

PON Characteristics:

Overview:

A passive optical network system is implemented as an optical line termination (OLT) serving some multiple of optical network units (ONUs) located at the subscriber premises.

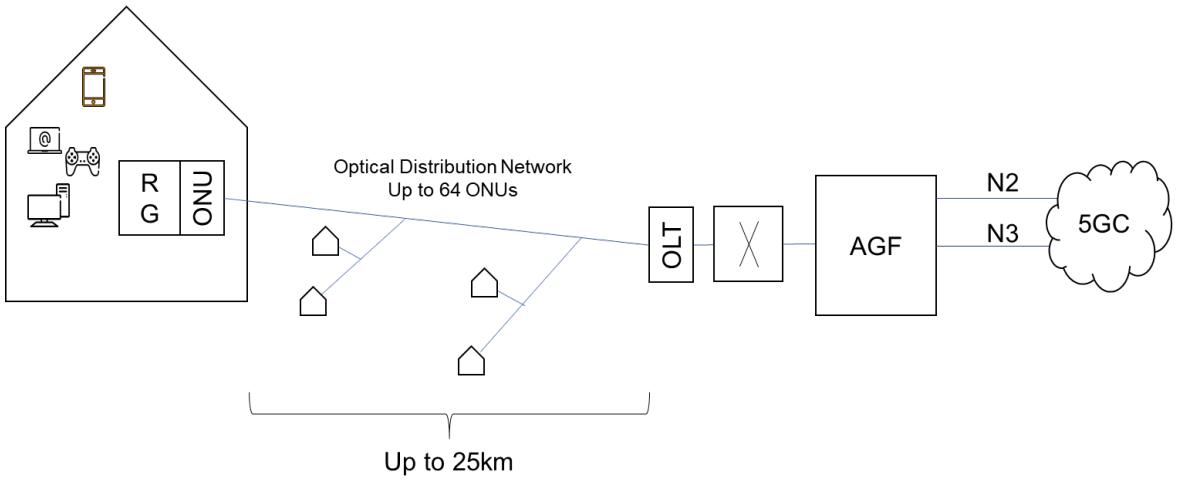

Figure 30: PON access to 5GC Example

A PON is p2mp, with broadcast transmission downstream and TDMA upstream. As such the downstream traffic from the OLT to any ONU is visible to all ONUs. PON systems implement AES encryption and its use is recommended on all bi-directional GEM ports with a unique key being assigned to each GEM port.

Multicast traffic can receive two classes of treatment:

- a VLAN can be designated as a multicast VLAN in which case all downstream Ethernet frames are sent on an unencrypted GEM port
- A VLAN can be designated as an N:1 VLAN, in which case all BUM downstream Ethernet frames are replicated onto the set of bi-directional GEM ports that are members of that VLAN

So for bi-directional GEM ports the visibility of traffic by a malicious agent would be no different than that for any ONU not served by the bi-directional GEM port. The traffic would be encrypted and therefore not visible to the other ONUs or any man in the middle monitoring.

PON systems have a reach of 20 to 25km without repeaters. This permits the OLT to be deployed in a secure facility, typically a central office.

The ONU (subscriber termination) is typically indoor. Deployments exist whereby the ONU is deployed at the building ingress and a media converter is used to convert the transport to G.fast or VDSL in order to re-use the existing indoor wiring.

Access and Targeting:

That PON is encrypted means the only useful insertion points for a physical malicious agent is at the OLT or the ONU. In most deployment scenarios both can be considered to be housed in secure facilities. The exception to this is when an external to the premise media converter is used to translate frames over PON to frames over the home network media.

Concealment of breaking into the physical media:

PON systems work on a schema of having a registration number and a serial number. The OLT is pre-configured with a list of valid ONU serial numbers or a list of valid ONU registration numbers. The OLT will periodically solicit the serial number of an ONU, in the former case the serial number is checked against the valid set of serial numbers. In the latter case if the serial number is not recognized, the registration ID is solicited and checked against the valid registration number list. The registration ID (which acts as a provisioned shared secret) is also used for key derivation.

For XG-PON this can be further augmented with registration ID based key derivation and mutual authentication of the OLT and ONU. The threat models and security features of G-PON is discussed on section 12 of ITU-T G.984.3 [39] and for XG-PON is discussed in section 15 of ITU-T G.987.3 [40].

Challenges with a Malicious Agent connected to a UNI of the Access Network

A different attack vector from inserting a malicious agent in the path would be for the malicious agent to be connected to the access network as an actual subscriber.

Accountability:

A malicious actor connected to a specific access network that attempted to subvert the local network via DOS attacks, attempts to impersonate neighbors etc. can be identified, shut down, and legal recourse pursed by an operator.

Very limited or no visibility of neighbor's traffic:

As outlined above, subscribers are typically logically isolated in the access network, with the only model that provides any visibility at all being the N:1 VLAN model.

Targeting:

The malicious agent would have no information to correlate what little information it gleaned from the access network with the target.

Small possible target community:

Compared to the larger internet, attempting to compromise the access of other subscribers in a given access network provides a small target landscape.

Access Connectivity Models:

TR-101/156/167/178 define a number of L2 connectivity models for exchange of Ethernet frames between a 5G-RG and an AGF:

Ethernet aggregation 1:1 VLAN mode

Single tagged and double tagged 1:1 VLAN mode for Ethernet aggregation provides a logical p2p connection between the 5G-RG and the AGF. Therefore, no traffic is exposed outside the 5G-RG/AGF pair. The network side tagging is added/removed by the operator-controlled access node therefore cannot be manipulated by an agent connected to the access. One RG connected to a double tagged VLAN mode connection cannot monitor or insert traffic into another double tagged service instance.

Ethernet aggregation N:1 VLAN mode

N:1 VLAN provides logical p2p connectivity for "known" Ethernet frames; these are frames for which the correct port to forward to has been "learned" by the MAC learning process in bridging entities in the forwarding path. Unknown frames are flooded "split horizon" within the topology of an individual N:1 VLAN instance. This differs from normal bridging. The reference to split horizon is that there is a distinct sender and receiver set of end-stations for flooded traffic in each of the upstream and downstream directions. A frame originating with an RG and directed upstream will only be delivered to one or more AGFs connected to the same virtual LAN instance. A frame originating with an AGF and directed downstream will be flooded on all downstream ports by any bridging element that has not "learned" the port via which the destination MAC can be reached. Frames received by 5G-RGs other than for the 5G-RG addressed by the destination MAC address in the frame will be silently discarded.

Once the forwarding path for a given MAC address has been established, the connectivity is logically p2p and frames directed to a particular subscriber are not exposed to other end-stations.

Information learned by bridging elements in the path between a 5G-RG and an AGF may be aged out. The duration of the aging timer is configurable. There are also interactions between the aging of MAC entries, aging of ARP cache information and proprietary features that limit the amount of actual user traffic exposed by the flooding of frames with unknown destination addresses.

Access Nodes may perform MAC anti-spoofing measures to ensure one end-station does not try to impersonate another, either to hi-jack connectivity or to perform a denial of service attacks.

Some DSL access nodes may perform MAC NAT. This was originally motivated by incompetently executed NIC cards where the manufacturer did not ensure a unique MAC address per card. This mitigates spoofing by ensuring the MAC address associated with a specific customer port are unique and controlled by the AN operator.

Ethernet aggregation TLS mode

TLS mode was intended for business services, therefore simply offers a LAN service and ubiquitous L2 connectivity between all participating end stations in the virtual LAN instance. This is not proposed for use for 5G-RG to AGF connectivity so is not considered further.

Observations:

The BBF specified access networks with the exception of TLS mode prevent L2 connectivity or observability between a malicious actor and a targeted subscriber with the exception of random flooding of unknown frames in the N:1 VLAN model. If both are connected to the internet, both are reachable and interconnected via L3, however this is no different than the situation for any host connected to the internet, therefore any further attempts to mitigate connectivity and observability at L2 offer no tangible benefit and a malicious actor being connected to the same L2 access network as any target offers no advantage.

Expanded Attack Surface with 5G:

It is worth observing that extending the 5G control plane to the 5G-RG and devices served by the premises Wi-Fi expands the attack surface for a malicious actor. However, encryption of the user plane does nothing to mitigate this threat. NAS is ciphered and integrity protected separately, therefore the actual attack surface ultimately is no different than it is for FN-RGs (which have successfully used an unencrypted user plane for the past 25 years).

Other Risks

There are numerous security risks that encryption of the access segment of an end-to-end path cannot mitigate. These include malware, phishing, ransomware, web-based attacks, etc. A full taxonomy can be found in [41] These are attractive to malicious actors as they require little investment and target a large community.
It is also worth noting that the majority of devices in the home are connected via Wi-Fi which if not properly secured offers a significant backdoor. However, this is primarily an issue for older deployed FN-RGs as the standardization of automated means of securing Wi-Fi has made significant strides.

Other mitigations:

Since the Snowden revelations, there has been a significant increase in the use of end-to-end encryption. This has not been uniquely driven by security concerns as the conclusion of the security community is that encryption only slows down a state actor with significant resources. It has also been used by major web players as a tool to prevent network ossification. It is also a near mandatory component of ecommerce. One conclusion is that a safe assumption is that all traffic of consequence is already encrypted and in a more secure end-to-end form.

Impact of encryption:

Encryption is performed using block ciphers, typically using 128-bit or less block size.
A block cipher typically uses multiple “rounds” of encryption which means each “round” acts upon the block output of the last round, and therefore is a sequential process that cannot be pipelined. Not only is this computationally intensive, it also introduces additional latency in packet processing. RGs in general have limited compute resources, therefore ciphering will have a disproportionate impact on performance.

I.2 Conclusion

The original purpose of this examination of access network security was to explore the utility of encryption between a 5G-RG and an AGF, which is only a small portion of the end-to-end path. We would observe that when the totality of threat vectors is examined, there is a hierarchy of security risks. Within that hierarchy the higher up the protocol stack one goes, the more opportunistic and indiscriminate the attack vectors become.

Of these risks the only ones that appear to be mitigated by encryption of traffic exchanged between a 5G-RG and an AGF in currently deployed wireline networks is that of the deployment of a physical malicious agent that focuses on a specifically targeted subscriber. Access networks themselves provide adequate subscriber isolation. This implies a malicious non-state actor with access to technical resources and motivated by other than economic factors (as the opportunistic techniques that target the end system offer a much higher risk reward profile, especially in this era of increasingly pervasive end-to-end encryption). We suggest non-state actor as state actors typically collude with the operator for either large scale monitoring and data collection (e.g., the NSA in the United States) or legal intercept and have access to secured operator facilities.

Given the above considerations mandating IPSEC even as an option for operators as a PDU session transport between the 5G-RG and the AGF places an unreasonable quality of experience and economic burden on WWC implementations in proportion to the threats it actually addresses.

Appendix II. Mitigating the Impact of Outages

A normal session lifecycle that accounted for service outages would appear as:

1. registration
2. session establishment including resource allocation
3. service outage
4. release resources, session state and de-register
5. service restoration
6. go to 1

This would assume perfect knowledge of all events by all actors. If there is imperfect and unsynchronized knowledge of outages by the actors involved (RG, AGF, AMF, rest of the 5GC), it is possible to envision a number of scenarios whereby the overall system was either unaware of the outage, or one of the actors unaware, or, due to misalignment of timers, a common view of status did not exist. In these scenarios, recovery could be simplified and made more scalable by "strategic hiding" of an outage.

Examples of this would include:

1) Receiving an IP session initiation for an FN-RG that was considered to be registered and connected and having an associated PDU session in place. This could happen if an FN-RG reset when the link was unsupervised, or there had been a link outage detected by the FN-RG but not yet by the AGF. If there was a corresponding PDU session in place before the link fault was detected, the IP session initiation could simply be mapped to the existing PDU session, and cached session parameters at the AGF and in the 5GC employed to facilitate IP session restoration.
2) The existing defined transition from CM-CONNECTED to CM-IDLE on AGF upon a detection of an outage is already a form of "strategic hiding", because, if the FN-RG connectivity is restored while RM state on the AGF is still RM-REGISTERED, the AGF will be able to resume the PDU session sending a Service Request.
3) Hiding of an outage detected by supervision could be enhanced by the use of a local timer running at the AGF to be started instead of advertising the outage to the AMF. The AGF upon expiry of the local timer would perform UE initiated de-registration procedures. If connectivity was restored prior to the expiry of the timer, the session state might be in place, and not require a Service Request to re-establish connectivity to the 5GC.
4) In case of frequent losses of connectivity in the wireline access network, the AGF could implement a strategic hiding of the flapping events. That could be achieved by informing AMF about the loss of connectivity with a certain delay from detection with the AN Release procedure.

It should be noted that "strategic hiding" of events are implementation dependent features and should not be "silent": the information should be exposed to Operator's IT systems to facilitate troubleshooting and service monitoring.

Note: For a 5G-RG the connectivity is always supervised by the AGF as well as by 5G-RG. In particular, for the purpose of Hybrid Access it is necessary to expose outages to the 5GC.
Therefore, there are fewer situations where an outage can or should be mitigated and therefore, for 5G-RG support, strategic hiding of outages in the wireline access network is NOT recommended.

End of Broadband Forum Technical Report TR-470