Technical Report

TR-457
FMIF Functional Requirements

Issue: 1
Issue Date: April 2023

Notice

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

Intellectual Property

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

Terms of Use

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

2. NO WARRANTIES
THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER'S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

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

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

Issue History

Issue Number	Approval Date	Release Date	Issue Editor	Changes
1	17 April 2023	17 April 2023	Donald Eastlake, Futurewei Mengmeng Li, China Mobile	Original

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

Editors: Donald Eastlake, Futurewei
Mengmeng Li, China Mobile

Work Area Director(s): Manuel Paul, Deutsche Telekom
Christele Bouchat, Nokia

Project Stream Leader(s): Venkatesh Padebettu, Juniper

Table of Contents

Executive Summary 6

1 Purpose and Scope 7

1.1 Purpose 7
1.2 Scope 7

2 References and Terminology 8

2.1 Conventions 8
2.2 References 8
2.3 Definitions 9
2.4 Abbreviations 12

3 Technical Report Impact 13

3.1 Security 13
3.2 Privacy 13

4 5G FMC architecture with FMIF 14

4.1 FMIF Interfaces 15

5 High-level requirements of an FMIF 16

6 Functional features and requirements 17

6.1 Authentication/Authorization/Identity management 17
6.2 Security 17
6.2.1 N1 (NAS) Security for FMIF 17
6.2.2 N2 Security 17
6.2.3 User Plane Data Security (N3) 18
6.3 User Plane 18
6.3.1 User Plane Maximum Transmission Unit (MTU) Considerations 19
6.3.2 QoS Marking Aspects 20
6.4 Control Plane 20
6.4.1 Modes of BNG Interworking with FMIF 21
6.4.2 FMIF-5GC Control Plane 22
6.4.3 FMIF-BNG Control Plane 22
6.5 QoS 26
6.5.1 RG level QoS Provisioning 27
6.6 FMIF functions for core network signaling 28
6.7 N2 connections 28
6.8 FMIF support for slicing and AMF selection 28
6.9 Connection Management State on FMIF 28
6.10 Detection of FN-RG equipment change 29
6.11 FN-RG IP session initiation requirements 29
6.12 Void 31

7 Co-Location Options 32

7.1 Co-located FMIF and UPF 32
7.2 Co-located FMIF and BNG 33

8 Procedures call flows 35

8.1 FN-RG IP Session Initiation with PPPoE 35
8.2 FN-RG IP Session Initiated with DHCPv4 39
8.3 FN-RG IP Session Initiation with DHCPv6 41
8.4 FN-RG IP Session Initiation with RS Followed by DHCPv6 43

8.5 Registration Management Procedure for FN-RG....45
8.6 Service Request Procedure for FN-RG....46
8.7 Session Initiation Procedure for FN-RG....46
8.8 Deregistration Procedure for FN-RG....46
8.9 FN-RG or Network Requested PDU Session Modification via W-5GAN....46
8.10 FN-RG/BNG or Network Requested PDU Session Release via W-5GAN....47
8.11 FN-RG AN Release via W-5GAN....48
8.12 Configuration Update Procedure for FN-RG....50
8.12.1 Configuration Update procedure for Access and Mobility Management related parameters....50
8.12.2 Configuration Update procedure for transparent FN-RG policy delivery....50

Table of Figures

Figure 4-1: Architecture for interworking for FN-RG and for coexistence. 15
Figure 6-1: User Plane via FMIF for FN-RG....18
Figure 6-2: FMIF Control Plane 21
Figure 6-3: N2 Control Plane....22
Figure 6-4: BNG-FMIF Control Plane Messages....23
Figure 6-5: RM/CM State Transitions....29
Figure 7-1: Co-Located FMIF and UPF Architecture....32
Figure 7-2: Co-located FMIF and BNG Architecture 34
Figure 8-1: FN-RG IP Session Initiation with PPPoE....36
Figure 8-2: FN-RG IP Session Initiation with DHCPv4....40
Figure 8-3: FN-RG IP Session Initiation with DHCPv6....42
Figure 8-4: FN-RG IP Session Initiation with RS followed by DHCPv6....44
Figure 8-5: FN-RG/BNG or Network Requested PDU Session Release via W-5GAN 47
Figure 8-6: FN-RG AN Release via W-5GAN....49
Figure 8-7: Configuration Update Procedure for transparent UE policy delivery via W-5GAN 51

Table of Tables

Table 1: FMIF-BNG RADIUS Message Summary....24

Executive Summary

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

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

The Fixed Mobile Interworking Function (FMIF) is a logical function deployed between a Broadband Network Gateway (BNG) and the 5G core network, thus providing access from a wireline access network Fixed Network-Residential Gateway (FN-RG) to the 5G core. (For such access without a BNG, see the current issue of TR-456 (AGF Functional Requirements).)

1 Purpose and Scope

1.1 Purpose

In 2017-2018, BBF WWC Work Area studied 5G Fixed Mobile Convergence, FMC, and its impacts on interfaces being defined by 3GPP for release 16 and further releases. BBF concluded its study by December 2018, and it resulted in a series of liaisons with requests from BBF to 3GPP SA2 – those requests have been considered in the normative phase of 3GPP Release 16.

TR-457 specifies the 5G Fixed Mobile Interworking Function (5G FMIF) and its functional requirements to enable the wireline-based operators to wholesale their 3GPP 5G services to the 3GPP 5G service operators, while keeping the wireline core functionalities. In particular, the wireline-based operators still keep their own service edge, i.e., BNG, for the wireline subscriber and service control and management. When there is a need for 3GPP 5G service provisioning to its subscribers, the wireline-based operator will interwork with the 3GPP 5G service operator for requesting 3GPP 5G service access.
.

1.2 Scope

The scope of this Technical Report is to describe the functional requirements of the Fixed Mobile Interworking Function that are necessary to support interworking between the BBF wireline access networks and 3GPP 5G networks and to enable FN-RGs to use services that are based on the 3GPP 5G core network.

The FMIF, deployed standalone behind a BNG, is a function architected to provide interworking with the 3GPP 5G core network support for an unmodified but appropriately configured BNG function.
The BNG TR-178 [5] supports the V interface for FN-RG, which identifies the facility ID as signaled by the access network and authenticates the FN-RG. The BNG supports existing VLAN tags and packet priority indication methods as defined by TR-101i2 [1].

Where convenient, functional requirements herein are specified by referenced to TR-456i2. In some cases, even when this is not done, the corresponding section of TR-456i2 may be helpful in understanding this document.

Hybrid access is out of scope for this version of the document: only an RG with wireline access is considered here. Only a single PDU session of type IPv4, IPv6, or IPv4/v6 is supported. Ethernet and unstructured PDU sessions are out of scope. Management of FN-RG address through a local address pool at the BNG is not supported.

For this issue of TR-457, the FMIF is assumed to be an integrated implementation. The impact of control plane and user plane separation (CUPS) on these flows, and the exact call flows between the FMIF-CP and FMIF-UP 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. These words are always capitalized. More information can be found be in RFC 8174 [17].

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

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

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

Document	Title	Source	Year
[1] TR-101 Issue 2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[2] TR-124 Issue 6	Functional Requirements for Broadband Residential Gateway Devices	BBF	2020
[3] TR-146	Subscriber Sessions	BBF	2013
[4] TR-177	IPv6 in the context of TR-101	BBF	2017
[5] TR-178 Issue 2	Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2017
[6] TR-341	Radius Attributes Catalog	BBF	2016
[7] TR-456 Issue 2	AGF Functional Requirements	BBF	2022
[8] TR-470 Issue 2	5G Wireless Wireline Architecture	BBF	2022
[9] RFC 1661	The Point-to-Point Protocol (PPP)	IETF	1994
[10] RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)	IETF	1999
[11] RFC 2865	Remote Authentication Dial In User Service (RADIUS)	IETF	2000

[12]	RFC 2866	RADIUS Accounting	IETF	2000
[13]	RFC 2869	RADIUS Extensions	IETF	2000
[14]	RFC 3162	RADIUS and IPv6	IETF	2001
[15]	RFC 4679	DSL Forum Vendor-Specific RADIUS Attributes	IETF	2006
[16]	RFC 5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	IETF	2008
[17]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words	IETF	2017
[18]	RFC 8201	Path MTU Discovery for IP version 6	IETF	2017
[19]	3GPP TS 23.003	Technical Specification Group Core Network and Terminals; Numbering, addressing and identification, Release 15	3GPP	
[20]	3GPP TS 23.316	Wireless and wireline convergence access support for the 5G System	3GPP	Latest version
[21]	3GPP TS 23.501	System Architecture for the 5G System	3GPP	
[22]	3GPP TS 23.502	Procedures for the 5G System	3GPP	
[23]	3GPP TS 23.503	Policy and Charging Control Framework for the 5G System, Stage 2, Release 15	3GPP	
[24]	3GPP TS 24.501	Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3	3GPP	Latest version
[25]	3GPP TS 29.281	General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)	3GPP	Latest version
[26]	3GPP TS 29.413	Application of the NF Application Protocol (NGAP) to non-3GPP access	3GPP	Latest version
[27]	3GPP TS 33.501	Security architecture and procedures for 5G System	3GPP	Latest version
[28]	3GPP TS 38.413	NG-RAN; NG Application Protocol (NGAP)	3GPP	Latest version

2.3 Definitions

The following terminology is used throughout this Technical Report:

Access Network (AN)	A network used by a subscriber device to access a service edge, typically IP edge, i.e., BRAS, BNG, P-GW, 5G core.
Wireline Access Network	Access network conforming with TR-101/TR-178 ([1]/[5]), that can be, for example, optical fiber, electrical cable, or fixed wireless connection. The egress interface of a wireline access network is either V or (N2, N3).
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. They are N2 for the control plane and N3 for the user plane.
5G Access Network (5GAN)	This comprises 5G radio ANs (NG RANs) and 5G wireline ANs connecting to a 5G core.

FN-RG	An RG not supporting 5G NAS. The FN-RG is an RG specified by TR-124i5.
N1	Reference point between UE and the AMF. In the context of this Technical Report, it is also the reference point between FMIF and AMF.
N2	Reference point between W-5GAN and the AMF. On the W-5GAN side, in the context of this Technical Report, the termination point is the FMIF.
N3	Reference point between W-5GAN and the UPF. On the W-5GAN side, in the context of this Technical Report, the termination point is the FMIF.

Definitions of 3GPP concepts: The following definitions report a summary of 3GPP definitions. In case of the inconsistency between the text in the following and 3GPP definition, the 3GPP 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 in the case of different IP domains or overlapping IP addresses.
Network Slice	A logical network that provides specific network capabilities and network characteristics.
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.
NSI ID	An identifier for a Network Slice instance.
Network Slice Selection Assistance Information (SM-NSSAI)	SM-NSSAI = Slice Service Type (SST) [+ Slice Differentiator (SD)] Using Network Slice Selection Policy (NSSP), the UE associates its applications with SM-NSSAIs and determines the PDU session which this traffic should be routed to.
NSSP (Network Slice Selection Policy)	It is the set of SM-NSSAI that a UE is authorized to access. It is stored in the UE and corresponds to the NSSAI in the subscriber information in the network database.
NSSAI	
Allowed NSSAI	NSSAI provided by the serving PLMN network during, e.g., a registration procedure, indicating the S-NSSAIs value that the UE could use in the serving PLMN of the current registration area.
Configured NSSAI	An NSSAI that has been provisioned in the UE. For instance, the 5G-RG may store a configured NSSAI for VoIP traffic applicable to one or more PLMN.
Requested NSSAI	NSSAI provided by the UE to the Serving PLMN during registration. Subscribed S-NSSAI: S-NSSAI based on subscriber information, which a UE is subscribed to use in a PLMN.
PDU session	Temporal association between the UE and a Data Network that provides a PDU connectivity service. A session can be IP, Ethernet or unstructured.

Access & Mobility Function (AMF)	The AMF is a 5GC-CP function that terminates N1, the control interface with UEs, and N2, the control interface with access networks. It is responsible for mobility & 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.
Session Management Function (SMF)	The SMF is a 5GC control plane function. Its main functionalities: • establishing • modifying and releasing sessions • maintaining tunnel(s) between UPF and access network • UPF control and selection • address allocation • policy and QoS enforcement, including traffic usage report control 5GC-UP: The 5GC user plane is a chain of UPFs.
User Plane Function (UPF)	The UPFs provide the following functions: • PDU session point of interconnection to 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 session • 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.
User Data Management (UDM)	The UDM has two parts, the application front end (FE) and the User Data Repository (UDR). The data stored in the UDR is accessed via FE and includes:: • User subscription data, including identifiers, security credentials, access and mobility related and session related data • Policy data
Authentication Server Function (AUSF)	The AUSF supports the authentication server functionalities as defined in 3GPP.
Transport MTU	This is the MTU of the mobile network on the N3 and N9 interfaces. This is typically the infrastructure MTU less the overhead of GTP tunneling.

Wireline access MTU	This is the maximum transfer unit established for the concatenated V & A10 reference points. This would be 1492 for PPPoE and 1500 for IPoE.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	3rd Generation Partnership Project
5G-RG	Routing gateway with 5G NAS
5GC	5G Core Network
AAA	Authentication, Authorization and Accounting
ACS	Auto-Configuration Server (TR-069)
AGF	Access Gateway Function
AMF	Access and Mobility Management Function
AN	Access Node
AUSF	Authentication Server Function
BBF	Broadband Forum
BPCF	Broadband Policy Control Function
BNG	Broadband Network Gateway
DHCP	Dynamic Host Configuration Protocol
DN	Data network
FFS	For Future Study
FMIF	Fixed Mobile Interworking Function
FN-RG	Fixed Routing Gateway without NAS
GTP-u	GPRS Tunneling Protocol User Plane
GW	Gateway
IPoE	Internet Protocol over Ethernet
IPv4v6	Dual stack of IPv4 and IPv6
MS-BNG	Multi-Service BNG
NAS	Non-Access Stratum
OAM	Operations, Administration and Management
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PPPoE	Point-to-Point Protocol over Ethernet
(R)AN	(Radio) Access Network
RG	Residential Gateway
SMF	Session Management Function
STB	Set Top Box
TCI	Tag Control Information
TEID	GTP-u tunnel ID
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function

3 Technical Report Impact

3.1 Security

Security provides "a form of protection where a separation is created between the assets and the threat." In the case of the FMIF, assets exist on the communications paths between the FMIF and the functions to which it is connected, namely the BNG, AMF, and UPF. In addition, assets exist within the FMIF itself.

The risk of compromise of the FMIF communications is dependent on the threats in the environment through which those communications pass and the security of communications protocol used in those communications. For example, communication between the FMIF and the BNG uses the RADIUS protocol which provides security when properly utilized. Appropriate security measures must be taken to secure communications paths to and from the FMIF when the security of the protocol in use on a path provides insufficient protections against the threats to the security of that communication.

The security risk of penetration of the FMIF itself through means other than its communications interfaces is dependent on the security of the FMIF against physical access. Appropriate security measures must be taken to secure the premises where the FMIF is housed.

3.2 Privacy

Privacy involves the need to ensure that information to, from, and between customers can only be accessed by those who have the right to do so. Further, privacy requirements can vary by regulatory region. In general, two ways to ensure privacy are recognized:

- Preventing data from being copied to a non-intended destination.
- Encrypting data, so that it cannot be understood even if it is intercepted.

Existing privacy mechanisms are in place on the Radius interface of the FMIF and 3GPP privacy mechanisms are in place on the N1, N2, and N3 interfaces.

4 5G FMC architecture with FMIF

The 5G FMC architecture with FMIF (Fixed Mobile Interworking Function), i.e., the interworking model, enables the FN-RG to access the 5GC via the BNG and FMIF and to use services delivered by the 5GC, as shown in Figure 4-1. The FMIF is a function that supports the interactions with the BNG and the interfaces towards the 5GC including the N2 and N3 interfaces, and as well the N1 interface on behalf of the FN-RG. The FN-RG is an RG not supporting 5G capabilities, e.g., the N1 interface.

The FMIF may be split into control plane, FMIF-CP, and user plane, FMIF-UP. The control plane and user plane separation (CUPS) of the FMIF is out of scope of this document.

This model can be used for the case that the migration completion is defined as the time that service providers are willing to stop using their deployed BNGs (wireline core network) and to start using the 5GC (assuming that the 5GC will be able to support all wireline access services) and as well as replacing all the FN-RGs with 5G-RG.

The 5G FMC architecture with FMIF must support both legacy services (that do not require the 5GC) and the converged services (that are delivered by the 5GC). As a result, there are two types of sessions, interworking sessions and coexistence sessions, managed by the BNG.

- The interworking sessions are for the services delivered by the 5GC, which are passed to the 5GC via the FMIF (see Figure 4-1). Such sessions do not use the separate AAA function shown but instead use the RADIUS connection to the FMIF which emulates a RADIUS server. These sessions will only be requested and established when there is such a service request from the FN-RG.
- The coexistence sessions are for the legacy services that do not require 5GC and are managed by the BNG only. These BNG sessions do not use the RADIUS connection to and services provided by the FMIF but instead use a logically separate AAA function as shown in Figure 4-1. These coexistence sessions also use the A10 interface that goes directly to the Data Network rather than to the FMIF (see Figure 4-1).

  Note: If the BNG supports both types of sessions at the same time, it determines which FN-RG sessions use the 5GC or legacy services. How this is implemented in the BNG is out of scope for this document.

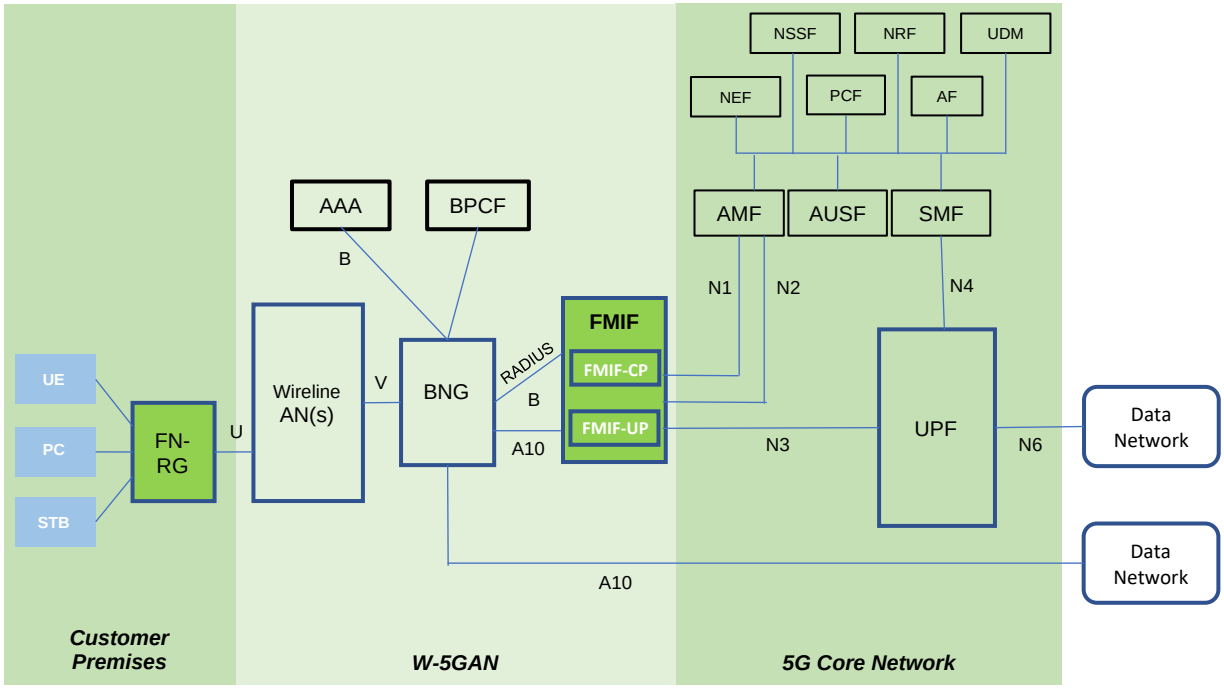

Figure 4-1: Architecture for interworking for FN-RG and for coexistence.

The service-based interfaces for 5GC are defined in TS 23.501 [21].

4.1 FMIF Interfaces

The BNG TR 178 [5] supports the V interface for FN-RG, which identifies the facility ID as signaled by the access network and authenticates the FN-RG (see Figure 4-1). The BNG supports existing VLAN tags and packet priority indication methods as defined by TR 101i2 [1].

The FMIF attached to a BNG shall support N1 and N2 interfaces for the UE located behind the BNG, and generate all the relevant N1 / N2 signaling for an FN-RG that has been identified / connected via the wireline access network (AN). In order to support this, RADIUS Interface (B) is used for control plane interaction between the BNG and FMIF.

The FMIF shall map each user plane connection from the BNG to a PDU session in the 5GC and provide relevant signaling on the N1 and N2 interfaces, and data on the N3 interfaces. The BNG-FMIF interaction support is depicted in Figure 4-1.

In particular, the FMIF:

- Acts as a RADIUS server to the BNG. Moreover, the FMIF gets via RADIUS Interface (B) the related status information from BNG.
- Maps 5GC information into RADIUS Vendor-Specific Attributes (VSAs) and User Plane state. RADIUS Interface (B) is also used to transport information, such as the Line ID (i.e., the identifier of the FN-RG), from the BNG towards the FMIF
- Maps each user plane connection from the BNG to a PDU session in the 5GC and vice versa
- Generates and terminates N1 on behalf of the FN-RG
- Generates and terminates all the relevant N2 signaling
- Generates and terminates N3 for GTP-u tunnel encapsulation and decapsulation

5 High-level requirements of an FMIF

The FMIF supports 3GPP 5G N1 on behalf of the FN-RG and 3GPP 5G N2 interfaces on behalf of the FN-RG and generates all the relevant 3GPP 5G N1 / 3GPP 5G N2 signaling for an FN-RG that has been identified and connected via the wireline access network. Moreover, the 5G-FMIF shall map each user plane Layer 3 (L3) connection from the BNG to a 3GPP 5G PDU session in the 5G Core network and provide relevant signaling on the 3GPP 5G N1, 3GPP 5G N2, and data on 3GPP 5G N3 interfaces.

The high-level requirements of an FMIF are the following ones:

[R-FN-1] The FMIF MUST support N1 as defined in TS 23.316 [20], TS24.501 [24] and modified in this Technical Report.

[R-FN-2] The FMIF MUST support N2 as defined in TS 23.316 [20], TS 23.501 [21], TS 29.413 [26] and modified in this Technical Report.

[R-FN-3] The FMIF MUST support N3 as defined in TS 23.316 [20], TS 23.281 [25] and modified in this Technical Report.

[R-FN-4] The FMIF MUST support RADIUS interface with BNG to support control signaling transmission.

[R-FN-5] The FMIF MUST support A10 interface with BNG to support user traffic transmission.

[R-FN-6] The FMIF MUST support the connection management for FN-RG connected to 5GC via W-5GAN as defined in TS 23.502 [22] clause 5.5.2.

6 Functional features and requirements

6.1 Authentication/Authorization/Identity management

In order to access the 5GC, each subscriber is allocated one 5G Subscription Permanent Identifier (SUPI) for use within the 3GPP system. The SUPI is the permanent identity which identifies the subscriber, and it is used only inside the 3GPP system. The privacy for SUPI is defined in 3GPP TS 33.501 [27] and in TS 23.003 [19]. The SUPI, in respect to the 5G system, is never provided by UE to the network element, but it is confined to the Core network and exchanged between the network functions in the core network. The UE in the procedure communicates its Subscription Concealed Identifier (SUCI). The exception is the case of Emergency Services where the identification of UE takes precedence over the privacy requirements.

[R-FN-7] The FMIF MUST generate the SUCI as defined in TS 23.003 [26] clause 2.2B and TR-470 [8] clause 7.5, and encode its parts as follows:
SUPI-type=2 (Global Line ID);
Home Network Identifier= corresponds the realm part of SUPI in NAI format;
Routing Indicator=0 (decimal digit);
Protection Scheme ID=0x0 (NULL scheme);
Scheme Output= corresponds the username part of Global Line ID. An operator may build GLI, as specified in TR-470 [8] clause 7.2, using the Line ID source and Line ID obtained by means of the Agent-Circuit-ID and Agent-Remote-ID RADIUS Attributes, as defined in RFC 4679 [15], received from the BNG.

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

SUCI Encoding for FN-RG in FMIF

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

[R-FN-8] The FMIF MUST encode the SUCI provided to 5G Core Network for an FN-RG using the null protection scheme as defined in TS 23.003 [26] and TS 33.501 [21] Annex C.

[R-FN-9] The FMIF MUST respond with “Access-Reject” to the BNG and report an error to management if a GLI cannot be generated for an FN-RG.

6.2 Security

The subsections below specify N1 (NAS), N2, and N3 (User Data Plane) security for the FMIF.

6.2.1 N1 (NAS) Security for FMIF

Procedures and requirements are as in Section 6.2.1 of TR-456i2 [7] with all occurrences of “AGF” replaced with “FMIF”.

6.2.2 N2 Security

Procedures and requirements are as in Section 6.2.2 of TR-456i2 [7] with all occurrences of “AGF” replaced with “FMIF”.

6.2.3 User Plane Data Security (N3)

Procedures and requirements are as in Section 6.2.3 of TR-456i2 [7] with all occurrences of “AGF” replaced with “FMIF”.

6.3 User Plane

The user plane tunnel encoding employed for PDU exchange between an FMIF and an FN-RG is based on the traditional wireline protocols documented in TR-101/178. The protocol stack used for user plane is shown in Figure 6-1.

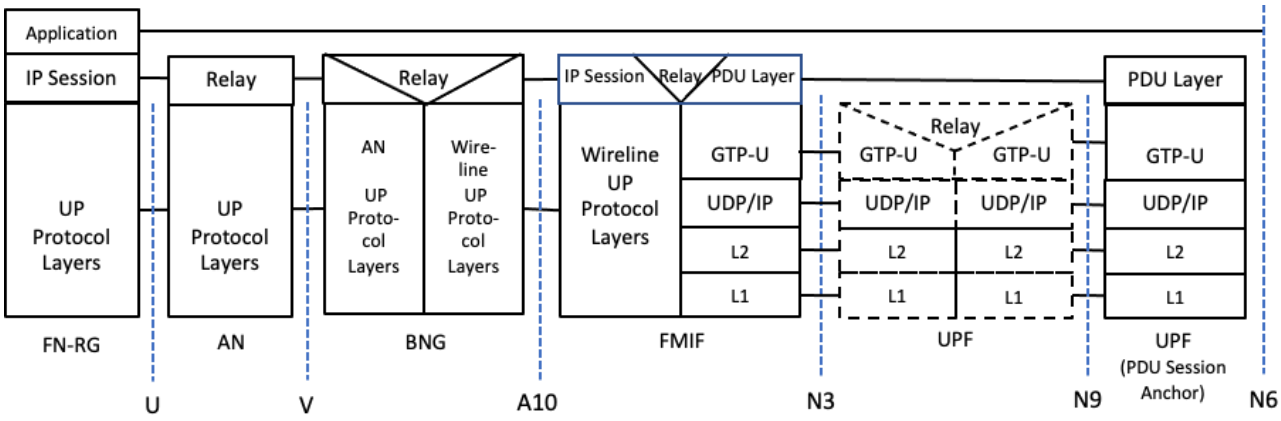

Figure 6-1: User Plane via FMIF for FN-RG

The user plane connection between FN-RG and FMIF follows the IP-session lifecycle management as defined in TR101/TR178 ([1]/[5]) and between an FMIF and UPF follows the PDU session management as defined in 3GPP TS 23.502 [22]. An FMIF proxies the FN-RG to establish the user plane tunnel by initiating PDU Session establishment according to the PDU Session information.

The BNG and FMIF are connected by the A10 interface. From the BNG point of view, the FMIF is treated as a “DN”. This makes sure that there will be no extra BNG functions required to support an FMIF.

Note: It is assumed that no IP network address translation between the BNG and FMIF.

A BNG can support converged sessions via the FMIF and legacy sessions directly to the DN by selecting which A10 interface to use. There could be multiple such legacy session A10 interfaces and multiple such converged session A10 interfaces each of which may require a different routing context. Which A10 interface to use for each FN-RG may be configured.

Note: Use of RADIUS to dynamically determine which A10 interface to use is FFS.

The FMIF is the mapping point between an IP session and a PDU session. The FMIF needs to map an IP session to a PDU session in the upstream direction and map a PDU session to an IP session in the downstream direction.

Since BNG and FMIF communicate through the A10 interface, the interworking at the FMIF is Layer 3 to Layer 3 model (L3/L3 Interworking), where an IP session is identified by IP address of the FN-RG which is assigned by the 5GC. The IP address of the FN-RG is the key for mapping between an IP session and a PDU session.

[R-FN-10] An FMIF MUST maintain a database for mapping between an IP session and a PDU session which contains a mapping relationship table between the set of IP addresses assigned to the FN-RG and that of the BNG, and another mapping relationship table among the IP address of the FN-RG, GTP-u tunnel ID (TEID) at the FMIF, and the GTP-u tunnel ID (TEID) at the UPF.

[R-FN-11] An FMIF MUST support allocating the TEID of a GTP-u tunnel at its FMIF endpoint to be used during PDU Session establishment.

[R-FN-13] An FMIF MUST support mapping an IP session to a PDU session based on the source IP address of the packets received from a BNG in the upstream direction and encapsulating the packets into a corresponding GTP-u tunnel with its TEID stored at the FMIF in the mapping relationship table in the database.

[R-FN-14] An FMIF MUST decapsulate the tunnel packets and send the IP packets to the BNG based on the destination IP address of the IP packets.

6.3.1 User Plane Maximum Transmission Unit (MTU) Considerations

Due to possible mismatch between the N3/N9/N6 interfaces MTU and A10 interface MTU, an FMIF might need to fragment and/or reassemble and perform path MTU processing. Fragmentation at the BNG and re-fragmentation at the FMIF is undesirable and means to avoid this are FFS.

[R-FN-15] The FMIF MUST support IP fragmentation and IP path MTU discovery for PDU sessions carrying IPv4 traffic upstream from the A10 interface towards an N3 interface.

[R-FN-16] A combined FMIF/UPF MUST support fragmentation and IP path MTU discovery for PDU sessions carrying IPv4 traffic upstream from an A-10 interface towards an N6 or N9 interface.

[R-FN-17] The FMIF MUST support the IPv6 Path MTU Discovery procedure as defined in RFC 8201 [18] as follows:

- For downstream IPv6 traffic of a PDU session exceeding a A10-interface limit, the FMIF generates an ICMPv6 Packet Too Big error message.
- The FMIF handles any ICMPv6 Packet Too Big message destined to one of its local GTP-U IP addresses to learn an MTU for the GTP-U peer. The FMIF MUST further enforce this MTU in one of the following ways:
  - By fragmenting the GTP-U packets toward the peer after encapsulation
  - By fragmenting upstream IPv4 traffic of a PDU session, generating an ICMP Packet Too big message for upstream IPv4 traffic of a PDU session, and by generating an ICMPv6 Packet Too big message for upstream IPv6 traffic of a PDU session.

[R-FN-18] The FMIF MUST support IP fragmentation and reassembly of GTP-U transport on the N3 interface.

[R-FN-19] Combined FMIF/UPF MUST support IP fragmentation and reassembly of GTP-U transport on the N9 interface.

Note that in order to avoid FMIF fragmenting or reassembling GTP-U PDUs, it is highly recommended that the nodes between UPF and FMIF have IPv4 or IPv6 MTUs large enough so that IP fragmentation is not required.

Note that in case of a need for fragmentation due to an intermediate tunnel with a limiting MTU, it is recommended traffic be fragmented at the end points. This will reduce the load of fragmenting and

reassembling traffic on the Tunnel Endpoints. This optimization can be adopted on N6 interface for the traffic to be tunneled on N3/N9 Interfaces by an UPF towards an FMIF.

[R-FN-20] A combined FMIF/UPF SHOULD constrain the upstream MTU to that of a local N6 interface for PDU sessions where the combined UPF is the ultimate UPF.

[R-FN-21] The FMIF interfaces MUST have configurable MTU.

[R-FN-22] An FMIF MUST constrain the upstream MTU to that of the transport MTU of the mobile network for any sessions relayed over an N3 or N9 interface.

[R-FN-23] The FMIF MUST be able to be configured with the transport MTU of the mobile network and use that value for upstream MTU processing.

6.3.2 QoS Marking Aspects

The following requirements apply to the FMIF:

[R-FN-24] The FMIF MUST only support Standardized and Pre-configured 5QI values, i.e., support Non-dynamic 5QI Descriptors as defined in TS 38.413 [28] clause 9.3.1.28, without the optional parameters.

[R-FN-25] For each PDU session, the FMIF MUST derive and maintain an up-to-date list of QFI and DSCP mapping pairs for downstream traffic and QFI and DSCP mapping pairs for upstream traffic. For this, the FMIF MUST use the mapping information in the RG-LWAC and the QFI-5QI mapping information received from the 5GC, in QoS flow management related messages (N2 PDU session resource setup/modification/release requests).

[R-FN-26] If downstream remarking of IP DSCP is indicated by either local configuration or the RG-LWAC marking controls TLV, the FMIF MUST remark the IP packet with the configured DSCP for the 5QI.

[R-FN-27] The FMIF MUST mark the IP DSCP of downstream traffic sent on the A-10 interface to correspond to the traffic class for the 5QI of the packet. This may be:

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

[R-FN-28] If upstream remarking of IP DSCP is indicated by either local configuration or the RG-LWAC marking controls TLV the FMIF MUST remark the IP packet with the configured DSCP for the 5QI.

[R-FN-29] If upstream remarking of IP DSCP of the GTP-U encapsulated packet on N3 is indicated by local configuration the FMIF MUST remark the IP Header of the GTP-U encapsulated IP Packet on the N3 interface with the configured DSCP for the 5QI.

[R-FN-30] If upstream reflection of IP DSCP is indicated by local configuration, the FMIF SHOULD remark the IP Header of the GTP-U encapsulated IP Packet on the N3 interface with the IP DSCP of the incoming packet.

6.4 Control Plane

The FMIF Control Plane communicates with the 5GC and BNG as shown in Figure 6-2.

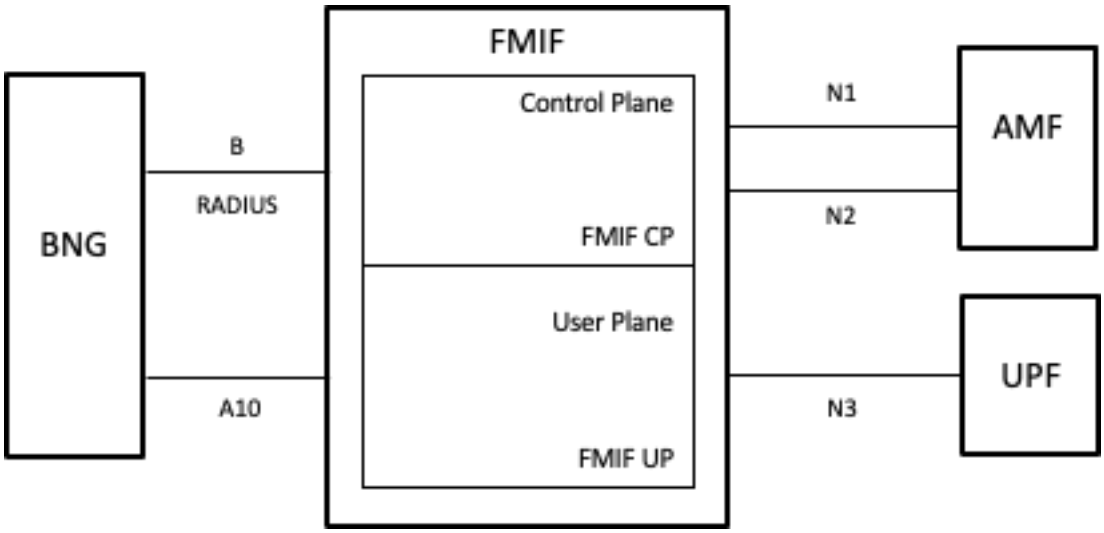

Figure 6-2: FMIF Control Plane

6.4.1 Modes of BNG Interworking with FMIF

A BNG connected to an FMIF (via the B (RADIUS) and A10 interfaces) can support PPPoE and DHCP subscribers as listed below. If the RADIUS Access-Request Message has the Framed-Protocol Attribute with the value 1 (PPP), then the first PPPoE case below applies. Otherwise, the second DHCP case applies.

- In the case of PPPoE subscribers, the BNG terminates the PPPoE session and IPv4 address assignment is obtained using NAS messaging and communicated to the BNG via attributes in the RADIUS Access-Accept Message (see 6.4.2.2). For IPv6 over PPPoE, a Router Advertisement (RA) prefix is communicated in the RADIUS Access-Accept Message (see 6.4.2.2) and the BNG acts as a Stateful DHCPv6 relay (see below).

- For DHCP clients, then one of the following two cases apply:
  - The BNG acts as a stateful DHCP/DHCPv6 relay for IPv4 and/or IPv6, and those messages are forwarded by the FMIF between the BNG and the UPF.
  - The BNG acts as in the previous point for DHCPv6 but acts as a DHCP server for IPv4 obtaining the IPv4 address via RADIUS. To perform IPv4 address assignment in this fashion, the FMIF is configured for such cases to obtain that IPv4 address using NAS messaging.

[R-FN-31] To support IPv4 sessions, the BNG MUST be configured with an IPv4 address to reach the DHCP server.

[R-FN-32] To support IPv6 sessions, the BNG MUST either use the IPv6 All_DHCP_ Servers multicast address or be configured with an IPv6 address to reach the DHCPv6 server.

[R-FN-33] The FMIF MUST snoop DHCP and DHCPv6 control packet exchanges and track the client identifier and/or line-id and any addresses or prefixes assigned to the client.

The FMIF is not a full DHCP relay but is a lightweight snooping forwarder. It will have the Line ID from the RADIUS Access-Request Message and can match this against the Line ID in the options carrying the Line ID in DHCP/DHCPv6 upstream messages to determine the mapping between the subscriber IP (Src IP) and the N2 Tunnel towards the UPF in the upstream direction.

6.4.2 FMIF-5GC Control Plane

An FMIF proxies 5G control plane connectivity for a FN-RG connected to that FMIF through a BNG. The protocol stack used as shown in Figure 6-3.

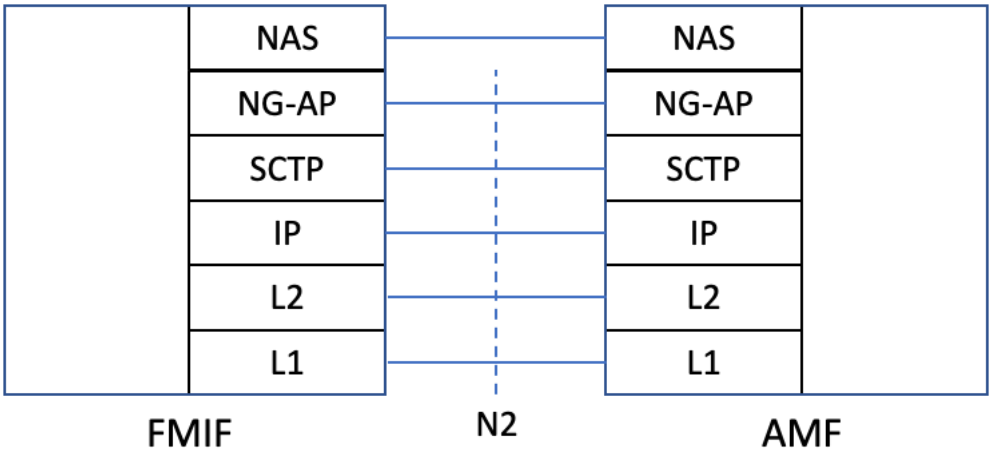

Figure 6-3: N2 Control Plane

The FMIF treats the IP session initiation, discussed in Section 6.11, as a trigger to perform a proxy registration for the FN-RG and establishes the NAS connection with the AMF where the NAS message overlays the N2 interface as defined for 5G-RG.

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

Session and Service Continuity (SSC) mode 2 and SSC mode 3 (TS 23.501 [21]) require behaviors in PDU session life cycle management that cannot be coordinated with an FN-RG. Therefore, for FN-RG support, SSC mode 1 is used.

[R-FN-34] An FMIF initiating a PDU session in response to an FN-RG IP session trigger MUST request SSC mode 1 (TS 23.501 [21]).

6.4.3 FMIF-BNG Control Plane

RADIUS (RFC 2865 [11]) is used in the AAA control plane between the BNG and the FMIF as shown in Figure 6-4. RADIUS is the only mechanism for the FMIF to get triggers from the BNG and the only way for the FMIF to control the BNG. The FMIF acts as a RADIUS authentication server (RFC 2865 [11]), a RADIUS accounting server (RFC 2866 [12]), and a RADIUS dynamic authorization client (RFC 5176 [16]).

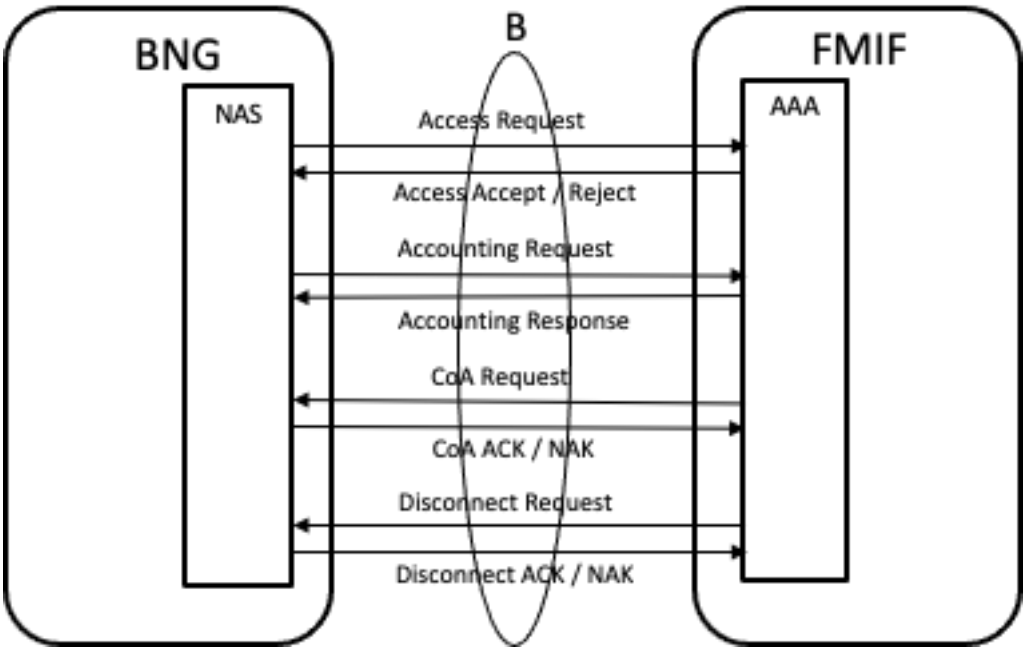

Figure 6-4: BNG-FMIF Control Plane Messages

The table below summarizes RADIUS messages including those used to implement the FMIF-BNG control plane.

FMIF – BNG RADIUS Message Summary			
From BNG to FMIF		**Meaning**	
	Access-Request		IP session initiation from the BNG
	Accounting-Request / Interim-Update		Report incremental accounting information Acknowledged but ignored by FMIF
	Accounting-Request / Off		Accounting not being supported Acknowledged but ignored by FMIF
	Accounting-Request / On		Accounting being supported Acknowledged but ignored by FMIF
	Accounting-Request / Start		IP Session has been started
	Accounting-Request / Stop		IP Session Release as requested by BNG / FN-RG
	CoA-ACK		Change IP session parameters success
	CoA-NAK		Change IP session parameters failure
	Disconnect-ACK		Terminate IP session success
	Disconnect-NAK		Terminate IP session failure
From FMIF to BNG		**Meaning**	
	Access-Accept		FN-RG session authenticated
	Access-Challenge		Part of CHAP authentication

	Access-Reject		FN-RG session rejected
	Accounting-Response		Confirms receipt of Accounting-Request
	CoA-Request		Change session parameters
	Disconnect-Request		IP Session Release requested by FMIF / 5GC

Table 1: FMIF-BNG RADIUS Message Summary

RADIUS messages begin with a fixed size header that indicates the message type, message identifier (to aid in matching requests and replies), and a 16-byte Authenticator field; all other information is encoded as type-length-value attributes. The BNG is assumed to meet the RADIUS support requirements given in TR-101 issue 2 [1]. All attributes whose use is required by this document are listed in TR-341 [6] as being standardized by the IETF or the BBF and are supported by BNGs; however, some of these may, in any particular BNG implementation, use a different, possibly vendor specific attribute ID to indicate that attribute.

[R-FN-35] An FMIF MUST be configurable as to the attribute IDs, including vendor specific IDs, it accepts to identify any particular attribute value whose support is required by this document.

[R-FN-36] RADIUS messages in both directions between the BNG and the FMIF MUST include all IETF and BBF attributes listed in Sections 4 and 5 of TR-341 [6] whose occurrence is required by TR-341 (i.e., have an occurrence count with a minimum of “1”) and MUST NOT include any such attributes prohibited by TR-341 (i.e., whose occurrence count is “0”).

Other text in this document may require or prohibit the inclusion in RADIUS messages between the FMIF and the BNG of attributes whose inclusion TR-341 [6] indicates as optional.

With the 5GC, accounting is actually performed by the UPF. The FMIF acts as if it is a RADIUS accounting server so that RADIUS accounting messages can be used for control purposes between the FMIF and the BNG but there is no need for the FMIF to perform actual accounting.

6.4.3.1 RADIUS Access-Request

The BNG sends a RADIUS Access-Request message to the FMIF to authenticate the RG and start an IP session. Such an Access-Request message includes any AN parameters (see TS 24.502 Table 9.3.2.2.2-3) needed by the FMIF either directly or through information from which the needed AN parameters can be derived. Other AN parameter information may be configured at the FMIF. If the FMIF is using CHAP, it responds with a RADIUS Access-Challenge message.

[R-FN-37] The BNG MUST be configured to include both the Agent-Circuit-ID attribute and the Agent-Remote-ID attribute (RFC4679 [15]) in RADIUS Access-Request messages to the FMIF and the FN-RG MAC address as the value of a Calling-Station-Id attribute (RFC 2865 [11]).

[R-FN-38] When a RADIUS Access Request message is received, the FMIF MUST store the identity of the FN-RG for the duration of any resulting registration. This includes the FN-RG MAC address in the value of the Calling-Station-Id attribute (RFC 2865 [12]).

[R-FN-39] The BNG MUST be configured to include the Framed-Protocol Attribute in RADIUS Access-Request Messages with a protocol value of 1 (PPP) for PPPoE clients.

The FMIF acts as a proxy and performs authentication with the 5GC. If 5GC authentication succeeds, an Access-Accept message is returned to the BNG; otherwise, an Access-Reject message is returned to the BNG. If no response with a correct Response Authenticator is received for a RADIUS Access-Request message, it is retransmitted as in usual RADIUS practice.

Note: Communication of parameters to the BNG in RADIUS messages is FFS.

6.4.3.2 RADIUS Access-Accept, Access-Reject

If authentication and authorization checks succeed, the FMIF returns a RADIUS Access-Accept message to the BNG in response to the BNG's RADIUS Access-Request. The attributes in the Access-Accept provide the configuration information needed by the BNG to provide service to the customer.

- In the case of a PPPoE client of the BNG, this includes the address(es) assigned to the FN-RG by the 5GC with any IPv4 address in a Framed-IP-Address attribute (RFC 2865 [11]) and any IPv6 address Framed-Interface-Id attribute (RFC 3162 [14]). For an IPv6 PPPoE client, the RADIUS Access-Accept message is delayed until a Router Advertisement (RA) is received by the FMIF and any /64 IPv6 prefix received in an RA is included in that Access-Accept message in a Framed-IPv6-Prefix attribute (RFC 3162 [15]).
- In the case of a DHCP client of the BNG, the IPv6 address assigned to the FN-RG by the 5GC are not included in the RADIUS Access-Accept but discovered by the client using DHCPv6. And, in this case, IPv4 address is similarly discovered using DHCP unless the BNG is acting as a DHCP server in which case the FMIF is configured to provide the clients IPv4 address to the BNG as in the PPPoE case.

If authentication and authorization checks fail, the FMIF returns a RADIUS Access-Reject message to the BNG in response to the BNG's RADIUS Access-Request. Only Proxy-State and an optional text message attributes are allowed in an Access-Reject message.

6.4.3.3 RADIUS Access-Challenge

The FMIF sends a RADIUS Access-Challenge message to the BNG in response to a RADIUS Access-Request message if the FMIF is requiring CHAP authentication. If the BNG is configured to support CHAP for the FMIF, this prompts the BNG to send a new RADIUS Access-Request message in response to the challenge including the State attribute from the Access-Challenge and the challenge response value in the User-Password attribute. This credential is validated by the FMIF against configured or AANI information in the RG-LWAC. If the BNG is not configured to support CHAP for the FMIF, the BNG treats the RADIUS Access-Challenge message as an Access-Reject message.

6.4.3.4 RADIUS Accounting-Request

All RADIUS Accounting-Request messages are from the BNG to the FMIF and include the Acct-Status-Type attribute whose value determines the sub-type of Accounting-Request as follows: Start, On, Interim-Update, Off, and Stop. These sub-types are discussed below.

6.4.3.4.1 Accounting-Request / Start / Interim-Update / Stop

An Accounting-Request / Start message is sent by the BNG to the FMIF to indicate that it has begun providing service to the customer.

An Accounting-Request / Interim-Update message [RFC2869] is used after an Accounting-Request / Start and before an Accounting-Request / Stop to send cumulative interim usage statistics to the FMIF. Since the FMIF is not actually doing accounting, this message is useless in the BNG to FMIF context. The RADIUS accounting server can indicate it wishes to receive Interim-Updates by including the Acct-Interim-Interval RADIUS attribute (RFC 2869 [13]) in its Access-Accept message to the BNG.

[R-FN-40] The FMIF MUST NOT request RADIUS Accounting-Request / Interim-Update messages and MUST ignore such messages other than to acknowledge them with an Accounting-Response message.

An Accounting-Request / Stop message is sent by the BNG to the FMIF to indicate that it has ceased proving service to the customer. This message may include usage statistics, but these will be ignored by the FMIF as the FMIF is not actually doing accounting.

6.4.3.4.2 Accounting-Request / On / Off

An Accounting-Request / On message indicates that the BNG is supporting accounting. An Accounting-Request / Off message indicate that accounting is not being supported. Since the FMIF is not actually doing accounting, the following requirement applies.

[R-FN-41] The FMIF MUST ignore RADIUS Accounting-Request / On and Accounting-Request / Off messages other than to acknowledge them with an Accounting-Response message.

6.4.3.5 RADIUS Accounting-Response

The RADIUS Accounting-Response message is sent from the FMIF to the BNG to acknowledge the receipt of an Accounting-Request message. Lack of an acknowledgement with a correct Response Authenticator field causes request re-transmission as in normal RADIUS practice. An Accounting-Response message is not required to have any attributes in it.

6.4.3.6 RADIUS CoA-Request, CoA-ACK, and CoA-NAK

A RADIUS CoA-Request (Change-of-Authorization Request) message is sent by the FMIF to the BNG to dynamically change customer IP session authorizations and/or parameters. Because the FMIF is originating the request to the BNG, the FMIF is said to be acting as a Dynamic Authorization Client (RFC 5176 [16]). A CoA-Request message may include RADIUS Filter-ID (11) and/or NAS-Filter-Rule (92) attributes.

If all requested changes are completed successfully, the BNG sends the FMIF a CoA-ACK message to acknowledge receipt and successful completion of the CoA-Request message. If any requested change cannot be completed, then none of the requested changes are made and a CoA-NAK message is returned to the FMIF to acknowledge receipt of the unsuccessful CoA-Request message. Lack of a CoA-ACK or CoA-NAK with a correct Response Authenticator field causes request re-transmission of the CoA-Request as in normal RADIUS practice.

6.4.3.7 RADIUS Disconnect-Request, Disconnect-ACK, and Disconnect-NAK

A RADIUS Disconnect-Request message is sent from the FMIF to the BNG to terminate customer IP sessions(s) on the BNG and discard all associated session context. Because the FMIF is originating the request to the BNG, the FMIF is said to be acting as a Dynamic Authorization Client (RFC 5176 [16]). A Disconnect-Request message can include only NAS and session identification attributes; if any other attributes are included, the Disconnect-Request fails and a Disconnect-NAK is returned.

If all associated session context was discarded and the customer session(s) are no longer connected, the BNG sends the FMIF a Disconnect-ACK message to acknowledge receipt and successful completion of the Disconnect-Request message; a Disconnect-ACK message may contain the Acct-Terminate-Cause (49) attribute with value set to 6 for Admin-Reset. If the BNG was unable to disconnect one or more IP session and discard all associated session context or if the Disconnect-Request included a disallowed attribute, the BNG sends the FMIF a Disconnect-NAK message to acknowledge receipt of the unsuccessful Disconnect-Request message. Lack of a Disconnect-ACK or Disconnect-NAK with a correct Response Authenticator field causes request re-transmission of the Disconnect-Request as in normal RADIUS practice.

6.5 QoS

6.5.1 RG level QoS Provisioning

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

For 5G WWC similar QoS mechanisms are expected on a per-subscriber or RG-level basis for wireline access to accommodate legacy FN-RG QoS characteristics. This means the FMIF will accept QoS characteristics from the 5GC, transmitting them to the BNG to apply and enforce, with the BNG communicating relevant upstream information to the FN-RG to enforce. To configure the QoS characteristics of the legacy access networks on the BNG and FMIF, the FMIF receives information from the 5GC known as the RG-Level Wireline Access Characteristics (RG-LWAC). As noted in TS 23.316 [20] , these parameters are transparent to the 5GC; it neither interprets nor acts on these parameters, thereby preserving existing 3GPP behavior. The RG-LWAC thus serves as means to map 5G QoS management to a wireline access model; the FMIF in turn communicates QoS characteristics to the BNG using RADIUS CoA-Request messages.

RG-Level Wireline Access 5G QoS Characteristics

This part of TR-457 is the same as the “RG-Level Wireline Access 5G QoS Characteristics” part of TR-456i2 with “AGF” replace with “FMIF” and “UE” replaced with “RG”.

Note: Applicability and communication of RGLWAC components is FFS.

PDU Session Level QoS Characteristics

TS 23.316 [20] specifies that each PDU Session of a FN-RG may be configured with a Session-AMBR that limits the aggregate bandwidth for all Non-GBR QoS Flows for the Session. This is retrieved from the UDM via the SMF during Session Initiation and signaled to the UPF over N4. These QoS characteristics are enforced on the UPF. For a collocated FMIF and UPF, the PDU session appears as an additional scheduling layer in the QoS hierarchy. For a stand-alone FMIF, Session-AMBR is only enforced at the UPF.

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

[R-FN-42] The FMIF SHOULD support GBR QoS flows for FN-RG, if the QoS flow includes only DL traffic filters. In this case, functionality equivalent to TR-456i2 [7] requirements [R-5G-50], [R-5G-51], and [R-5G-52] is to be supported.

Network Access Model

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

QoS Representation on FMIF

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

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

6.6 FMIF functions for core network signaling

A descriptive summary and requirement is provided in Section 6.6 (AGF functions for core network signaling) of TR-456i2 [7] with "AGF" replaced by "FMIF".

6.7 N2 connections

N2 connection support requirements are as specified in TR-456i2 [7] Section 6.7 with "AGF" replaced by "FMIF".

6.8 FMIF support for slicing and AMF selection

Support for slicing and AMF selection requirements is as specified in TR-456i2 [7] for FN-RG only, that is Section 6.8 of TR-456i2 with

1. "AGF" replaced by "FMIF", and
2. all "R-5G" requirements and requirement [R-FN-45] deleted.

6.9 Connection Management State on FMIF

Connection Management State on the FMIF and its requirements are as specified in TR-456i2 [7] for FN-RG (i.e., an AGF operating in adaptive mode) with all occurrences of "AGF" replaced by "FMIF" and Figure 21 in TR-456i2 [7] replaced with Figure 6-5 below.

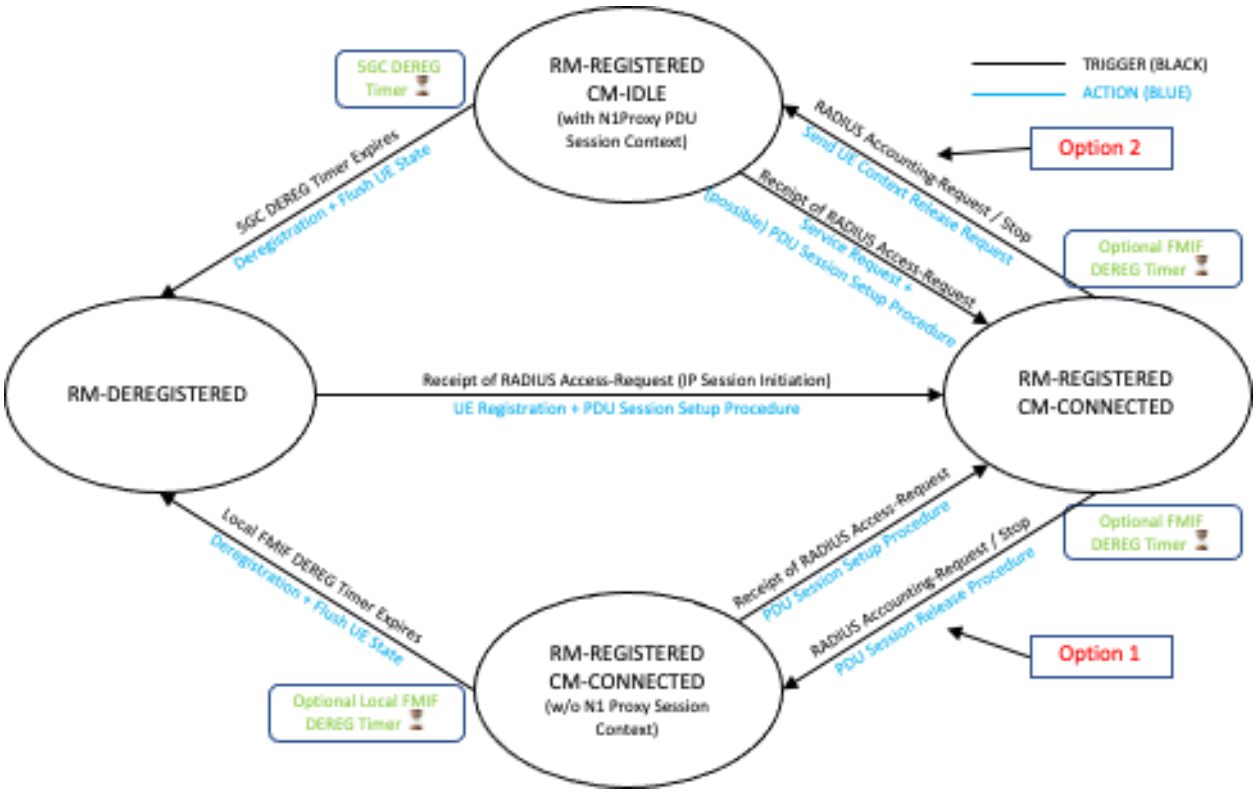

Figure 6-5: RM/CM State Transitions

6.10 Detection of FN-RG equipment change

FN-RG equipment change is detected by the BNG. The BNG signals this to the FMIF with the RADIUS Accounting-Request/Stop message as it does for session termination for any reason. On receipt of this message, the FMIF performs the FN-RG deregistration procedures if the FMIF is in the RM-REGISTERED state. The FMIF does not need to know why the session was terminated.

6.11 FN-RG IP session initiation requirements

The following requirements apply when an FMIF is involved in the FN-RG IP session initiation procedures:

[R-FN-43] The FMIF, when formulating the PDU SESSION ESTABLISHMENT REQUEST documented in clause 7.3.4 of TS 23.316 [20] on behalf of an FN-RG, MUST determine the PDU Session Type by a local configuration.

[R-FN-44] When establishing the PDU session, the FMIF MUST conform to the Selected PDU Session Type indicated by the PDU SESSION ESTABLISHMENT ACCEPT received from the 5GC.

[R-FN-45] With regards to [R-FN-44], if the selected PDU session type is IPv4, the 5GC provides an IPv4 address to the FMIF, and then the FMIF passes this IPv4 address to the BNG as the value of a Framed-IP-Address RADIUS attribute (Section 5.8 of RFC 2865 [11]).

[R-FN-46] With regards to [R-FN-44], if the selected PDU session type is IPv6, the 5GC provides an IPv6 Interface Identifier to be assigned to FN-RG to the FMIF as well as an SMF LLA information

element, and then the FMIF passes this IPv6 Interface Identifier to the BNG as the value of a Framed-Interface-Id RADIUS attribute (Section 2.3 of RFC 3162 [14]).

[R-FN-47] With regards to [R-FN-44], if the selected PDU session type is IPv4v6, the FMIF will use Framed-IP-Address and Framed-Interface-Id RADIUS Attributes to pass the information received from the 5GC in the PDU SESSION ESTABLISHMENT ACCEPT to the BNG.

[R-FN-48] If the FN-RG allowed session type is IPv6 or IPv4v6, the FMIF SHOULD forward any Router Solicitation sent by the FN-RG to the 5GC.

[R-FN-49] If the Router Solicitation sent by the FN-RG as specified in [R-FN-48] contains the Source Link-Layer Address Option, the FMIF SHOULD remove it before sending the message to the SMF.

[R-FN-50] The FMIF MUST relay the DHCPv6 messages exchanged between 5GC and the FN-RG if the session type is IPv4v6 or IPv6.

Note: [R-FN-48], [R-FN-49], and [R-FN-50] apply to both session initiation and maintenance throughout session lifetime

For FN-RG procedures, the Line ID information is a requirement for Registration and PDU Session Initiation. As described in TR-470 [8] Section 7.1, the Line ID is derived from metadata added by deployed access equipment that allows the client-facing interface to be identified. This metadata information is inserted by the Access Node in every eligible message transmitted by the FN-RG to the BNG to initiate an IP session (including PPPoE PADI and PADR, Router Solicitation, DHCPv4 control packets such as DISCOVER, REQUEST, etc. and DHCPv6 control packets such as SOLICIT, REQUEST, etc.). The BNG in turn includes this information in its RADIUS Access Request to the FMIF.

At most one IPv4 and one IPv6 stack per FN-RG are allowed and only one PDU session per FN-RG is supported. To accomplish that it is necessary for the FMIF to limit to one the number of PDU sessions requested from the 5GC, independently of the number of stacks requested by the FN-RG. This means the first requested stack triggers, via the BNG, the PDU session establishment for the one PDU session, the second stack (if allowed) will share the same PDU session.

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

Once in RM-REGISTERED state, the FN-RG may transition between CM-IDLE and CM-CONNECTED states as explained in TR-456i2 [7].The transitions may be triggered by detected changes in the wireline connectivity by BNG, causing the BNG to send RADIUS Accounting-Request / Stop messages to the FMIF.

If the FN-RG state is RM-REGISTERED/CM-CONNECTED on the FMIF, it means the FMIF has in place at least an IP session mapped to a PDU session.

The following requirements codify the description above:

[R-FN-51] The FMIF MUST limit the PDU sessions in place for an FN-RG to one.

[R-FN-52] The FMIF MUST be able to map the IPv4 and IPv6 IP sessions initiated by the same FN-RG to a common IPv4v6 PDU session.

[R-FN-53] If the FN-RG state is RM-DEREGISTERED on the FMIF, and if the BNG receives a message initiating an IP session (and in the case of PADI, subsequent exchange until the RG type can be ascertained by LCP exchange) and sends a RADIUS Access-Request message to FMIF, the FMIF MUST perform the Registration and the PDU session establish procedures on behalf of the FN-RG.

[R-FN-54] If the FN-RG state is RM-REGISTERED/CM-IDLE, if the BNG receives a message initiating an IP session and the customer equipment identifier is the same used for the Registration, then the FMIF SHOULD perform the Service Request procedure on behalf of the FN-RG in response to a RADIUS Access Request message from the BNG.

[R-FN-55] If the FN-RG state is RM-REGISTERED/CM-IDLE, when the FMIF detects a session initiation from the BNG through the receipt of a RADIUS Access Request message from the BNG, the FMIF SHOULD perform the Service Request procedure on behalf of the FN-RG.

[R-FN-56] When negotiating the stacks for the FN-RG, the FMIF MUST conform to the Selected PDU Session Type indicated by the PDU SESSION ESTABLISHMENT ACCEPT received from the 5GC.

[R-FN-57] While the FN-RG state is RM-REGISTERED/CM-CONNECTED on the FMIF, if the FMIF has in place an IP session mapped to an IPv4v6 PDU session and receives from the FN-RG a message initiating a different stack, the FMIF MUST add the second stack to the mapping as per [R-FN-52].

[R-FN-58] While the FN-RG is in the RM-REGISTERED state on the FMIF, if the FN-RG has initiated an IPv6 session via an RS or a DHCPv6 Solicitation to the BNG and in the PDU SESSION ESTABLISHMENT ACCEPT the 5GC indicates that FN-RG is not allowed to use the IPv6 stack (Selected PDU Session Type=IPv4), the FMIF SHOULD not deregister the FN-RG.

[R-FN-59] While the FN-RG is in the RM-REGISTERED state on the FMIF, if the FN-RG has initiated an IPv4 session via a DHCPv4 Discover to the BNG and in the PDU SESSION ESTABLISHMENT ACCEPT the 5GC indicates that FN-RG is not allowed to use the IPv4 stack (Selected PDU Session Type=IPv6), the FMIF SHOULD not deregister the FN-RG.

6.12 Void

This section is intentionally blank.

7 Co-Location Options

7.1 Co-located FMIF and UPF

The FMIF is defined as a logical function. Implementing the FMIF and UPF in separate physical 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 FMIF and an UPF as a combined implementation. The combined FMIF/UPF supports the following external interfaces: N1, N2, N3, N4, N6, N9, B, and A10 interfaces. The internal N3 interface and whether any kind of tunneling is needed are left for implementation.

The combination of UPF with FMIF 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 FMIF/UPF. As a consequence, the combined FMIF/UPF still offers an external N3 interface on FMIF for sessions that do not use UPF co-location or require capabilities not available in the co-located/combined implementation. See Figure 7-1 (N9 interface omitted).

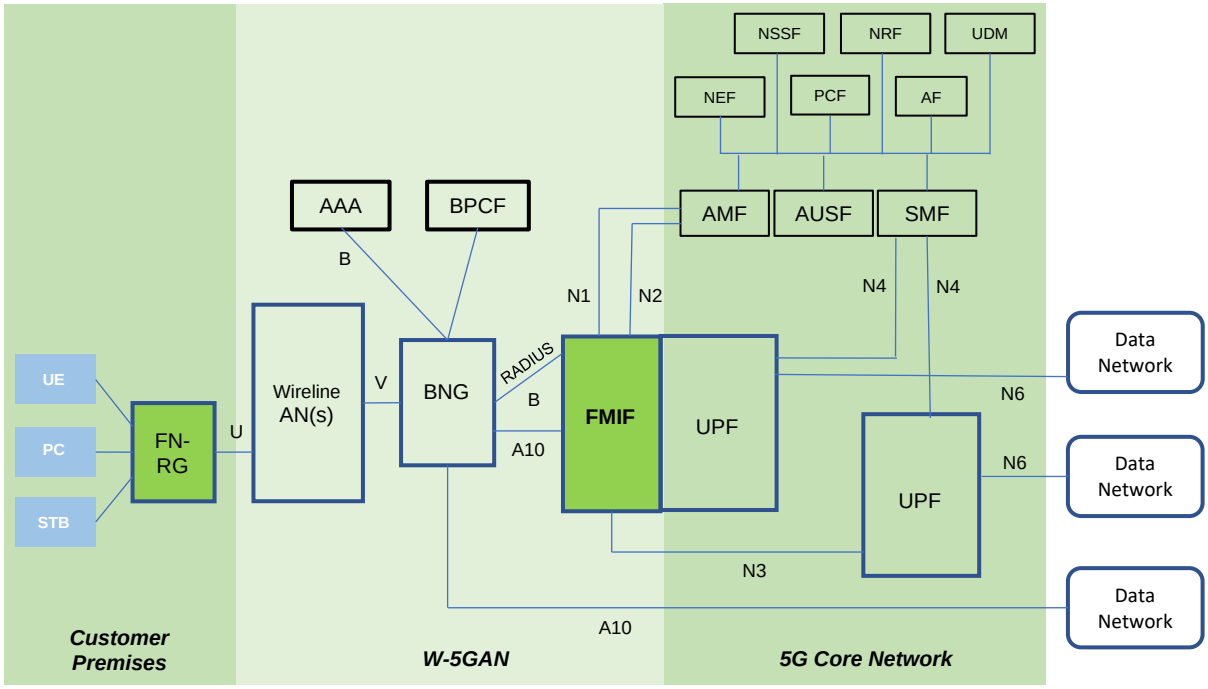

Figure 7-1: Co-Located FMIF and UPF Architecture

UPF selection is provided by the SMF. Hence the SMF decides if a PDU session uses the co-located UPF. The FMIF provides information that is used by the SMF to understand that this FMIF instance supports a co-located UPF. During PDU session establishment request, the FMIF sends the FMIF identity parameters to the AMF. The AMF relays FMIF identity parameters to the SMF, which can then select the co-located UPF. The SMF is aware of UPF co-location with FMIF either based on local configuration or with the assistance of NRF (the FMIF information being stored as part of the UPF NF profile). If the SMF selects the co-located UPF, the

FMIF receives the UPF information from the SMF that matches the co-located UPF and then uses the internal N3 interface.

UPF co-location still allows the option of network slicing. The FMIF and collocated UPF form a convergence slice themselves for a particular group of subscribers as the collocated UPF can also support wireless access. This also does not preclude the case of using different, and/or chaining with more, UPFs that are part of the slice.

[R-FN-60] The FMIF SHOULD support UPF co-location (a.k.a. Combined FMIF/UPF).

[R-FN-61] When the FMIF supports UPF co-location, the requirements below apply:

[R-FN-62] The FMIF MUST support sending FMIF identity parameters to AMF over N2, as part of session management, as described in TS 23.316 [20] Section 7.1.

[R-FN-63] The FMIF MUST support UPF as specified in 3GPP TS 23.501 [27], based on the specific aspects linked to wireline access described in 3GPP TS 23.316 [20].

[R-FN-64] The FMIF MUST support a regular N3 interface to support the case where SMF does not select the co-located UPF.

7.2 Co-located FMIF and BNG

An FMIF co-located with BNG as shown in Figure 7-2 is based on implementing FMIF combined with BNG. The result has the same requirements and capabilities as an AGF (TR-456i2 [7]) that only implements adaptive mode integration except that it also supports co-existence sessions.

Practically, the co-located FMIF can be implemented by upgrading existing BNGs with additional mechanisms and interfaces to support convergence. In particular, the 5G core will terminate N1, N2 and N3 interfaces from the co-located FMIF, identically as from a standalone FMIF. However, the interface between the BNG and FMIF is internal and left to vendors implementation, while the standalone FMIF is subject to interoperability with external BNG instances.

There are several advantages related to FMIF co-location. The reuse of the BNG installed base may be less costly than acquiring new platforms. Operationally it could be less disruptive to add the FMIF function to an existing node rather than deploying and integrating new nodes. The combined implementation could include some beneficial performance optimizations (e.g., lack of tunneling overhead).

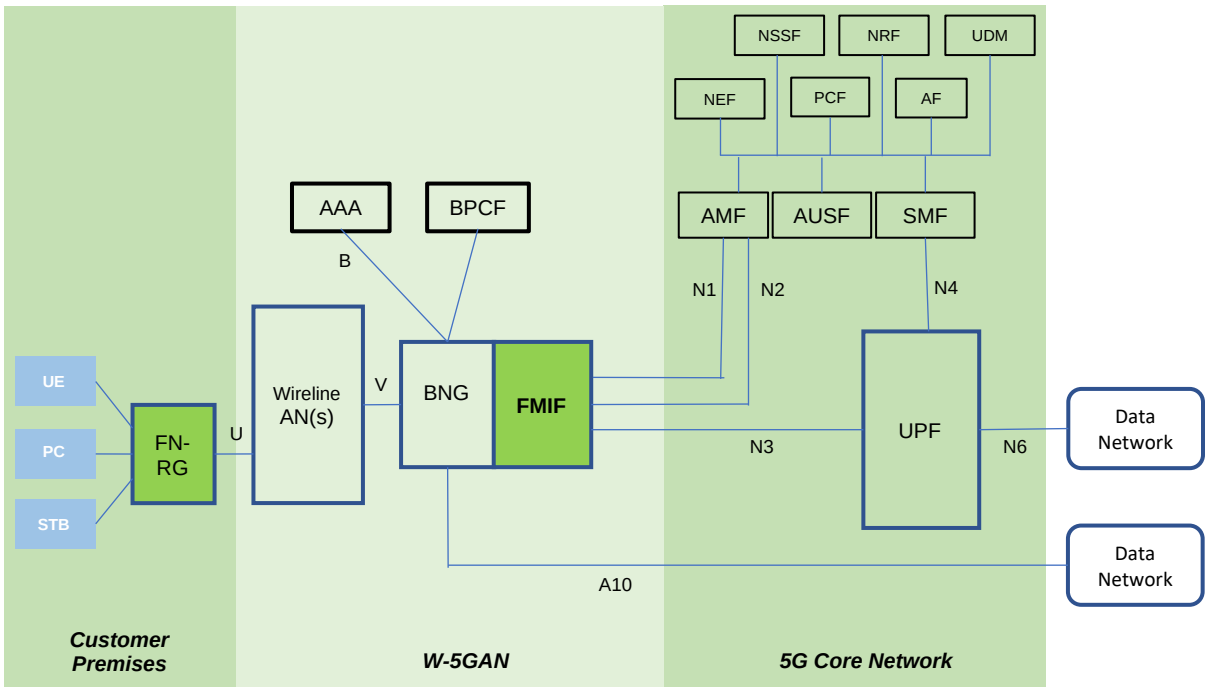

Figure 7-2: Co-located FMIF and BNG Architecture

As specified in clause 4 of this document, there are two types of sessions managed by the co-location of FMIF and BNG: interworking sessions and co-existence sessions. The interworking sessions use the N1, N2, and N3 interfaces connected to the 5G core network, as with an AGF, while the co-existence sessions use the A10, AAA, and BPCF interfaces and can be implemented in the BNG functionality of the co-located FMIF and BNG. The same configuration method can be used to selected whether a customer gets an interworking or a co-existence session as is used for a standalone BNG.

8 Procedures call flows

8.1 FN-RG IP Session Initiation with PPPoE

The following figure shows the call flow procedures of FN-RG IP session initiation with PPPoE.

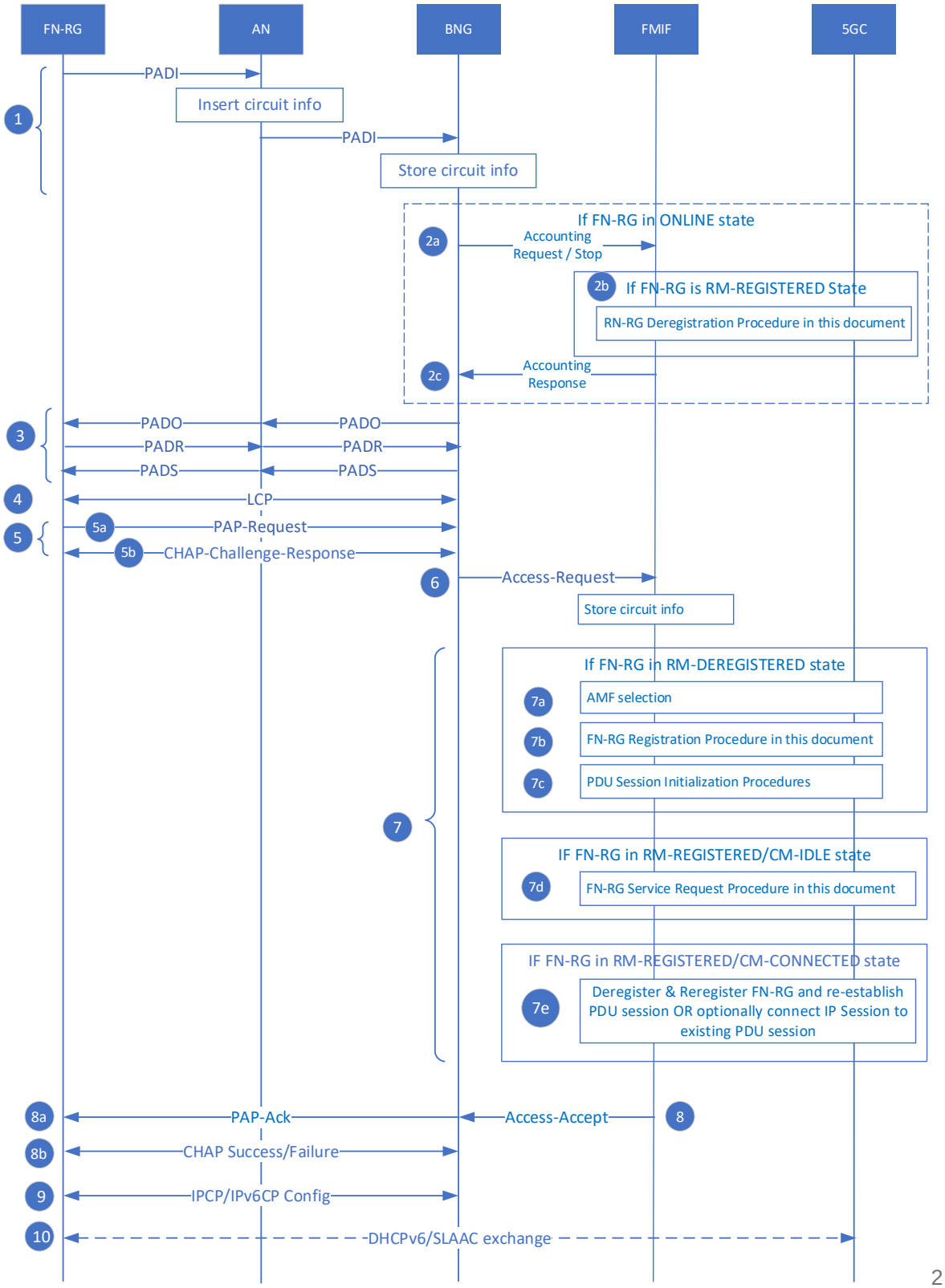

Figure 8-1: FN-RG IP Session Initiation with PPPoE

1. The FN-RG starts a PPPoE session and begins with a PADI message based on Section 5 of RFC 2516 [10].

   The AN receives the PPPoE PADI message and inserts PPPoE tags into the PADI message, then forwards the entire message to the BNG. The PPPoE tags include the PPPoE Circuit and Remote ID tags as defined in TR-101 issue 2 [1]. These PPPoE tags are treated as the Line ID as specified in TR-470 [8].

   On receving the PADI message, the BNG will store the subscriber's information (FN-RG MAC address, TCI (Tag Control Information), & Line ID) obtained from the Ethernet header and PPPoE tags.

2. The BNG and FMIF will handle the IP session according the current state of the FN-RG:

   2a. If the FN-RG is in the ONLINE state at the BNG, the BNG will send a RADIUS Accounting-Request / Stop message to the FMIF to release the IP session.

   2b. When the FMIF receives the Accounting-Request / Stop message, if the FN-RG is in the RM-REGISTERED state, the FMIF will initiate the FN-RG Deregistration Procedure described in this document and proceed to step 2c.

   2c. The FMIF will reply to the BNG with an Accounting-Response message to confirm the IP session release.

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

4. After the PPPoE discovery process completes, both the BNG and FN-RG establish the link layer through the LCP packet message exchanges as described in Section 5 of RFC 1661 [9]. The LCP Configure-Request and Configure-Ack messages are exchanged between the FN-RG and BNG via the AN. For an FN-RG, there is no 5G Vendor Specific Option (VSO) included in the LCP Configure-Request and if such an option were included, it would be ignored by the BNG.

5. After the LCP message exchange, it will be determined whether PAP or CHAP authentication will be used.

   5a. If PAP authencation is used: the FN-RG sends a PAP request to the BNG, it will trigger the BNG to send an Access-Request that inlcudes PAP credentials to the FMIF.

   5b. If CHAP auntencation is used: the BNG initiates a challenge to FN-RG. The FN-RG responds to the challenge to the BNG, it will trigger the BNG to send an Access-Request that inlcudes the challenge response from FN-RG to the FMIF.

6. The BNG sends an Access-Request message to the FMIF. The following information used to help authenticate the FN-RG will be included:

   - Line ID: the Line ID will be inlcuded as the value of the Agent-Circuit-ID attribute and the Agent-Remote-ID attribute (RFC 4679 [15]).
   - The source MAC address of the FN-RG: the MAC address will be included as the value of a Calling-Station-Id attribute (Section 5.31 of RFC 2865 [11]).
   - The PAP credentials or CHAP response.

   The FMIF will derive the Line-ID from the received Access-Request message and store that Line-ID.

7. On receipit of the Access-Request message, the FMIF will then handle the IP session initiation according to the current registration and connection state of the FN-RG:

   If the FN-RG's state is RM-DEREGISTERED:

   7a. Refers to the procedures of 6a as defined Section 8.1.1 TR-456i2 [7].

   7b. Refers to the procedures of 6b as defined Section 8.1.1 TR-456i2 [7].

7c. Upon successful registration, the FMIF validates the credentials presented by the FN-RG with configured or AACI information in the RG-LWAC. PDU session initiation does not proceed upon unsuccessful validation of credentials. That may result in immediate deregistration of the FN-RG, or transition to the CM-IDLE state. Upon successful validation of credentials, the FMIF establishes a PDU session as defined in Section 6.11 of this document. The 5GC, when formulating the reply to PDU SESSION ESTABLISHMENT REQUEST, takes into account the PDU session type requested by the FMIF and the user's subscription data stored in the UDM with the latter being authoritative.

According to the PDU SESSION ESTABLISHMENT ACCEPT received from the 5GC, the FMIF learns which PDU session types the subscriber is permitted. This information is in the Selected PDU Session Type field. If the session type requested is v4 and only v6 is authorized by the 5GC or if the session type requested is v6 and only v4 is authorized by the 5GC, the PDU SESSION ESTABLISHMENT REQUEST will fail which will result in a RADIUS Access-Reject message to the BNG. Otherwise, one of the following three cases occurs:

i. If the Selected PDU Session Type is IPv4, the 5GC network provides an IPv4 address to the FMIF. This IPv4 address can be fixed or dynamic, according to the user subscription.

   The FMIF passes this IPv4 address to the BNG by replying with an Access-Accept message to the BNG, the IPv4 address will be included as the value of a Framed-IP-Address attribute (Section 5.8 of RFC 2865 [11]).

ii. If the Selected PDU Session Type is IPv6, the 5GC in the PDU SESSION ESTABLISHMENT ACCEPT message also provides the FMIF with:

   - The IPv6 Interface Identifier to be assigned to FN-RG;
   - The "SMF LLA information element".

   The FMIF passes the IPv6 Interface Identifier to the BNG by replying with an Access-Accept message to the BNG; the IPv6 Interface Identifier will be inlcuded as the value of a Framed-Interface-Id attribute (Section 2.3 of RFC 3162 [14]).

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

If the FN-RG's state is RM-DEREGISTERED:

7d. The FMIF performs the Service Request Procedure for FN-RG in this document.

If the RM-REGISTERED/CM-CONNECTED:

7e. The FMIF will deregister and re-register the FN-RG and reestablish the PDU session OR MAY simply connect the IP session to the existing PDU session.

Note: If the selected PDU session type is IPv6 or IPv4v6, the 5GC SMF is expected to initiate an unsolicited Router Advertisement (RA) that may contain a prefix information option which is returned to the BNG in a Framed-IPv6-Prefix RADIUS attribute in the RADIUS Access-Accept message. In any case, an RA will be sent by the BNG as a response to an RS initiated by the FN-RG.

8. When the Access-Accept is received by the BNG, the FN-RG has been successfully "authenticated" by the FMIF. Then either:

   8a. The BNG sends a PAP Ack to the FN-RG.
   8b. The BNG sends a CHAP success to the FN-RG.

9. The FN-RG will then proceed to opening the NCPs for the IP session as specified in TR-101/TR-178 ([1]/[5]).

10. Refer to step 8 defined in Section 8.1.1 of TR-456i2 [7], with the FMIF acting in the role of the “AGF” or “AGF-UP”.

Note that steps 3, 4, 5, and 6 might occur before step 2c, in which case the FMIF should reply with an Access-Reject and the BNG Access-Request will be retried later.

8.2 FN-RG IP Session Initiated with DHCPv4

The following figure shows the call flow procedures for an FN-RG IP session initiation with DHCPv4:

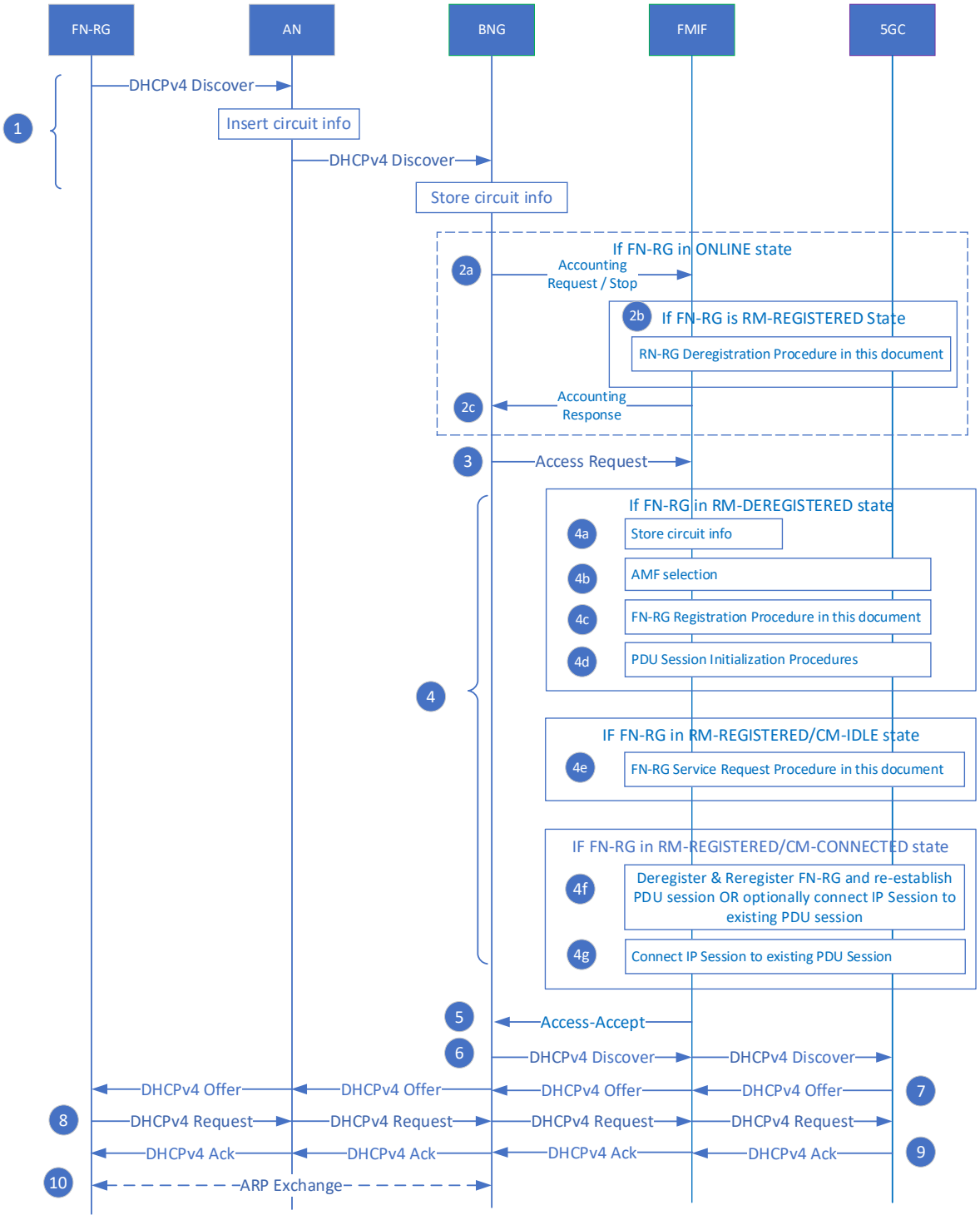

Figure 8-2: FN-RG IP Session Initiation with DHCPv4

1. The FN-RG sends a DHCPv4 Discover message to the BNG via the AN based on Section 5.6.2 of TR-146 [3].

The AN receives the DHCPv4 Discover message. It inserts Line ID information in option 82 into this message and forwards the entire message to the BNG as per Section 3.8.2 of TR-101 Issue 2 [1].

On receving the DHCPv4 Discover message, the BNG will store the subscriber's information according to TR-101/TR-178 ([1]/[5]).

2. The BNG will handle the IP session according the current state of the FN-RG, and the FMIF will handle the IP session and PDU session according to BNG's request.

   If the FN-RG is in the ONLINE state at the BNG:

   2a. If the FN-RG is in ONLINE state, the BNG will send a RADIUS Accounting-Request / Stop message to the FMIF to release the IP session.

   2b. When recieves the Accounting-Reqeust / Stop message, if the FN-RG is in the RM-REGISTERED state, the FMIF will initiate the FN-RG Deregistration Procedure described in this document and proceed to step 2c.

   2c. The FMIF will reply with an Accounting-Response message to the BNG to confirm the IP session release.

3. The BNG sends an Access-Request message to the FMIF. The following information will be included to help authenticate the FN-RG:
   - Line ID: the Line ID will be inlcuded as the value of the Agent-Circuit-ID attribute and the Agent-Remote-ID attribute (RFC 4679 [15]).
   - The source MAC address of the FN-RG: the MAC address will be included as the value of a Calling-Station-Id attribute (Section 5.31 of RFC 2865 [11]).
4. On receiving the Access-Request message, the FMIF will then handle the IP session initiation as the procedures of step 3 defined in Section 8.1.3 of TR-456i2 [7]. Where the FMIF functions as the role of an integrated AGF-UP and AGF-CP.
5. Once it receives the PDU SESSION ESTABLISHMENT ACCEPT message from the 5GC SMF, the FMIF sends a RADIUS Access-Accept message to the BNG to confirm the access. However, if the session type requested is v4 and only v6 is authorized by the 5GC or if the session type requested is v6 and only v4 is authorized by the 5GC, the PDU SESSION ESTABLISHMENT REQUEST will fail which will result in a RADIUS Access-Reject message to the BNG.
6. On receiving the Access-Accept message, the BNG will relay the previous received DHCPv4 Discover message to the FMIF, and the FMIF will relay the DHCPv4 Discover message to the 5GC via the established PDU session.
7. The 5GC in turn sends a DHCP offer message to the FN-RG via the FMIF, BNG, and AN.
8. The FN-RG responds a DHCP request message to the 5GC.
9. The 5GC confirms the DHCP lease with a DHCP Ack message.
10. The FN-RG will then typically resolve the MAC address of the default gateway with an ARP request where the BNG proxies a reply with its own MAC address.

8.3 FN-RG IP Session Initiation with DHCPv6

Figure 8-3 below shows the call flow for the FN-RG IP session initiation with the FMIF initiated by DHCPv6.

This procedure applies to FN-RGs that are able to start DHCPv6 negotiation without having received a RA with either 'M' or 'O' flag set to 1. In case the FN-RG does not have this ability, the procedure that applies is the one that requires the FN-RG sending a RS as documented in Section 8.4.

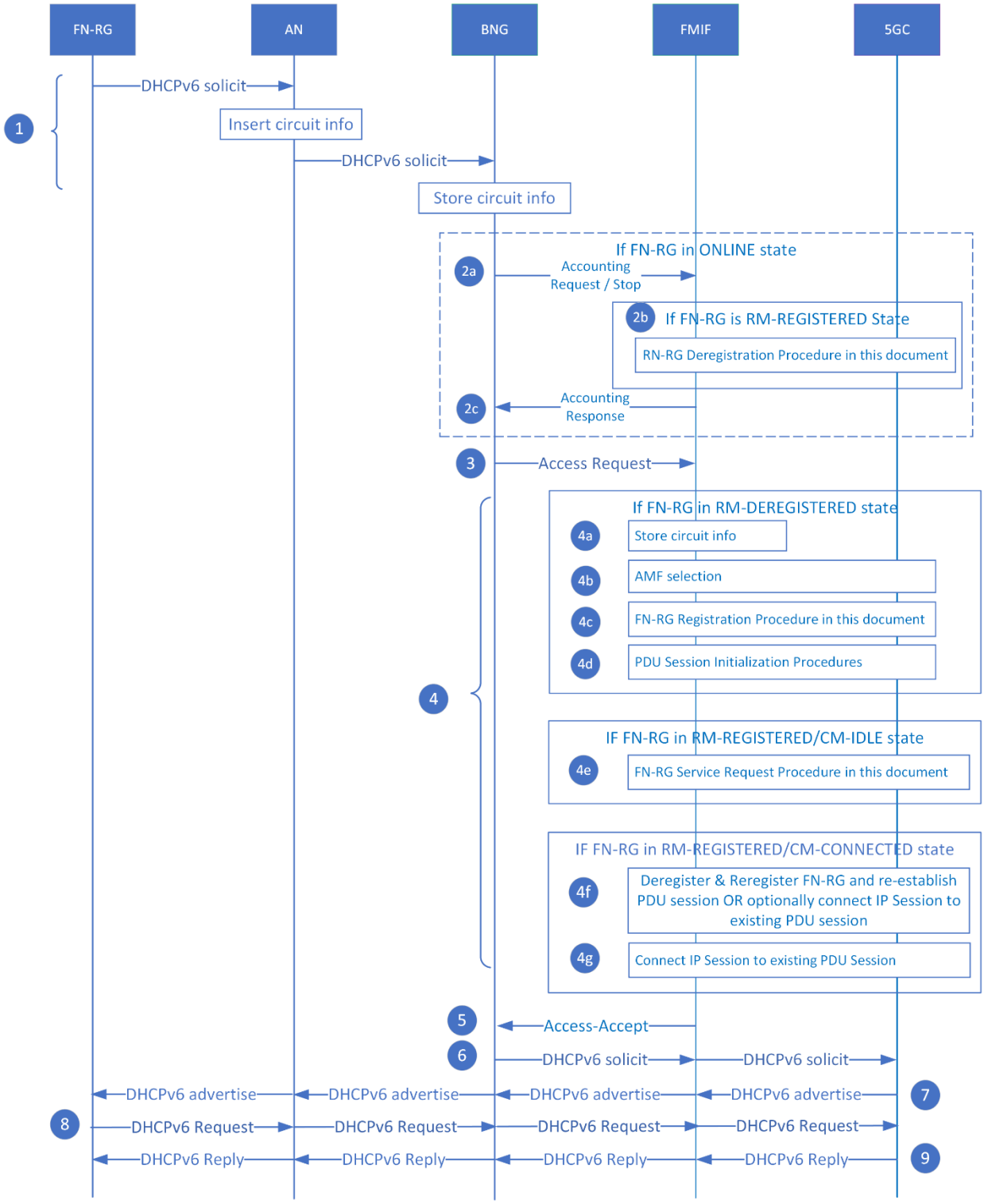

Figure 8-3: FN-RG IP Session Initiation with DHCPv6

1. The FN-RG sends a DHCPv6 Solicit message to the BNG via the AN based on Section 5.6.2 of TR-146 [3]. On receiving the DHCPv6 Solicit message, the BNG will store the subscriber's information according to TR-101/TR-178 [1]/[5].

The AN receives the DHCPv6 Solicit message. The AN will insert option 18 and/or option 37 'line identification information'. The AN then forwards the entire message to the FMIF.

2. The BNG will handle the IP session according the current state of the FN-RG, and the FMIF will handle the IP session and PDU session according to BNG's request. If the FN-RG is in the ONLINE state at the BNG:

   2a. The BNG will send a RADIUS Accounting-Request / Stop message to the FMIF to release the IP session.

   2b. When the FMIF recieves the Accounting-Reqeust / Stop message, if the FN-RG is in the RM-REGISTERED state, the FMIF will initiate the FN-RG Deregistration Procedure described in this document and proceed to step 2c.

   2c. The FMIF will reply with an Accounting-Response message to the BNG to confirm the IP session release.

3. The BNG sends an Access-Request message to the FMIF. The following information will be included to help authenticate the FN-RG:
   - Line ID: the Line ID will be inlcuded as the value of the Agent-Circuit-ID attribute and the Agent-Remote-ID attribute (RFC 4679 [15]).
   - The source MAC address the FN-RG: the MAC address will be included as the value of a Calling-Station-Id attribute (Section 5.31 of RFC 2865 [11]).
4. On receiving the Access-Request message, the FMIF will then handle the IP session initiation as the procedures of step 3 defined in Section 8.1.3 of TR-456i2 [7]. Where the FMIF functions as the role of an integrated AGF-UP and AGF-CP.
5. Once it receives the PDU SESSION ESTABLISHMENT ACCEPT message from the 5GC SMF, the FMIF sends a RADIUS Access-Accept message to the BNG to confirm the access. However, if the session type requested is v4 and only v6 is authorized by the 5GC or if the session type requested is v6 and only v4 is authorized by the 5GC, the PDU SESSION ESTABLISHMENT REQUEST will fail which will result in a RADIUS Access-Reject message to the BNG.
6. On receiving the Access-Accept message, the BNG will relay the previous received DHCPv6 Solicit message to the FMIF, and the FMIF will relay the DHCPv6 Solicit message to the 5GC via the established PDU session.
7. The 5GC in turn sends a DHCPv6 Advertise Message to the FN-RG via the FMIF, BNG, and AN.
8. The FN-RG responds with a DHCPv6 Request Message to the 5GC.
9. The 5GC confirms the DHCPv6 lease with a DHCPv6 Reply Message.

8.4 FN-RG IP Session Initiation with RS Followed by DHCPv6

The following Figure 8-4 shows the call flow procedures of an FN-RG IP session initiation with RS followed by DHCPv6. It illustrates the scenario when an RS is the first indication of IPv6 IP session initiation. A DHCPv6 exchange may follow. This covers the scenarios of SLAAC-only and RA followed by DHCPv6 to either negotiate a delegated prefix (IA_PD) or obtain other attributes such as DNSv6 addresses using DHCPv6 INFORM.

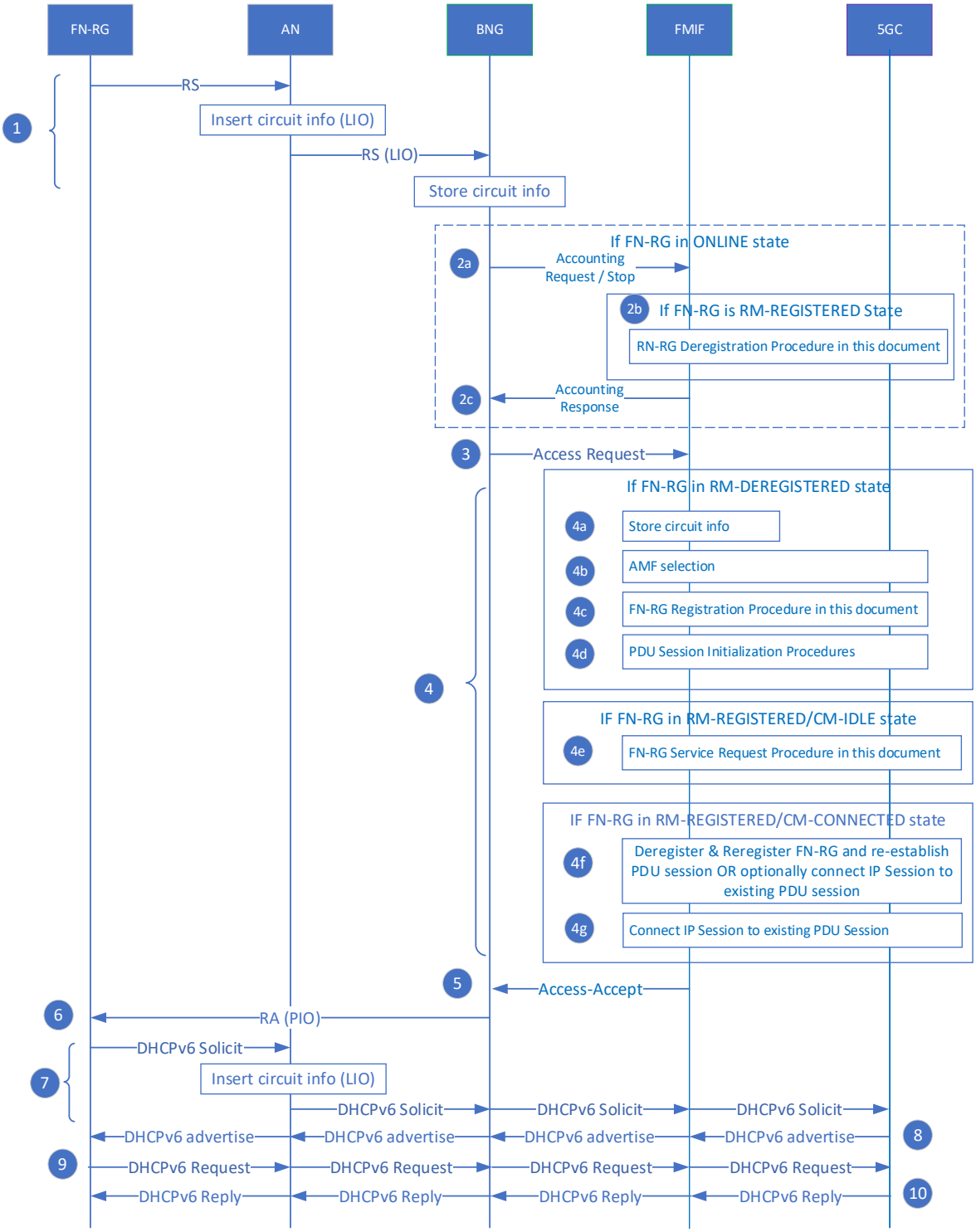

Figure 8-4: FN-RG IP Session Initiation with RS followed by DHCPv6

1. The FN-RG sends a Router Solicit (RS) message to the BNG via the AN based on Section 5.6.2 of TR-146 [3].

The AN receives the RS message. It inserts the Line ID option as per Annex 'A' of TR-177 corrigendum 1 [4] and in turn forwards the entire message to the BNG.

On receiving the Router Solicit message, the BNG will store the subscriber's information according to TR-101/TR-178 [[1]/[5]].

2. The BNG will handle the IP session according the current state of the FN-RG, and the FMIF will handle the IP session and PDU session according to BNG's request.

   If the FN-RG is in the ONLINE state at the BNG:

   2a. The BNG will send a RADIUS Accounting-Request / Stop message to the FMIF to release the IP session.

   2b. When the FMIF recieves the Accounting-Reqeust / Stop message, if the FN-RG is in the RM-REGISTERED state, the FMIF will initiate the FN-RG Deregistration Procedure described in this document and proceed to step 2c.

   2c. The FMIF will reply with an Accounting-Response message to the BNG to confirm the IP session release.

3. The BNG sends an Access-Request message to the FMIF. The following information used to help authenticate the FN-RG will be included:
   - Line ID: the Line ID will be inlcuded as the value of the Agent-Circuit-ID attribute and the Agent-Remote-ID attribute (RFC 4679 [15])
   - The source MAC address of the FN-RG: the MAC address will be included as the value of a Calling-Station-Id attribute (Section 5.31 of RFC 2865 [11]).
4. On receiving the Access-Request message, the FMIF will then handle the PDU session initiation following the procedures of step 3 defined in Section 8.1.5 of TR-456i2 [7] with the FMIF functioning as the integrated AGF-UP and AGF-CP.
5. Once it receives the PDU SESSION ESTABLISHMENT ACCEPT and, if the PDU session type is IPv6 or IPv4v6, the Router Advertisement (RA) message from the 5GC SMF, the FMIF sends a RADIUS Access-Accept message to the BNG to confirm the access. If a prefix information option was received in an RA it is returned to the BNG in a Framed-IPv6-Prefix attribute in the Access Accept message. However, if the session type requested is v4 and only v6 is authorized by the 5GC or if the session type requested is v6 and only v4 is authorized by the 5GC, the PDU SESSION ESTABLISHMENT REQUEST will fail which will result in a RADIUS Access-Reject message to the BNG.
6. The BNG sends a router advertisement (RA) to the FN-RG.
7. Steps 7-10 are the same as the steps 6-9 defined in Section 8.1.5 of TR-456i2 [7] with the FMIF functioning as the integrated AGF

Note: The BNG is a stateful DHCPv6 relay.

8.5 Registration Management Procedure for FN-RG

Since an FN-RG is a legacy device that does not support N1, the FMIF handles NAS signaling on behalf of the FN-RG. The procedure is as per Section 8.1.6 of TR-456i2 [7] with the following changes:

- The FMIF filles the role of the "AGF" or "AGF-CP".
- Step 1 is changed to refer to this document as follows:

1. In order to carry out the registration procedure, it is a pre-requiste that a connection exists between the FN-RG and BNG via PPPoE, DHCP or SLAAC using one of:

a. Steps 1-5 of FN-RG IP Session Initiation with PPPoE (Section 8.1)
b. Steps 1-2 of FN-RG IP session initiation with DHCPv4 (Section 8.2)
c. Steps 1-2 of FN-RG IP session initiation with DHCPv6 (Section 8.3)
d. Steps 1-2 of FN-RG IP session initiation with RS followed by DHCPv6 (Section 8.4).

After authentication, the FMIF selects an AMF as per step 2 in 3GPP TS 23.316 [20] subclause 7.2.1.3.

8.6 Service Request Procedure for FN-RG

When the BNG hides a line flapping on its subscriber side this procedure is not needed. If such a line problem is not hidden, the BNG will signal this as an end of session by sending a RADIUS Accounting-Request Stop to the FMIF.

The Service Request Procedure described below is initiated by the FMIF when the state of the FN-RG on the FMIF is (CM-IDLE, RM-REGISTERED). If successful it transitions the CM state to CONNECTED. (See also TR-456i2 [7].)

The procedure is as per Section 8.1.7 of TR-456i2 [7] with the following changes:

- The BNG and FMIF fill the role of the “AGF” or “AGF-CP”.
- Step 1 is changed to refer to this document as follows:

1. The FN-RG connects to the BNG which in turn connects to the FMIF via PPPoE, DHCP, or SLAAC using one of:
    a. Steps 1-5 of FN-RG IP session initiation with PPPoE (Section 8.1)
    b. Steps 1-2 of FN-RG IP session initiation with DHCPv4 (Section 8.2)
    c. Steps 1-2 of FN-RG IP session initiation with DHCPv6 (Section 8.3)
    d. Steps 1-2 of FN-RG IP session initiation with RS followed by DHCPv6 (Section 8.4).

8.7 Session Initiation Procedure for FN-RG

Session initiation procedure for FN-RG is as specified in TR-456i2 [7] Section 8.1.8 with “AGF” and “AGF-CP” replaced by “FMIF”.

8.8 Deregistration Procedure for FN-RG

The Deregistration procedures defined in the section of the same name in TR-456i2 [7] can be applied to FMIF without any changes.

8.9 FN-RG or Network Requested PDU Session Modification via W-5GAN

Requirements and procedures are as in TR-456i2 [7] Section 8.1.10 with “AGF” replaced by “FMIF”.

8.10 FN-RG/BNG or Network Requested PDU Session Release via W-5GAN

The PDU session release procedure is triggered by:

- DHCP lease expiry (**Note:** The relationship between DHCP lease management and PDU session management is FFS)

- receipt of a RADIUS Accounting-Request/Stop from the BNG which acts on behalf of FN-RG

- 5GC action

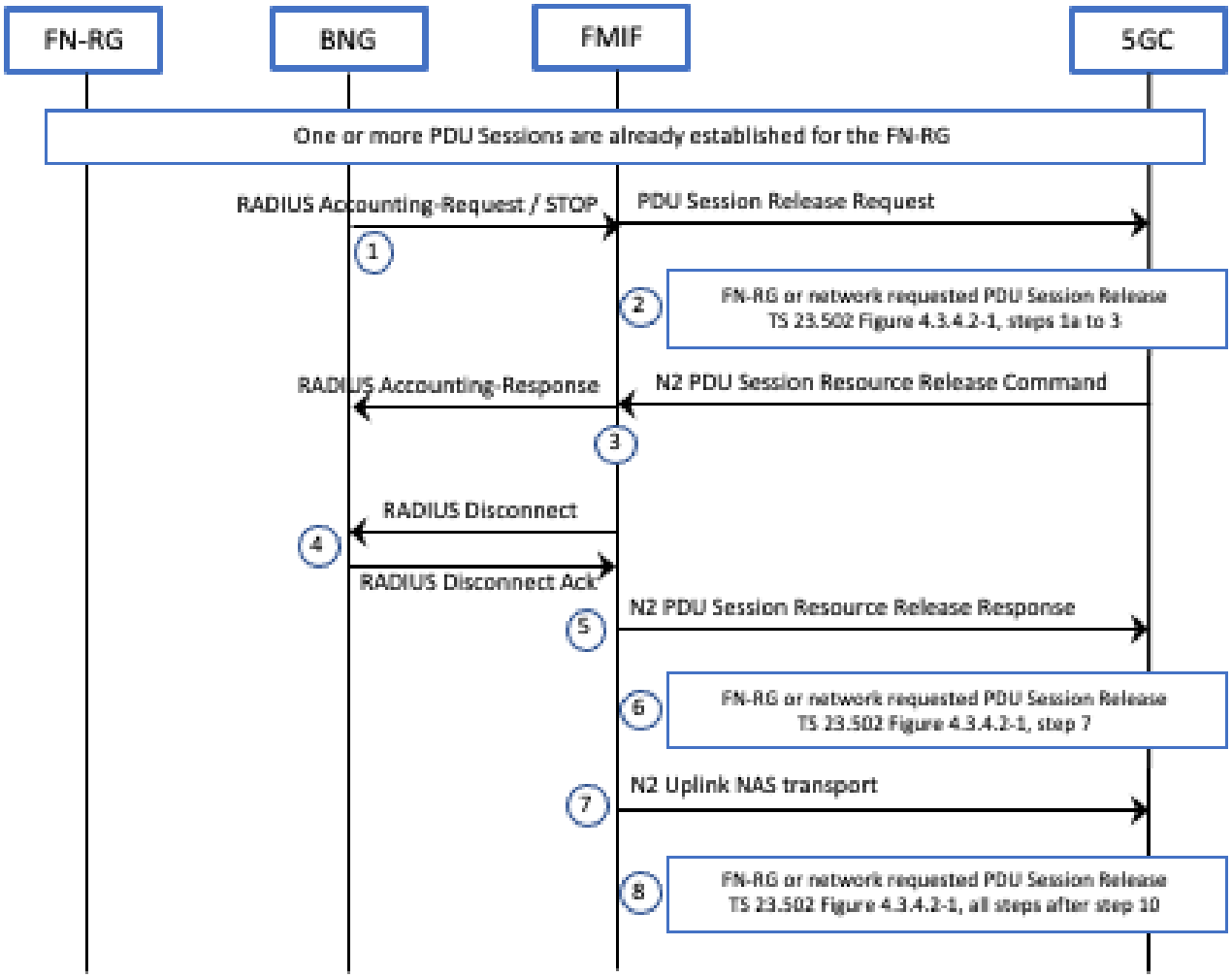

Figure 8-5: FN-RG/BNG or Network Requested PDU Session Release via W-5GAN

This procedure, as shown in Figure 8-5, is as per clause 7.3.7 of TS 23.316 [20], which is in turn referring to clause 7.3.3 with the following clarifications:

1. To initiate this procedure, it is a prerequisite that connectivity exists between the BNG and FMIF and has at least one FN-RG IP session mapped to a PDU session established between the FMIF and UPF as per step 1 of clause 7.3.3 of TS 23.316 [20].

The FMIF creates a PDU Session Release Request towards the 5GC on behalf of FN-RG/BNG as per bullet 3 in clause 7.3.7 in TS 23.316 [20].

2. The 5GC executes step 3 as in clause 7.3.3 in TS 23.316 [20].

3. The FMIF receives N2 PDU Session Resource Release Command from 5GC as per step 4 of clause 7.3.3 in TS 23.316 [20].

4. If the PDU Session Release was requested by the BNG, UP resources have already been released and a RADIUS Accounting-Response is sent to the BNG. (This step may occur earlier or later in this sequence.)

   If the PDU Session Release is network requested, upon receiving the N2 Release Request message, the FMIF triggers the release of the corresponding UP resources as per bullet 4 of clause 7.3.7 in TS 23.316 [20] by sending a RADIUS Disconnect-Request to the BNG.

5. On receipt of the RADIUS Disconnect-ACK, the FMIF sends a N2 PDU Session Resource Release Response towards the 5GC as per step 6 of clause 7.3.3 in TS 23.316 [20].

6. Step 7 is executed in 5GC as per clause 7.3.3 in TS 23.316 [20].

7. The FMIF directly creates an Uplink NAS Transport Message towards the 5GC, which contains the PDU Session Release Ack as per bullet 5 in clause 7.3.7 in TS 23.316 [20].

8. Step 11 is executed in 5GC as per clause 7.3.3 in TS 23.316 [20].

8.11 FN-RG AN Release via W-5GAN

The AN Release Procedure for the FN-RG is used to release the NG-AP signaling connection and the associated N3 user plane connections between the W-5GAN and the 5GC.

The AN release procedure may be triggered by a loss of connectivity with the FN-RG detected by the BNG which will send a RADIUS Accounting-Request / Stop message to the FMIF. It may be started by the FMIF with a N2 UE Context Release Request to the AMF and a RADIUS Disconnect-Request to the BNG. Upon receiving the N2 UE Context Release command as a reply from the AMF, the FMIF flushes the FN-RG N2 context, the N3 resources and the IP session resources, retaining the N1 context as proxy UE. Besides that, the FMIF starts a local non-3GPP Implicit Deregistration timer using the default value or the value received from by the AMF in the in NAS Registration Accept message (as documented in TS 24.501 [24] clause 8.2.7.17). The N1 context related to the FN-RG is retained by the FMIF as proxy UE until the non-3GPP Implicit Deregistration timer expires.

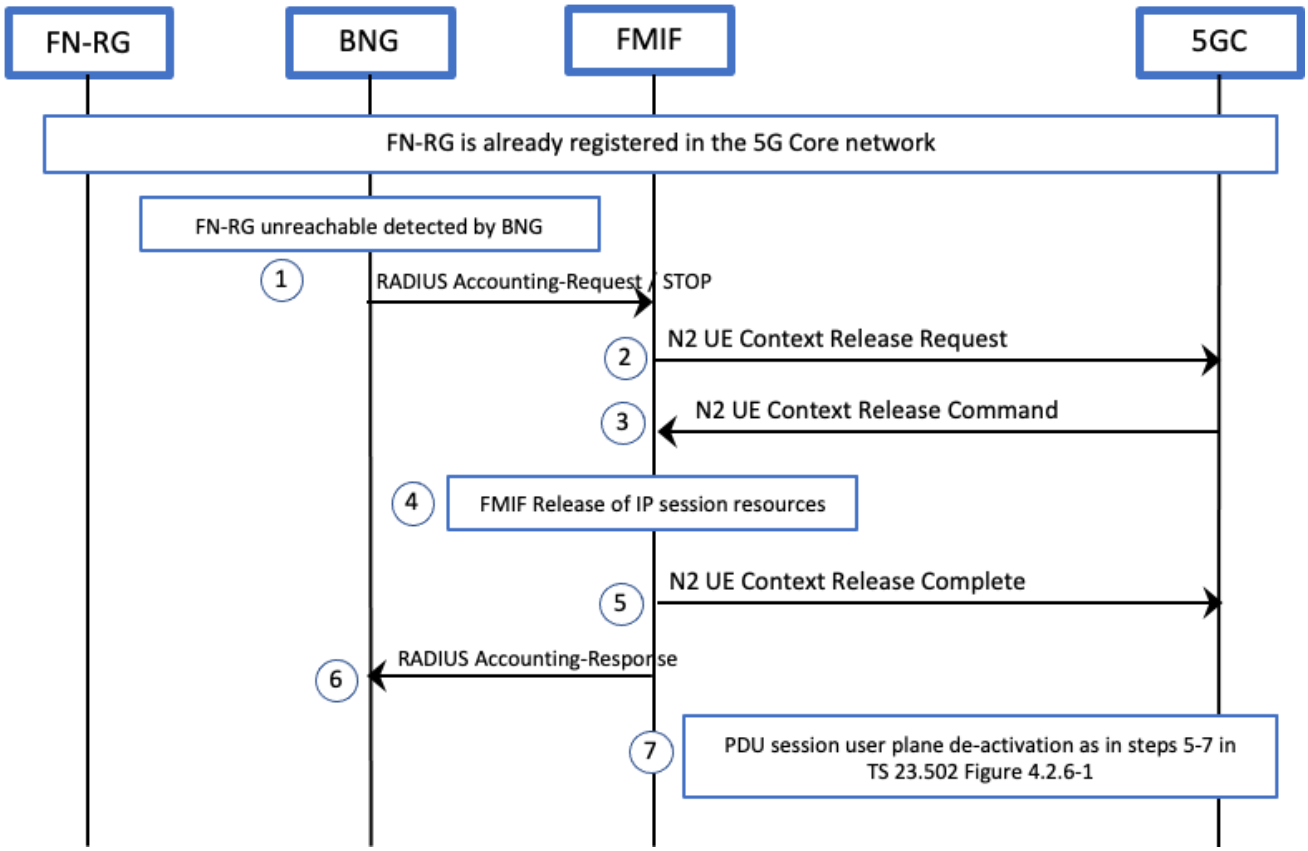

Figure 8-6: FN-RG AN Release via W-5GAN

The AN Release procedure, as shown in Figure 8-6, is as per clause 7.2.5.3 of TS 23.316 [20], which in turn refers to clause 7.2.5.2 with the following clarifications:

1. It is a prerequisite that the FN-RG is registered into the 5GC. The FMIF may have a PDU session established on behalf of the FN-RG as per step 1 of clause 7.2.5.2 in TS 23.316 [20].

   The BNG detects that the FN-RG is unreachable and sends a RADIUS Account-Request / Stop message to the FMIF which serves as the trigger for initiating this procedure as per step 2 in clause 7.2.5.2 in TS 23.316[20]. This may be via liveness detection means (e.g., LCP Echo Requests).

2. The FMIF sends a N2 UE Context Release Request to 5GC as per step 3 of clause 7.2.5.2 in TS 23.316 [20].

3. The FMIF receives a N2 UE Context Release Command from the 5GC as per step 4 of clause 7.2.5.2 in TS 23.316 [20].

4. The FMIF initiates the release of the IP session local resources as per bullet 2 of clause 7.2.5.3 in TS 23.316 [20]. The release process is entirely a local action and involves the release of state and scheduler appearances at the FMIF.

5. The FMIF next sends a N2 UE Context Release Complete to the 5GC as per step 6 of clause 7.2.5.2 in TS 23.316 [20].

6. The FMIF sends a RADIUS Accounting-Response to the BNG. (This message may be sent earlier in this sequence after step 1.)

7. This is followed by PDU session user plane deactivation in the 5GC as per step 7 of clause 7.2.5.2 in TS 23.316 [20].

8.12 Configuration Update Procedure for FN-RG

This procedure is used by the network to update the FN-RG configuration which consists of:

- Access and mobility management related parameters provided by the AMF.

- FN-RG related Policy provided by the PCF. The use of URSP to determine PDU session type, DNN, and NSSAI is FFS.

8.12.1 Configuration Update procedure for Access and Mobility Management related parameters

The procedure is as specified in Section 8.1.13.1 of TR-456i2 [7] with the following changes:

- "AGF", AGF-CP", and "AGF-UP" are replaced by "FMIF"
- If AN Release is required, the procedure is as in Section 8.11 of this document.
- The Registration procedure is as in Section 8.5 of this document.

8.12.2 Configuration Update procedure for transparent FN-RG policy delivery

The procedure is as specified in Section 8.1.13.2 of TR-456i2 [7] with the following changes:

- "AGF", "AGF-CP", and "AGF-UP" are replaced by "FMIF"
- Step 3 is replaced by the text below and Figure 20 in TR-456i2 is replaced by Figure 8-4 below.

3. The FMIF maps the policy, to the extent it can, into RADIUS Filter-ID (11) and/or NAS-Filter-Rule (92) attributes and transmits these to the BNG in a RADIUS CoA-Request. The FMIF then updates the policy provided by the 5GC for the FN-RG and sends the result to the 5GC in an N2 Uplink NAS Transport message as per step 4 of clause 4.2.4.3 of TS 23.502 [22] which contains the Manage UE Policy Complete message. In this issue of the specification, the FMIF ignores the UE policy rules, but sends a positive result.

Note: There is no signaling or message exchange between the FMIF and FN-RG for this procedure.

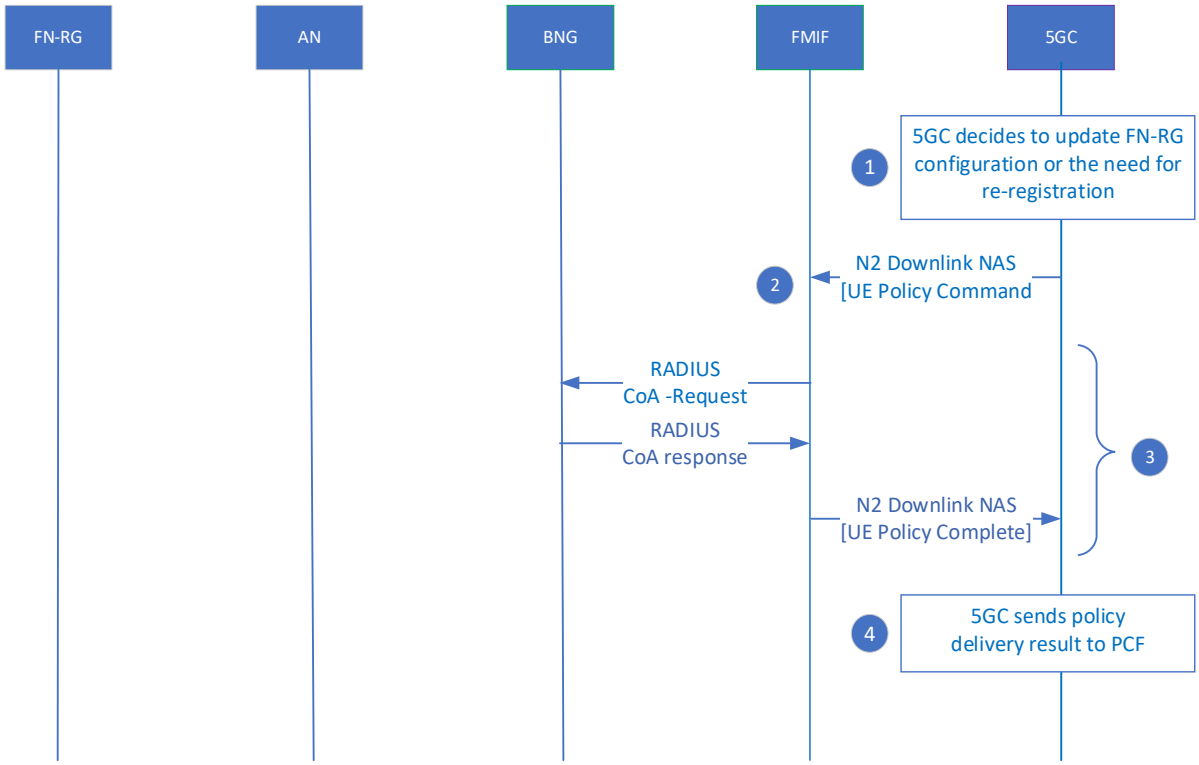

Figure 8-7: Configuration Update Procedure for transparent UE policy delivery via W-5GAN

End of Broadband Forum Technical Report TR-457