Technical Report

TR-458
Wireless and Wireline Convergence with Control and User Plane Separation. Reference Architecture, Interface, and Protocol Specification

Issue: 1
Issue Date: August 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	Issue Date	Issue Editor	Changes
01	August 2023	Kenneth Wan, Nokia Donald Eastlake, Futurewei	Issue 1

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

Editor: Kenneth Wan, Nokia
Donald Eastlake, Futurewei

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

Project Stream Leader(s): Venkatesh Padebettu, Juniper

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This Technical Report specifies the architecture and requirements for Control and User Plane Separation (CUPS) for Wireless Wireline Convergence (WWC) functions, specifically the Access Gateway Function (AGF). The separation of the Control Plane and User Plane in these functions enables more efficient use of resources and simplifies operations. The 3GPP Packet Forwarding Control Protocol (PFCP) is specified as the State Control Interface (SCi) protocol for programming subscriber forwarding state between the Control Plane and User Plane. This Technical Report includes PFCP protocol extensions which are required to support WWC use cases.

1 Purpose and Scope

1.1 Purpose

This document specifies the architecture and requirements for AGF CUPS. The architecture designates functions to either the control plane or user plane and defines the interfaces between the control plane and user plane. Requirements on both interfaces and protocols help ensure interoperability between vendors' control planes and user planes. Although the AGF control plane and user plane are separated, the goal is to ensure the same service offerings of a standalone AGF. In addition, new capabilities can be realized through control plane and user plane separation such as independent control plane and user plane scaling, independent control plane and user plane life cycle management, and simplifying operations by using a centralized control plane for configuration.

1.2 Scope

The following are in scope for the AGF CUPS and the co-located AGF-UP and UPF:

- High level architecture
- Procedure call flows
- Functional Requirements

The following aspects of PFCP use between the control and user planes are in scope as needed to support the above items:

- Protocol message types and session procedures
- Protocol extensions

The following details for the FMIF, co-located FMIF and UPF, and co-located FMIF are for further study (FFS):

- FMIF CUPS
- CUPS Procedure call flows.
- Functional Requirements.

The following are considered out of scope for this TR:

- Functions in clause 5 of TS 38.410 [27], Paging, Mobility Management, Warning Message Transmission, Configuration Transfer, Location Reporting, UE Radio Capability Management, Report of Secondary RAT data volumes and RIM Information Transfer functions.
- Wholesale deployment scenarios (excluding third-party access networks and L2TP support) and IPTV

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 2119 [10].

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-069 Amendment 4	CPE WAN Management Protocol	BBF	2018
[2] TR-101 Issue 2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[3] TR-156	Using GPON Access in the context of TR-101	BBF	2010
[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-456 Issue 2	AGF Functional Requirements	BBF	2022
[7] TR-459 Issue 2	Multi-Service Disaggregated BNG with CUPS. Reference Architecture, Deployment Models, interface, and Protocol Specifications	BBF	2023
[8] TR-470 Issue 2	5G Wireless Wireline Architecture	BBF	2022
[9] RFC 1661	The Point-to-Point Protocol (PPP)	IETF	1994
[10] RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[11] RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)	IETF	1999

[12] RFC 3046	DHCP Relay Agent Information Option	IETF	2001
[13] RFC 3772	Point-to-Point Protocol (PPP) Vendor Protocol	IETF	2004
[14] RFC 6788	The Line Identification Option	IETF	2012
[15] RFC 6973	Privacy Considerations for Internet Protocols	IETF	2013
[16] RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words	IETF	2017
[17] RFC 8415	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	IETF	2018
[18] RFC 8822	5G Wireless Wireline Convergence User Plane Encapsulation (5WE)	IETF	2021
[19] TS 23.316	Wireless and wireline convergence access support for the 5G System	3GPP	Latest Version
[20] TS 23.501	System Architecture for the 5G System	3GPP	Latest Version
[21] TS 23.502	Procedures for the 5G System	3GPP	Latest Version
[22] TS 24.501	Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3	3GPP	Latest Version
[23] TS 29.244	Interface between the Control Plane and the User Plane Nodes; Stage 3	3GPP	Latest Version
[24] TS 29.281	General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)	3GPP	Latest Version
[25] TS 29.413	Application of the NG Application Protocol (NGAP) to non-3GPP access	3GPP	Latest Version
[26] TS 29.510	Network Repository Services; Stage 3	3GPP	Latest Version
[27] TS 38.410	NG-RAN; NG general aspects and principles	3GPP	Latest Version
[28] TS 38.413	NG-RAN; NG Application Protocol (NGAP)	3GPP	Latest Version
[29] TS 38.415	NG-RAN; PDU session user plane protocol	3GPP	Latest Version

2.3 Definitions

The following terminology is used throughout this Technical Report.

Broadband UPF (B-UPF)	A data plane element that combines the function of the AGF-UP and the UPF. The B-UPF supports network-facing interfaces (N3, N6, and N9), access-facing interfaces (V, and N3 as applicable), and interfaces to AGF-CP and SMF (N4).
Combined AGF-UPF	AGF and UPF functions can be combined into a single implementation (“Combined AGF-UPF”), as detailed in BBF TR-470i2 [8] and BBF TR-456i2 [6], with a co-located UPF. The co-location happens on a per PDU session basis. An externally connected UPF may also be present, and the requirements (service-wise) of the PDU session will dictate which option is used. This combination is seen as beneficial to achieve a technological optimization of implementations, reducing complexity in practice. The resulting function supporting the CUPS architecture, called “Broadband UPF (B-UPF)”, is specified in this document. The AGF parameter (WAgfInfo), as defined by 3GPP in TS 38.413 clause 9.2.5.3 [28] and TS 29.510 [26], applies.

PFCP Session	Defined by 3GPP. A CP function controls the packet processing in the UP function by establishing, modifying, or deleting PFCP Session contexts and by provisioning specific forwarding rules for this context
Subscriber Session	Subscriber sessions are used to represent all traffic that is associated with a FN-RG or a 5G-RG by a given service provider to provide a context for policy enforcement

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	3rd Generation Partnership Project
5G-RG	5G Routing Gateway (with 5G NAS)
5GC	5G Core Network
5WE	5G Wireless Wireline Convergence User Plane Encapsulation
AAA	Authentication, Authorization and Accounting
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
B-UPF	Broadband UPF
CPE	Customer Premises Equipment
CPR	Control Packet Redirect
CUPS	Control and User Plane Separation
DHCP	Dynamic Host Configuration Protocol
DN	Data network
F-TEID	Fully Qualified TEID
FAR	Forwarding Action Rules
FFS	For Further Study
FMIF	Fixed Mobile Interworking Function
FN-RG	Fixed Network Gateway without NAS
GLI	Global Line ID
GTP-U	GPRS Tunneling Protocol User Plane
GPON	Gigabit Passive Optical Networking
GW	Gateway
IE	Information Element
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator

LCP	Link Control Protocol
LDRA	Lightweight DHCPv6 Relay Agent
LLA	Link Local Address
LNS	L2TP Network Server
Mi	Management Interface
MS-BNG	Multi-Service BNG
NAS	Non-Access Stratum
NSH	Network Service Header
OAM	Operations, Administration and Management
PADI	PPPoE Active Discovery Initiation
PADR	PPPoE Active Discovery Reply
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PDI	Packet Detection Information
PDR	Packet Detection Rule
PFCP	Packet Forwarding Control Protocol
PDU	Protocol Data Unit
PII	Personal Identifying Information
PPPoE	Point-to-Point Protocol over Ethernet
QER	QoS Enforcement Rules
QoS	Quality of Service
RA	Router Advertisement
RAN	Radio Access Network
RG	Residential Gateway
RG-LWAC	RG-Level Wireline Access Characteristics
RS	Router Solicit
SCi	State Control Interface
SEID	Sx Session ID
SLAAC	Stateless Address Auto-Configuration
SMF	Session Management Function
TEID	Traffic Endpoint ID
TR	Technical Report
TR-456i2	TR-456 issue 2
TR-459i2	TR-459 issue 2
TR-470i2	TR-470 issue 2
UDM	Unified Data Management
UE	User Equipment
UPF	User plane Function
URR	Usage Reporting Rule
USP	User Services Platform
VRF	Virtual Router and Forwarding

VSNP	Vendor Specific Network Protocol
W-5GAN	Wireline 5G Access Network
WA	Work Area
WLAN	Wireless Local Area Network.

3 Technical Report Impact

3.1 Energy Efficiency

Energy Efficiency of an AGF may be impacted by migrating from standalone to control and user plane separation. Such separation allows dynamic scaling of both the control and user plane according to the subscriber population which may lead to optimized equipment deployment and therefore, energy consumption. However, energy consumption can also increase depending on deployment factors such as power per node, geographic dispersion of user plane, and use of generic hardware not optimized for specific network functions.

Regulatory differences related to electrical power, Heating, Ventilation and Air Conditioning (HVAC) and fire protection between traditional Central Offices and datacenters are out-of-scope for this document.

3.2 Security

Security provides "a form of protection where a separation is created between the assets and the threat." In the case of the AGF, assets exist on the communications paths between them and the functions to which they are connected, namely the AMF, UPF, AN, and BNG. In addition, assets exist within the AGF themselves.

The risk of compromise of the communications is dependent on the threats in the environment through which those communications pass and the security of communications protocol used in those communications. Appropriate security measures must be taken to secure communications paths to and from the AGF 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 AGF CP or UP themselves, through means other than their communications interfaces, is dependent on their security against physical access. Appropriate security measures must be taken to secure the premises where they are housed.

Any implementation should include documentation of special requirements that apply specifically to that implementation – such as measures needed to ensure that only authorized parties can access, or modify, configuration for underlying network infrastructure and that traffic associated with one subscriber cannot be intercepted by other subscribers.

Because of the distribution of control and data plane functions, the CUPS protocols must include capabilities for providing secure and authenticated communication between distributed components of the AGF, specifically for the in-scope communication between CP and UP components. Operators should consider using these capabilities as an important means for preventing attacks intended, for example, to divert or disable data forwarding capabilities through control plane impersonation.

3.3 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.

The AGF are subject to privacy concerns and particularly to those functions and interfaces included as “in scope” in the “Scope” section 1.2 of this document.

In network protocols, privacy concerns, beyond the protection of potentially private data, focus on two aspects:

1) The potential for tracking of users through exposure of Personal Identifying Information (PII);
2) The potential for correlation of user activity over time through persistent use of network identifiers.

Because of its distributed nature, the same (or highly correlated) identifying information may be seen at several points in the network, allowing for identification of a target subscriber or an AGF component. This increases the potential exposure to privacy violations.

Implementers should include information as to what privacy protection is provided in the implementation, (e.g., avoiding direct or inferable relationships between subscriber PII and network identifiers, avoiding persistent use of identifiers during different stages of subscriber activation, use and deactivation, minimizing the extent to which PII is included in the protocol, or stored at components, etc.) and explicitly include details of any unavoidable (or required) use and/or storage of PII.

AGF CP and UP component implementations should include privacy considerations such as those listed in related standards and similar activities such as IETF RFC 6973 [15] – entitled “Privacy Considerations for Internet Protocols” – that includes some of the history relating to privacy considerations, and suggests “legally generic” (e.g., recognizing that the definitions and handling of privacy differ across legal jurisdictions) guidance that can be used as “food for thought” in designing network protocols independent of specific legal framework(s).

4 WWC CUPS architecture

4.1 AGF architecture

Figure 4-1 illustrates the set of AGF functions and interfaces that have been defined in TR-456i2 [6] to support the deployment scenarios described in TR-470i2 [8]. The AGF can serve both FN-RG and 5G-RG. Each RG type requires a different AGF control plane (CP) function. Operators utilize a combination of AGF functions to provide different types of broadband converged service(s). The AGF has access, network, and control signal interfaces. The access and network interface are user plane interfaces.

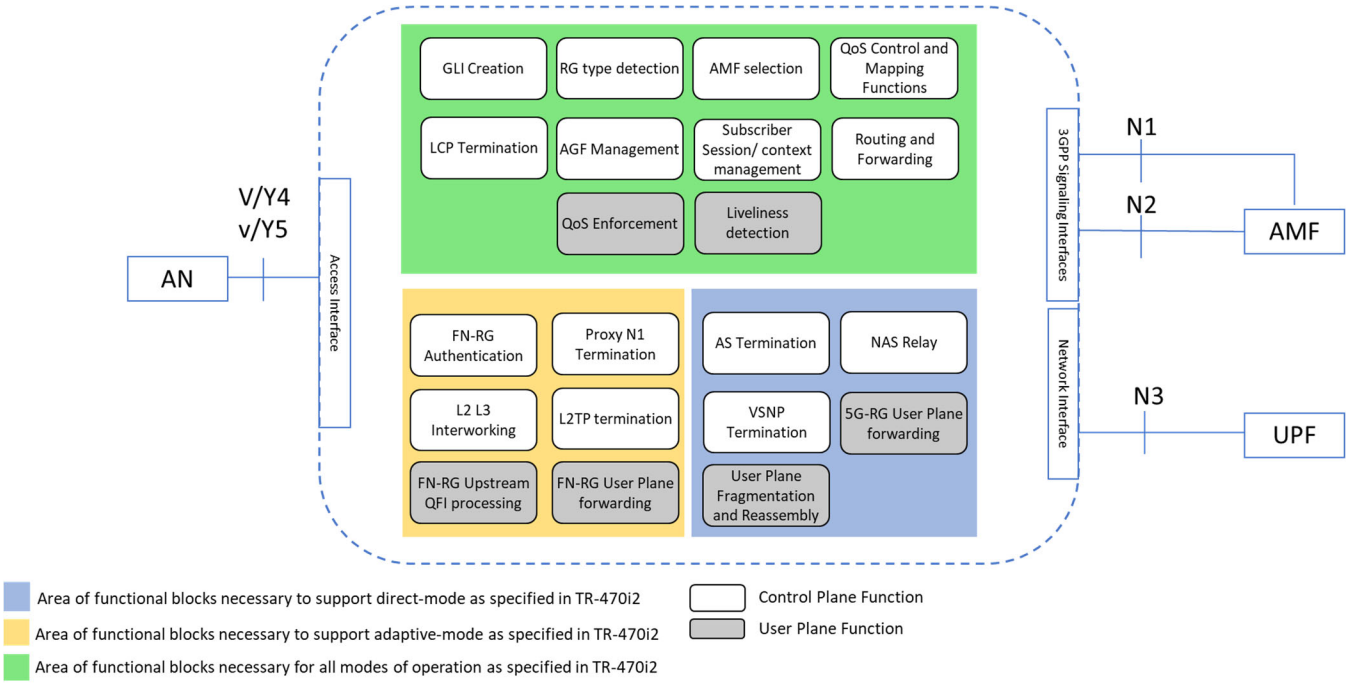

Figure 4-1: AGF standalone functional blocks and interfaces

4.1.2 AGF Functions

The AGF utilizes different functional blocks to provide connectivity between wireline RGs to the 5GC. Table 1 lists the functional blocks within the AGF.

Table 1: Functional Blocks of an AGF

AGF Functions		Additional Description	TR reference
For All AGF Modes of Operations	GLI Creation	Construction of the Global Line ID	TR-470i2 [8]
	RG type detection	Differentiating a FN-RG or a 5G-RG	TR-456i2 [6]
	AMF selection		TR-456i2 [6]
	QoS Control and Mapping Function	Process QoS profiles sent by the AMF including the RG-LWAC	TR-456i2 [6] TR-470i2 [8]
	LCP Termination	Processing PPP LCP control packet	TR-456i2 [6]
	AGF Management	Node management	TR-456i2 [6]
	Session/context Management	Mapping of PDU session	TR-456i2 [6]
	User Plane Fragmentation and Reassembly	Fragmentation of 5WE packets	TR-456i2 [6]
	QoS Enforcement	Enforcing QoS profile and RG-LWAC	TR-456i2 [6]
	Liveliness detection	PPPoE LCP echo	TR-456i2 [6]
	DHCP	DHCP Server and Relay function	TR-456i2 [6]
	Datapath forwarding	Forwarding for AGF-UP	TR-456i2 [6]
To Support Adaptive-Mode	FN-RG authentication	Specifically, for PPPoE FN-RG	TR-456i2 [6]
	Proxy N1 Termination	Processing N1 messages from 5GC	TR-456i2 [6]
	L2 and L3 interworking	Data plane function to allow user plane connectivity between wireline and 5GC	TR-456i2 [6]
	L2TP termination	Processing L2TP control messages	TR-456i2 [6]
	FN-RG User Plane forwarding	Forwarding of data packets including: PPPoE, IPoE, and L2TP data packets	TR-456i2 [6]
	PPP/PPPoE		TR-456i2 [6]
To Support Direct-Mode	AS Termination	To allow sending and processing of AS messages	TR-456i2 [6]
	NAS Relay		TR-456i2 [6]
	PPP VSNP	To process NAS message encapsulated in a VSNP message	TR-456i2 [6]
	5G-RG User Plan Forwarding	Forwarding of data packets: 5WE	TR-456i2 [6]

4.1.3 AGF Interfaces

The following interfaces are defined in TR-456i2 [6]:

- V-interface: The Ethernet interface between the Access Node and the AGF. It is also the interface between the L2TP LAC and the AGF
- V/Y4: Defined in TR-470i2 [8], the interface between an AGF and a wireline access network supporting a 5G-RG.
- V/Y5: Defined in TR-470i2 [8], the interface between an AGF and a wireline access network supporting an FN-RG.
- N1: Defined in 3GPP TS 24.501 [22] as the interface between the 5G-RG and AMF as per 3GPP TS 23.316 [19]. In the FN-RG case, it is also a logical interface between the AGF and AMF as per 3GPP TS 23.316 [19].
- N2: Defined in 3GPP TS 38.413 [28] as an interface between the AGF and AMF as per 3GPP TS 23.316 [19].
- N3: Defined in 3GPP TS 29.281 [24] as the interface between the AGF and UPF as per 3GPP TS 23.316 [19].

The access interfaces on the AGF terminates various access types such as broadband and fixed mobile connections. Table 2 specifies the AGF access interfaces cross referenced to relevant TRs and its respective protocol stacks.

Table 2: AGF interfaces

Interfaces	Protocol Supported	Additional Information
V/Y4	5WE	5WE as defined in RFC 8822 [18]
	AS	AS protocol requirements and procedures are defined in TR-456i2 [6]
	VSNCP/VSNP	VSNCP and VSNP requirements and procedures are defined in TR-456i2 [6]
	PPPoE	PPPoE is part of the control plan protocol used by the AGF which is defined in TR-456i2 [6]
V/Y5	IPoE PPPoE PPPoL2TP	
N1	NAS	NAS protocol requirements and procedures are defined in 3GPP TS. 24.501 [22]
N2	NG-AP over SCTP	Interface is defined in 3GPP TS 23.501 [20] NG-AP protocol requirements and procedures are defined in 3GPP TS 38.413 [28] Application of NG-AP to non-3GPP access is defined in 29.413 [25].
N3	IP Packet over GTP	Interface is defined in 3GPP TS 23.501 [20] N3 requirements and procedures are further defined in 3GPP TS 38.415 [29] GTP protocol is defined in 3GPP TS 29.281 [24]

4.2 AGF CUPS architecture

Below is an AGF CUPS architecture that supports both FN-RG and 5G-RG. The CUPS architecture utilizes the same functional blocks as the AGF described in Figure 4-1, but the functional blocks are split between the Control Plane (CP) and User Plane (UP). The CP communicates to the AMF through the N1 and N2 interface for FN-RG and the N2 interface for 5G-RG.

Overall, the architecture and requirements of AGF CUPS shares commonality with DBNG-CUPS as defined in TR-459i2 [7], especially FN-RG. This document is primarily intended to identify architecture and requirements that are either unique to AGF CUPS or differs by necessity from TR-459i2 [7] references.

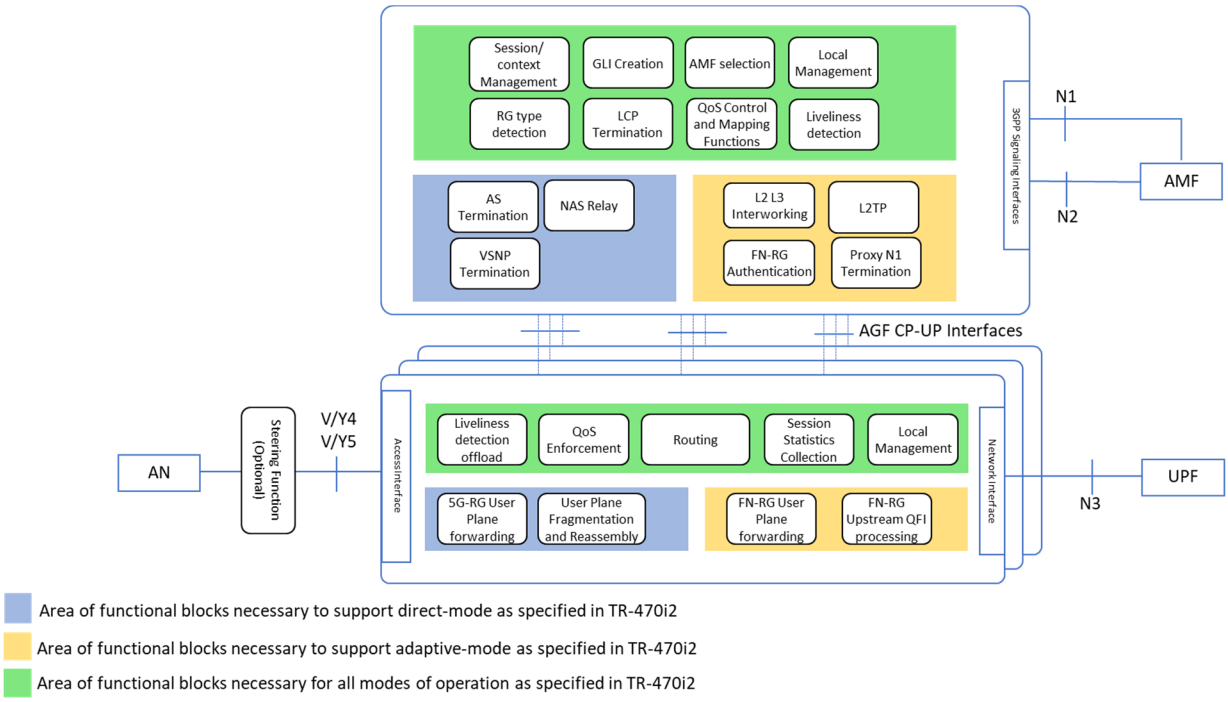

Figure 4-2: High level architecture of a standalone AGF with CUPS

The combination of the CP functions is referred to as the CP of the AGF (AGF-CP). Similarly, the combination of UP specific functions is referred to as the UP of the AGF (AGF-UP). The AGF-UP is responsible for forwarding of subscriber traffic.

4.2.1 AGF-CP Functions

The AGF-CP performs control plane functions such as 3GPP control signaling and relay, AS signaling, QoS management function, FN-RG related control function, and 5G-RG related control function.

AGF-CP functions are divided into:

- FN-RG related control functions:
  - L2/L3 interworking function – DHCP relay, IPv6 LLA processing
  - PPPoE and PPP termination
  - L2TP control messages – processing L2TP control packets from LAC
  - FN-RG authentication for PPP – processing PAP/CHAP
  - Proxy N1 Termination – processing N1 NAS messages
- 5G-RG related control function
  - AS Termination – exchange AS message with an 5G-RG
  - NAS Relay

    - VSNP Termination – process NAS message within VSNP
- Common AGF control function
    - Session/Context Management
    - GLI Creation
    - AMF Selection
    - Local Management
    - RG type detection
    - LCP Termination
    - QoS Control and Mapping Functions
    - Liveliness detection

4.2.1.1 AGF-CP Northbound Interfaces

The northbound interfaces: N2 interface terminated on the AGF-CP.

4.2.2 AGF-UP Functions

Once the AGF-CP programs the AGF-UP PFCP rule for the subscriber traffic forwarding, the AGF-UP performs forwarding, traffic management, and policy enforcement on the subscriber traffic. The following functions are part of AGF-UP:

- FN-RG specific
    - Forwarding based on FN-RG encapsulation, header manipulation
    - Upstream QFI processing
- 5G-RG specific
    - Forwarding based on 5G-RG encapsulation
- Common AGF data plane function:
    - Subscriber Forwarding
    - Subscriber Routing: Includes both routing control and forwarding (UPF function of B-UPF)
    - Liveliness detection offload: Includes the generation and processing of PPP echo messages that are offloaded from the AGF-CP for the purposes of improving scalability and/or failure detection times. In this case, the AGF-UP needs to inform the AGF-CP of any relevant changes in keepalive state.
    - Fragmentation and Reassembly of 5WE packets
    - QoS Enforcement
    - User Plane reassembly and fragmentation
    - Local Management
    - Operational Statistics are FFS

4.2.2.1 AGF-UP Interfaces

The access interface (V), V/Y4, and V/Y5, and network interface (N3) that forwards subscriber data traffic belongs to the AGF-UP.

4.2.3 Interfaces between AGF-CP and AGF-UP

With the separation of the CP and UP, interfaces are required to facilitate communication between the AGF-CP and AGF-UP.

4.2.3.1 Management Interface

The AGF-CP provides a Management Interface (Mi) for configuration shown in Figure 4-3. The AGF-CP manages its associated AGF-UPs and is responsible for pushing configurations and retrieving operational

state and status to and from the AGF-UPs. Some examples of the configurations that are pushed to the AGF-UPs are routing protocol configuration and templates.

It must be noted that an AGF-CP can be deployed with a variety of AGF-UPs or even B-UPF, described in section 4.3, from different vendors. Each vendor's user plane is unique, with different internal representation of system resources, different hardware resources and different physical configurations which are all transparent to the AGF-CP.

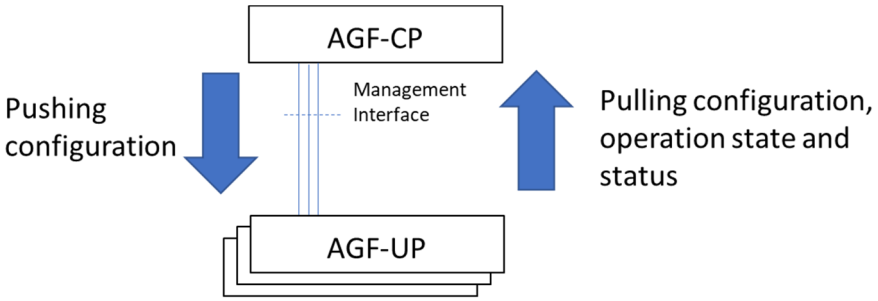

Figure 4-3: AGF CUPS Management Interface

4.2.3.2 Control Packet Redirection Interface

A separate interface is required to forward and tunnel control packets such as FN-RG control packets (DHCP and PPPoE) and control packets (DHCP) from the 5GC through the user plane to the control plane. Figure 4-4 is a flow diagram that provides an example of the control messages that are tunneled from wireline RGs through the AGF-UP to the AGF-CP.

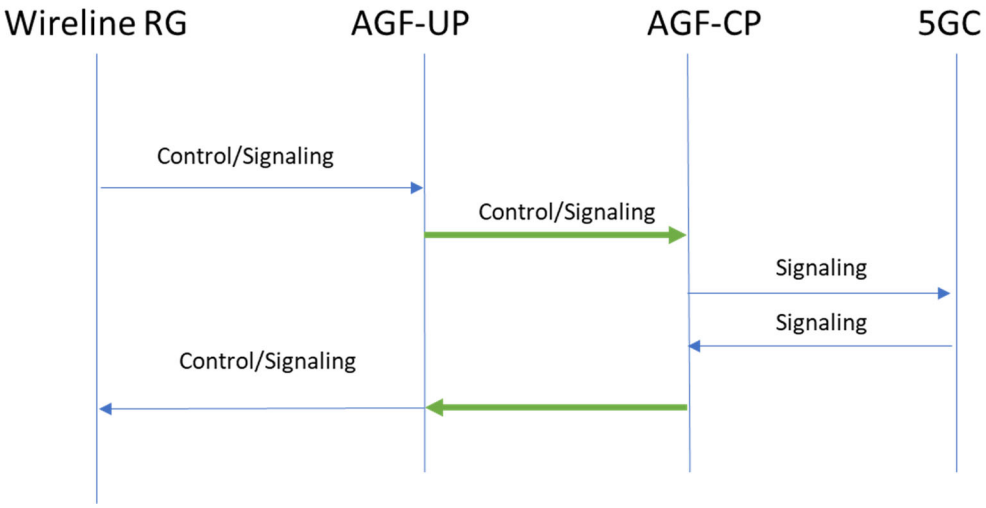

Figure 4-4: Example of Control and User Plane control message exchange

This shows that a Control Packet Redirect Interface (CPR Interface) and Server Control Packet Redirect Interface (Server CPR Interface) between the AGF-UP and AGF-CP is required for triggering subscriber authentication. The CPR interface is not performing the authentication. The network separation between AGF-CP and AGF-UP can vary from a small layer 2 domain to a layer 3 multi hop network. Therefore, control packets are sent over a tunnel. Figure 4-5 below illustrates the requirement of a CPR Interface and Server CPR Interface.

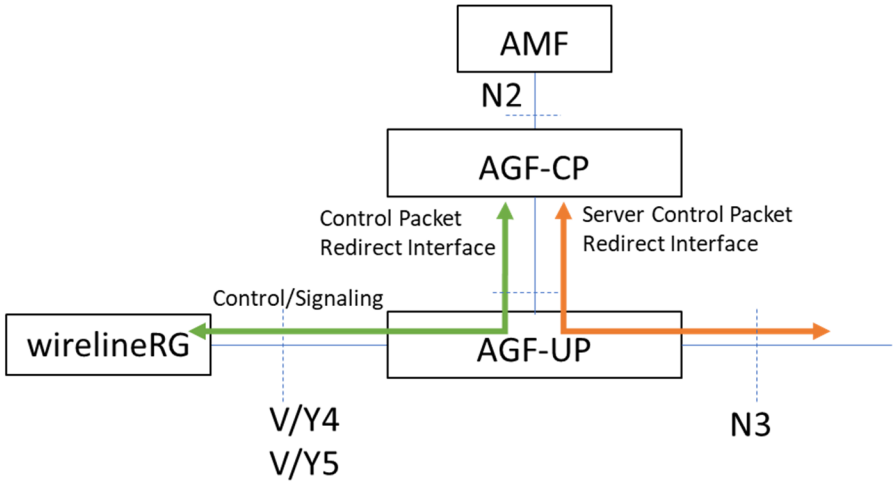

Figure 4-5: Control Packet Redirect Interface

A wireline RG starts a broadband session with control messages. The AGF-UP must redirect these control messages to the AGF-CP. This default redirect rule is signaled by the AGF-CP to AGF-UP subsequently after a successful association between the AGF-CP and AGF-UP. The AGF-UP can have:

- Session context for the subscriber session (a known session on the AGF-UP)
- No session context for a subscriber (an unknown subscriber on the AGF-UP, for example, new subscriber connecting to the network for the first time).

Since the AGF-CP is decoupled from the AGF-UP, the AGF-CP has no access circuit information (for example logical port, etc.). Therefore, the AGF-UP is required to include data plane information as meta-data when redirecting control packets.

The control packet exchange between the RG and AGF acting as an DHCP relay is realized by the existing default CPR Interface and subscriber session CPR Interface that are used for existing access models described in TR-459i2 [7]. The control packet exchange between AGF DHCP relay and external DHCP server is via UPF/SMF, however, requires a new CPR Interface channel between AGF-CP and AGF-UP for the AGF-CP to send DHCP control packets to UPF via the AGF-UP and for the AGF-UP to redirect external server originated DHCP control packets to the AGF-CP. This new session Server CPR Interface channel, depicted by the orange arrow in Figure 4-5 above, is per subscriber and used to exchange packets between UPF and the AGF-CP via the AGF-UP for that subscriber.

4.2.3.3 State Control Interface

The State Control Interface (SCi) is used to program a forwarding rule to redirect control packets between user plane and control plane. Once the wireline RG initiates a control message, the AGF-CP installs traffic forwarding rules to the AGF-UP as shown in Figure 4-6. Successful installation of the traffic rules is indicated by an acknowledgement from the AGF-UP. After the traffic rules are programmed onto the AGF-UP, the AGF-UP forwards the subscriber data and control traffic according to the rules.

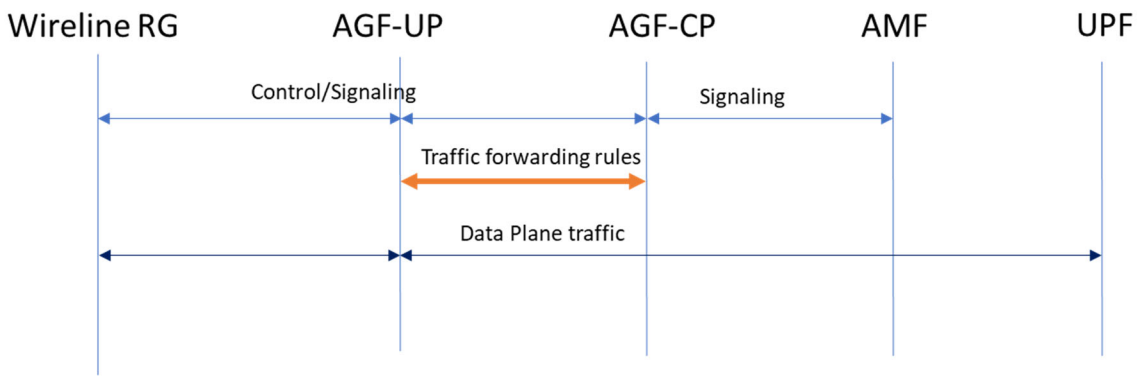

Figure 4-6: Example of Control Plane pushing forwarding rules to the User Plane

Figure 4-7 illustrates the third interface, SCi, that is required to program control message and data traffic detection and forwarding rules.

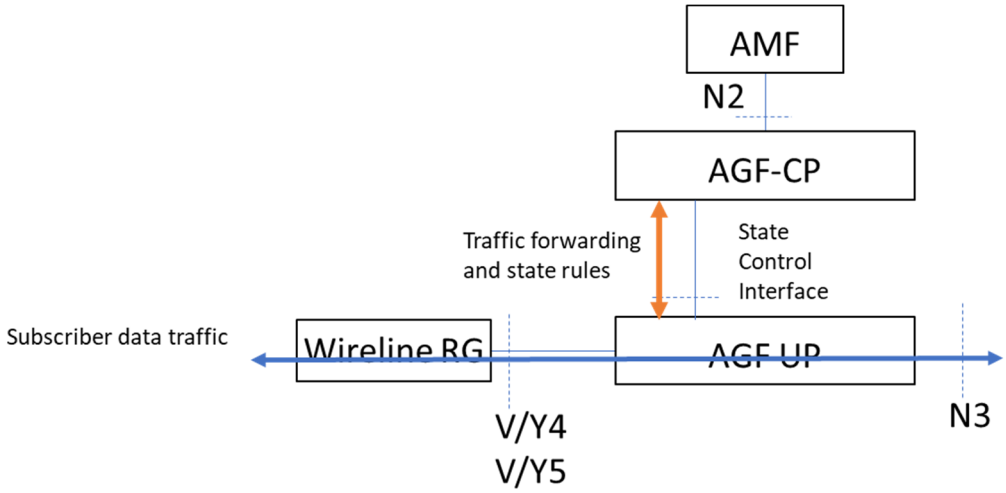

Figure 4-7: State Control Interface

4.3 Broadband-UPF (B-UPF) Architecture

The B-UPF is a combined User Plane function of the AGF-UP and the 3GPP defined UPF.

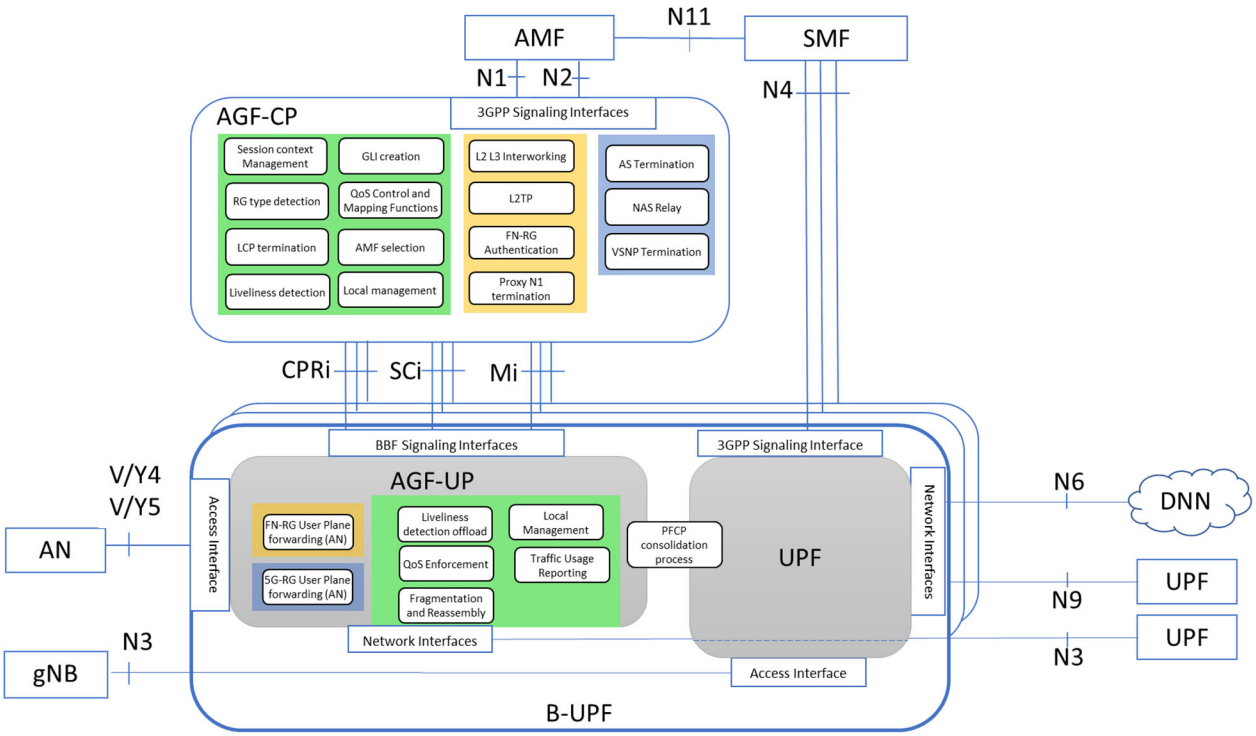

Figure 4-8: B-UPF Architecture

In this diagram there are two N3 interface:

1. The N3 interface from the AGF-UP Network Interfaces connects to an external UPF.
2. The N3 Interface from the UPF Access Interface to an external gNodeB.

4.3.1 B-UPF functions

The B-UPF contains both the AGF-UP and UPF. The B-UPF connects to both the AGF-CP and the SMF. The detail of the AGF-UP function is already covered in Section 4.2.2. The detailed interworking of the SMF and UPF is the work of 3GPP and is out of scope of this document. The B-UPF establishes two separate PFCP sessions, one with the AGF-CP and one with SMF (N4) respectively, for a single subscriber session. The B-UPF may consolidate processing PFCP forwarding rules, such as QoS rules to optimize the actual data forwarding rules to be programed on the B-UPF.

4.3.1.1 B-UPF Interfaces

The B-UPF interfaces consist of the same interfaces as an AGF-UP. In addition, the B-UPF supports the relevant 3GPP UPF interfaces, for example the N4 interfaces to communicate to the SMF, the N6 interface to the data network, or the N9 interface to another UPF.

The B-UPF also supports V/Y4 and V/Y5 interface towards 5G-RG and FN-RG respectively.

4.4 AGF CUPS QoS

For detailed description on AGF QoS use case and RG-LWAC, please refer to TR-456i2 [6] and TR-470i2 [8]. This document focuses on enabling the CUPS architecture to off the same AGF QoS functionalities. The objective is to apply the RG-LWAC QoS parameters received during the registration process to the subscriber PDU session(s). Section 4.4.1 to 4.4.4. describe QoS use cases.

4.4.1 Pre-provisioned QoS profile on AGF-UP

In this use case, the operator is expected to have prior knowledge of RG-LWAC parameters and derive different QoS profiles containing different combinations of RG-LWAC QoS parameters. These QoS profiles are pre-provisioned on the AGF-UP and can be expressed as names or identifiers. During subscriber session creation through the SCi interface, the AGF-CP references these pre-installed QoS profiles by names or identifiers on the AGF-UP to be applied to the subscriber session.

The four main types of profiles are:

1. An ingress profile that may include all Traffic Classes
2. An egress profile that may include all Traffic Classes
3. An egress scheduler profile (for both queues and policers)
4. An ingress scheduler profile (for both queues and policers)

Note: All other types of profiles are for FFS.

The method of how profiles are installed on the AGF-UP is out of scope for this document.

The advantage of utilizing QoS profile identifier, is to reduce the rules required (in terms of bits and bytes) to be sent over the SCi interface when provisioning the subscriber session forwarding rules.

[R-1] The AGF-CP MUST be able to send the QoS profile identifiers through the SCi interface.

[R-2] The AGF-UP MUST apply the QoS profile for all PDU sessions of a FN-RG.

[R-3] The AGF-UP MUST apply the QoS profile for all PDU sessions of a 5G-RG.

[R-4] The AGF-UP MUST support the QoS profiles which are referenced by the AGF-CP.

[R-5] The AGF-UP MUST support applying the QoS profile identifiers sent by the AGF-CP to a subscriber PDU session.

4.4.2 Dynamic QoS

In this case, the AGF-CP has the ability to apply the individual QoS parameters received from the RG-LWAC to the AGF-UP during subscriber session setup.

The advantage of dynamic QoS is to provide full flexibility to program individual QoS parameters as RG-LWAC which may not be pre-determined or deterministic.

[R-6] The AGF-CP MUST support signaling RG-LWAC dynamic QoS PFCP IEs to the AGF-UP through PFCP.

[R-7] The AGF-UP SHOULD support the signaling of dynamic QoS Capability through the PFCP IE BBF UP feature flag.

If [R-7] is supported, the following requirement applies:

[R-8] The AGF-UP MUST support the processing of dynamic RG-LWAC QoS IEs signaled through PFCP.

4.4.3 Dynamic QoS with pre-defined QoS Profile

In this case, the AGF-CP has the ability to apply both individual QoS parameters and QoS profiles received from the RG-LWAC to the AGF-UP during subscriber session setup.

This section is for FFS.

4.4.4 Default QoS profile

A default profile is pre-configured on the AGF-UP similar to Section 4.4.1. The default QoS profile is used when the AGF-CP does not include the QoS rules identifier during subscriber PFCP Session Establishment.

[R-9] The AGF-UP MUST support a default QoS profile.

[R-10] In the case of any errors in programming the QoS rules received from the AGF-CP, the AGF-UP MUST reject the establishment or modification of the PFCP session.

[R-11] In the case where no QoS rules is received from the AGF-CP, the AGF-UP MUST apply a locally configured default QoS profile to PDU sessions

5 WWC CUPS Procedure call flows

5.1 AGF-CP and AGF-UP PFCP Association

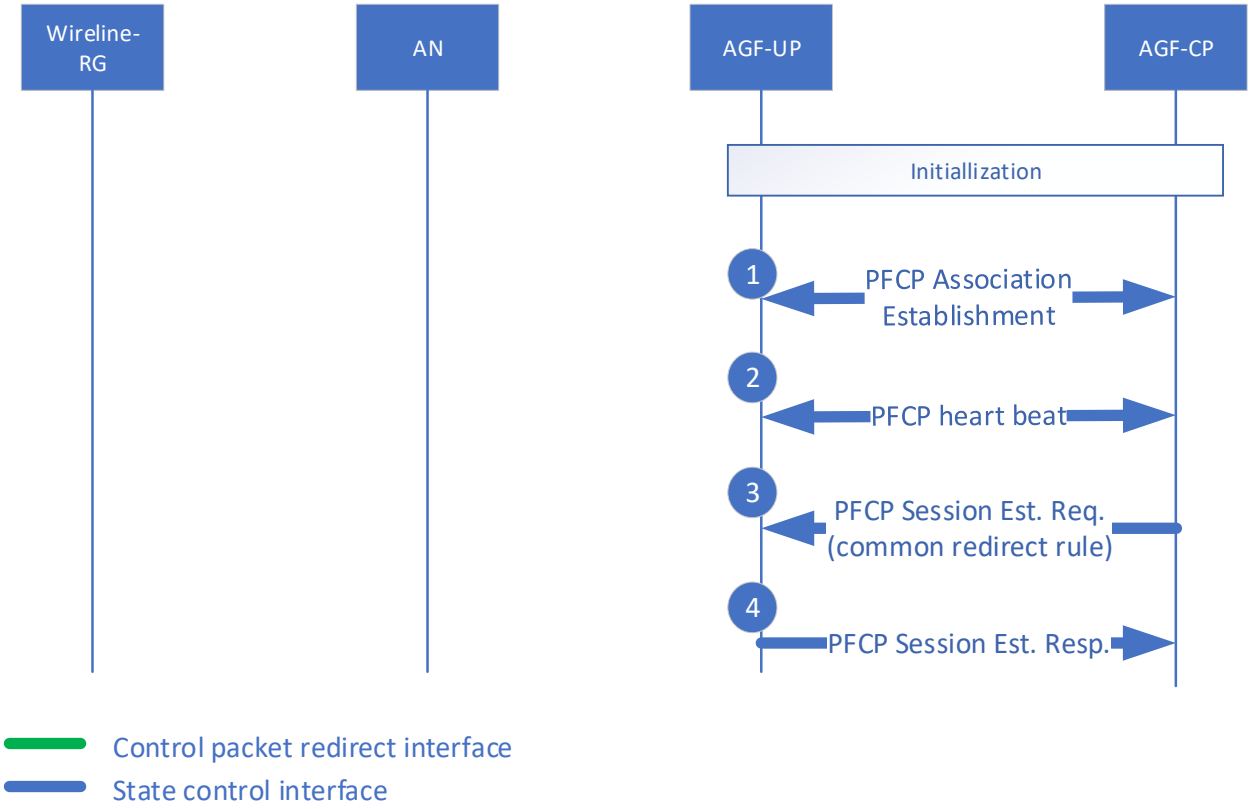

Figure 5-1: AGF-CP and AGF-UP PFCP Association

Prior to step 1 the initialization and the life cycle management of the AGF-UP and AGF-CP are beyond the scope of this document.

Steps:

1. Either AGF-CP or AGF-UP triggers a PFCP Association Setup procedure as outlined in 3GPP TS 29.244 section 6.2.6 [23]
   [conditional] If the AGF-UP supports the B-UPF function, it SHOULD indicate this to the AGF-CP during PFCP association such that the AGF-CP can use this information when constructing the WAgfInfo IE.
2. Once the PFCP association is formed, the AGF-CP and AGF-UP begin exchanging PFCP heartbeat messages.
3. The AGF-CP sends a PFCP Session Establishment Request, as outlined in 3GPP TS 29.244 [23] section 6.3.2, to program default forwarding rules to redirect unknown control and signaling messages to the AGF-CP for processing (i.e., FN-RG DHCP and PPPoE control packets., 5G-RG control packets).
   The redirection utilizes a default GTP tunnel with a NSH header for all control and signaling packets. The GTP tunnel TEID is allocated by the AGF-UP. The NSH header provides the AGF-CP context of the origin of the subscriber control packet such as the logical port.
4. The AGF-UP informs the AGF-CP that the forwarding rules have been successfully applied.

5.2 AGF-CP default redirection tunnel

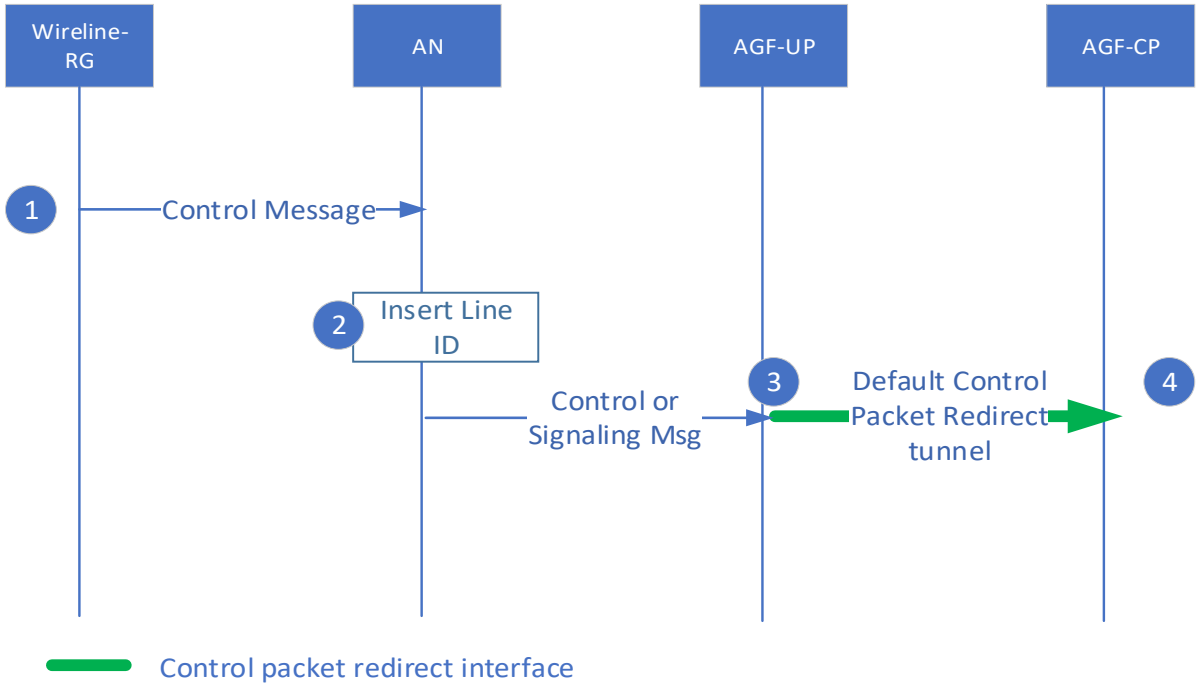

Figure 5-2: AGF-CP default redirection tunnel

For this section, the term Wireline-RG is used for representing both FN-RG and 5G-RG.

Note: For all additional CPR interface tunnel support (such as per logical port), please refer to TR-459i2 [7].

Steps:

1. The Wireline-RG connects to the wireline network for the first time. There are no PFCP sessions associated to this Wireline-RG yet. Examples of control or signaling packets that the Wireline-RG sends to the AN for requesting a service connection:
   - PADI
   - DHCP
   - DHCPv6
   - RS
2. The AN inserts a line-ID inside the control packet
3. The Wireline-RG control packet does not match any existing PFCP session PDI matching rules. The control packets match on the default Common Control Packet Redirect Rule and are redirected to the AGF-CP through the CPR interface. The AGF-UP tunnels the control packet through a GTP tunnel with an NSH header.
4. The AGF-CP receives the control packet and required information to prepare an N2 message to the AMF.

For FN-RG, AGF-CP will also initiate proxy N1 signaling via N2.

5.3 For FN-RG

Note the following procedures only apply to an AGF that has been configured to support adaptive mode.

5.3.1 FN-RG IP Session Initiation with PPPoE using immediate PFCP session setup

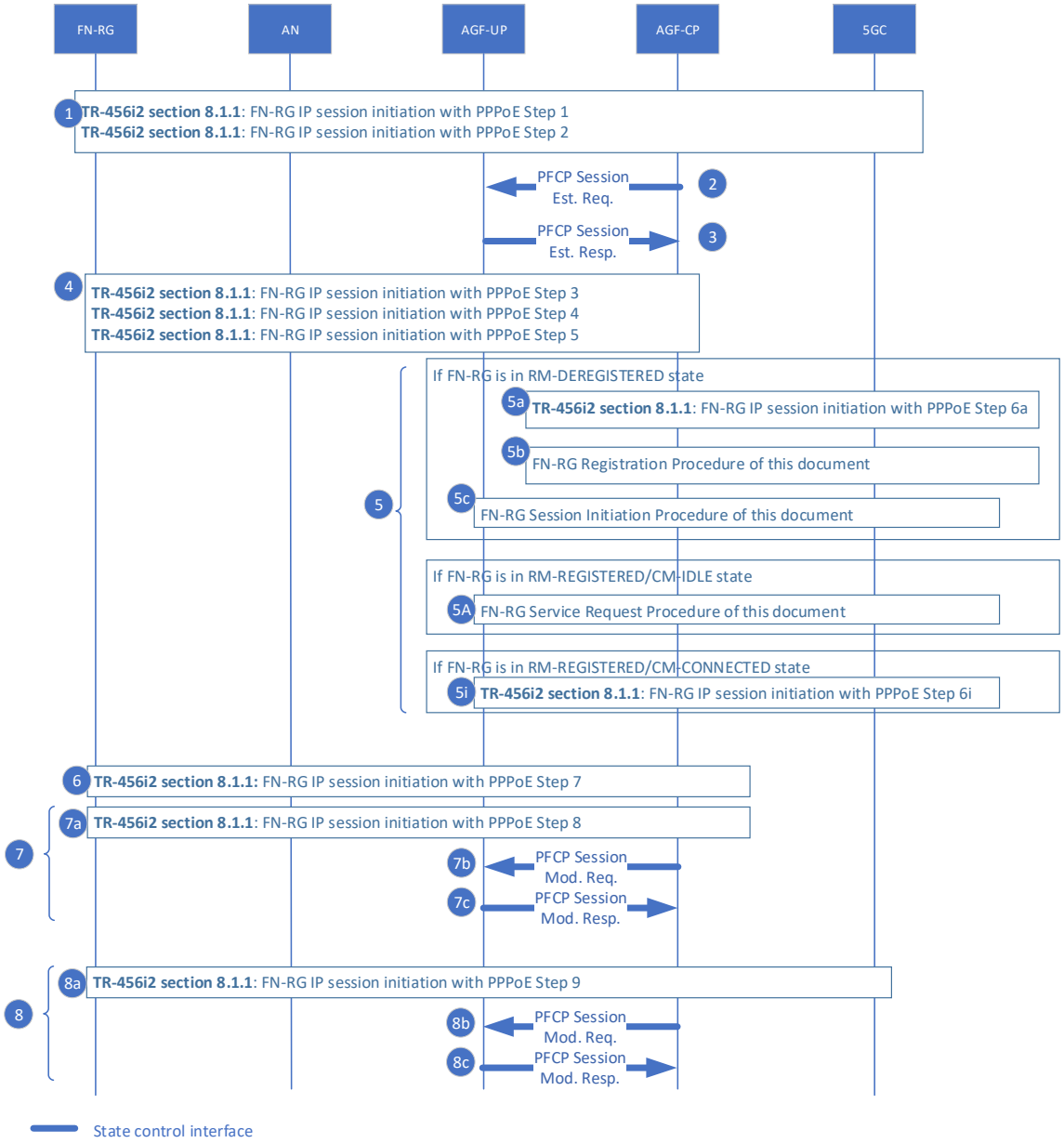

Figure 5-3: FN-RG IP Session Initiation with PPPoE using immediate PFCP session setup

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.1. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 and 2 of TR-456i2 [6]section 8.1.1

2. The AGF-CP determines that the PPPoE message is from a non-registered subscriber. This triggers the AGF-CP to perform a PFCP Session Establishment procedure with the AGF-UP to program PFCP forwarding rules to redirect PPPoE control messages to the AGF-CP.
3. The AGF-UP informs the AGF-CP that the forwarding rules were successfully programed with a PFCP Session Establishment Response message.
4. Correspond to step 3-5 of TR-456i2 [6] section 8.1.1. The PPPoE control messages are forwarded between the FN-RG and the AGF-CP utilizing the dedicated subscriber session redirect tunnel over the CPR Interface setup in step 2 and 3.
5. Correspond to step 6 of TR-456i2 [6] section 8.1.1
   If the FN-RG is in RM-DEREGISTERED
   - 5a. Correspond to 6a of TR-456i2 [6] section 8.1.1.
   - 5b. Correspond to 6b of TR-456i2 [6] section 8.1.1 and follows the registration procedure described in TR-456i2 [6] section 8.1.6
   - 5c. Correspond to 6c of TR-456i2 [6] section 8.1.1 but follows the PDU session procedure described in section 5.3.8 of this document

   If the FN-RG is in RM-REGISTERED/CM-IDLE
   - 5A. Correspond to 6A of TR-456i2 [6] section 8.1.1 but follows the Service Request procedure described in section 5.3.7 of this document

   If the FN-RG is in RM-REGISTERED/CM-CONNECTED
   - 5i. Correspond to 6i of TR-456i2 [6] section 8.1.1.
6. Correspond to step 7 of TR-456i2 [6] section 8.1.1
7. IPv4 address assignment is performed via NAS. The forwarding rules to include the IPv4 address would have occurred in step 5.
8. 8a correspond to Step 9 of TR-456i2 [6] section 8.1.1. 8b and 8c can take place in parallel with 8a, and multiple session modification requests/response may be required, one for RA and one for DHCPv6 (e.g., when delegated prefix is assigned) as these would occur independently.
   - 8b. A PFCP Session Modification Request is sent AGF-UP to update the data path rule with IPv6 address and/or prefix assigned to the FN-RG
   - 8c. A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.

Note:

- If the same FN-RG requires a new IP session, then a new PFCP session is established.
- For use case where DHCPv6 and SLAAC over PPPoE, the Session Server CPR Interface establishes a GTP tunnel to be used by IPv6 PDU session. In the IPv6CP case, the GTP tunnel would be used by the 5GC to forward both RA and DHCPv6 control packets. The Session Sever CPR Interface should be completed by 8a for both SLAAC and DHCPv6 address assignment. It is optional in step 8 for the AGF-CP to update the forwarding with the learnt the IPv6 address and/or prefix(es) of the FN-RG via snooping/proxy/relay.

5.3.2 FN-RG IP Session initiation with PPPoE using delayed PFCP session setup

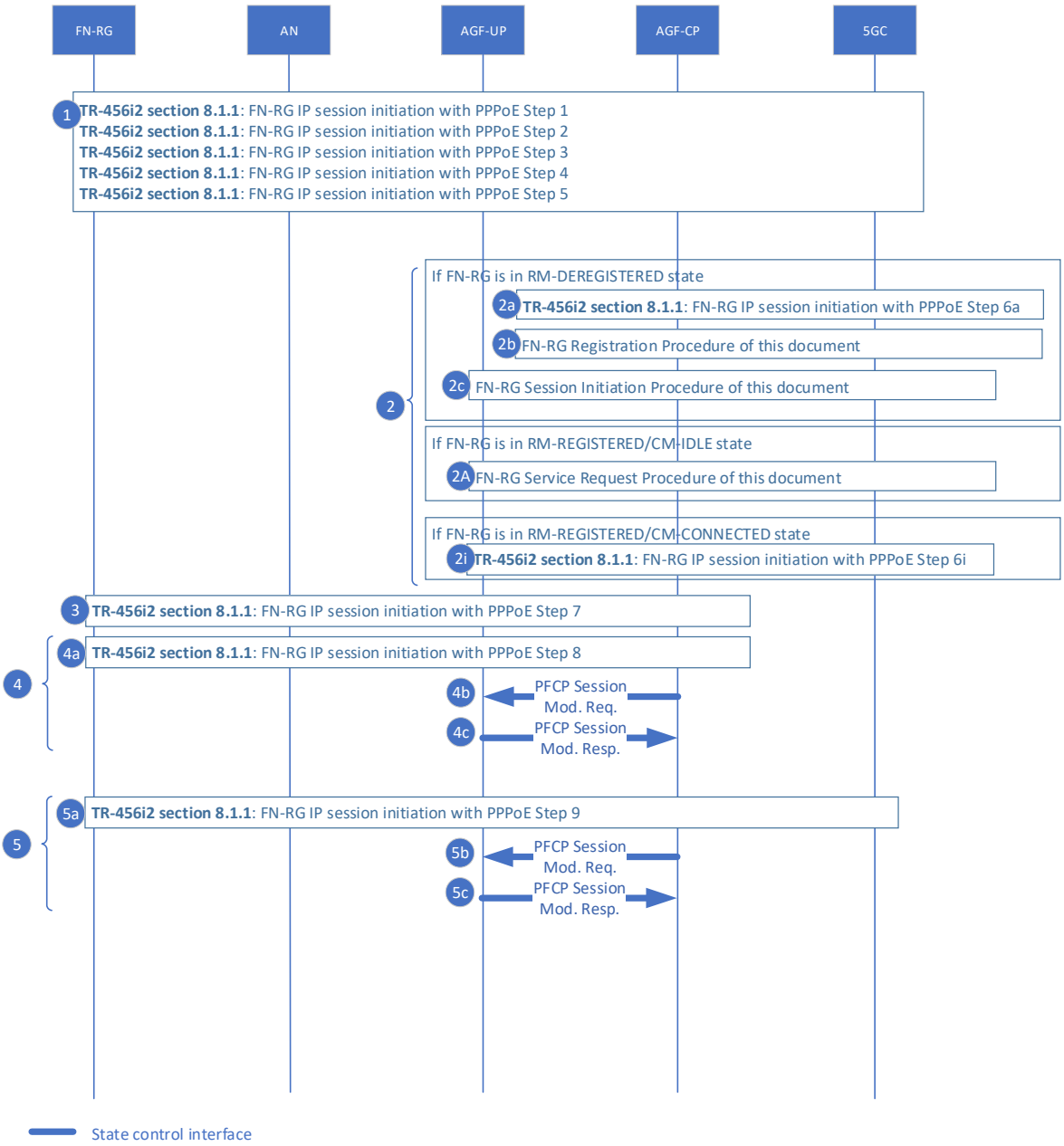

Figure 5-4: FN-RG PPPoE session initialization delay model

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.1. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 to 5 of TR-456i2 [6] section 8.1.1
2. Correspond to step 6 of TR-456i2 [6] section 8.1.1
   If the FN-RG is in RM-DEREGISTERED
   2a. Correspond to 6a of TR-456i2 [6] section 8.1.1.

2b. Correspond to 6b of TR-456i2 [6] section 8.1.1 but follows the FN-RG Registration Procedure session procedure described in TR-456i2 [6] section 8.1.6.

2c. Correspond to 6c of TR-456i2 [6] section 8.1.1. PFCP Session Establishment occurs in this step, please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.

If the FN-RG is in RM-REGISTERED/CM-IDLE

2A. Correspond to 6A of TR-456i2 [6] section 8.1.1. PFCP Session Establishment occurs in this step, please refer to section 5.3.7 for the FN-RG Service Request procedure in section 5.3.7 of this document.

If the FN-RG is in RM-REGISTERED/CM-CONNECTED

2i. Correspond to 6i of TR-456i2 [6] section 8.1.1. PFCP Session Establishment occurs within this step, please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.

3. Correspond to step 7 of TR-456i2 [6] section 8.1.1
4. IPv4 address assignment is performed via NAS. The forwarding rules to include the IPv4 address would have occurred in step 2.
5. 5a correspond to Step 9 of TR-456i2 [6] section 8.1.1. 5b and 5c can take place in parallel with 5a, and multiple session modification requests/response may be required, one for RA and one for DHCPv6 (e.g., when delegated prefix is assigned) as these would occur independently.

5b. A PFCP Session Modification Request is sent AGF-UP to update the data path rule with IPv6 address and/or prefix assigned to the FN-RG

5c. A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.

Note:

- If the same FN-RG requires a new IP session, then a new PFCP session is established.
- For use case where DHCPv6 and SLAAC over PPPoE, the Session Server CPR Interface establishes a GTP tunnel to be used by IPv6 PDU session. In the IPv6CP case, the GTP tunnel would be used by the 5GC to forward both RA and DHCPv6 control packets. The Session Sever CPR Interface should be completed by 5a for both SLAAC and DHCPv6 address assignment. It is optional in step 5 for the AGF-CP to update the forwarding with the learnt the IPv6 address and/or prefix(es) of the FN-RG via snooping/proxy/relay.

5.3.3 FN-RG IP Session Initiation with DHCPv4

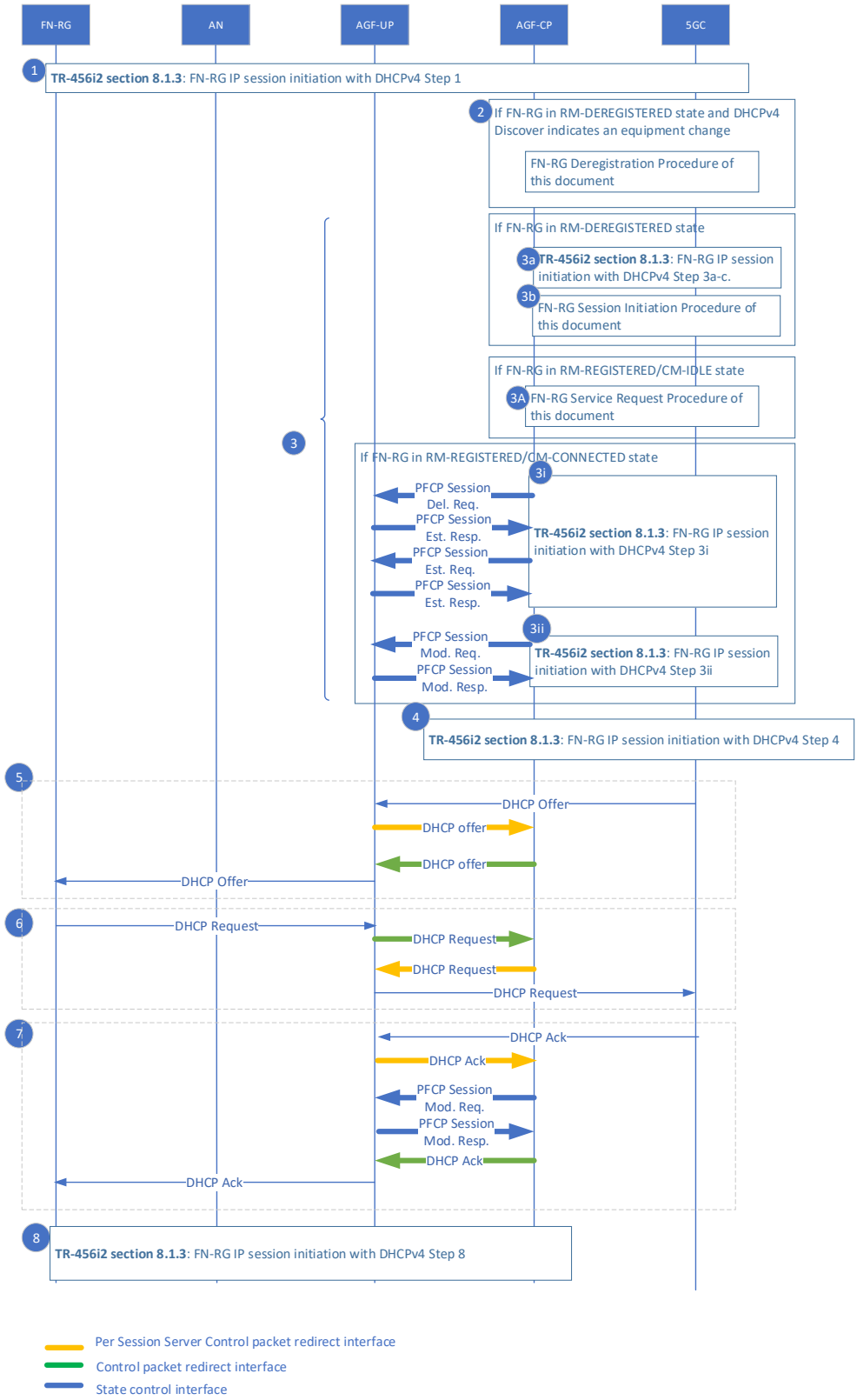

Figure 5-5: FN-RG IP session initialization with DHCPv4 model

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.3. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 of TR-456i2 [6] section 8.1.3
2. If the FN-RG is in RM-DEREGISTERED and DHCPv4 Discovery indicates an equipment change, please refer to section 5.3.9 for the FN-RG Deregistration procedure.
3. Correspond to step 3 of TR-456i2 [6] section 8.1.3
   If the FN-RG is in RM-DEREGISTERED
   - 3a. Correspond to 3a-c of TR-456i2 [6] section 8.1.3
   - 3b. Correspond to 3d of TR-456i2 [6] section 8.1.3. For PFCP Session Establishment occurs in this step, please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.

   If the FN-RG is in RM-REGISTERED/CM-IDLE
   - 3A. Correspond to 3A of TR-456i2 [6] section 8.1.3. PFCP Session Establishment occurs in this step, please refer to section 5.3.7 for the FN-RG Service Request procedure in section 5.3.7 of this document.

   If the FN-RG is in RM-REGISTERED/CM-CONNECTED
   - 3i. Correspond to 3i of TR-456i2 [6] section 8.1.3. Please refer to section 5.3.9 for the FN-RG deregistration procedure in this document, and please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.
   - 3ii The AGF-CP determines that the DHCP message is from a non-registered subscriber. This triggers the AGF-CP to perform a PFCP Session Establishment procedure with the AGF-UP to program PFCP forwarding rules to redirect DHCP control messages to the AGF-CP. Step 3i and 3ii of TR-456i2 [6] section 8.1.3 interleaves with PFCP Session Establishment Request. The request may include:
     - TEID request from the AGF-UP
     - QoS profile
     - PDU session ID
     - Matching on the logical port and Layer 2 header information.
4. Correspond to step 4 of TR-456i2 [6] section 8.1.3. The AGF-CP sends the DHCP discovery packet over the server session CPR interface to the AGF-UP. The AGF-UP further forwards the DHCP discovery packet to the UPF via the N3 interface.
5. DHCPv4 message offer may be redirected to AGF-CP for header manipulation, proxy, and snooping purposes. The AGF-CP performs DHCPv4 relay function.
6. DHCPv4 message request may be redirected to AGF-CP for header manipulation. The AGF-CP performs DHCPv4 relay function.
7. The 5GC sends a DHCP ack to the FN-RG to complete the DHCPv4 address assignment. The DHCPv4 packet is redirected to the AGF-CP for the AGF-CP to learn the IP address assigned. The AGF-CP may initiate a PFCP Session Modification procedure to update the traffic forwarding rules to update the match rule on the subscriber IPv4 address.
8. Correspond to step 8 of TR-456i2 [6] section 8.1.3.

Note:

- If the same FN-RG requires a new DHCPv4 session, then a new PFCP session is established.
- The Server CPR Interface should be completed by step 4 for the forwarding of DHCP control packets to and from the 5GC.

5.3.4 FN-RG IP Session Initiation with DHCPv6

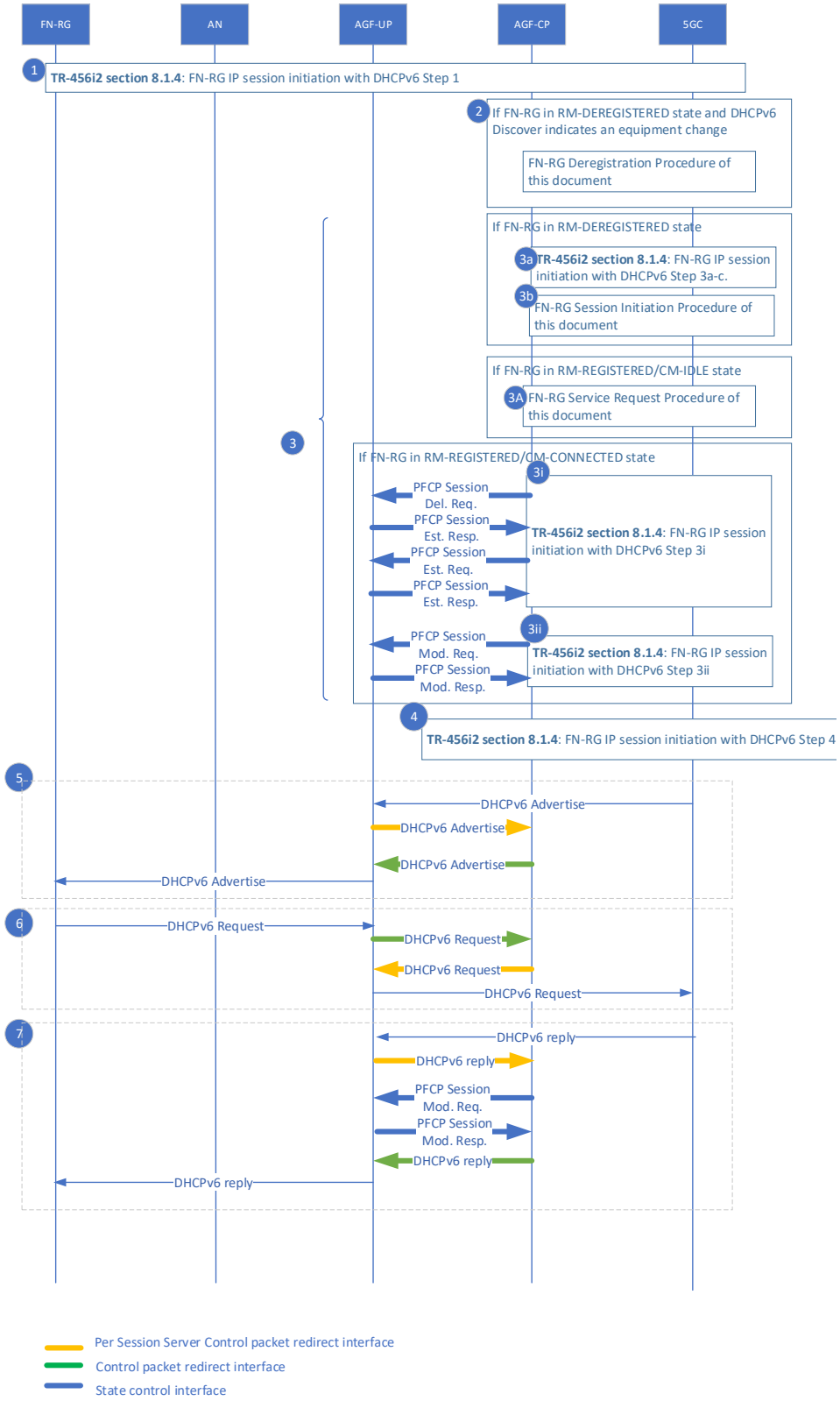

Figure 5-6: FN-RG IP session initialization with DHCPv6 model

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.4. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 of TR-456i2 [6] section 8.1.4
2. If the FN-RG is in RM-DEREGISTERED and DHCPv6 Solicit indicates an equipment change, please refer to section 5.3.9 for the FN-RG Deregistration procedure.
3. Correspond to step 3 of TR-456i2 [6] section 8.1.4

   If the FN-RG is in RM-DEREGISTERED

   3a. Correspond to 3a-c of TR-456i2 [6] section 8.1.4

   3b. Correspond to 3d of TR-456i2 [6] section 8.1.4. For PFCP Session Establishment occurs in this step, please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.

   If the FN-RG is in RM-REGISTERED/CM-IDLE

   3A. Correspond to 3A of TR-456i2 [6] section 8.1.4. PFCP Session Establishment occurs in this step, please refer to section 5.3.7 for the FN-RG Service Request procedure in section 5.3.7 of this document.

   If the FN-RG is in RM-REGISTERED/CM-CONNECTED

   3i. Correspond to 3i of TR-456i2 [6] section 8.1.4. Please refer to section 5.3.9 for the FN-RG deregistration procedure in this document, and please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.

   3ii The AGF-CP determines that the DHCPv6 message is from a non-registered subscriber. This triggers the AGF-CP to perform a PFCP Session Establishment procedure with the AGF-UP to program PFCP forwarding rules to redirect DHCPv6 control messages to the AGF-CP. Step 3i and 3ii of TR-456i2 [6] section 8.1.4 interleaves with PFCP Session Establishment Request. The request may include:

   - TEID request from the AGF-UP
   - QoS profile
   - PDU session ID
   - Matching on the logical port and Layer 2 header information.
4. Correspond to step 4 of TR-456i2 [6] section 8.1.4. The AGF-CP sends the DHCPv6 solicit packet over the server session CPR interface to the AGF-UP. The AGF-UP further forwards the DHCPv6 solicit packet to the UPF via the N3 interface.
5. DHCPv6 advertise message offer may be redirected to AGF-CP for header manipulation, proxy, and snooping purposes. The AGF-CP performs DHCPv6 relay function.
6. DHCPv6 request message may be redirected to AGF-CP for header manipulation. The AGF-CP performs DHCPv6 relay function.
7. The 5GC sends a DHCPv6 reply to the FN-RG to complete the DHCPv6 address assignment. The DHCPv6 packet is redirected to the AGF-CP for the AGF-CP to learn the IP address assigned. The AGF-CP may initiate a PFCP Session Modification procedure to update the traffic forwarding rules to update the match rule on the subscriber IPv4 address.
8. Correspond to step 8 of TR-456i2 [6] section 8.1.4.

Note:

- If the same FN-RG requires a new DHCPv6 session, then a new PFCP session is established.
- The Server CPR Interface should be completed by step 4 for the forwarding of DHCPv6 control packets to and from the 5GC.

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

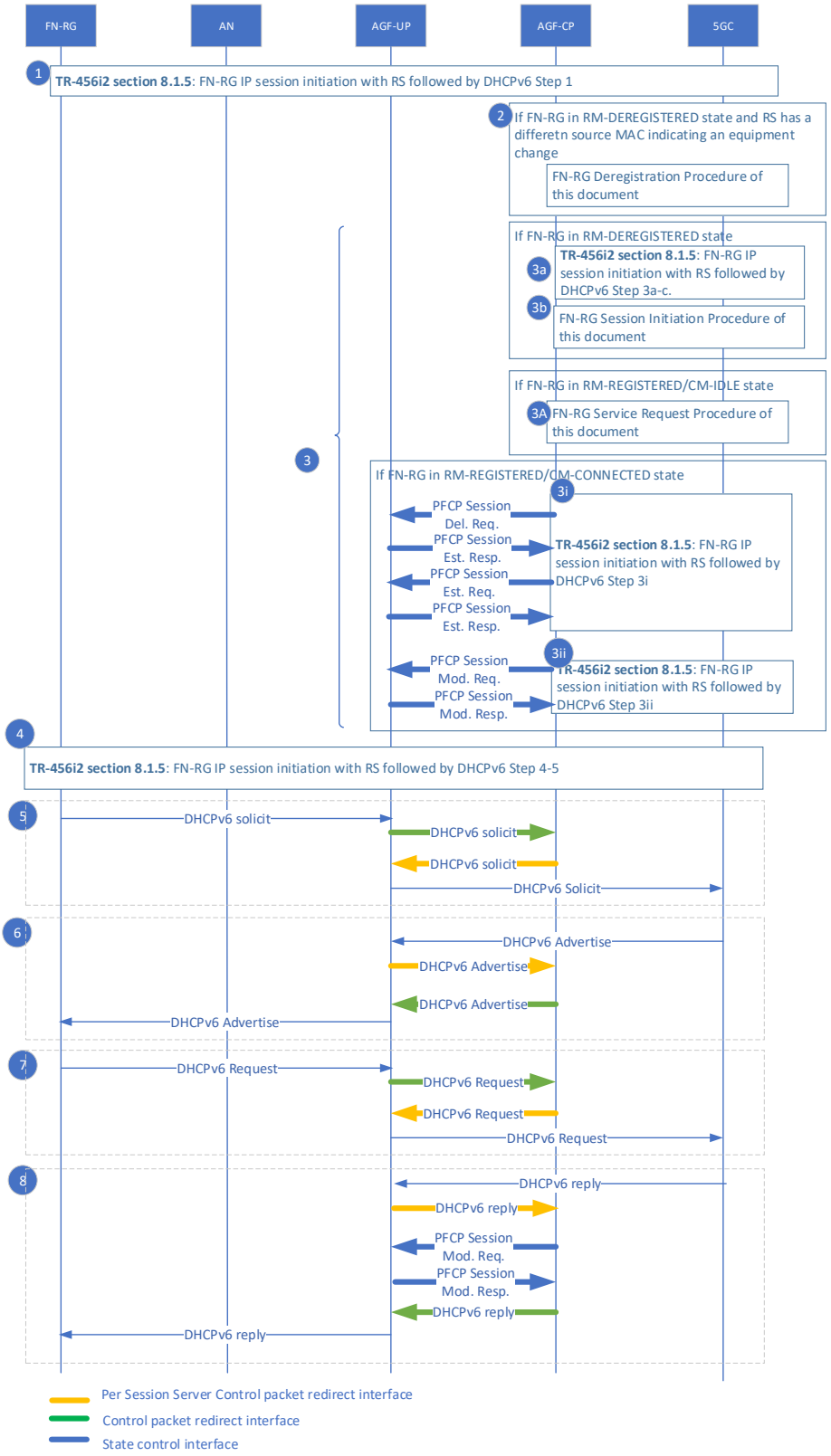

Figure 5-7: FN-RG IP session initialization with RS Followed by DHCPv6 model

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.5. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 of TR-456i2 [6] section 8.1.5
2. If the FN-RG is in RM-DEREGISTERED and Router Solicit indicates an equipment change, please refer to section 5.3.9 for the FN-RG Deregistration procedure.
3. Correspond to step 3 of TR-456i2 [6] section 8.1.5
   If the FN-RG is in RM-DEREGISTERED
   - 3a. Correspond to 3a-c of TR-456i2 [6] section 8.1.5
   - 3b. Correspond to 3d of TR-456i2 [6] section 8.1.5. For PFCP Session Establishment occurs in this step, please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.

   If the FN-RG is in RM-REGISTERED/CM-IDLE
   - 3A. Correspond to 3A of TR-456i2 [6] section 8.1.5. PFCP Session Establishment occurs in this step, please refer to section 5.3.7 for the FN-RG Service Request procedure in section 5.3.7 of this document.

   If the FN-RG is in RM-REGISTERED/CM-CONNECTED
   - 3i. Correspond to 3i of TR-456i2 [6] section 8.1.5. Please refer to section 5.3.9 for the FN-RG deregistration procedure in this document, and please refer to section 5.3.8 for the FN-RG session initiation procedure in this document.
   - 3ii The AGF-CP determines that the DHCPv6 message is from a non-registered subscriber. This triggers the AGF-CP to perform a PFCP Session Establishment procedure with the AGF-UP to program PFCP forwarding rules to redirect DHCPv6 control messages to the AGF-CP. Step 3i and 3ii of TR-456i2 [6] section 8.1.5 interleaves with PFCP Session Establishment Request. The request may include:
     - TEID request from the AGF-UP
     - QoS profile
     - PDU session ID
     - Matching on the logical port and Layer 2 header information.
4. Correspond to step 4 and 5 of TR-456i2 [6] section 8.1.5.
5. The RG sends the DHCPv6 solicit packet to the AGF-CP which will redirect the DHCPv6 solicit over the server session CPR interface to the AGF-UP. The AGF-UP further forwards the DHCPv6 solicit packet to the UPF via the N3 interface.
6. DHCPv6 advertise message offer may be redirected to AGF-CP for header manipulation, proxy, and snooping purposes. The AGF-CP performs DHCPv6 relay function.
7. DHCPv6 request message may be redirected to AGF-CP for header manipulation. The AGF-CP performs DHCPv6 relay function.
8. The 5GC sends a DHCPv6 reply to the FN-RG to complete the DHCPv6 address assignment. The DHCPv6 packet is redirected to the AGF-CP for the AGF-CP to learn the IP address assigned. The AGF-CP may initiate a PFCP Session Modification procedure to update the traffic forwarding rules to update the match rule on the subscriber IPv4 address.

Note:

- If the same FN-RG requires a new IpoEv6 session, then a new PFCP session is established.
- The Server CPR Interface should be completed by step 4 for the forwarding of both SLAAC and DHCPv6 control packets to and from the 5GC.

5.3.6 FN-RG IP Session Initiation using L2TP

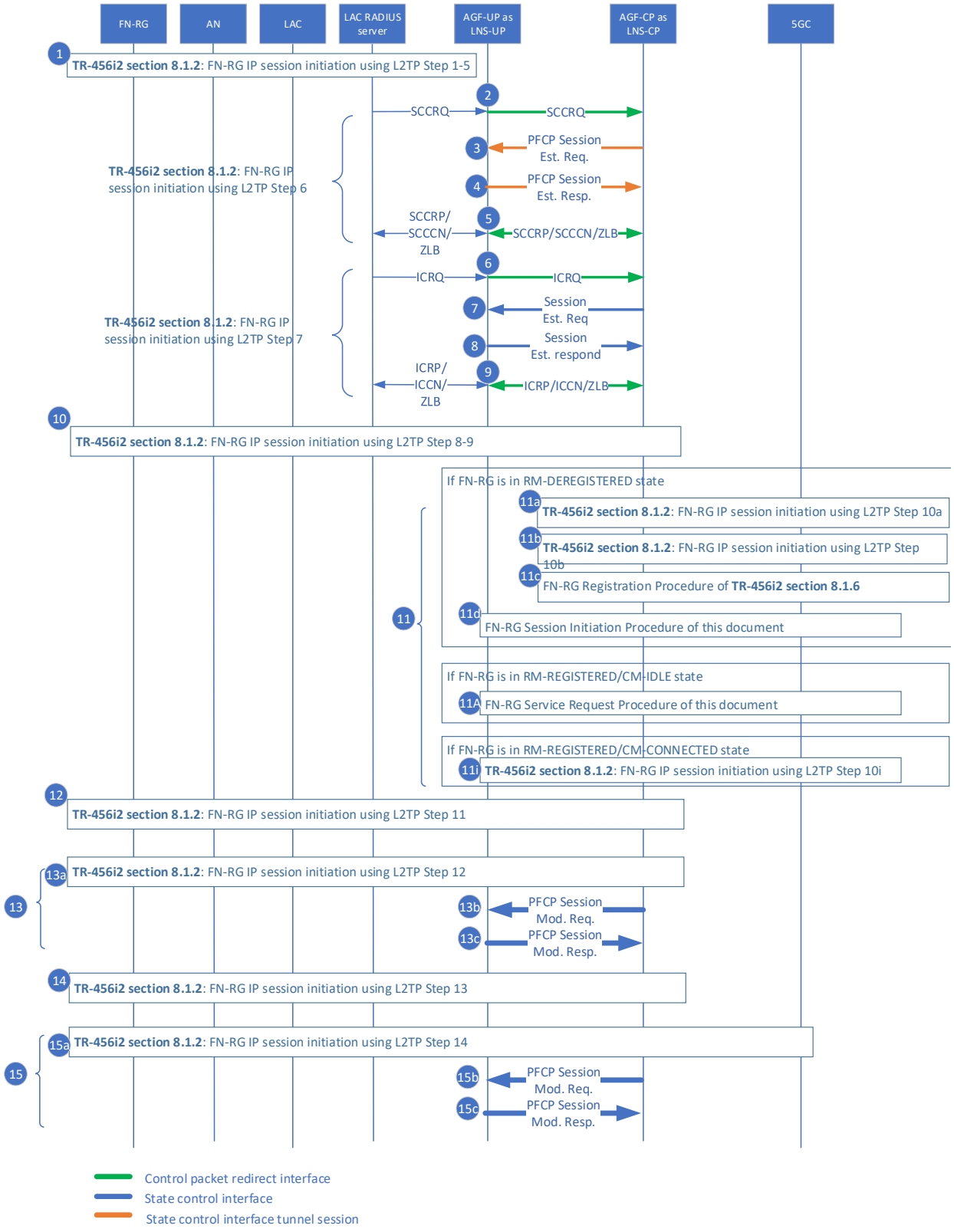

Figure 5-8: FN-RG IP session initialization using L2TP model

Steps:

1. Correspond to step 1 to 5 of TR-456i2 [6] section 8.1.2
2. Correspond to step 1 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
3. Correspond to step 2 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
4. Correspond to step 3 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
5. Correspond to step 4 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
6. Correspond to step 5 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
7. Correspond to step 6 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
8. Correspond to step 7 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
9. Correspond to step 8 of TR-459i2 [7] section 4.5.26 where the DBNG-CP and DBNG-UP is replaced by AGF-CP and AGF-UP respectively.
10. Correspond to step 8 and 9 of TR-456i2 [6] section 8.1.2 between FN-RG and AGF-CP
11. Correspond to step 10 of TR-456i2 section 8.1.2

    If the FN-RG is in RM-DEREGISTERED

    11a. Correspond to 10a of TR-456i2 [6] section 8.1.2.
    11b. Correspond to 10b of TR-456i2 [6] section 8.1.2.
    11c. Correspond to 10c of TR-456i2 [6] section 8.1.2 and follows the registration procedure described in TR-456i2 [6] section 8.1.6.
    11d. Correspond to 10d of TR-456i2 [6] section 8.1.2 but follows the PDU session procedure described in section 5.3.8 of this document.

    If the FN-RG is in RM-REGISTERED/CM-IDLE

    11A. Correspond to 10A of TR-456i2 [6] section 8.1.2 but follows the Service Request procedure described in section 5.3.7 of this document.

    If the FN-RG is in RM-REGISTERED/CM-CONNECTED

    11i. Correspond to 10i of TR-456i2 [6] section 8.1.2.
12. Correspond to step 11 of TR-456i2 section 8.1.2 between FN-RG and AGF-CP
13. 13a correspond to step 12 of TR-456i2 [6] section 8.1.2. 13b and 13c are optional since it is possible in step 11 to have programmed the data path forwarding rules including the IPv4 address already. 13b and 13c can take place in parallel with 13a.

    13b. [optional] A PFCP Session Modification Request is sent to the AGF-UP to update the data path rule with an IPv4 address assigned to the FN-RG
    13c. [optional] A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.
14. Correspond to step 13 of TR-456i2 [6] section 8.1.2
15. 15a correspond to step 14 of TR-456i2 section 8.1.2. 15b and 15c can take place in parallel with 15a. Step 15b and 15c may occur multiple times as exchanges may be required for RA-prefix and DHCPv6.

    15b. A PFCP Session Modification Request is sent AGF-UP to update the data path rule with IPv6 address and/or prefix assigned to the FN-RG
    15c. A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.

Note:

- The Server CPR Interface should be completed by step 15a.

5.3.7 Service Request Procedure for FN-RG

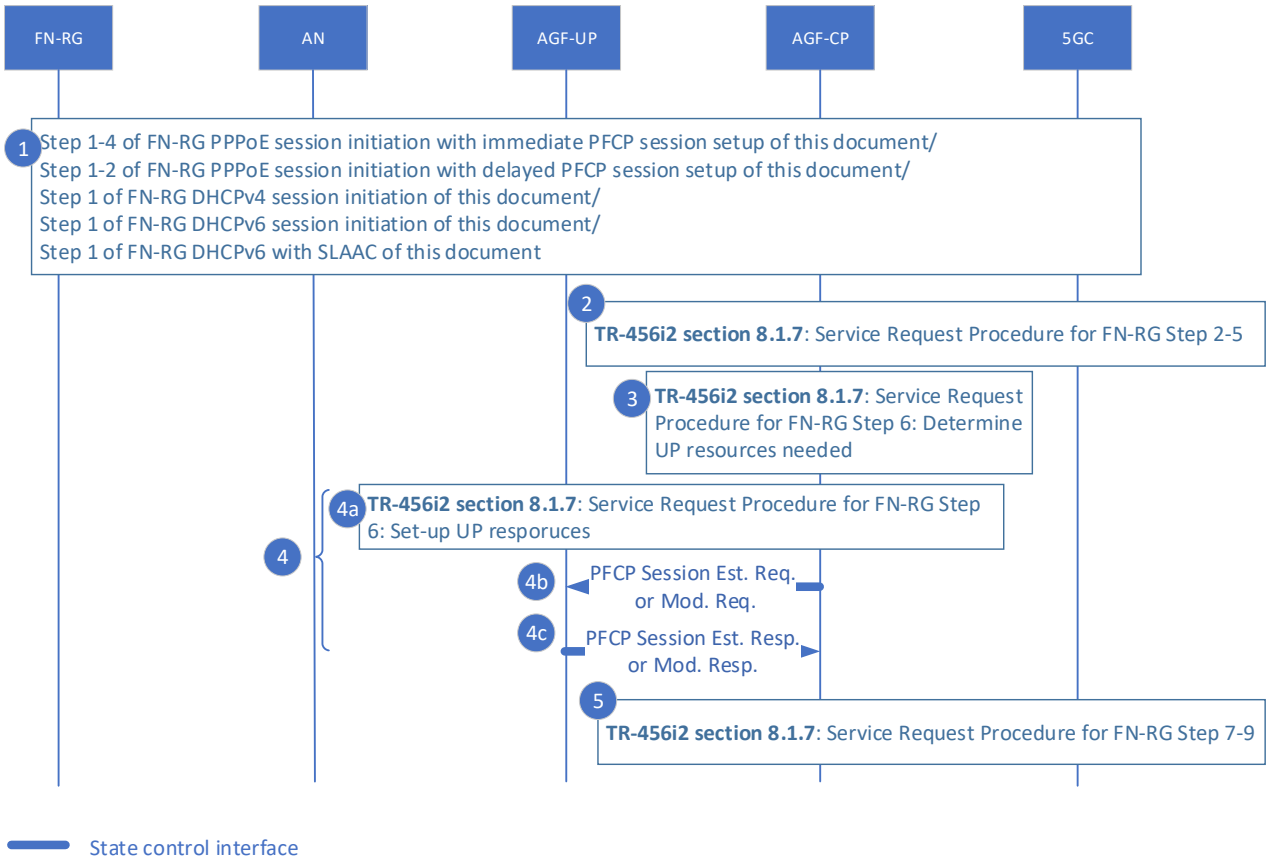

Figure 5-9: Service Request Procedure for FN-RG

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.7. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. In order to carry out the service request procedure, it is a pre-requisite that a connection exists between the FN-RG and AGF-CP via PPPoE, DHCP or SLAAC using one of:
   a. Steps 1-4 of FN-RG PPPoE session initiation with immediate PFCP session setup (Section 5.3.1)
   b. Steps 1 of FN-RG PPPoE session initiation with delayed PFCP session setup (Section 5.3.2)
   c. Step 1, 2, and 3A of FN-RG DHCPv4 session initiation (Section 5.3.3)
   d. Step 1, 2, and 3A of FN-RG DHCPv6 session initiation (Section 5.3.4)
   e. RS followed by DHCPv6 (Section 5.3.5).

   After authentication, the AGF-CP selects an AMF based on the AN parameters and local policy.
2. Correspond to step 2-5 of TR-456i2 [6] section 8.1.7.
3. Correspond to step 6 of TR-456i2 [6] section 8.1.7 where the AGF-CP “Determines the UP resources needed.”
4. 4a correspond to Step 6 of TR-456i2 [6] section 8.1.7 where the AGF-CP “Set-up UP resources”. 4b and 4c can take place in parallel with 4a.
   4b. [conditional, if this is for the FN-RG delay model] A PFCP Session Establishment Request is sent to the AGF-UP to update the data path rule.
   [conditional, if this is for the FN-RG immediate mode] A PFCP Session Modification Request is sent to the AGF-UP to update the data path rule.

4c. [conditional, if this is for the FN-RG delay model] A PFCP session establishment response is sent to inform the AGF-CP that the data rules are successfully installed. [conditional, if this is for the FN-RG immediate mode] A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.

5. Correspond to step 7-9 of TR-456i2 [6] section 8.1.7.

Note: The Session Server CPR Interface should be completed by step 4b for the 5GC to forward both RA and DHCPv6 control packets.

5.3.8 Session Initiation Procedure for FN-RG

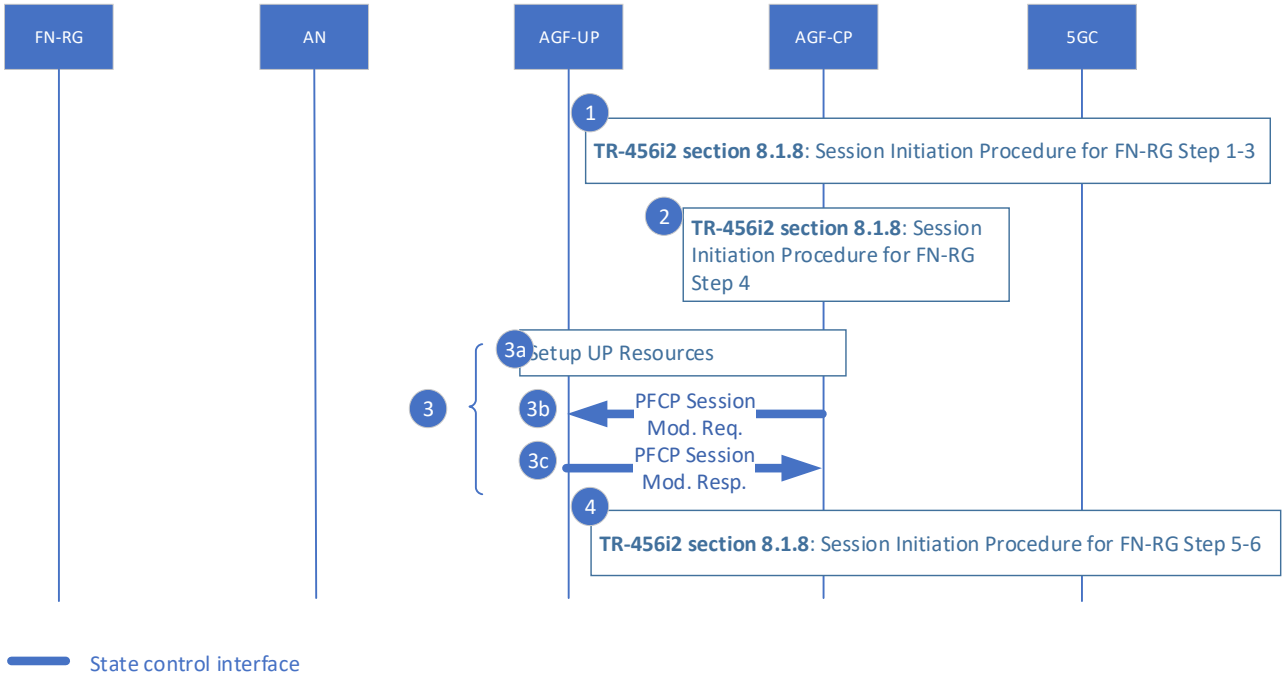

Figure 5-10: Session Initiation Procedure for FN-RG

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.7. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1-3 of TR-456i2 [6] section 8.1.8.
2. Correspond to step 4 of TR-456i2 [6] section 8.1.8.
3. 3a correspond to procedure taken after step 4 of TR-456i2 [6] section 8.1.8 where the AGF-CP setup resources on AGF-UP. 3b and 3c can take place in parallel with 3a.

   3b. A PFCP Session Modification Request is sent AGF-UP to update the data path rule.
   3c. A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.
4. Correspond to step 5-6 of TR-456i2 [6] section 8.1.8.

Note: The Session Server CPR Interface should be completed by step 3b for the 5GC to forward both RA and DHCPv6 control packets.

5.3.9 Deregistration Procedure for FN-RG

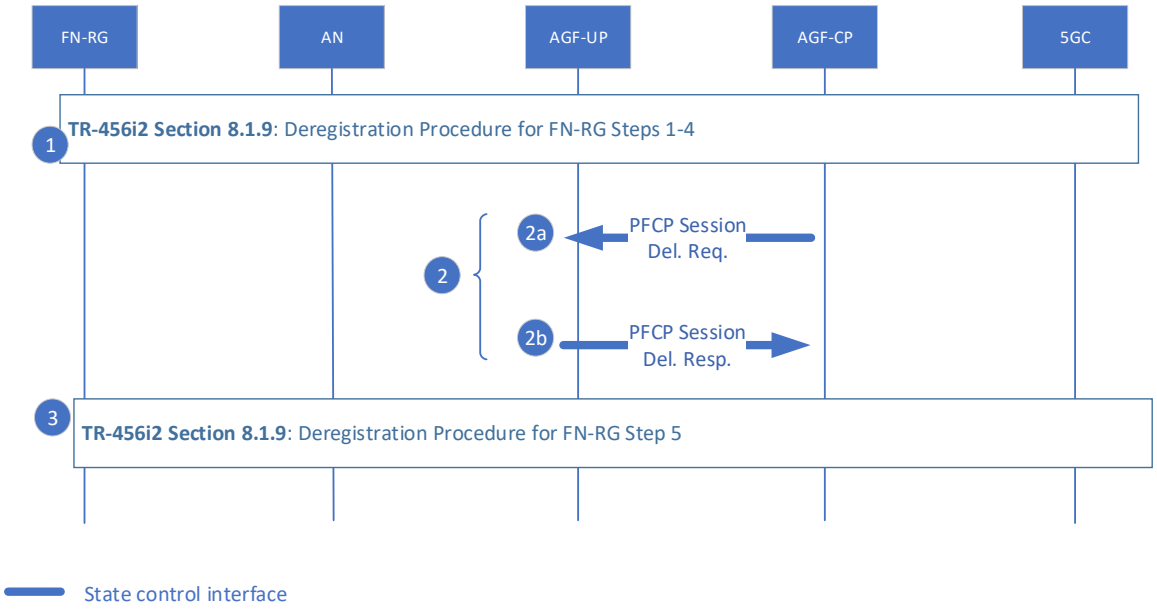

Figure 5-11: Deregistration Procedure for FN-RG

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.1.9. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 to 4 of TR-456i2 [6] section 8.1.9
2. 2a. A PFCP session deletion request is sent to the AGF-UP to remove the PFCP session for the FN-RG
   2b. A PFCP session deletion response is sent to inform the AGF-CP that the deletion was successful.
3. Correspond to step 5 of TR-456i2 [6] section 8.1.9

Note: The termination of a single IP session only deletes the associate PFCP session. All other PFCP sessions for other IP sessions of the FN-RG are to remain connected.

5.3.10 Support for Static IPv4 Addressing

This section corresponds to TR-456i2 [6] section 8.1.14. To construct the Line as per TR-456i2 [6] “2. Line ID and/or Line ID Source for a Static subscriber”.

- Corresponding to 2a of TR-456i2 [6] section 8.1.14: The Line ID (circuit ID and/or remote ID) is locally configured on the AGF-UP and is sent via the NSH header.

- Corresponding to 2b of TR-456i2 [6] section 8.1.14: Once the subscriber IP data packet is sent to the AGF-CP via the CPR Interface, a local configuration can map the IP address can correspond circuit or remote ID. For the GLI can be constructed by the VLAN(s)/MAC/Port/IP address retrieved from the NSH header information and/or the IP Address from the customer packet.
    - To specify a specific port or VLAN for the static IP subscriber, the AGF-CP and program as specific forwarding rule for the default CPR Interface specifying a specific port or VLAN to be redirected to the CP.

- A sudden change of the MAC address of the subscriber will send the subscriber traffic to the default CPR Interface, as the foreign MAC address will no longer match per session CPR Interface.
- To protect the AGF-CP from unwanted static IP traffic, the AGF-CP should support R-53, and R-54 of TR-459i2 [7].

5.4 For 5G-RG

5.4.1 5G-RG Registration Management Procedure

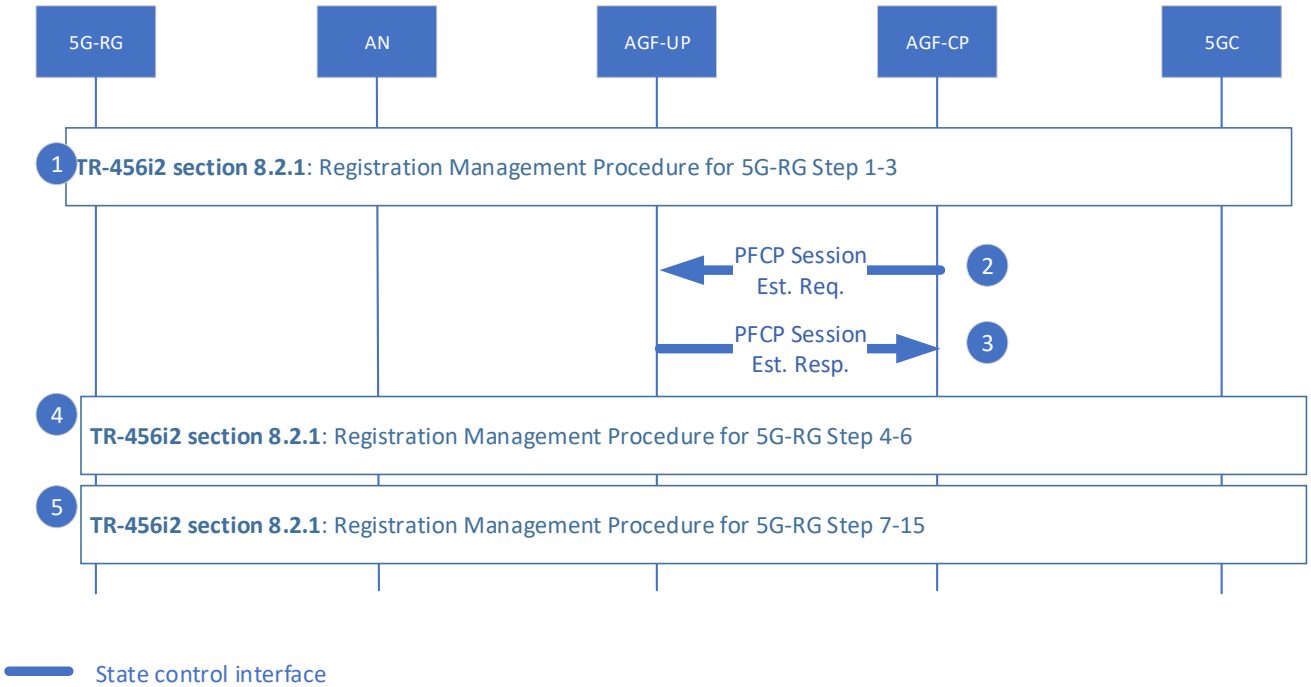

Figure 5-12: 5G-RG Registration Management Procedure

Note: For delayed model, the latest point where PFCP Session Establishment Request MUST occur is after AGF-CP receiving LCP ACK. Please refer to TR-459i2 [7] section 6.5.1 for more information.

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.2.1. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 to 3 of TR-456i2 [6] section 8.2.1
2. When the AGF-CP determines that the PPPoE message is from a non-registered subscriber, this triggers the AGF-CP to perform a PFCP Session Establishment with the AGF-UP to program PFCP forwarding rules to redirect control and signaling messages to the AGF-CP.
3. The AGF-UP informs the AGF-CP that the forwarding rules were successfully programed with a PFCP Session Establishment Respond message.
4. Correspond to step 4 to 6 of TR-456i2 [6] section 8.2.1
5. Correspond to step 7 to 15 of TR-456i2 [6] section 8.2.1

5.4.2 5G-RG Service Request Procedure via W-5GAN

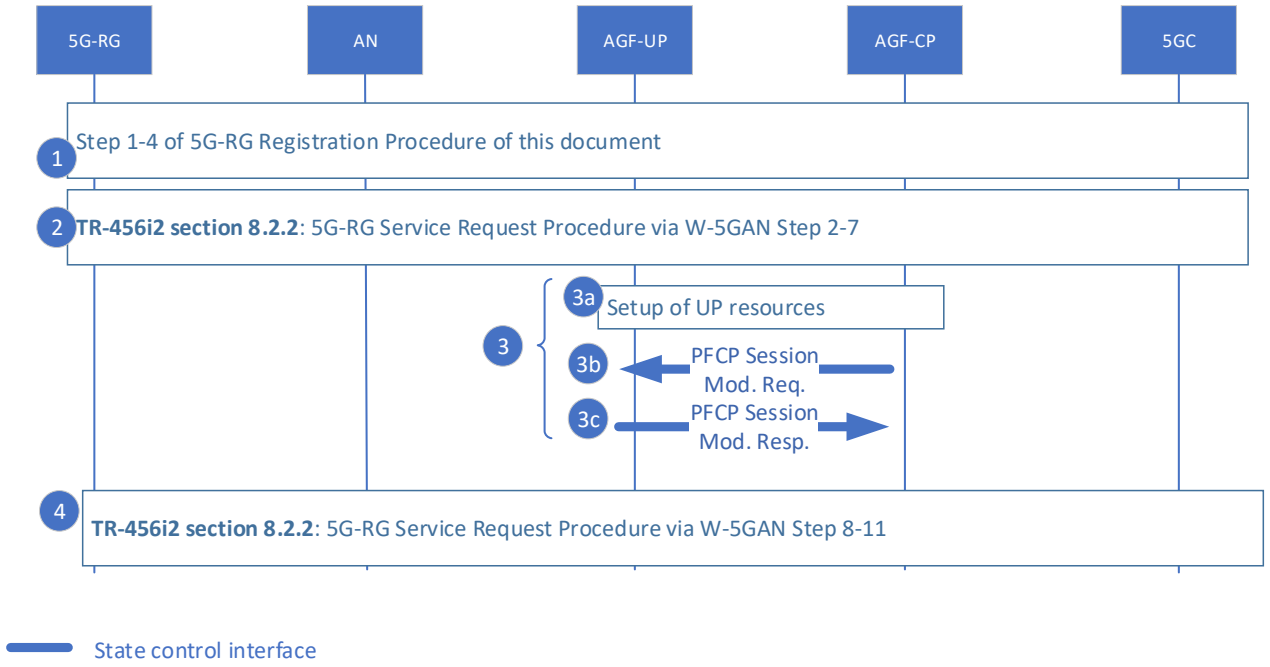

Figure 5-13: 5G-RG Service Request Procedure

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.2.2. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. The 5G-RG connects to AGF-CP as per steps 1 to 4 of the 5G-RG registration procedure of this document in section 5.4.1
2. Correspond to step 2 to 7 of TR-456i2 [6] section 8.2.2
3. 3a performs the actual setup of the UP resources after step 7 of TR-456i2 [6] section 8.2.2. 3b and 3c can take place in parallel with 3a.
   - 3b. A PFCP Session Modification Request is sent AGF-UP to update the data path rule to allow bi-direction data traffic forwarding for the 5G-RG PDU session.
   - 3c. A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.
4. Correspond to step 8 to 11 of TR-456i2 [6] section 8.2.2

5.4.3 5G-RG PDU Session Initiation/Establishment via W-5GAN

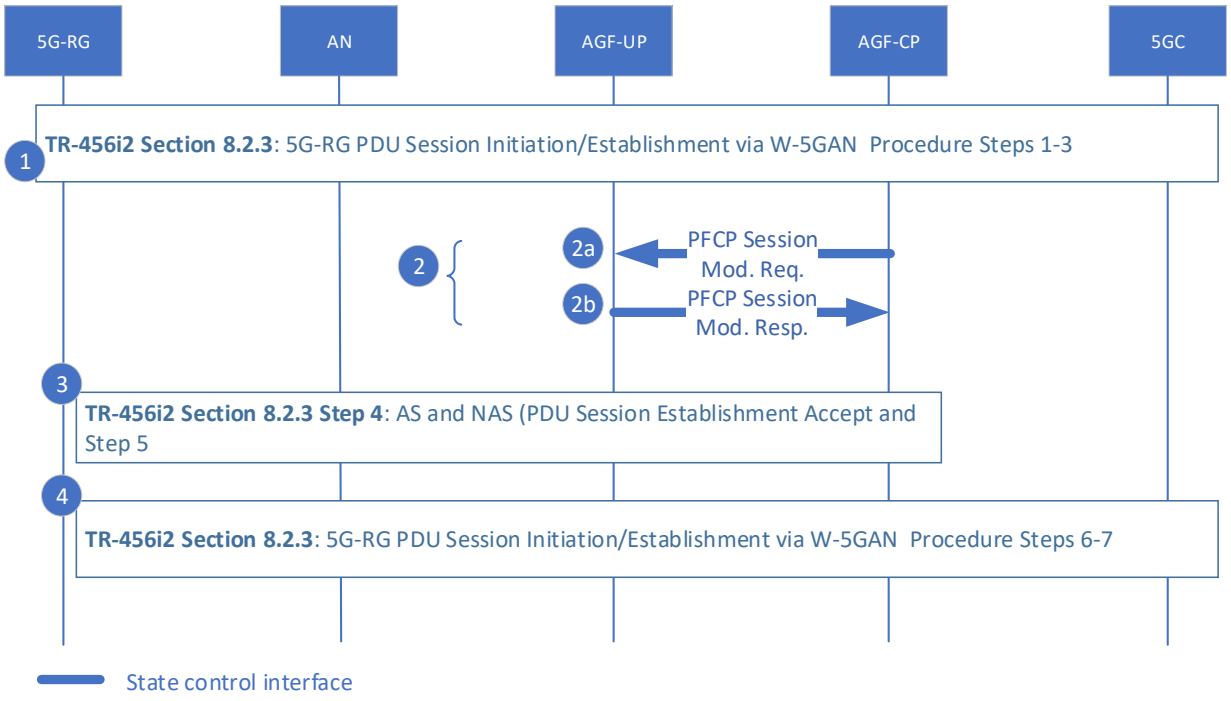

Figure 5-14: 5G-RG PDU Session Initiation/Establishment via W-5GAN

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.2.3. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 to 3 of TR-456i2 [6] section 8.2.3
2. PFCP Session Modification
   - 2a. A PFCP Session Modification Request is sent AGF-UP to update the data path rule to allow bi-direction data traffic forwarding for the 5G-RG PDU session.
   - 2b. A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.
3. Correspond to the rest of TR-456i2 [6] section 8.2.3 step 4 starting at the third paragraph and Step 5 of TR-456i2 [6] section 8.2.3
4. Correspond to step 6 to 7 of TR-456i2 [6] section 8.2.3

5.4.4 Deregistration Procedure for 5G-RG

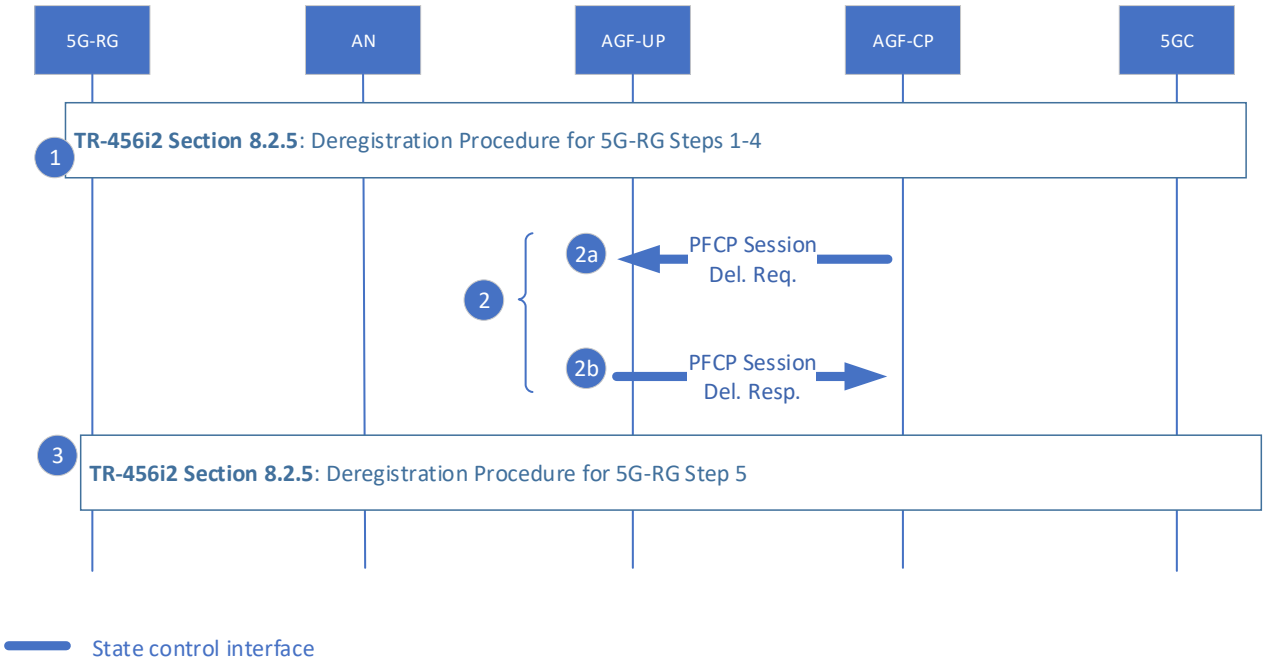

Figure 5-15: Deregistration Procedure for 5G-RG

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.2.5. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 to 4 of TR-456i2 [6] section 8.2.5
2. 2a. A PFCP session deletion request is sent to the AGF-UP to remove the PFCP session for the 5G-RG.
   2b. A PFCP session deletion response is sent to inform the AGF-CP that the deletion was successful.
3. Correspond to step 5 of TR-456i2 [6] section 8.2.5

5.4.5 5G-RG or Network Requested PDU Session Modification via W-5GAN

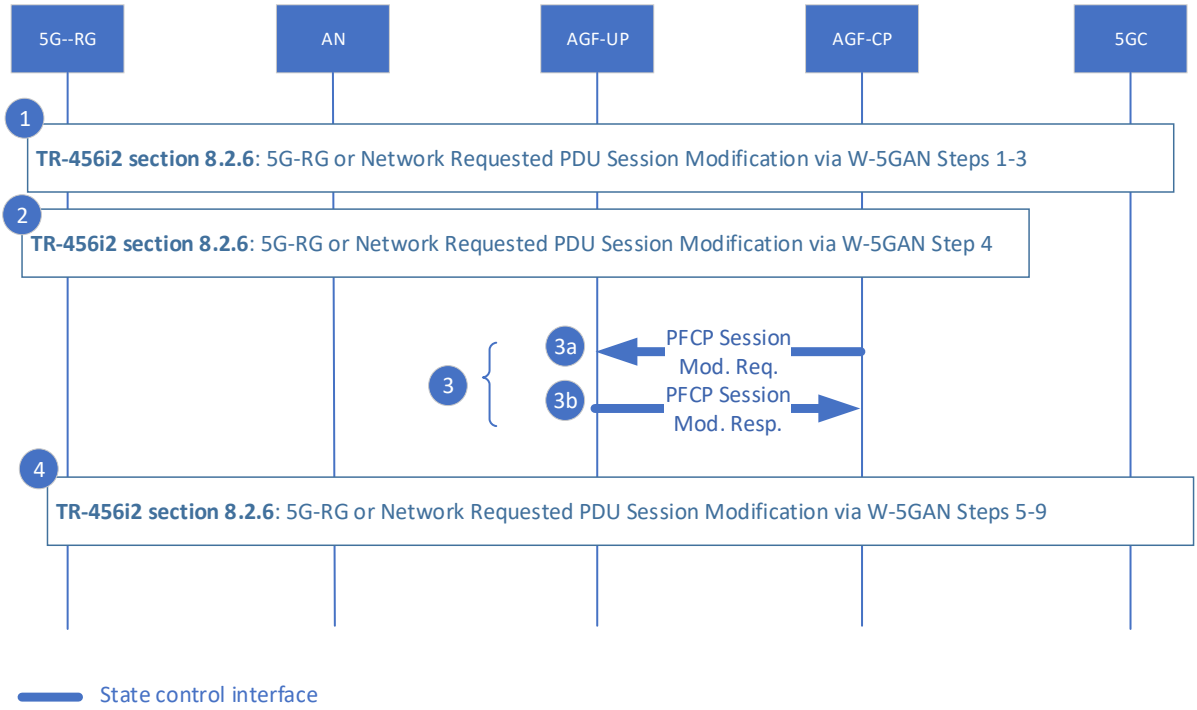

Figure 5-16: 5G-RG or Network Requested PDU Session Modification via W-5GAN

This call flow corresponds to the call flow described in TR-456i2 [6] section 8.2.6. The messaging between the AGF-CP to AMF utilizes the N2 interface.

Steps:

1. Correspond to step 1 to 3 of TR-456i2 [6] section 8.2.6
2. Correspond to step 4 of TR-456i2 [6] section 8.2.6
3. PFCP Session Modification
   - 3a. A PFCP Session Modification Request is sent AGF-UP to update the data path rule to allow bi-direction data traffic forwarding for the 5G-RG PDU session.
   - 3b. A PFCP Session Modification Response is sent to inform the AGF-CP that the data rules are successfully installed.
4. Correspond to step 5 to 9 of TR-456i2 [6] section 8.2.6

5.5 B-UPF call flow correlating Network Instance and F-TEID

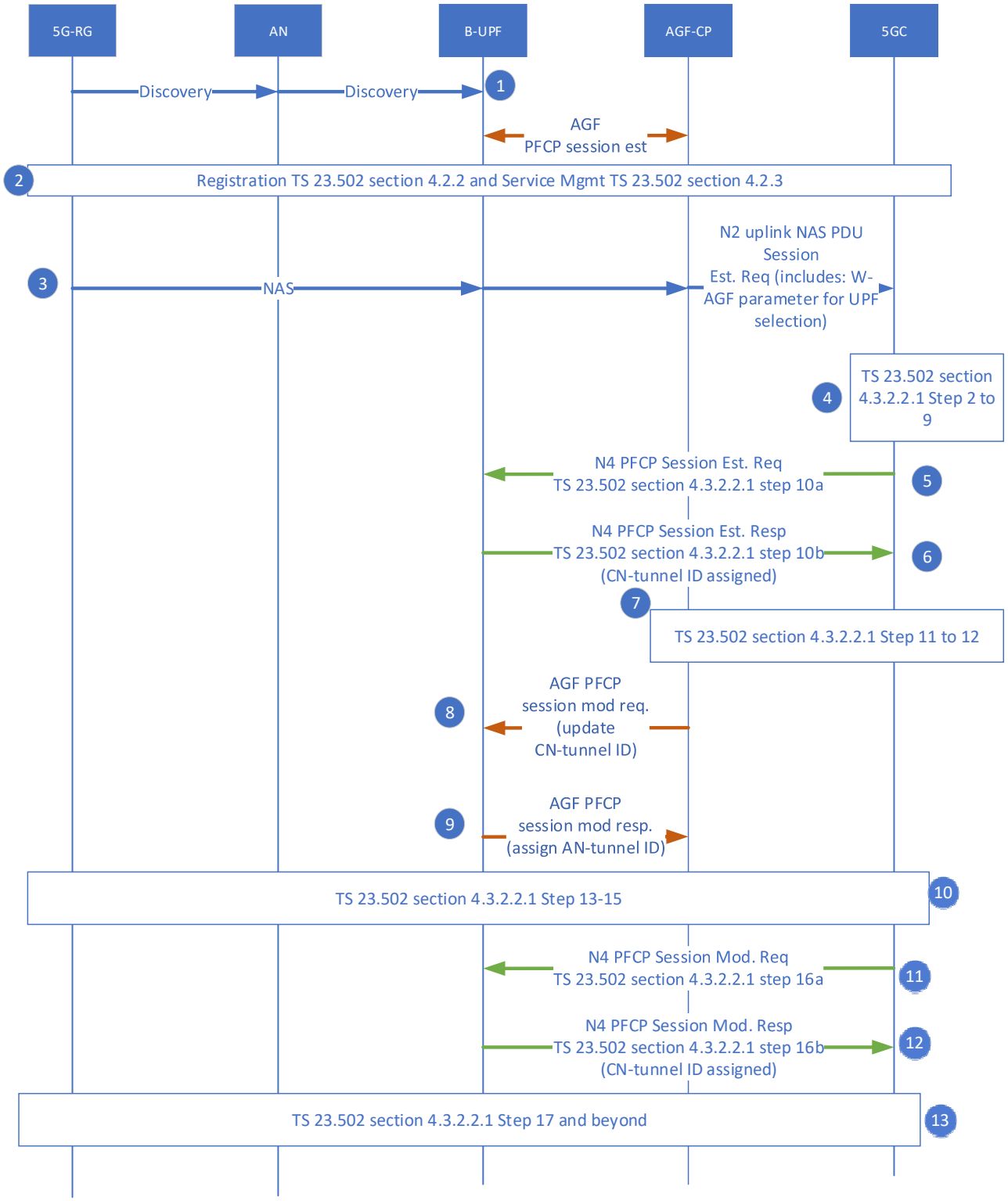

Figure 5-17: B-UPF call flow correlating Network Instance and F-TEID

Steps:

1. The AGF-CP initiates a PFCP session after the first discovery message from the 5G-RG. The AGF-CP instructs the B-UPF to redirect control and signaling to AGF-CP through the CPR interface. The data path information available only includes access information (the Logical port of 5G-RG and Ethernet header of 5G-RG). However, the forwarding for the network is still missing (TEID, Network Instance)

2. The 5G-RG and the 5GC finishes Registration Management Procedure and Service Request Procedure as highlighted in TS 23.502 [21] section 4.2.2 and 4.2.3.
3. The 5G-RG initiates a PDU Session Establishment Request as highlighted in TS 23.502 [21] section 4.3.2.2 UE Requested PDU Session Establishment step 1. In this case, the AGF-CP includes the B-UPF as the W-AGF parameter as highlighted in TR-456i2 [6].
4. The 5GC completes TS 23.502 [21] section 4.3.2.2.1 step 2 to 9. The UPF selection in step 8 is the B-UPF.
5. The 5GC establishes a PFCP session with the B-UPF through N4 following step 10a in TS 23.502 [21] section 4.3.2.2.1. There is no information here that allows the B-UPF to correlate the two PFCP sessions yet. The SMF should also inform the B-UPF that this PFCP session is to be combined. This can be accomplished by utilizing the PFCP IE Network Instance, example below:
    - Network-Instance for a normal PFCP session indicates the VRF instance for the N3 interface
    - Network-Instance for the combined AGF-UP and UPF indicates that the session can be combined within the B-UPF such as: "b-upf.broadband-forum.org"
6. The B-UPF responds to the SMF through N4 following step 10b in section 4.3.2.2.1 of TS 23.502 [21]. The B-UPF also returns the TEID (CN-tunnel ID) to the SMF. This TEID is later sent to the AGF-CP through the AMF. The AGF-CP informs the B-UPF through PFCP the GTP TEID to use to reach the CN.
7. The 5GC completes TS 23.502 [21] section 4.3.2.2.1 step 11 to 12.
8. The AGF-CP modifies the PFCP session with the B-UPF through SCi following step 10a in section 4.3.2.2.1 of TS 23.502 [21]. The B-UPF receives both the Network Instance and the TEID and is able to correlate the two PFCP sessions (one between the SMF/B-UPF and one between the AGF-CP/B-UPF). The B-UPF recognizes the matching Network Instance and the TEID that it has assigned to itself in step 5 and 6. With the correlation of the PFCP session, this allows data path forwarding rules optimization on the B-UPF. The data path has the following information:
    - Access information
        i. Logical port
        ii. Ethernet header
        iii. UE IP address
        iv. All framed routes
    - Network information
        i. Network instance
        ii. Forwarding action
9. The B-UPF responds to the SMF through N4 following step 10b in section 4.3.2.2.1 of TS 23.502 [21]. The B-UPF returns the AN-tunnel-ID (TEID) for the AGF-CP.
10. The 5G-RG and 5GC completes TS 23.502 [21] section 4.3.2.2.1 step 13 to 15.
11. The SMF modifies the PFCP session with the B-UPF through N4 following step 16a in section 4.3.2.2.1 of TS 23.502 [21].
12. The B-UPF responds to the SMF through N4 following step 16b in section 4.3.2.2.1 of TS 23.502 [21]. The B-UPF receives the TEID, but the information is not critical for forwarding as the B-UPF already has enough information in Step 8 to correlate the PFCP session.
13. The 5G-RG and 5GC completes TS 23.502 [21] section 4.3.2.2.1 step 17 and beyond.

6 Technical Requirements

For the rest of this document, when applicable AGF-CP are simply referred to as ‘CP’ and AGF-UP are simply referred to as ‘UP’. This term does not suggest that these elements are consolidated but is used to simplify references in the document.

For requirements referencing TR-459i2 [7], please note that DBNG-CP is replaced with AGF-CP and DBNG-UP is replaced with AGF-UP.

6.1 State Control Interface Requirement

This section lists the functional requirements for SCi.

[R-12] The State Control Interface MUST support PFCP protocol as defined in 3GPP TS 29.244 [23]

[R-13] The State Control Interface MUST support the communication of forwarding rules to allow the handling of RG data traffic over the Y4 and Y5-interface as documented in Table 2.

[R-FN-1] The State Control Interface MUST support the communication of forwarding rules to allow the handling of FN-RG control traffic over the Y4-interface as documented in Table 2.

[R-5G-1] The State Control Interface MUST support the communication of forwarding rules to allow the handling of 5G-RG control message signaling over the N1 as documented in Table 2.

[R-14] The State Control Interface MUST be extended to support the communication of forwarding rules to allow the handling of subscriber traffic over the N3 interface.

6.2 Control Packet Redirection Interface Requirement

The CPR Interface is an interface between CP and UP. It is used to tunnel signaling and control packets between the V or the N3 interface to the CP via the UP.

[R-15] AGF CUPS MUST support R-43, R-47, R-48, R-49, R-50, R-53, R-54, and R-55 of TR-459i2 [7]. Where DBNG-CP and DBNG-UP are replaced by AGF-CP and AGF-UP respectively.
Note: R-48 Data trigger host is not applicable.

[R-16] The AGF-CP MUST be able to signal the AGF-UP to update the forwarding action matching specific control messages from the N3 interface per subscriber.

[R-FN-2] The AGF-CP MUST be able to signal per subscriber session control packet redirection rules to instruct the AGF-UP to forward subscriber-originated DHCP/DHCPv6 control packets from the AGF-CP to the 5GC via N3.

[R-FN-3] The AGF-CP MUST be able to signal per subscriber session control packet redirection rules to instruct the AGF-UP to tunnel subscriber-bound DHCP/DHCPv6 control messages received from the N3 interface to the AGF-CP.

[R-17] The AGF-CP MUST be able to send control packets to the N3 interface through the AGF-UP

6.3 Management Interface Requirement

The Management interface between the CP and the UP provides two main functions: configuration and operational state retrieval of AGF-UP.

One of the main functions of the CUPS Management Interface is configuration of functions and services. Data models present the most powerful and flexible approach to configure devices, services, and to monitor their operational state. Also, it is advantageous to support the ability to use machine tools to automate generation, manipulation, and parsing of the configuration data received state information. Extensible Markup Language (XML) was designed to store and transport data. For example, XML is designed to be self-descriptive and is human-readable.

[R-18] The Management Interface MUST support requirements as listed in TR-459i2 [7] [R-58] [R-59] [R-60] and [R-63].

[R-19] The Management Interface SHOULD support requirements as listed in TR-459i2 [7] [R-61] and [R-64].

6.4 AGF-CP requirements

[R-20] The AGF-CP must support R-47 as specified in TR-459i2 [7].
[R-21] The AGF-CP MUST support the N2 interface as defined in Table 2.

6.5 AGF-UP requirements

[R-22] The AGF-UP MUST support R-60 as specified in TR-459i2 [7].
[R-23] The AGF-UP MUST support N3 interface as defined in Table 2
[R-24] The AGF-UP MUST support the V/Y4 and V/Y5 protocol as defined in Table 2

6.6 B-UPF requirements

As outlined in TR-456i2 [6] during session management the B-UPF should support the sending of "WAGFinfo" parameter to the AMF over N2. This brings for the following requirements:
[R-25] During PFCP association, the B-UPF SHOULD identify itself as a combined AGF+UPF element to the AGF-CP.
[R-26] The AGF-CP MUST utilize the B-UPF Address or FQDN as part of the WAGFInfo as defined in TS 29.510 [26].

When the AGF-UP and UPF are combined (called the B-UPF), the following ([R-27] to [R-28]) are only applicable to the use case describe in section 4.3.
[R-27] The AGF-CP SHOULD be able to signal a Network Instance representing the null N3 to assist the B-UPF in correlating the corresponding SMF PFCP session.
[R-28] When signalled by [R-27], the B-UPF SHOULD use the combination of both PFCP IE Network Instance and F-TEID [23] to correlate the two PFCP session between the SMF/B-UPF and between the AGF-CP/B-UPF.

6.7 5WE Data Packets Requirements

As specified in 3GPP TS 23.501 [20] regarding Reflective QoS "Non 3GPP access are expected to send transparently the QFI and RQI to the UE".
[R-29] The AGF-UP MUST set the R-bit in the 5WE header to the value indicated by the RQI on the N3 interface.

Specified in 3GPP TS 23.501 [20], AN is also responsible to transfer the QFI value transparently between the 5GC and the UE.
[R-30] For DL data traffic, AGF-UP MUST set the QFI in the 5WE header to the value indicated by the GTP header from the N3 interface.
[R-31] For UL data traffic, AGF-UP MUST set the QFI in the GTP header to the value indicated by the 5WE header from the Y5 interface.

6.8 PFCP Requirements

[R-32] For bit 8/8, if the AGF-UP indicates this capability, the AGF-UP MUST apply all QoS profiles sent by the AGF-CP during the PFCP session establishment and modifications.
[R-33] For bit 9/1, if the AGF-UP indicates this capability, the AGF-UP MUST apply all QoS attributes sent by the AGF-CP during the PFCP session establishment and modifications.

7 PFCP overview

PFCP is the selected CUPS protocol for AGF SCi and is used to program subscriber forwarding state, control packet redirection rules, and data packet forwarding rules. PFCP is a 3GPP-specified protocol that was introduced in 3GPP Release 14. Details of the protocol can be found in TS 29.244 [23] “Interface between the Control Plane and User Plane Node”. PFCP addresses the technical and functional requirements listed in this document.

PFCP contains two main message types: node messages and session messages. Node messages are mainly used to form an association between the CP and the UP. Session messages are mainly used to program the subscriber forwarding state. Both node and session messages utilize information elements (IEs) for communication between the CP and the UP. Most IEs are extensible, details on IE extensibility are covered in TS 29.244 [23] Table 8.1.2-1. The following section describes the IE extensions required to support TR-456i2 [6] AGF requirements and procedures and also the use case of B-UPF defined in this document.

Note: In this section, each PFCP session uniquely maps to a subscriber forwarding state and “subscriber forwarding state” is hereinafter referred to as simply “session”.

7.1 PFCP messages

The following is a brief introduction for common PFCP messages used by the CP and UP. For the complete list of PFCP messages and their details, please refer to 3GPP TS 29.244 [23].

All 3GPP PFCP IEs based in TR-458 are described in 3GPP Release 17 PFCP IEs from TS 29.244 [23].

7.1.1 PFCP node messages

For more information on PFCP node Messages please refer to 3GPP 29.244 [23]
AGF CUPS supports the same messages as defined in TR-459i2 [7] table 7, with the following exceptions:

- The IEs “Maximum ACL Chain Length”, “BBF-Node-Info create”, “BBF-Node-Info modify”, “BBF-Node-Info delete”, and any sub-IEs are not required for AGF CUPS.
- The PFCP Node Report Request and PFCP Node Report Response messages are not required for AGF CUPS.

7.1.2 PFCP session messages

For more information on PFCP session Messages please refer to 3GPP TS 29.244 [23]

PFCP session report messages are used when the AGF-UP needs to notify the AGF-CP of a local LCP keepalive failure.

AGF CUPS supports the same messages as defined in TR-459i2 [7] tables 9 through 16. The following IEs do not need to be supported:

- “BBF ACL” and all sub-IEs.
- “Create URR”, “Update URR”, “Remove URR”, “Query URR”, and all sub-IEs.
- “BBF SGRP ID”
- “Usage Report” and all sub-IEs.
- “PFCPSRReq-Flags”

Note: AGF CUPS follows MS-DBNG CUPS (TR-459i2 [7]) PFCP procedures where traffic endpoint is used to optimize the PDI rule.

7.2 General PFCP information exchanges for a subscriber session

For the AGF use cases, this document separates PDRs into two categories.

- PDRs to match on subscriber control or signaling packets
  - Typically require a minimum of four PDRs
    - To redirect control packets from access to the CP through the CPR Interface
    - To redirect control packets from CP back to access through the CPR Interface. Control packets can include: DHCP, PPP discovery packets, router solicits, and NAS.
    - To redirect control packets from N3 to the CP through session server CPR interface
    - To redirect control packets from CP to the N3 through session server CPR interface
- PDRs to match on subscriber data packets
  - Again, typically require a minimum of two PDRs
    - To forward traffic upstream by matching on data packets arriving from the V interface and forwarding the packets to the N3 interface
    - To forward traffic downstream by matching on GTP encapsulated packets from the N3 interface and forwarding the packets back to the RG.

Therefore, a typical subscriber session requires at least 6 PDRs.

7.2.1 General PFCP rules for control packet redirection

For redirecting control or signaling packets from the UP to the CP, the following grouped IEs are typically used:

- PDR – Identifies the rule.
- PDI – A grouped IE to specify the matching criteria using the source interface and the traffic endpoint. Filter rules are sometimes used to match on more specific sub-flow. Detail in section 7.2.4.
- FAR – Specify the forwarding action and the destination for the redirected control packet. The control messages are encapsulated for tunneling.

A typical template is shown in **Table 3** below for control packet redirection from the UP to the CP through the CPR Interface.

Table 3: Example of a PDR for Control Packet Redirection from UP to CP

Direction	PDR	FAR

Control packet from the RG to CP	PDR ID
	Precedence
	PDI:
	  Source Interface
	  Traffic-Endpoint
	  Filter
	FAR ID
		FAR ID
		Apply Action
		Forwarding Parameters:
		  Destination Interface
		  Outer Header Creation

For redirecting control packets from the CP to the UP, the following list of grouped IEs are typically used:

- PDR – Identifies the rule.
- Outer header removal – Removes the tunnel encapsulation from the control packet.
- PDI – A grouped IE to specify the matching criteria using the source interface and the traffic endpoint.
- FAR – Specify the forwarding action, the destination, and the traffic endpoint for the control packet.

From the attributes above, a typical template is shown in **Table 4** below for control packet redirection from the AGF-CP to the AGF-UP through the CPR interface.

Table 4: Example of a PDR for Control Packet Redirection from CP to UP

Direction	PDR	FAR

Control packet from the CP to RG	PDR ID
	Precedence
	Outer Header Removal
	PDI:
	  Source Interface
	  Traffic-Endpoint
	  F-TEID = choose
	FAR ID
	
	Create Traffic Endpoint
		FAR ID
		Apply Action
		Forwarding Parameters:
		  Destination Interface
		  Linked Traffic Endpoint ID

7.2.2 General PFCP rules for Control Packet Redirection between AGF-CP to N3

These PFCP rules are required for forwarding bi-direction in-band control packets from the AGF-CP to the N3 interface, for example ICMPv6 and DHCPv6 packets. The rules follow TR-459i2 [7] section 6.2.3.

The key difference between the PFCP rules for AGF vs. DBNG is that the in-band control packets (such as ICMPv6 and DHCPv6) are session specific and therefore the traffic endpoint context is required.

For **Table 5**, the following modification is required to include the Traffic-Endpoint. In addition, the SDF filter is required to match on DHCPv6 packets for relay purposes and optionally for ICMPv6 packets if snooping is required.

Table 5: PFCP traffic rule example for in-band control packet from N3 to AGF-CP

Direction	PDR	FAR

Control packet from N3 to AGF-CP	PDR ID
	Precedence
	Outer Header Removal = Remove
	GTP-U
	PDI:
	  Source Interface = Core
	  Network Instance = "xyz"
	  SDF Filter = DHCPv6/ICMPv6
	  Traffic-Endpoint
	FAR ID
	
	Create Traffic Endpoint
		FAR ID
		Apply Action = forward
		Forwarding Parameters:
		  Destination Interface= CP-function
		  Outer Header Creation

For **Table 6**, the following modification is required to include GTP header creation.

Table 6: PFCP traffic rule example for in-band control packet from AGF-CP to N3

Direction	PDR	FAR

Control packet from AGF-CP to N3 via AGF-UP	PDR ID
	Precedence
	Outer Header Removal = Remove
	GTP-U
	PDI:
	  Source Interface=CP-function
	  Local F-TEID = Choose
	FAR ID
		FAR ID
		Apply Action
		Forwarding Parameters:
		  Destination Interface = Core
		  Network Instance = "xyz"
		  Outer Header Creation

For more information regarding server packet redirection, please refer to TR-459i2 [7].

7.2.3 General PFCP rules for data packet redirection

For the upstream direction, data packets from the RG are tunneled through the N3 interface. PFCP utilizes a list of IEs to program the subscriber data forwarding. The following is a list of group IEs typically used for wireline:

- PDR – Identifies the rule.
- PDI – A grouped IE to specify the matching criteria using a combination of source interface and traffic endpoint. Filter rules are sometimes used to match on more specific sub-flow.
- FAR – Specify the forwarding action and the destination for the data packet.

Below in Table 7, a typical template for upstream data packet forwarding is shown. Traffic is forwarded from the RG through the UP to the N3 interface.

Table 7: Example of a PDR for upstream data packet forwarding through the UP

Direction	PDR	FAR

Upstream	PDR ID
	BBF Outer Header Removal
	PDI:
	  Source Interface
	  Traffic-Endpoint
	  Filter
	FAR ID
	
	Create QER
	Create Traffic Endpoint
		FAR ID
		Apply Action
		Forwarding Parameters:
		  Destination Interface
		  Network-Instance

***Bolded text indicates BBF PFCP extension**

For the downstream direction, GTP encapsulated packets are routed from the N3 interface to the UP and are forwarded back to the RG, the following list of grouped IEs are typically used:

- PDR – Identifies the rule.
- PDI – A grouped IE to specify the matching criteria using the source interface and the traffic endpoint.
- FAR – Specify the forwarding action, the destination, and the traffic endpoint for the user packet.

Below in Table 8, a typical template for downstream data packet forwarding is shown. Traffic is forwarded from the network core through the UP and then to the subscriber.

Table 8: Example of a PDR for downstream data packet forwarding through the UP

Direction	PDR	FAR

Downstream	PDR ID
	PDI:
	  Source Interface
	  Traffic-Endpoint
	  F-TEID = choose
	FAR ID
		FAR ID
		Apply Action
		Forwarding Parameters
		  Destination Interface
		  BBF Outer Header Creation
		  Linked Traffic Endpoint ID

***Bolded text indicates BBF PFCP extension**

7.2.4 General Information PFCP Filter IEs

Please refer to TR-459i2 [7] section 6.4.4.

7.2.5 General Information on Network Service Header

Please refer to TR-459i2 [7] section 6.4.5 and replace DBNG with AGF.

7.2.6 Examining PDR rules for a B-UPF

7.2.6.1 Overview of PDR rules for an AGF-UP and a 5GC UPF

There are two distinct PFCP sessions, one between the AGF-CP and AGF-UP and one between the SMF and UPF.

When considering a single PDU session, for the AGF PFCP session, there are at least two basic data PDRs as explained in section 7.2. For the SMF PFCP session, there are typically two basic data PDRs as follows:

- To forward traffic upstream by matching on data packets arriving from a GTP tunnel and forwarding the packets to N6.
- To forward traffic downstream by matching on IP packets from N6 back to a GTP tunnel.

Below is a figure depicting the four typical PDR rules required for data plane forwarding, two between the AGF-CP and AGF-UP and two between the SMF and UPF. These four PDR rules enable bi-directional subscriber traffic forwarding between the RG to N6.

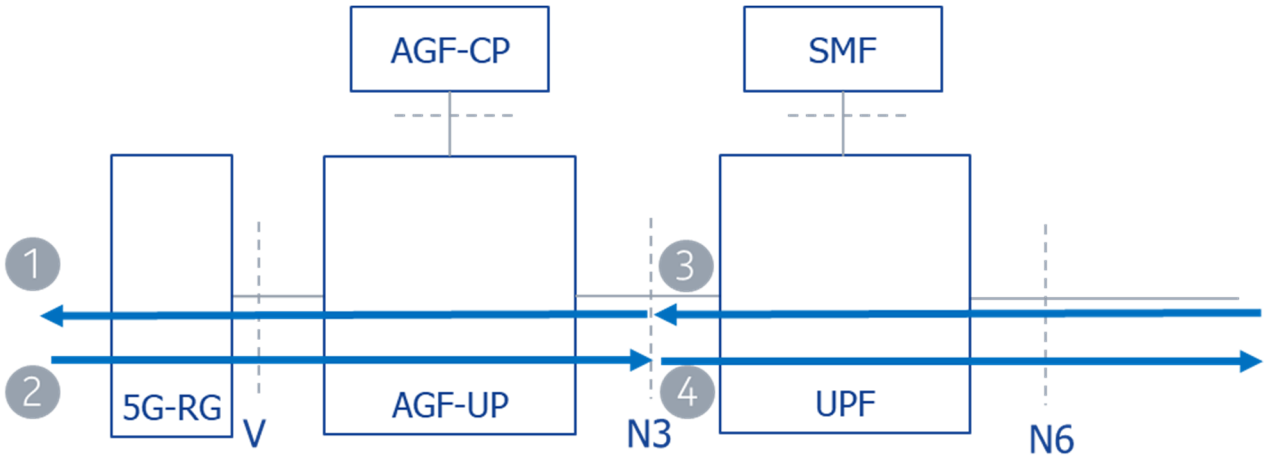

Figure 7-1: PDR Rules

Below Table 9 is a simplification of the PFCP PDR rules received on the AGF-UP and 5GC UPF. The PDR number corresponds to the arrow depicted in Figure 7-1.

Table 9: PDR Rules

Direction	AGF-UP	
Downstream	PDR ID = 1 Outer Header Removal = GTP PDI: Source Interface = core Traffic-Endpoint = TEID Network Instance FAR ID **Summary: MATCH and remove TEID**	FAR ID Apply Action Forwarding Parameters Destination Interface = access Network Instance BBF Outer Header Creation Linked Traffic Endpoint ID
Upstream	PDR ID = 2 BBF Outer Header Removal PDI: Source Interface Traffic-Endpoint = logical-port = Network Instance	FAR ID Apply Action Forwarding Parameters: Destination Interface = Core Network Instance Outer Header Creation = GTP

	Filter = IP any to any FAR ID	**Summary: Generate TEID**

Direction	UPF	
Downstream	PDR ID = 3 PDI: Source Interface = core Traffic-Endpoint = UE-IP Framed-routes Network Instance FAR ID	FAR ID Apply Action Forwarding Parameters Destination Interface = access Network Instance Outer Header Creation = GTP **Summary: Generate TEID**
Upstream	PDR ID = 4 Outer Header Removal = GTP PDI: Source Interface = access Traffic-Endpoint = UEIP = Network Instance Filter = IP any to any FAR ID **Summary: MATCH and remove TEID**	FAR ID Apply Action Forwarding Parameters: Destination Interface = N6 Network Instance

7.2.6.2 PDR rules for B-UPF

When the AGF-u and 5GC UPF are combined it is called the B-UPF, there are still two distinct PFCP sessions on the B-UPF, one session between the AGF-CP and the B-UPF and one session between the SMF and the B-UPF. By combining the AGF-u and UPF, the B-UPF can provide optimization to the N3 interface, removing the need to tunnel packets through GTP on N3. Specifically, in Table 9 the PFCP rules highlighted in green and yellow can be removed, as one rule performs a GTP encapsulation, a corresponding subsequent rule immediately de-encapsulate the GTP packet. Below figure depicts the AGF-CP and SMF connected to a B-UPF.

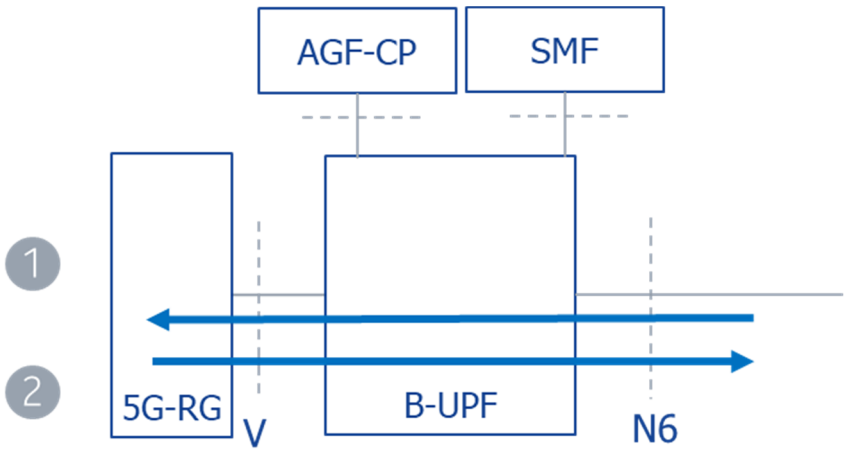

Figure 7-2: B-UPF PDR Rules

The following table is simply a representation of combined B-UPF PFCP rules where the N3 interface is removed. Implementation of the actual PFCP rules optimization may differ between vendors. The PDR number correspond to the arrow depicted in Figure 7-2: B-UPF PDR Rules.

Table 10: B-UPF PDR Rules

Direction	B-UPF	
Downstream	PDR ID = 1 PDI: Source Interface = core Traffic-Endpoint = UE-IP Framed-routes Network Instance FAR ID	FAR ID Apply Action Forwarding Parameters Destination Interface = access Network Instance BBF Outer Header Creation Linked Traffic Endpoint ID
Upstream	PDR ID = 2 BBF Outer Header Removal PDI: Source Interface Traffic-Endpoint = logical-port = Network Instance Filter = IP any to any FAR ID	FAR ID Apply Action Forwarding Parameters: Destination Interface = N6 Network Instance

When the PFCP rules are consolidated, the following must be considered.

- Ensure the same UPF (B-UPF) is selected
- Correlating the two different PFCP sessions on the B-UPF
- Concatenating QoS rules
- Concatenating Usage Reporting rules for accounting purpose

7.2.6.3 Correlation by the use of PFCP IE F-TEID and Network Instance

The B-UPF provides the option of N3 optimization, eliminating the need of GTP tunneling between AGF-UP and UPF. The B-UPF stitches together two separate PFCP sessions between the AGF-CP and the B-UPF and between the SMF and the B-UPF. In this section, the correlation of the two PFCP sessions is achieved by using two PFCP IEs [23]: the F-TEID (Fully Qualified – Traffic Endpoint ID) and Network Instance.

Both the SMF and AGF-CP require the B-UPF to allocate F-TEID for the GTP tunnel, which is a native procedure defined in 3GPP TS 29.244 [23]. By utilizing the B-UPF to perform TEID assignment, the B-UPF can ensure:

1. TEIDs advertised for CN-tunnel and AN-tunnel are always unique for the SMF and the AGF-CP respectively
2. B-UPF is able correlate two separate PFCP sessions by utilizing the unique TEID it has assigned to itself

Further, in the B-UPF case, the PFCP IE Network Instance on N3 does not exist and is no longer a network instance. The N3 in this case is essentially a “null” Network Instance. The SMF can utilize name such as “bupf.broadband-forum.org” to inform the B-UPF that this PFCP session is to be stitched together with the AGF PFCP session. Together with the F-TEID and the network instance, the B-UPF can fully correlate the two separate PFCP sessions. The correlation of the PFCP session is an enabler for the B-UPF to perform further data plane optimizations.

7.3 PFCP use case and Information Element exchange

7.3.1 FN-RG multiple IP session support

The FN-RG initiates an IP connection to the 5GC through the use of control packets which include: PPP PADI, DHCPv4, DHCPv6, SLAAC, or a data packet. Each of these connection attempts initiates a new PFCP session. If the same FN-RG requires additional IP connection, each connection is a new PFCP session.

[R-FN-4] The AGF-CP MUST be able to support separate PFCP session for each IP session on the FN-RG, which each IP session can be a dual stack IP session. Where each IP session is a separate subscription on the AGF.

When the registration is successful, the 5GC informs the AGF-CP via the AMF for a PDU Session Establishment Request, the AGF-CP modifies the existing PFCP session to add the PDU session. For every new IP session initiated by the FN-RG, the AGF-CP establishes a new PFCP session.

7.3.2 5G-RG multiple IP session support

The AGF-CP utilizes one PFCP session to support all PDU sessions from a 5G-RG. The PFCP session contains both control packet forwarding rules (NAS and AS) and also data forwarding rules for all PDU sessions.

[R-5G-2] The AGF-CP MUST be able to use a single PFCP session to support all control signaling and PDU sessions within a 5G-RG.

7.3.3 Use Case: FN-RG PPPoE with immediate PFCP session setup

For the PPPoE use case, data forwarding rules are generally split between control packet redirection and data packet forwarding. During PFCP Session Establishment, only control packets such as PPP discovery, link control, network control packets, ICMPv6, DHCPv6 should be redirected to the CPR Interface. There should not be any PFCP data forwarding rules.

For PPPoE IPv4 data traffic, the AGF-CP is required to modify the PFCP session to add bi-directional IPv4 data traffic forwarding between the V and N3 interface.

For PPPoE IPv6 data traffic, the AGF-CP is required to modify the PFCP session to add bi-directional IPv6 data traffic forwarding between the V and N3 interface.

7.3.3.1 PFCP Control Packet Redirection rules

The Session Establishment corresponds to:

- Section 5.3.1 FN-RG PPPoE session initialization with immediate PFCP Session setup steps 2 and 3.
- Section 5.3.7 Service Request Procedure for FN-RG Steps 4b and 4c.

In general, the PFCP rules follows TR-459i2 [7] section 6.3.3.1. However, the following are the key differences:

- The AGF-CP may choose to redirect ICMPv6 Router Advertisement from N3 to the AGF-CP for snooping purposes.
- For DHCPv6, the AGF-CP programs the PFCP rules on the AGF-UP to redirect DHCPv6 control packets to the AGF-CP for relay purposes.

7.3.3.2 PFCP Data Packet Forwarding rules

The Session Modification corresponds to:

- Section 5.3.1 FN-RG PPPoE session initialization with immediate PFCP Session setup steps 7b and 7c.
- Section 5.3.7 Service Request Procedure for FN-RG Steps 4b and 4c
- Section 5.3.8 Session Initiation Procedure for FN-RG Steps 3b and 3c

In general, the PFCP rules follows TR-459i2 [7] section 6.3.3.2. However, the following are the key differences:

- The data traffic from the FN-RG requires both PPPoE and Ethernet header removal followed by a GTP header encapsulation then forwarded to the N3 interface.
- Returning traffic from the N3 interface requires the GTP header removal and re-inserting the full Ethernet header including the PPPoE before forwarding to the FN-RG.

7.3.4 Use Case: FN-RG IPoE with immediate PFCP session setup

For the IPoE use case, data forwarding rules are generally split between control packet redirection and data packet forwarding. During PFCP Session Establishment, only control packets such as DHCP, DHCPv6, ICMPv6 packets are redirected to the CPR Interface. The AGF-CP will also program the AGF-UP to redirect DHCP, DHCPv6 and ICMPv6 messages from the N3 interface to the AGF-CP via the subscriber session server CPR Interface for relay and snooping purposes.

For IPv4 data traffic, the AGF-CP modifies the PFCP session to add bi-directional IPv4 data traffic forwarding between the V and N3 interface.

For IPv6, the AGF-CP requires modification to the PFCP session for the data plane. Data forwarding rules are installed for bi-directional IPv6 forwarding between the V and N3 interface.

Note: The delay model for DHCP relay in TR-459i2 [7] is not applicable to AGF CUPS.

7.3.4.1 PFCP Control Packet Redirection rules

The Session Establishment corresponds to:

- Section 5.3.3 FN-RG DHCPv4 session initialization steps 2.
- Section 5.3.4 FN-RG DHCPv6 session initialization steps 2.
- Section 5.3.5 FN-RG DHCPv6 with SLAAC session initialization steps 2.
- Section 5.3.7 Service Request Procedure for FN-RG Steps 4b and 4c.

In general, the PFCP rules follows TR-459i2 [7] section 6.3.2.1. However, the following are the key differences:

- For both DHCP and DHCPv6, the AGF-CP programs the PFCP rules on the AGF-UP to redirect DHCP and DHCPv6 control packets to the AGF-CP for relay purposes.
- For IPv6 SLAAC address assignment, the AGF-UP must redirect RS and RA control packets to the AGF-CP for snooping and also alternation of the LLA IPv6 address.

7.3.4.2 PFCP IPoE Data Packet Forwarding rules

The Session Modification corresponds to:

- Section 5.3.3 FN-RG DHCPv4 session initialization steps 5.
- Section 5.3.4 FN-RG DHCPv6 session initialization steps 5.
- Section 5.3.5 FN-RG DHCPv6 with SLAAC session initialization steps 6.
- Section 5.3.7 Service Request Procedure for FN-RG Steps 4b and 4c
- Section 5.3.8 Session Initiation Procedure for FN-RG Steps 3b and 3c

In general, the PFCP rules follows TR-459i2 [7] section 6.3.2.2. However, the following are the key differences:

- The data traffic from the FN-RG requires Ethernet header removal followed by a GTP header encapsulation then forwarded to the N3 interface.
- Returning traffic from the N3 interface requires GTP header removal and re-inserting the full Ethernet header before forwarding to the FN-RG.

7.3.5 Use Case: 5G-RG PFCP session setup

For the 5G-RG use case, data forwarding rules are generally split between control packet redirection and data packet forwarding. A dedicated PFCP session is established for control packets such as PPP discovery, link control, VSNCP, and VSNP only and these packets are redirected to the CPR Interface.

Afterward authentication and registration, the 5G-RG establishes PDU sessions. The AGF-CP modifies the existing PFPC session for the 5G-RG to add forwarding rules for bi-directional data traffic forwarding between the V and N3 interface. The AGF-CP may add optional rules to redirect DHCP, DHCPv6, and ICMPv6 packet for snooping purpose.

7.3.5.1 PFCP Control Packet Redirection rules

The Session Establishment corresponds to:
- Section 5.4.1 5G-RG Registration Management Procedure steps 2 and 3.

In general, the PFCP rules follow TR-459i2 [7] section 6.3.3.1 for PPPoE. However, the following are the key differences:
- The AGF-CP redirects PPP protocol VSNP and VSNCP instead of NCP.
- The AGF-CP starts LCP to track 5G-RG inactivity.

7.3.5.2 PFCP Data Packet Forwarding rules

The Session Modification corresponds to:
- Section 5.4.2 5G-RG Service Request Procedure via W-5GAN Steps 3b and 3c
- Section 5.4.3 5G-RG PDU Session Initiation/Establishment via W-5GAN Steps 3b and 3c

In general, the PFCP rules follow TR-459i2 [7] section 6.3.3.2 for PPPoE. However, the following are the key differences:
- The data traffic from the 5G-RG requires both 5WE and Ethernet header removal followed by a GTP header encapsulation then forwarded to the N3 interface.
- Returning traffic from the N3 interface requires the GTP header removal and re-inserting the full Ethernet header including the 5WE header before forwarding to the 5G-RG.

The following BBF defined IE extension is required:
- **Traffic-Endpoint IE extensions required**: As defined in TR-459i2 [7], with the addition of 5WE session ID.
- **BBF outer header removal IE extension required:** As defined in section <please check the correct reference for PFCP IE, used to be 7.7.1>, with the addition of 5WE session ID.

7.3.5.3 Optional PFCP rule for address snooping

In addition to PFCP data forwarding rules listed above, the AGF-CP might optionally choose to redirect DHCP, DHCPv6 or SLAAC messages from the AGF-UP to the AGF-CP for snooping purposes.

In general, the same PFCP rules from section 7.2.3 are used. The ingress Ethernet packet filter matches on 5WE packets together with SDF filter to match on DHCP, DHCPv6, or SLAAC messages and are redirected to the AGF-CP first for snooping purpose. Afterward, the control packets are forwarded to the N3 interface within the GTP tunnel. Returning traffic from the N3 interface are matched against an SDF filter to be redirected to the AGF-CP first before forwarding to the 5G-RG with the full Ethernet and 5WE header. The IEs required are the same as section 7.2.3

7.4 Modeling AGF CUPS QoS with PFCP

7.4.1 Modeling pre-define QoS Profile with PFCP

In this model, the full QoS profiles are pre-provisioned on AGF-UP(s). The AGF-CP would apply a specific QoS profile to each 5G-RG or FN-RG on the AGF-UP. The QoS profiles are applied per RG (PFCP session) and not per PDU. Therefore, the PFCP IEs are applied at the session level. Further, as defined in TR-456i2 [6], R-53 and R-56 respectively, the QoS profile should be differentiated by upstream and downstream direction. The extended IE would include the combination of the following elements as specified from TR-470i2 [8]:

- QoS profile name: a QoS profile for both upstream and downstream direction
- UL Police descriptor name
- UL TC Police descriptor name
- DL Descriptor name
- DL TC Descriptor name
- DL Police descriptor name
- DL TC Police descriptor name

7.4.2 Modeling dynamic QoS with PFCP

As defined in 3GPP 23.501, each PDU session has a unique QFI to 5QI mapping. TR-456i2 [6] further define 5QI to Traffic Class mapping for serving wireline use cases. The AGF-CP contains both standardized and pre-configured 5QI values and is able correspond QFIs directly to the Traffic Class per PDU session.

As defined in TR-456i2 [6], Traffic Class are composed of various QoS parameters such as queues, aggregation rates, policers, and burst values. The AGF-CP conveys the actual QoS parameters of the traffic class to be enforced on the AGF-UP. In other words, the AGF-CP programs QoS rules on the AGF-UP to map QFI directly to various QoS parameters such as rates and burst values.

3GPP 29.244 [23] already defined QoS rules known as QoS Enforcement Rules which could be reused. In the case of AGF, each PDU session contains 1 PDR for upstream and 1 PDR for downstream data traffic forwarding. A high-level example of a QER rule and a PDI referencing a QER rule is provided below:

- QER rule 1: perform QoS action PIR/CIR/remarking/etc.
- PDR rule 1: PDI match QFI 1 perform QER rule 1

Below is a diagram depicting the mapping from QFI to the QoS parameters. In the case of AGF CUPS, the AGF-CP can communicate the final direct mapping to the AGF-UP, without burdening the AGF-UP with the intermediate steps.

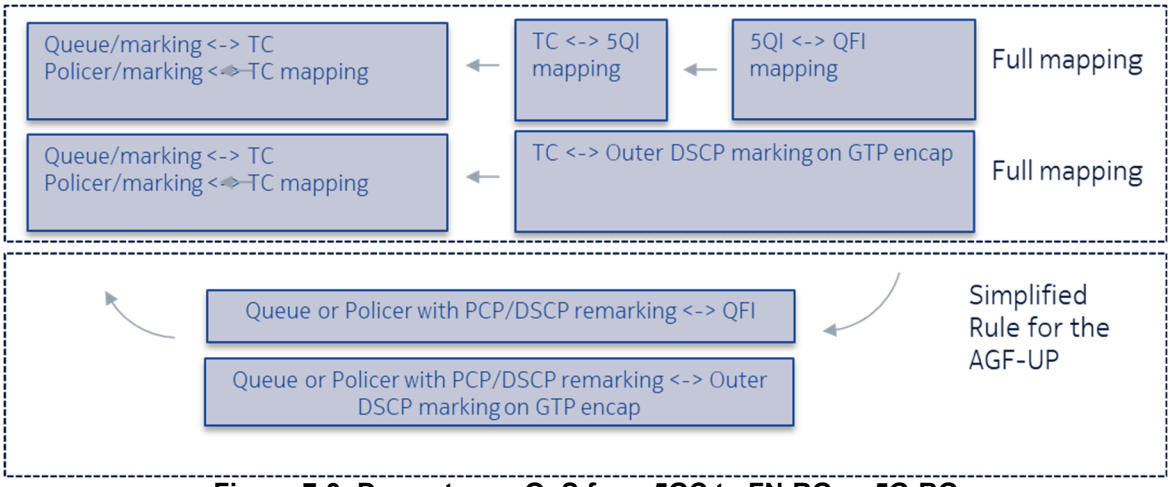

Figure 7-3: Downstream QoS from 5GC to FN-RG or 5G-RG

Similarly for the Upstream direction.

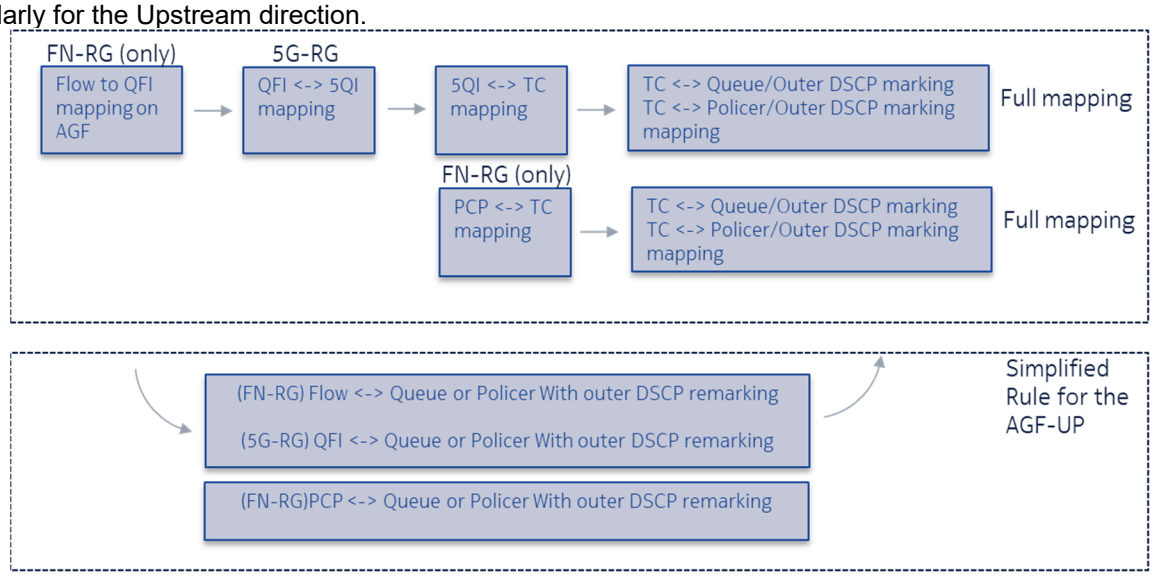

Figure 7-4: Upstream QoS from FN-RG or 5G-RG to 5GC

Wireline Traffic Classes are defined in TR-178 section 5.4.3, referred by TR-456i2 [6] section 6.3 QoS section. TR-178 further establishes [R-275] where each traffic class would contain both a priority and a weight.

Note: The TC QER would require priority IE, weight IE, mapped to the TC name. The method of how these IEs is communicated form the AGF-CP to the AGF-UP is FFS.

A PDR rule matches on a particular QFI/DSCP for a specific PDU session and will reference the TC QER which can be sent earlier for example during registration or during the PDU session establishment of the first session.

Further, TR-470i2 [8] defined RG-LWAC with the ability to provide two types of QoS descriptors:

1. A scheduler for the RG.
2. At most 8 Traffic Classes common to all PDU sessions of the RG.

The AGF-CP is responsible to translate these QoS descriptors to two types of QERs:

- TC QER – specifies per traffic class QoS parameters. For example, perform QoS action PIR/CIR/remarking/etc.

- RG QER – specifies the aggregate rate for the RG that the TC QERs are subject to. For example, perform QoS action PIR/CIR

The following table gives an overview of PFCP IEs applicability to TC QERs and RG QERs.

Table 11: PFCP IEs applicability to TC QERs and RG QERs

IE	TC QER	RG QER
QER ID	yes	yes
BBF PIR	yes	yes
BBF CIR	yes	yes
QFI	yes	no
BBF Parent QER	yes	no
BBF Traffic Enforcement Type	yes	yes
BBF PBS	yes	yes
BBF CIRmax	yes	yes
BBF CBS	yes	yes
BBF TC Name	yes	no

7.4.2.1 PFCP QER and PDR PDI reference

Each RG contains up to 8 TC QER rules per direction (upstream and downstream) and each PDU session can reference these TC QER rules. A PDU session contains multiple PDR rules for data forwarding. Within a PDR, a PDI match rule is used to match on QoS Classification values (such as QFI, DSCP, and p-bit).

Each PDR PDI references one TC QER rules. When a PDR PDI rule references the same QER rule, this indicates that the PDR PDI rule shares the QoS resource. i.e., shares the same queue or policer and the rates, priorities, marking as defined in the QER.

There is an RG QER per direction (upstream and downstream) which serves as an aggregate rate for the RG. There is at most 1 RG QER for all PDU sessions.

Note: encoding wise, PFCP QERs can contain both upstream and downstream information as an optimization.

To allow for hierarchical QoS between TC QER rules to RG QER rule, please refer to section 7.4.2.2.1 for information on how TC QER rules references an RG QER.

7.4.2.2 General PFCP information relating to QER

The AGF-CP installs TC QER and RG QER rules onto the AGF-UP during the registration process and are common for all PDU sessions within a RG. The TC QER(s) and the RG QER are available on the AGF-UP before or during the first PDU session is established

7.4.2.2.1 General PFCP information relating to 5G-RG QER rules

Below is an example of QER rules installed during the registration process and is not an exhaustive list. Key parameter includes:

- TC name to specify the name of the Traffic Class

Table 12: Traffic Class QER

TC QER
QER: TC name Rate Remark …

To link the TC QER to the RG QER, the concept of parent QER is used.

- Parent of the QER rule for hierarchical rate shaping. In some cases, a parent QER might not be applicable.

Table 13: Linking of Traffic Class QER to RG QER

Linking TC QER to RG QER
TC QER (1..8): QER parent 9 RG QER 9: Rate …

Below is an example of a simplified rule which focuses on QoS on a single PDU session. The Upstream rule matches on a 5WE ID representing a PDU session and references QER. In the upstream direction there is an aggregate QER for the entire RG.

Table 14: PDR for Upstream data traffic from V/Y4 to N3

Direction	PDR	FAR
Upstream V/Y4 to N3	PDR (1..n) PDI: 5WE 1 QER (1..8) [reference] FAR ID	FAR ID Apply Action Forwarding Parameters: Destination Interface Network-Instance

Below is an example of a downstream rule which matches on a TEID with a QFI value and references QER. In the table below, QER 1 to 8 are TC QERs and QER 9 serves as the RG QER.

Table 15: PDR for Downstream data traffic from N3 to V/Y4

Direction	PDR	FAR
Downstream N3 to V/Y4	PDR 1 PDI: TEID 1 QFI 1 QER (1..8) [reference] FAR ID	FAR ID Apply Action Forwarding Parameters: Destination Interface Network-Instance

7.4.2.2.2 General PFCP information relating to FN-RG QER rules

Below is a simplified rule which focuses on QoS on a single PDU session. The Upstream rule matches on both SDF filter and Ethernet filter to identify on the subscriber data packet and reference QER. The QER rule does not differ from the 5G-RG QER rule

Below is an example of a PDR PDI match and the action performed:

- Match on an IP and Ethernet header and perform QFI marking and outer DSCP marking
- Match on entire PDU session and set rate

Table 16: PDR for Upstream data traffic from V/Y5 to N3

Direction	PDR	FAR
Upstream V/Y5 to N3	PDR (1..n) PDI: Ethernet Filter 1 SDF 1 QER (1..8) [reference] FAR ID	FAR ID Apply Action Forwarding Parameters: Destination Interface Network-Instance UL Transport level marking

Below is an example of a downstream rule which matches on a TEID with a QFI value or the outer IP DSCP marking and reference the QER. QER 1 to 8 are TC QERs and QER 9 serve as the RG QER.

Table 17: PDR for Downstream data traffic from N3 to V/Y5

Direction	PDR	FAR
Downstream N3 to V/Y5	PDR 1 PDI: TEID 1 QFI 1 SDF 1 QER (1..8) [reference] FAR ID	FAR ID Apply Action Forwarding Parameters: Destination Interface Network-Instance

7.5 BBF PFCP Information Element Summary

Table 18 is an applicability table for each AGF use case, where each entry has the following meaning:

- "Yes" indicates that the IE indicated MUST be included for that particular use case.
- "--" indicates that the IE indicated is not applicable to that particular use case.
- “Cond” means the IE MUST be included based on the use case.

The BBF extended PFCP IEs are found in TR-459i2 [7]. And the 3GPP PFCP IEs are found in TS 29.244 [23].

This table does not contain IEs that are related to node level messaging. For example, IEs typically sent in PFCP associations such as UP Function Features, or IEs related to load/overload are not included in the table.

Table 18: PFCP IEs and related use case

IE Type Value (Decimal)	Information Elements	Reference	Use Case		
			FN-RG PPPoE	FN-RG IPoE	5G-RG
32769	Logical Port	TR-459i2 [7] Section 6.9	Yes	Yes	Yes
32770	BBF Outer Header Creation	TR-459i2 [7] Section 6.9	Yes	Yes	Yes
32771	BBF Outer Header Removal	TR-459i2 [7] Section 6.9	Yes	Yes	Yes
32772	PPPoE Session ID	TR-459i2 [7] Section 6.9	Yes	--	--
32773	PPP protocol	TR-459i2 [7] Section 6.9	Yes	--	Yes
32774	Verification Timers	TR-459i2 [7] Section 6.9	Yes	--	Yes
32775	PPP LCP Magic Number	TR-459i2 [7] Section 6.9	Yes	--	Yes
32776	MTU	TR-459i2 [7] Section 6.9	Yes	--	Yes
32777	L2TP tunnel endpoint	TR-459i2 [7] Section 6.9	Yes	--	--
32778	L2TP session ID	TR-459i2 [7] Section 6.9	Yes	--	--
32779	L2TP type	TR-459i2 [7] Section 6.9	Yes	--	--
32780	PPP LCP connectivity	TR-459i2 [7] Section 6.9	Yes	--	Yes
32781	L2TP Tunnel	TR-459i2 [7] Section 6.9	Yes	--	--
32822	BBF 5WE Session ID	Section 7.7.4	--	--	Yes
32823	BBF Traffic Enforcement Type	Section 7.7.5	Cond	Cond	Cond

32824	BBF PCP	Section 7.7.6	Cond	Cond	Cond
32825	BBF TC Name	Section 7.7.7	Cond	Cond	Cond
32826	BBF PBS	Section 7.7.8	Cond	Cond	Cond
32827	BBF CBS	Section 7.7.9	Cond	Cond	Cond
32828	BBF CIRmax	Section 7.7.10	Cond	Cond	Cond
32829	BBF Parent QER ID	Section 7.7.11	Cond	Cond	Cond
32820	BBF QoS Profile Name	Section 7.7.12	Cond	Cond	Cond
32832	BBF UL Policing Descriptor Name	Section 7.7.13	Cond	Cond	Cond
32833	BBF DL Policing Descriptor Name	Section 7.7.14	Cond	Cond	Cond
32834	BBF UL TC Policing Descriptor Name	Section 7.7.15	Cond	Cond	Cond
32835	BBF DL TC Policing Descriptor Name	Section 7.7.16	Cond	Cond	Cond
32836	BBF DL Descriptor Name	Section 7.7.17	Cond	Cond	Cond
32837	BBF DL TC Descriptor Name	Section 7.7.18	Cond	Cond	Cond
1	Create PDR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
2	PDI	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
3	Create FAR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
4	Forwarding Parameters	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
7	Create QER	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
9	Update PDR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
10	Update FAR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
11	Update Forwarding Parameters	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
14	Update QER	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
15	Remove PDR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
16	Remove FAR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
18	Remove QER	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
19	Cause	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
20	Source Interface	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
21	F-TEID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
22	Network Instance	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
23	SDF Filter	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
26	MBR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
27	GBR	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
28	QER Correlation ID	3GPP 29.244 [23] Section 8	--	--	--
29	Precedence	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
41	Forwarding Policy	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
42	Destination Interface	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
44	Apply Action	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
56	PDR ID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
57	F-SEID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
60	Node ID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
84	Outer Header Creation	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
89	CP Function Features	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
93	UE IP Address	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
95	Outer Header Removal	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
106	Activate Predefined Rules	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
107	Deactivate Predefined Rules	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
108	FAR ID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
109	QER ID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
113	PDN Type	3GPP 29.244 [23] Section 8	Yes	Yes	Yes

114	Failed Rule ID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
117	User Plane Inactivity Timer	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
127	Create Traffic Endpoint	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
128	Created Traffic Endpoint	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
129	Update Traffic Endpoint	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
130	Remove Traffic Endpoint	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
131	Traffic Endpoint ID	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
132	Ethernet Packet Filter	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
133	MAC address	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
134	C-TAG	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
135	S-TAG	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
136	Ethertype	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
153	Framed-Route	3GPP 29.244 [23] Section 8	Yes	Yes	Yes
155	Framed-IPv6-Route	3GPP 29.244 [23] Section 8	Yes	Yes	Yes

7.6 PFCP Group IE extension for Session Related Messages

This section highlights extensions required on grouped IEs such as PDR, PDI, FAR, to cover AGF CUPS use cases. PFCP IEs in this section includes a presence requirement, indicated by the letter "**P"**:

- Mandatory (M) indicates that this IE MUST be present if used.
- Conditional (C) indicates that this IE is conditional based on the use case specified.

7.6.1 PFCP Session Establishment Request

In the case where QoS Profile(s) are required to be applied for the subscriber session, the grouped IEs in the PFCP session establishment request message can include:

- BBF QoS Profile Name
- BBF UL Policing Descriptor Name
- BBF DL Policing Descriptor Name
- BBF UL TC Policing Descriptor Name
- BBF DL TC Policing Descriptor Name
- BBF DL Descriptor Name
- BBF DL TC Descriptor Name

Table 19: Information Elements in a PFCP Session Establishment Request

Information elements	P	Condition / Comment	IE Type
BBF QoS profile name	C	This IE shall contain the string of the QoS profile name both Upstream and Downstream direction	**BBF QoS profile name** Details in section 7.7.11
BBF UL Policing Descriptor Name	C	This IE shall contain the string of the UL Policing Descriptor name for the Upstream direction	**BBF UL Policing Descriptor Name** Details in section 7.7.13
BBF DL Policing Descriptor Name	C	This IE shall contain the string of the DL Policing Descriptor name for the Upstream direction	**BBF DL Policing Descriptor Name** Details in section 7.7.14
BBF UL TC Policing Descriptor Name	C	This IE shall contain the string of the UL TC Policing Descriptor name for the Upstream direction	**BBF UL TC Policing Descriptor Name** Details in section 7.7.15
BBF DL TC Policing Descriptor Name	C	This IE shall contain the string of the DL TC Policing Descriptor name for the Upstream direction	**BBF DL TC Policing Descriptor Name** Details in section 7.7.16
BBF DL Descriptor Name	C	This IE shall contain the string of the DL Descriptor name for the Upstream direction	**BBF DL Descriptor Name** Details in section 7.7.17
BBF DL TC Descriptor Name	C	This IE shall contain the string of the DL TC Descriptor name for the Upstream direction	**BBF DL TC Descriptor Name** Details in section 7.7.18

7.6.1.1 Create QER

The create QER grouped IE should include various QoS parameters.

Table 20: Create QER IE within PFCP Session Establishment Request

Octet 1 and 2	Create QER IE Type = 7 (decimal)		
Octets 3 and 4	Length = n		
Information elements	**P**	**Condition / Comment**	**IE Type**
The IEs below are re-used from 3GPP TS 29.244 [23]			
QER ID	M	This IE defines the unique identifier of the QER	**QER ID** (3GPP TS29.244 sec 8.2.75)
BBF PIR	O	This IE defines the PIR if the traffic enforcement type is policing, or the MBR if the traffic enforcement type is shaping.	**MBR** (3GPP TS29.244 sec 8.2.8)
BBF CIR	O	This IE defines the CIR if the traffic enforcement type is policing, or the GBR if the traffic enforcement type is shaping.	**GBR** (3GPP TS29.244 sec 8.2.9)
QFI	O	This will be used for an FN-RG to indicate the correct QFI on the N3 interface	**QFI** (3GPP TS29.244 sec 8.2.89)
The IEs below are already defined in 3GPP TS 29.244 [23], but are new in the QER scope			
BBF Parent QER	O	This IE shall define the parent rate this QER feeds into. When present, this QER and the referred QER MUST contain at least one rate. When not present no parent rate is defined for this QER. It is up to UP policy if a default parent rate (e.g., a port level scheduler) is required.	**BBF Parent QER ID** Detail in section 7.7.11
The IEs below are newly defined			
BBF Traffic Enforcement Type	O	This IE defines whether rates need to be applied using shaping or policing. When not present the default enforcement type is policing.	**BBF Traffic Enforcement Type** Details in section 7.7.5
BBF TC Name	O	This IE specifies the TC name of the QER	**BBF TC Name** Details in section 7.7.7
BBF PBS	O	This IE shall identify the Peak Burst Size	**BBF PBS** Details in section 7.7.8
BBF CBS	O	This IE shall identify the Committed burst Size	**BBF CBS** Details in section 7.7.9
BBF CIRmax	O	This IE shall identify the maximum Committed Burst Rate	**BBF CIRmax** Details in section 7.7.10

7.6.1.2 Forwarding Parameters

The Forwarding Parameter IE in FAR can include BBF DSCP Marking, UL Transport Level Marking, and BBF PCP Marking.

Table 21: Forwarding Parameters IE in FAR

Octet 1 and 2	Forwarding Parameters IE Type = 4 (decimal)		
Octets 3 and 4	Length = n		
Information elements	**P**	**Condition / Comment**	**IE Type**
The IEs below are re-used from 3GPP TS 29.244 [23]			
BBF DSCP Marking	O	This IE shall be present if QoS-Based marking of the IPv4 or IPv6 header DSCP fields is required on the V interface or the inner IP packet of the N3 interface. When not present, the UP policy will define a DSCP marking.	**DL Flow Level Marking** (3GPP TS29.244 sec 8.2.66)
UL Transport level marking	O	This IE shall be present if QoS-Based marking of the IPv4 or IPv6 header DSCP fields of the outer IP header is required on the N3 interface. When not present, please refer to the default behavior defined in TR-470i2 [8].	**Transport Level Marking** (3GPP TS29.244 sec 8.2.12)
The IEs below are newly defined			
BBF PCP Marking	O	This IE shall be present if QoS-based marking of either the PCP or DEI is required in the Outer Tag on the V interface. The VID bit of the S-Tag IE MUST NOT be set, as QER remarking does not apply to the S-VLAN ID value. When not present, UP policy will define a default PCP value to use in case an s-tag is added.	**BBF PCP marking** Details in section 7.7.6

7.6.1.3 Create Traffic Endpoint

The Create Traffic Endpoint grouped IE can include the 5WE Session ID.

Table 22: BBF extended Create Traffic Endpoint IE(s) within PFCP Session Establishment Request

Octet 1 and 2	Create Traffic Endpoint IE Type = 127(decimal)		
Octets 3 and 4	Length = n		
Information elements	**P**	**Condition / Comment**	**IE Type**
BBF Extended IEs below			
BBF 5WE Session ID	C	If present, this IE MUST be used to identify the 5WE session ID of the subscriber.	**BBF 5WE Session ID** Details in section 7.7.4

7.6.2 PFCP Session Modification Request

In the case where QoS Profile(s) are required to be applied for the subscriber session, the grouped IEs in the PFCP session modification request message can include:

- BBF QoS Profile Name
- BBF UL Policing Descriptor Name
- BBF DL Policing Descriptor Name
- BBF UL TC Policing Descriptor Name
- BBF DL TC Policing Descriptor Name
- BBF DL Descriptor Name
- BBF DL TC Descriptor Name

Table 23: Information Elements in a PFCP Session Modification Request

Information elements	P	Condition / Comment	IE Type
BBF QoS profile name	C	This IE shall contain the string of the QoS profile name both Upstream and Downstream direction which could lead to an addition, modification, or a deletion of the QoS profile	**BBF QoS profile name** Details in section 7.7.11
BBF UL Policing Descriptor Name	C	This IE shall contain the string of the UL Policing Descriptor name for the Upstream direction which could lead to an addition, modification, or a deletion of the UL Policing Descriptor	**BBF UL Policing Descriptor Name** Details in section 7.7.13
BBF DL Policing Descriptor Name	C	This IE shall contain the string of the DL Policing Descriptor name for the Upstream direction which could lead to an addition, modification, or a deletion of the DL Policing Descriptor	**BBF DL Policing Descriptor Name** Details in section 7.7.14
BBF UL TC Policing Descriptor Name	C	This IE shall contain the string of the UL TC Policing Descriptor name for the Upstream direction which could lead to an addition, modification, or a deletion of the UL TC Policing Descriptor	**BBF UL TC Policing Descriptor Name** Details in section 7.7.15
BBF DL TC Policing Descriptor Name	C	This IE shall contain the string of the DL TC Policing Descriptor name for the Upstream direction which could lead to an addition, modification, or a deletion of the DL TC Policing Descriptor	**BBF DL TC Policing Descriptor Name** Details in section 7.7.16
BBF DL Descriptor Name	C	This IE shall contain the string of the DL Descriptor name for the Upstream direction which could lead to an addition, modification, or a deletion of the DL Descriptor	**BBF DL Descriptor Name** Details in section 7.7.17
BBF DL TC Descriptor Name	C	This IE shall contain the string of the DL TC Descriptor name for the Upstream direction which could lead to an addition, modification, or a deletion of the DL TC Descriptor	**BBF DL TC Descriptor Name** Details in section 7.7.18

7.6.2.1 Update Traffic Endpoint

The Update Traffic Endpoint grouped IE can include the 5WE Session ID.

Table 24: BBF extended Create Traffic Endpoint IE(s) within PFCP Session Establishment Request

Octet 1 and 2	Create Traffic Endpoint IE Type = 127(decimal)		
Octets 3 and 4	Length = n		
Information elements	**P**	**Condition / Comment**	**IE Type**
BBF Extended IEs below			
BBF 5WE Session ID	C	If present, this IE MUST be used to identify the 5WE session ID of the subscriber.	**BBF 5WE Session ID** Details in section 7.7.4

7.7 PFCP Protocol IE extensions

The subsections below specify IE (Information Element) extensions to PFCP that are required to support WWC with CUPS.

7.7.1 BBF UP Function Features

The BBF UP Function Features IE indicates the features supported by the UP function and MUST be coded as depicted in Table 25.

Table 25: BBF UP Function Features

Feature Octet / Bit	Feature	Description
8/5	AGF-direct	Informs the AGF-CP that the UP supports direct AGF-UP functions.
8/6	AGF-adaptive	Informs the AGF-CP that the UP supports adaptive AGF-UP functions.
8/7	B-UPF	Informs the AGF-CP that the UP supports co-location of both AGF-UP and 5G UPF function.
8/8	AGF-profile-QoS	Informs the AGF-CP that the AGF-UP supports QoS profiles as defined in section 4.6.1
9/1	AGF-explicit-QoS	Informs the AGF-CP that the AGF-UP supports signaling of explicit QoS parameters as defined in section 4.6.2

Note:

- Feature flag AGF-profile-QoS and AGF-explicit-QoS can both be set, if the AGF-UP supports both AGF-profile-QoS and AGF-explicit-QoS as defined in section 4.6.3. If neither feature flags are set, the AGF-UP by default support only static QoS template as defined in section 4.6.4
- Feature flag AGF-direct and AGF-adaptive can both be set, if the AGF-UP supports both direct mode (5G-RG) and adaptive mode (FN-RG).
- Feature Octet/Bits 8/5, 8/6, 8/7, 8/8, and 9/1 are only applicable to the AGF use cases and is only sent during PFCP association.

7.7.2 BBF Outer Header Creation

This TR defines new NSH header values for the PFCP IEs BBF Outer Header Creation in TR-459i2 [7] section 6.9.3.

7.7.2.1 NSH header information

The following are two new values defined for NSH Header information in TR-459i2 [7] section 6.9.3.1.

- Circuit Identifier (type =4, Length=N): A circuit identifier
- Remote Identifier (type =5, Length=N): A remote Identifier

7.7.3 BBF Outer Header Removal

This TR defines a new value for the PFCP IEs BBF Outer Header Removal in TR-459i2 [7]

Table 26: BBF Outer Header Removal Description

Outer Header to be removed in the incoming packet	Value (Decimal)

Ethernet	1
PPPoE / Ethernet	2
PPP / PPPoE / Ethernet	3
L2TP	4
PPP / L2TP	5
5WE/Ethernet	**6**

- 5WE / Ethernet: Removes the 5WE header and Ethernet header including S-Tags and C-Tags.

7.7.4 BBF 5WE Session ID

The BBF 5WE Session ID IE MUST be encoded as Figure 7-5.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32822							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	BBF 5WE Session ID							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 7-5: 5WE Session ID

BBF 5WE Session ID
Encode a BBF 5WE Session ID as specified in RFC 8822.

7.7.5 BBF Traffic Enforcement Type

The BBF Traffic Enforcement Type IE MUST be encoded as in Figure 7-6

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32823							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7	Enforcement-type							
8 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 7-6: BBF Traffic Enforcement Type IE

Octet 7 is an enumeration indicating the traffic enforcement type, with possible values:

- 0x00: reserved
- 0x01: shaping
- 0x02: policing

7.7.6 BBF PCP

The BBF PCP IE MUST be encoded as in Figure 7-7.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 32824							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7	spare					PCP Value		
8 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 7-7: BBF PCP

The PCP Value is specified in IEEE 802.1p format.
Octet 7 / Bit 3 shall contain the most significant bit of the PCP value.

7.7.7 BBF TC Name

The BBF TC Name IE MUST be encoded as in Figure 7-8.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 32825							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	TC Name							

Figure 7-8: BBF TC Name

TC Name expressed as string.
Note: if a TC is referencing a number, it can be expressed as “1” in a string format.

7.7.8 BBF PBS

The BBF PBS IE MUST be encoded as in Figure 7-9.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 32826							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7	Spare						DLPBS	ULPBS
m to (m+7)	Uplink PBS							
p to (p+7)	Downlink PBS							
q to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 7-9: BBF PBS IE

The following flags are coded within octet 7:

- Bit 1 – ULPBS: If this bit is set to "1", then the Uplink PBS field shall be present, otherwise the Uplink PBS field shall not be present.
- Bit 2 – DLPBS: If this bit is set to "1", then the Downlink PBS field shall be present, otherwise the Downlink PBS field shall not be present.

At least one bit MUST be set to "1". Several bits may be set to "1".

The Uplink PBS and Downlink PBS fields shall be encoded as an Unsigned64 binary integer value. They shall contain the uplink or downlink PBS expressed in number of octets.

7.7.9 BBF CBS

The BBF CBS IE MUST be encoded as in Figure 7-10.

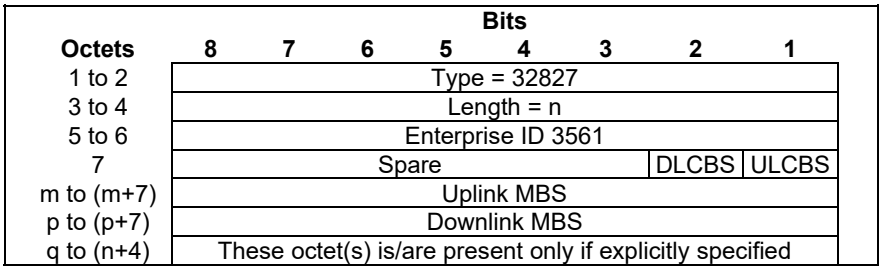

Figure 7-10: BBF MBS IE

The following flags are coded within octet 7:

- Bit 1 – ULPBS: If this bit is set to "1", then the Uplink PBS field shall be present, otherwise the Uplink CBS field shall not be present.
- Bit 2 – DLCBS: If this bit is set to "1", then the Downlink CBS field shall be present, otherwise the Downlink CBS field shall not be present.

At least one bit MUST be set to "1". Several bits may be set to "1".

The Uplink CBS and Downlink CBS fields shall be encoded as an Unsigned64 binary integer value. They shall contain the uplink or downlink CBS expressed in number of octets.

7.7.10 BBF CIRmax

The BBF CIRmax IE MUST be encoded as in Figure 7-11.

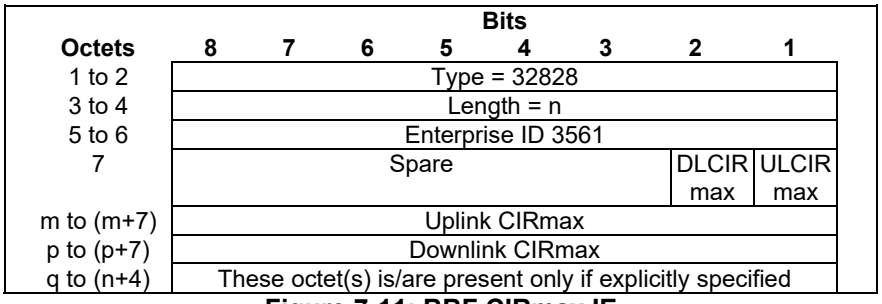

Figure 7-11: BBF CIRmax IE

The following flags are coded within octet 7:

- Bit 1 – ULCIRmax: If this bit is set to "1", then the Uplink CIRmax field shall be present, otherwise the Uplink CIRmax field shall not be present.
- Bit 2 – DLCIRmax: If this bit is set to "1", then the Downlink CIRmax field shall be present, otherwise the Downlink CIRmax field shall not be present.

At least one bit MUST be set to "1". Several bits may be set to "1".

The Uplink CIRmax and Downlink CIRmax fields shall be encoded as an Unsigned64 binary integer value. They shall contain the uplink or downlink CIRmax expressed in number of octets.

7.7.11 BBF Parent QER ID

The BBF Parent QER IE MUST be encoded as in Figure 7-12.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32829							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 10	Parent QER ID value							
11 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 7-12: BBF Parent QER ID IE

The Parent QER ID specifies the Parent QER (concept outlined in section 7.4.2.2.1) and the value shall be encoded as an Unsigned32 binary integer value.

7.7.12 BBF QoS Profile Name

The BBF QoS Profile Name is encoded as Figure 7-13.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32830							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	BBF QoS Profile Name							

Figure 7-13: BBF QoS Profile Name

The BBF QoS Profile Name is a string expressed with ASCII characters.

Applicable only to Session Modification request:

- If the BBF QoS Profile Name is empty (BBF QoS Profile Name length of 0), it removes the QoS Profile Name.
- If the same BBF QoS Profile Name is used, it overrides the existing BBF QoS Profile Name.

7.7.13 BBF UL Policing Descriptor Name

The BBF UL Policing Descriptor Name is encoded as Figure 7-14.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32831							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	BBF UL Policing Descriptor Name							

Figure 7-14: BBF UL Policing Descriptor Name

The BBF UL Policing descriptor name is a string expressed with ASCII characters.

Applicable only to Session Modification request:

- If the BBF UL Policing Descriptor Name is empty (BBF UL Policing Descriptor Name length of 0), it removes the BBF UL Policing Descriptor.
- If the same BBF UL Policing Descriptor is used, it overrides the existing BBF UL Policing Descriptor.

7.7.14 BBF DL Policing Descriptor Name

The BBF DL Policing Descriptor Name is encoded as Figure 7-15.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32832							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	BBF DL Policing Descriptor Name							

Figure 7-15: BBF DL Policing Descriptor Name

The BBF DL Policing descriptor name is a string expressed with ASCII characters.

Applicable only to Session Modification request:

- If the BBF DL Policing Descriptor Name is empty (BBF DL Policing Descriptor Name length of 0), it removes the BBF DL Policing Descriptor.
- If the same BBF DL Policing Descriptor is used, it overrides the existing BBF DL Policing Descriptor.

7.7.15 BBF UL TC Policing Descriptor Name

The BBF UL TC Policing Descriptor Name is encoded as Figure 7-16.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32833							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	BBF UL TC Policing Descriptor Name							

Figure 7-16: BBF UL TC Policing Descriptor Name

The BBF UL TC Policing descriptor name is a string expressed with ASCII characters.

Applicable only to Session Modification request:

- If the BBF UL TC Policing Descriptor Name is empty (BBF UL TC Policing Descriptor Name length of 0), it removes the BBF UL TC Policing Descriptor.
- If the same BBF UL TC Policing Descriptor is used, it overrides the existing BBF UL TC Policing Descriptor.

7.7.16 BBF DL TC Policing Descriptor Name

The BBF DL TC Policing Descriptor Name is encoded as Figure 7-17.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32834							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	BBF DL TC Policing Descriptor Name							

Figure 7-17: BBF DL TC Policing Descriptor Name

The BBF DL TC Policing descriptor name is a string expressed with ASCII characters.

Applicable only to Session Modification request:

- If the BBF DL TC Policing Descriptor Name is empty (BBF DL TC Policing Descriptor Name length of 0), it removes the BBF UL Policing Descriptor.
- If the same BBF DL TC Policing Descriptor is used, it overrides the existing BBF DL TC Policing Descriptor.

7.7.17 BBF DL Descriptor Name

The BBF DL Descriptor Name is encoded as Figure 7-18.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32835							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	BBF DL Descriptor Name							

Figure 7-18: BBF DL Descriptor Name

The BBF DL descriptor name is a string expressed with ASCII characters.

Applicable only to Session Modification request:

- If the BBF DL Descriptor Name is empty (BBF DL Descriptor Name length of 0), it removes the BBF DL Descriptor.
- If the same BBF DL Descriptor is used, it overrides the existing BBF DL Descriptor.

7.7.18 BBF DL TC Descriptor Name

The BBF DL TC Descriptor Name is encoded as Figure 7-19.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32836							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to (n+4)	BBF DL TC Descriptor Name							

Figure 7-19: BBF DL TC Descriptor Name

The BBF DL TC descriptor name is a string expressed with ASCII characters.

Applicable only to Session Modification request:

- If the BBF DL TC Descriptor Name is empty (BBF DL TC Descriptor Name length of 0), it removes the BBF DL TC Descriptor.
- If the same BBF DL TC Descriptor is used, it overrides the existing BBF DL TC Descriptor.

End of Broadband Forum Technical Report TR-458