Technical Report

TR-459
Control and User Plane Separation for a disaggregated BNG

Issue: 1
Issue Date: June 2020

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
1	9 June 2020	Kenneth Wan, Nokia	Original

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

Editor: Kenneth Wan, Nokia

Work Area Director(s): David Sinicrope, Ericsson

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This Technical Report specifies the architecture and requirements for a Disaggregated Broadband Network Gateway (DBNG). The separation of the control plane and user plane in the DBNG enables more efficient use of resources and simplifies operations. To allow multi-vendor interoperability, 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 broadband use cases.

1 Purpose and Scope

1.1 Purpose

This document specifies the architecture and requirements for a control plane and user plane separation of a Disaggregated Broadband Network Gateway (DBNG). The architecture designates Broadband Network Gateway (BNG) functions to either the control plane or user plane and also defines the interfaces between the control plane and user plane. Requirements on both interfaces and protocols helps ensure interoperability between different vendors' control planes and user planes. Use cases and deployment models are also captured. Although BNG control plane and user plane are separated, the goal is to ensure traditional broadband service offerings are maintained. 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 and user plane life cycle management, and simplifying operations by centralized control plane for configuration.

1.2 Scope

The following BNG functions and interfaces are in scope for control plane and user plane separation with respect to control, management, maintenance, and information exchange:

- Session Types:
  - TR-146 (PPPoEv4 and PPPoEv6, IPoEv4 and IPoEv6)
- Access side interfaces and protocols:
  - TR-25 V-interface (context LAC, LNS, and PTA)
  - TR-101 V-interface (PPPoE and IPoE)
  - TR-177 V-interface (IPv6 of TR-101)
  - TR-178 V-interface (IP/MPLS interface)
  - TR-187 V-interface (PPPoEv6 of TR-101)
  - TR-291 V-interface (IPoE)
  - TR-321 V-interface (Layer 2 over GRE)
  - TR-378 V-interface and S1u (LTE, GTP-u)
- Network side interface and protocols:
  - TR-25 L2TP
  - TR-178 A10 (IP/MPLS interface)
  - TR-187 A10 (L2TP over IP)
  - TR-291 S2a
- Control plane interface and protocols:
  - TR-134 (AAA and PDP)
  - TR-300 (Accounting and Charging)
  - TR-378 S11 (GTP-c),
- QoS functions:
  - TR-59 DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services
  - TR-101 Migration to Ethernet Based Broadband Aggregation (Section 5.2 Hierarchical Scheduling)
  - TR-178 Multi-service Broadband Network Architecture and Nodal Requirements (Section 7.1.6 Traffic filtering and QoS)
  - TR-300 Policy Convergence for Next Generation Fixed and 3GPP Wireless Networks (Section 6.2 Requirements for QoS control)
- Filter/Policy/ACL functions:
  - TR-59 DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services

    - TR-101 Migration to Ethernet Based Broadband Aggregation (Section 2.11 Policy Management, 3.7.4 Filtering)
    - TR-178 Multi-service Broadband Network Architecture and Nodal Requirements (Section 7.1.6 Traffic filtering and QoS)
    - TR-300 Policy Convergence for Next Generation Fixed and 3GPP Wireless Networks (Section 6.2 Requirements for QoS control)
    - TR-341 RADIUS attribute Catalog
- Integrated functions:
    - IPTV Multicast TR-101
    - WLAN-GW Access Controller TR-321
    - TWAG function TR-291
    - HAG function TR-384
    - Lawful Intercept TR-178

The following is within the scope of this project:

- Use cases and business drivers for Multi-Service BNG (MS-BNG) Control and User Plane Separation (CUPS)
- Deployment models for MS-BNG with CUPS
- An architectural reference picture of the functional blocks in the BNG, showing disaggregated control plane and user plane with their respective interfaces.
- Specification of the interface(s) between MS-BNG control plane and user plane
- Functional requirements of both Control Plane (CP) and User Plane (UP) with references to appropriate TRs and WTs including resiliency
- Specify a protocol for CUPS for each of the defined interfaces.
- Subscriber Management
- Policy Management
- Accounting
- Management architecture of user planes from the control plane
- It must be noted that this document considers DBNG User Plane (DBNG-UP) to be responsible for routing subscriber traffic. Both Routing control and data forwarding functions are considered to be residing on the DBNG-UP.
- Requirements for protocol extension are within scope of this project.

Out of scope:

- Further disaggregation of MS-BNG functions beyond CUPS.
- BNG functional distribution and virtualization
- With regards to “Specify protocol(s)” in the description and scope, this refers to specify by reference and not protocol design (e.g., elements of procedure and TLV formats). Specify in this use is identification of a protocol by reference and specification of its status (MUST, SHOULD, MAY) and under what conditions it is used. In general, protocol design is out of scope of this project.
- TR 317, as the architecture is more aligned with RG than the BNG.
- 3GPP have already produced technical specifications on Packet Gateway (PGW) control plane and user plane separation. This project will reuse 3GPP PGW defined TS and reuse 3GPP PGW CUPS TS 23.214 [20].
- The disaggregation of the routing function between control and user plane is out of scope of this document. Therefore, splitting the routing control and data forwarding between DBNG Control Plane (DBNG-CP) and DBNG-UP is also out of scope for this document.

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 [28].

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-25	Core Network Architecture for Access to Legacy Data Network over ADSL	BBF	1999
[2] TR-59	DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services	BBF	2003
[3] TR-69 Amendment 6	CPE WAN Management Protocol	BBF	2018
[4] TR-101 Issue 2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[5] TR-134 Corrigendum 1	Broadband Policy Control Framework (BPCF)	BBF	2013
[6] TR-145	Multi-service Broadband Network Functional Modules and Architecture	BBF	2012
[7] TR-146	Subscriber Sessions	BBF	2013
[8] TR-147	Layer 2 Control Mechanism for Broadband Multi-Service Architectures	BBF	2008
[9] TR-177	IPv6 in the Context of TR-101	BBF	2017

	Corrigendum 1			
[10]	TR-178 Issue 2	Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2017
[11]	TR-187 Issue 2	IPv6 for PPP Broadband Access	BBF	2013
[12]	TR-291	Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access	BBF	2014
[13]	TR-300	Policy Convergence for Next Generation Fixed and 3GPP Wireless Networks	BBF	2014
[14]	TR-321	Public Wi-Fi Access in Multi-service Broadband Networks	BBF	2015
[15]	TR-341	Radius Attributes Catalog	BBF	2016
[16]	TR-348	Hybrid Access Broadband Network Architecture	BBF	2016
[17]	TR-378	Nodal Requirements for Hybrid Access Broadband Networks	BBF	2019
[18]	TR-384	Cloud Central Office (CloudCO) Reference Architectural Framework	BBF	2018
[19]	TR-145	Multi-service Broadband Network Functional Modules and Architecture	BBF	2012
[20]	3GPP TS 23.214	Architecture enhancements for control and user plane separation of EPC nodes	3GPP	2019
[21]	3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access	3GPP	Dec 2019
[22]	3GPP TS 23.402	Architecture enhancements for non-3GPP accesses	3GPP	2019
[23]	3GPP TS 29.244	Interface between the Control Plane and the User Plane nodes	3GPP	Dec 2019
[24]	3GPP TS 29.274	3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3	3GPP	Dec 2019
[25]	3GPP TS 33.402	3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses	3GPP	Jun 2018
[26]	RFC 791	INTERNET PROTOCOL	IETF	1981
[27]	RFC 1661	The Point-to-Point Protocol (PPP)	IETF	1994
[28]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[29]	RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)	IETF	1999
[30]	RFC 2661	Layer Two Tunneling Protocol "L2TP	IETF	1999
[31]	RFC 2865	Remote Authentication Dial In User Service (RADIUS)	IETF	2000
[32]	RFC 2866	RADIUS Accounting	IETF	2000
[33]	RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs)	IETF	2006
[34]	RFC 4381	Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)	IETF	2006
[35]	RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	IETF	2006
[36]	RFC 5515	Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions	IETF	2009
[37]	RFC 5880	Bidirectional Forwarding Detection (BFD)	IETF	2010
[38]	RFC 5881	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)	IETF	2010
[39]	RFC 6973	Privacy Considerations for Internet Protocols	IETF	2013
[40]	RFC 7432	BGP MPLS-Based Ethernet VPN	IETF	2015
[41]	RFC 8300	Network Service Header (NSH)	IETF	2018

2.3 Definitions

The following terminology is used throughout this Technical Report.

AAA Client function	A logical entity that sends authenticating, authorizing and accounting requests to an AAA Server function. An example of an AAA client function contained with a network node is a Network Access Server (NAS) as described in RFCs 2865 [31] and 2866 [32]. Examples of AAA client function in BBF TRs are the BRAS of TR-059 [2] and the BNG of TR-101 [4]. (TR-134 [5])
AAA Server	A physical device that contains an AAA Server functions. (TR-134 [5])
AAA Server Function	A logical entity in the client-server relationship that replies to AAA Client Authentication, Authorization and Accounting requests. The AAA server function is typically responsible for receiving user connection requests, authenticating the user, and replying to the AAA Client function with an Accept or Deny response. The AAA Server function can return, as part of this reply, some or all of the configuration information necessary for the AAA client function to deliver service to the user. An AAA server function can act as a proxy client to other AAA server functions or other kinds of authentication servers. The AAA Server function does not contain any business logic other than basic authentication. (TR-134 [5])
Cold Standby	In general terms, a Cold Standby is a computing resource available in a DBNG with access to executable software and current configuration information. This generally provides a recovery time of tens of seconds.
C-Tag	Customer Tag
DBNG	Disaggregated BNG where the subscriber management function is separated between control plane and user plane.
Framed Route	This Attribute provides routing information to be configured for the user on the NAS. It is used in the Access-Accept packet and can appear multiple times. (RFC 2865 [31])
HAG	Hybrid Access Gateway. A logical function in the operator network implementing the network side mechanisms for simultaneous use of both fixed broadband and 3GPP access networks. (TR-378 [17])
Hot Standby	The protecting node is assigned to a working entity as its backup. The secondary node is configured, activated, and it maintains full operational state information so as to promptly take over the duties of the primary. To do so, it receives near real-time protocol information about that state. When a failure of the working instance is detected, the protecting node is able to work as a participant in all protocols. This generally provides a sub-second recovery time.
MS-BNG	TR-178 introduces the Multi-Service BNG (MS-BNG), which extends the capabilities of a traditional BNG to offer services to both residential and business customers as well as to allow mobile backhaul deployments. To achieve this, it performs Ethernet Aggregation and can either forward packets via MPLS or through IP Aggregation/routing. A MS-BNG is part of a TR-145 network architecture and can be deployed in a hierarchical BNG architecture. (TR-178 [10])
Protecting Instance	An instance that has been assigned to a particular working instance or a group of working instances.
S-Tag	Service Tag
TWAG	The trusted WLAN access gateway (TWAG) is the logical entity responsible for the 3GPP UE IP mobility service on the data plane between a Trusted BBF Access and 3GPP network.
Warm Standby	The protecting node is assigned to a working entity as its backup. The secondary node is configured, receives configuration updates, but it is not actively engaged in any protocol. Instead, the state information may be sent from the primary instance from time to time. This generally provides a recovery time of a few seconds.
WLAN	Wireless Local Area Network.
Working Instance	An instance of DBNG, whether CP DBNG-CP or DBNG-UP, that maintains both the current configuration and operational state.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization & Accounting
AC	Access Controller
ACL	Access Control List
AP	Access Point
BBF	Broadband Forum
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
CO	Central Office
CP	Control Plane
CPE	Customer Premises Equipment
CPR	Control Packet Redirect
CUPS	Control and User Plane Separation
DBNG	Disaggregated BNG
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EAP	Extensible Authentication Protocol
EMS	Element Management System
EPC	Enhanced Packet Core
ETH	Ethernet
FAR	Forward Action Rule
F-TEID	Fully Qualified Tunnel Endpoint Identifier
GRE	Generic Routing Encapsulation
GTP	GPRS Tunnelling Protocol
GTP-c	GTP for control plane
GTP-u	GTP user plane
GW	Gateway
HAG	Hybrid Access Gateway
HCPE	Hybrid CPE
ICCN	Incoming Call Connected
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ICRP	Incoming Call Reply
ICRQ	Incoming Call Request
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity

IP	Internet Protocol
IPCP	IP Control Protocol
IPoE	IP over Ethernet
IPoEv4	IPoE version 4
IPoEv6	IPoE version 6
IPTV	IP Television
IPv6	Internet Protocol version 6
IPv6CP	IPv6 Control Protocol
JSON	JavaScript Object Notation
L2	Layer 2
L2TP	Layer 2 Tunneling Protocol
L2TS	Layer 2 Tunneling switching
L2VPN	Layer 2 VPN
L3	Layer 3
LAC	L2TP Access Concentrator
LCP	Link Control Protocol
LI	Lawful Intercept
LNS	L2TP Network Server
LTE	Long Term Evolution
MAC	Media Access Control
MANO	Management and Orchestration
Mi	Management Interface
MLD	Multicast Listener Discovery
MME	Mobile Management Entity
MPLS	Multi-Protocol Label Switching
MRU	Maximum Receive Unit
MS-BNG	Multi-Service BNG
MTU	Maximum Transfer Unit
NAI	Network Access Identifier
NCP	Network Control Protocol
ND	Neighbor Discovery
NETCONF	Network Configuration Protocol
OAM	Operations Administration and Maintenance
OLT	Optical Line Terminal
OTT	Over the Top
PDI	Packet Detection Information
PDN	Packet Data Network
PDP	Policy Decision Point
PDR	Packet Detection Rule
PEP	Policy Enforcement Point
PFCP	Packet Forwarding Control Protocol
PGW	PDN GW
PIM	Protocol Independent Multicast
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PPPoEv4	PPPoE version 4
PPPoEv6	PPPoE version 6
PTA	PPP Termination and Aggregation
QoS	Quality of Service
RA	Router Advertisement

RADIUS	Remote Authentication Dial In User Service
RESTCONF	Representational State Transfer Configuration Protocol
RG	Residential Gateway
SCCCN	Start Control Connection Connected
SCCRP	Start Control Connection reply
SCCRQ	Start Control Connection Request
SCi	State Control interface
SGW	Serving GW
SLAAC	IPv6 Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
TEID	Traffic Endpoint Identifier
TLV	Type Length Value
TR	BBF Technical Report
TWAG	Trusted WLAN Access Gateway
TWAN	Trusted WLAN Access Network
TWAP	Trusted WLAN AAA Proxy
UP	User Plane
VLAN	Virtual Local Area Network
VLL	Virtual Leased Line
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WLAN-GW	WLAN Gateway
WT	BBF Working Text
XML	Extensible Markup Language
YANG	Yet Another Next Generation
ZLB	Zero Length Body

3 Technical Report Impact

3.1 Energy Efficiency

Energy Efficiency may be impacted migrating from standalone MS-BNG to DBNG. DBNG 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, geo 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

The DBNG is subject to the security concerns applicable to the MS-BNG, and particularly to those functions and interfaces included as “in scope” in the “Scope” section (1.2) of this document.

Security concerns for these functions and interfaces are described in the following TRs:

- TR-101 [4] “Migration to Ethernet-Based Broadband Aggregation” (L2 Security Considerations, section 3.7);
- TR-134 [5] “Broadband Policy Control Framework (BPCF)” (Security, section 3.3);
- TR-145 [6] “Multi-service Broadband Network Functional Modules and Architecture” (Security considerations for converged, multi-service networks, section 4.6.2);
- TR-146 [7] “Subscriber Sessions” (Security, section 3.3);
- TR-177 [9] “IPv6 in the context of TR-101” (Security, section 3.3; IPv6 Security Considerations, section 4.8; and L2 Security Considerations, section 5.5);
- TR-178(i2) [10] “Multi-service Broadband Network Architecture and Nodal Requirements” (Security, sections 3.3 and 5.4.8; and Security Requirements, section 5.6.3.6);
- TR-187 [11] “IPv6 for PPP Broadband Access (Security, section 3.3);
- TR-291 [12] “Nodal Requirements for Interworking between Next Generation and 3GPP Wireless Access” (Security, section 3.3);
- TR-321 [14] “Public Wi-Fi Access in Multi-service Broadband Networks” (section 3.3);
- TR-384 [18] “Cloud Central Office Reference Architectural Framework” (section 3.3);

Security concerns for relevant technologies are documented in several additional Standards. See, for example:

- Std. IEEE 802.1-2014 –
  - clause 8 (“Principles of Bridge Operations” – which includes some description of MAC layer security mechanisms),
  - clause 17.4 (“Security Considerations” relating to Bridge management),
  - clause 27.20 (“Security considerations” relating to Shortest Path Bridging);
- “Security Considerations” section of RFC 4364 [33] – “BGP/MPLS VPNs;”
- RFC 4381 [34] – “Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs);”
- “Security Considerations” section of RFC 7432 [40] – “BGP MPLS-Based Ethernet VPN.”

Where not explicitly described in directly relevant standards, implementations of DBNG should include a description of security considerations, possibly expanding on related referenceable standards.

In addition, any implementation of DBNG functionality 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.

Finally, because of the distribution of control and data plane functions defined for DBNG, the CUPS protocols must include capabilities for providing secure and authenticated communication between distributed components of the DBNG, specifically for the in-scope communication between CP and UP components, as indicated in Requirements [R-11] and [R-12].

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

The DBNG is subject to the privacy concerns applicable to the MS-BNG, and particularly to those functions and interfaces included as “in scope” in the “Scope” section 1.2 of this document.

Many people include information that would typically be addressed as a security concern – such as stored “private” data, connection specific information, etc. under the heading of privacy. Addressing the protection of these forms of privacy is provided through encryption of data exchanges between components.

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.

Privacy concerns for generic MS-BNG functions and interfaces are described in the following TRs:

- TR-134 [5] “Broadband Policy Control Framework (BPCF)” (Privacy, section 3.4);
- TR-291 [12] “Nodal Requirements for Interworking between Next Generation and 3GPP Wireless Access” (Privacy, section 3.4);
- TR-384 [18] “Cloud Central Office Reference Architectural Framework” (Privacy, section 3.4)

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 DBNG component. This increases the potential exposure to privacy violations.

In addition to security considerations described in section 3.3, DBNG 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 DBNG components, etc.) and explicitly include details of any unavoidable (or required) use and/or storage of PII.

DBNG component implementations should include privacy considerations such as those listed in related standards and similar activities such as:

- IEEE 802 current work to document recommended practices for creating new standards, as well as suggesting what to consider in implementing and deploying network technologies. This work may be published as early as sometime during the year 2019.
- IETF publication (in July, of 2013) of an Information RFC (RFC 6973 [39]) – 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 Introduction

The MS-BNG is an essential device that grants subscribers access to the internet and other private networks. It provides critical subscriber management functions, such as: authentication, IP address assignment, bandwidth allocation, and accounting. The MS-BNG also terminates various access types including: fixed wireline, fixed wireless, public Wi-Fi, and hybrid access.

The broadband services that MS-BNG supports include: VoIP, IPTV multicast, OTT video streaming, video game streaming, business VPN services, and many other IP services. As a result, the MS-BNG is taking on exponential subscriber growth as well as increased bandwidth demand which brings forth the following challenges:

- Over-utilizing a MS-BNG
- Under-utilizing a MS-BNG
- Managing and maintaining geographically distributed MS-BNG deployments
- Service provisioning across all deployed MS-BNGs
- Time to market services

The DBNG tackles these challenges by separating the subscriber management CP and UP. DBNG allows independent scaling of the CP and the UP to keep up with subscriber growth and subscriber bandwidth demands. The CUPS architecture also simplifies operations by maintaining a single management interface on the CP to manage all UPs.

This document provides the architecture, requirements, and call flows of a DBNG. In addition, DBNG State Control Interface (SCi) utilizes 3GPP defined Packet Forwarding Control Protocol (PFCP) for programming subscriber forwarding state. Section 6 provides the PFCP information element exchanges for typical MS-BNG use cases and PFCP Information Element extensions required to support wireline use cases.

4.1 MS-BNG Functional Architecture

Figure 1 illustrates the set of MS-BNG functions and interfaces that have been defined in BBF Technical Reports (TRs). Operators utilize a combination of MS-BNG functions to provide different types of broadband service(s). It should be noted that certain interfaces are not required depending on the selected MS-BNG functions (please refer to respective TRs for more detail on interface dependency). The MS-BNG consists of access, network, control and management interfaces. The control and management interfaces of an MS-BNG are commonly known as north bound interfaces. The access and network interfaces are user plane interfaces.

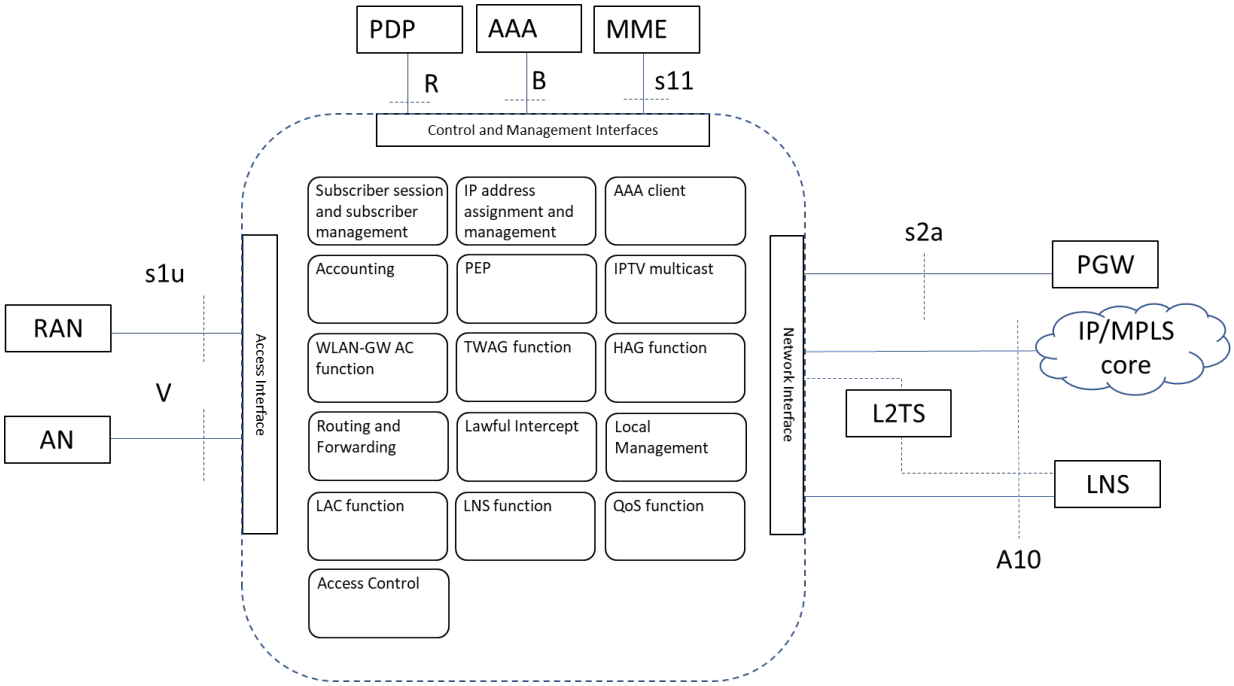

Figure 1: MS-BNG Functional blocks and interfaces

4.1.1 MS-BNG Functions

The MS-BNG utilizes different functional blocks to provide subscriber management functions including: AAA authentication, IP address assignment, policy enforcement, and accounting. In addition, the MS-BNG integrates other functional blocks such as Trusted Wi-Fi Access Gateway (TWAG) and Hybrid Access Gateway (HAG) to provide enhanced broadband services. Table 1 lists the functional blocks within the BNG:

Table 1: Functional Blocks of a MS-BNG

MS-BNG Functions	BBF TR references	MS-BNG functions specified in TRs
Subscriber session and subscriber management	TR-145, TR-25	IPoE, PPPoE session, and L2TP LAC session
IP address assignment and management	TR-101, TR-177, TR-178, TR-187, TR-341	IP address/prefix assignment through DHCPv4, DHCPv6, SLAAC, PPPoE, DHCPv6 over PPPoE, and SLAAC over PPPoE
AAA client	TR-101, TR-177, TR-178, TR-187, TR-134, TR-300, TR-341	Subscriber authentication
Accounting	TR-101, TR-177, TR-178, TR-187, TR-134, TR-300, TR-341	Subscriber accounting
Policy Enforcement Point (PEP)	TR-101, TR-177, TR-178, TR-187, TR-134, TR-300, TR-341	Subscriber filters and QoS rules
IPTV multicast	TR-101, TR-177, TR-178, TR-187, TR-134, TR-300	Subscriber IGMP/MLD processing
WLAN-GW Access Controller (AC)	TR-321	AC for Access Point (AP) management
TWAG	TR-291	Hand off broadband access to 3GPP
HAG	TR-348	Hybrid access
Routing and Forwarding	TR-101, TR-177, TR-178, TR-187	IGP, BGP, MPLS, PIM
Lawful Intercept (LI)	TR-178	Mirroring
Local Management		Local Management
L2TP Access Concentrator (LAC)	TR-25, TR-187	PPP based wholesale retail function
L2TP Network Server (LNS)	TR-25, TR-187	PPP based wholesale retail function
QoS	TR-101, TR-177, TR-178, TR-187, TR-134, TR-300, TR-341	QoS enforcement
Access Control	TR-147	Access Control can be part of an overall policy management framework. This includes aspects of QoS control, conditional access, as described in e.g. section 6.2

4.1.2 MS-BNG Interfaces

The following interfaces are defined in various BBF TRs:

- V-interface: Defined in TR-101 [4] as the Ethernet interface between the Access Node and the MS-BNG. Further, it includes the following capabilities: traffic aggregation, class of service distinction, and user isolation and traceability
- A10-interface: Defined in TR-25 [1] as the interface between the Regional Broadband network and the network service provider Point of Presences (POPs).
- R-interface: Defined in TR-134 [5] as the interface between the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The PEP is a function integrated into the MS-BNG.
- B-interface: Defined in TR-134 [5] as the interface between the PEP and the AAA server. The PEP is a function integrated in the MS-BNG, where it can receive/activate/modify/delete policies from AAA server.
- s1u: Defined in TR-378 [17] as the interface between the enhanced Node B (eNodeB) and the HAG as per 3GPP TS23.002
- s11: Defined in TR-378 [17] as the interface between the 3GPP Mobility Management Entity (MME) and the HAG.
- s2a: Defined in TR-291 [12] as the reference point between the TWAG and the 3GPP PDN GW. It is used for interworking between a Trusted BBF Access and 3GPP network and for supporting IP Network-Based Mobility. It conveys mobility and policy control from the 3GPP domain towards the TWAG.

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

Table 2: MS-BNG access interfaces

Interfaces	BBF TR references	Protocol Stacks	TR defined functions with respect to the access interfaces
V	TR-25, TR-101	IPoEv4, PPPoEv4	MS-BNG terminates PPPoE and IPoEv4 sessions. For LAC, the MS-BNG will terminate PPPoE sessions.
V	TR-177	IPoEv6	Based on TR-101, the MS-BNG terminates IPoEv6 sessions
V	TR-178	PPPoEv4, IPoEv4, IPoMPLS	Based on TR-101, the MS-BNG terminates IPoMPLS sessions
V	TR-187	PPPoEv6	Based on TR-178, the MS-BNG terminates PPPoEv6 sessions
V	TR-291	IPoE, L2oIPGRE	Based on TR-178, the MS-BNG integrates TWAG functions and terminates IPoE sessions
V	TR-321	IPoE, L2oIPGRE	Based on TR-178, the MS-BNG integrates access controller functions for public Wi-Fi and terminates IPoE sessions
V and s1u	TR-378	GTP (s1u), IPoE and PPPoE (V)	Based on TR-178, the MS-BNG integrates Hybrid Access Gateway functions and terminates PPPoE, GTP, and IPoE sessions

The MS-BNG connects subscriber IPoE or PPPoE session to the network core with a network interface. As highlighted in

Figure 1, the network interface also provides connectivity to wholesale service via L2TP or via MPLS. In addition, broadband service can also be offered via the 3GPP core network. Table 3 specifies the MS-BNG network interface cross referenced to relevant BBF TRs and their protocol stacks.

Table 3: MS-BNG network interfaces

Interfaces	BBF TR references	Protocol stacks	TR defined functions with respect to the network interfaces
A10	TR-25	L2TP	L2TP handoff to LTS or LNS
A10	TR-178	IPoEv4, MPLS	MS-BNG interfaces with the network core through IP/MPLS
A10	TR-187	IPoEv6	MS-BNG interfaces with the network core through IPv6
S2a	TR-291	GTP	MS-BNG that integrated TWAG function and interfaces with the 3GPP PGW

MS-BNG manages subscribers through control and management message exchanges with external elements. Typically, these includes AAA server, policy server, Accounting servers. Table 4 specifies the MS-BNG control and management interfaces cross referenced to relevant BBF TRs and their protocol stacks.

Table 4: MS-BNG control and management interfaces

Interfaces	TR references	Protocol stacks	TR defined functions with respect to the control and management interfaces
R	TR-134, TR-300	RADIUS, Diameter	Policy control framework
B	TR-134	RADIUS, Diameter	AAA service
S11	TR-378	GTP-c	Control interface between 3GPP MME and MS-BNG for session creation and session management

4.2 DBNG Functional Architecture

Utilizing the baseline MS-BNG figure in Figure 1, the MS-BNG interfaces and functional blocks are separated between the control plane and user plane. The functional architecture of the DBNG is shown in Figure 2. Please note: Figure 2 introduce a new steering function which is described in detail in section 4.2.4.1.

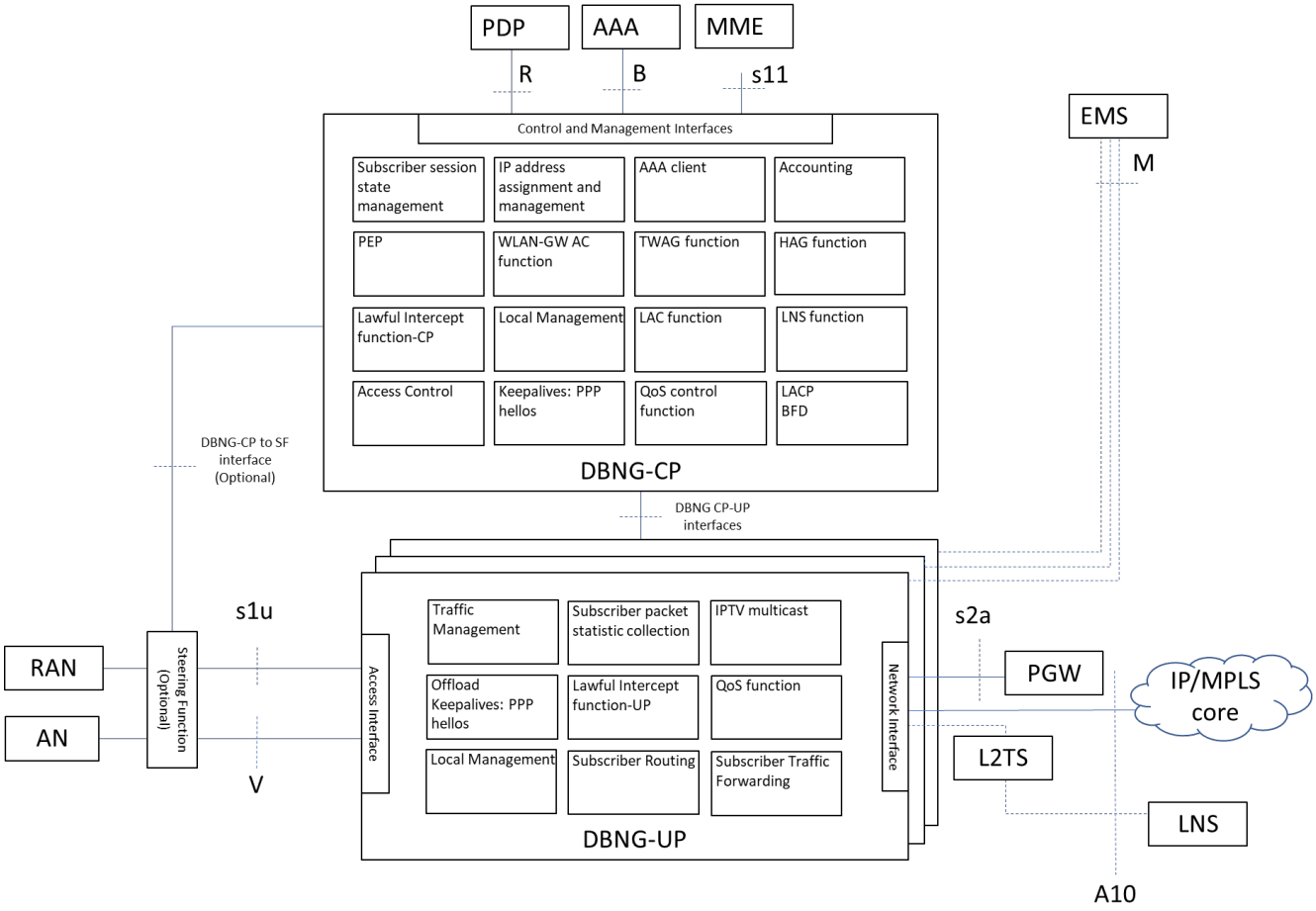

Figure 2: MS-BNG functions separating into Control Plane and User Plane

A combination of the control plane (CP) functions is referred to as a control plane of the DBNG (DBNG-CP). Similarly, a combination of user plane (UP) specific functions is referred to as a user plane of the DBNG (DBNG-UP). As specified in scope section 1.2, this document only focuses on routing function (both routing control and data forwarding) residing on the DBNG-UP. The DBNG-UP is responsible for routing all subscriber traffic.

4.2.1 DBNG-CP Functions

The DBNG-CP performs functions such as authentication via AAA servers and assigns IP address(es) to the subscriber. After the DBNG establishes a subscriber session, accounting updates are sent periodically to an accounting server. The following functions residing in the DBNG-CP include:

- Subscriber session state management

    - Managing PPPoE and IPoE session state.
- IP address assignment and management
    - Utilizing a PPPoE and an IPoE session to assign IPv4 address, IPv6 address, and/or IPv6 prefix are control plane related functions. After the address assignment has completed the control plane will signal forwarding rules to the user plane
- Accounting
    - Subscriber usage information is exchanged with accounting servers
- AAA client
    - Control message exchange with AAA servers
    - PPPoE, DHCPv4, and DHCPv6 initial message will trigger authentication with the AAA server
- PEP
    - After receiving the policies from a Policy Decision Point (PDP), the control plane will push these policies onto the DBNG-UP for enforcement.

In addition, TR-291 [12], TR-321 [14], and TR-384 [16] integrate further functions into the DBNG-CP.

- WLAN-GW: As explained in TR-321 [14], the access controller is integrated into the MS-BNG. Prior to address assignment, the end device performs EAP authentication with the AC. After a successful authentication, the MS-BNG will assign an IP address for the end device. The authentication of the AC and address assignment of the MS-BNG are all control plane processing. After the address assignment is completed the control plane will signal forwarding rules to the user plane.
- TWAG: As explained in TR-291 [12], TWAG performs wireline authentication with an IPoE subscriber. After a successful authentication, the TWAG function will signal the PGW to create a GTP tunnel. After the tunnel setup has completed, the address assignment will then be completed by the MS-BNG. The MS-BNG authentication/addressing function and the TWAG signaling are all control plane processing. After the address assignment has completed, the control plane will signal forwarding rules to the user plane.
- HAG: As explained in TR-348 [16], the hybrid access consists of a broadband connection and a 3GPP connection. The broadband connection is provided through traditional MS-BNG functions. The 3GPP connection follows 3GPP procedures where the eNodeB establishes tunnels to the HAG using procedure defined in 3GPP TS 29.274 [24]. Further address allocation for the 3GPP connections follows the PDP procedures. After the address assignment is completed the control plane will signal forwarding rules to the user plane for both the broadband and 3GPP connection.

Other DBNG-CP functions includes:

- Lawful Intercept Control Plane Function: Receives instruction from a lawful intercept mediation element and instructs the DBNG-UP lawful intercept actions.
- Management Interface: A management interface that allows management of a DBNG-CP and its many DBNG-UPs.
- DBNG-UP Selection Function: Described in section 4.2.4.1 is responsible for identifying the correct DBNG-UP to which a subscriber session should be connected, and signaling this selection to the Steering Function (in the case that the optional Steering Function is deployed).
- Keepalives: The DBNG-CP must be able to process and generate subscriber session keep-alive messages (including the generation and response to LCP Echo-Request and processing of LCP Echo-Reply messages) and it should possible for the DBNG-CP to offload selected subscriber session keep-alive message processing and generation to the DBNG-UP.
- LACP and BFD

4.2.1.1 DBNG-CP Northbound Interfaces

The northbound interfaces: R, B, and S11 are terminated on the DBNG-CP.

4.2.2 DBNG-UP Functions

Once the DBNG-CP completes authentication and address assignment, the DBNG-UP creates state related to forwarding for the subscriber session. The DBNG-UP performs forwarding, traffic management, and policy enforcement on the subscriber traffic. The following functions are part of DBNG-UP:

- Traffic Management: follows the instruction from the DBNG-CP on forwarding and related state for each subscriber session. For example, header manipulation, subscriber session termination, forwarding rules, filtering rules, and QoS rules.
- Subscriber packet statistic collection: the ability to collect per subscriber packet forwarding statistics

In addition, other DBNG functions that require immediate response may be located on the local DBNG-UP to improve scaling.

- IPTV Multicast: IGMP and MLD request are processed locally to provide the fastest channel change time.
- Subscriber Routing: Includes both routing control and forwarding
- Keepalive Messages: Includes the generation and processing of PPP echo messages that are offloaded from the DBNG-CP for the purposes of improving scalability and/or failure detection times. In this case, the DBNG-UP will need to inform the DBNG-CP of any relevant changes in keepalive state.
- Lawful Intercept: The user plane component of lawful intercept where mirrored packet must adhere to local country standard LI format.
- Local Control Plane: Process all the messages mentioned: IGMP, MLD, IGP, BGP, and keepalives.

4.2.2.1 DBNG-UP Interfaces

The access interface (V) and network interface (A10) that forward subscriber data traffic belong to the DBNG-UP. Optional management interface (M) for connecting to external EMS.

4.2.3 Interfaces between DBNG-CP and DBNG-UP

With the separation of the control and user plane, interfaces are required to facilitate communication between the DBNG-CP and DBNG-UP.

4.2.3.1 Management Interface

The DBNG-CP provides a Management Interface (Mi) for configuration shown in Figure 3. The DBNG-CP will manage its associated DBNG-UPs and is responsible for pushing configurations and retrieving operational state and status to and from the DBNG-UPs. For reference, this is similar to “configuration” and “show” commands for a traditional MS-BNG. Some examples of the configurations that are pushed to the DBNG-UPs are routing protocol configuration and QoS policy templates.

It must be noted that a DBNG-CP can be deployed with a variety of DBNG-UPs from different vendors. While traditional MS-BNGs have vendor proprietary internal representation of system resources, hardware resources and physical configurations are transparent to the DBNG-CP. The Mi would be used to communicate system resource information.

The Mi supports these functionalities, for example:

- Publishing of DBNG-UP operational data and resource information
- Notification of events and alarms between DBNG-CP and DBNG-UP

- Resource constructs such as interfaces described in TR-178 [10]

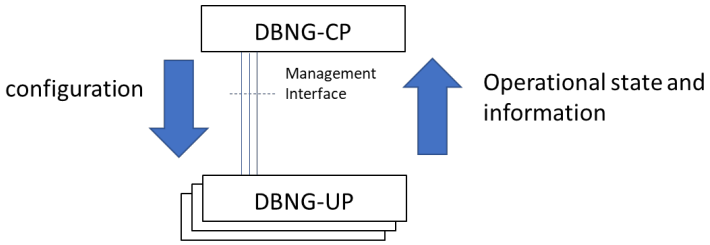

Figure 3: Management Interface

4.2.3.2 Control Packet Redirection Interface

A separate interface is required to forward and tunnel control packets such as DHCP, L2TP Control packets, PPPoE, and Neighbor Discovery packets through the user plane to the control plane. Figure 4 is a flow diagram that provides an example of the control messages that are tunneled from Residential Gateway (RG) through the DBNG-UP to the DBNG-CP.

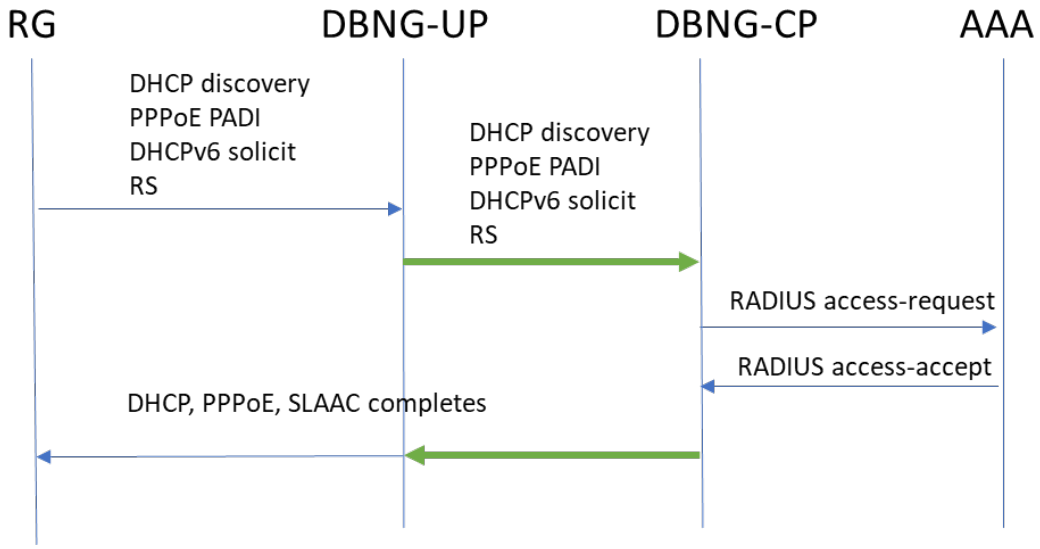

Figure 4: Example of Control and User Plane control message exchange

Figure 4 shows that a Control Packet Redirect Interface (CPR Interface) between the DBNG-UP and DBNG-CP is required for triggering subscriber authentication. With DBNG, the DBNG-CP and the DBNG-UP each become a separate network function. The network separation between DBNG-CP and DBNG-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 5 below illustrates the CPR Interface.

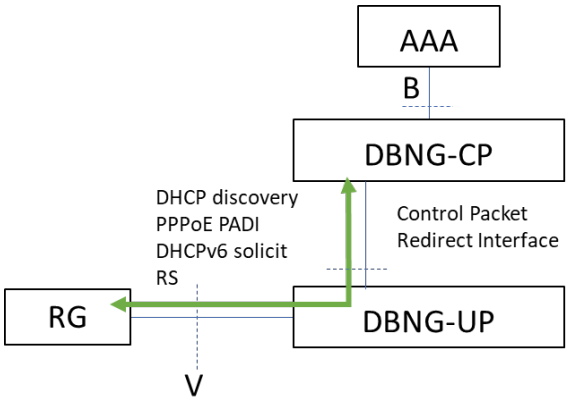

Figure 5: Control Packet Redirect Interface

A subscriber session typically starts with control messages from subscriber access, which may request one or more addresses. The DBNG-UP must redirect these control messages to the DBNG-CP. This default redirect rule would be signaled by the DBNG-CP to DBNG-UP after a successful association between the DBNG-CP and DBNG-UP. The DBNG-UP can have:

- Session context for a subscriber (a known subscriber on the DBNG-UP)
- No session context for a subscriber (a new subscriber connecting to the network for the first time).

Since the DBNG-CP is decoupled from the DBNG-UP, the DBNG-CP has no access circuit information (ex. logical port, etc.). Therefore, the DBNG-UP might need to include data plane information as meta-data when redirecting control packets.

4.2.3.3 State Control Interface

The State Control Interface (SCi) is used to program a default rule to redirect control packets between user plane and control plane. Once the subscriber has successfully authenticated, the DBNG-CP will install traffic forwarding rules and related states to the DBNG-UP as shown in Figure 6. Successful installation of the traffic rules will be indicated by an acknowledgement from the DBNG-UP. After the traffic rules are programmed onto the DBNG-UP, the DBNG-UP will forward the subscriber data traffic according to the rules.

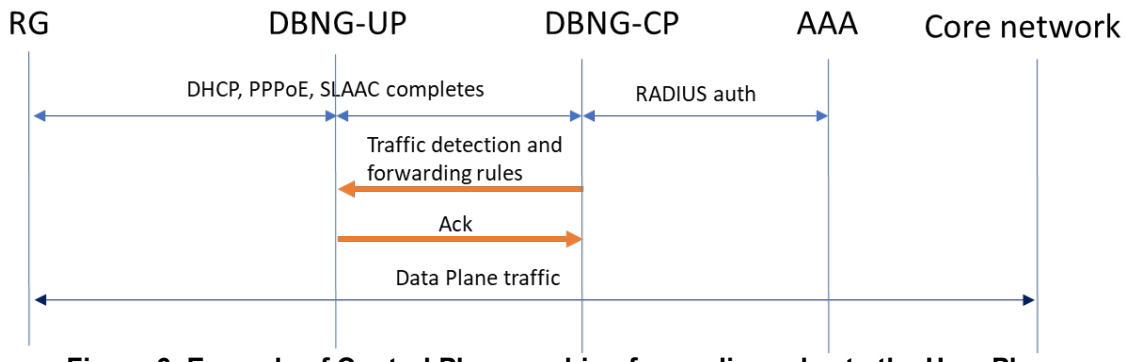

Figure 6: Example of Control Plane pushing forwarding rules to the User Plane

Figure 7 illustrates the third interface, SCi, that is required to program traffic detection and forwarding rules.

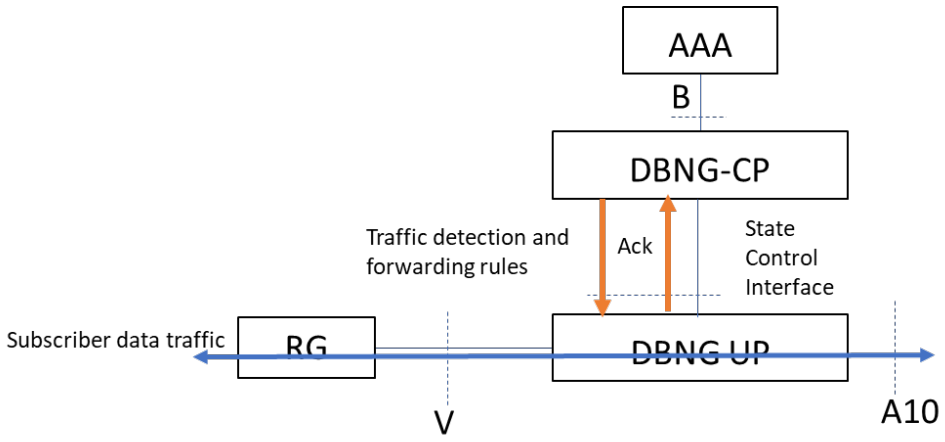

Figure 7: State Control Interface

Since MS-BNG can support different access types and protocols on the V interface, the traffic detection and forwarding rules must be flexible. Figure 8 below shows the different user plane combinations with respect to the MS-BNG functions as described in their respective TRs.

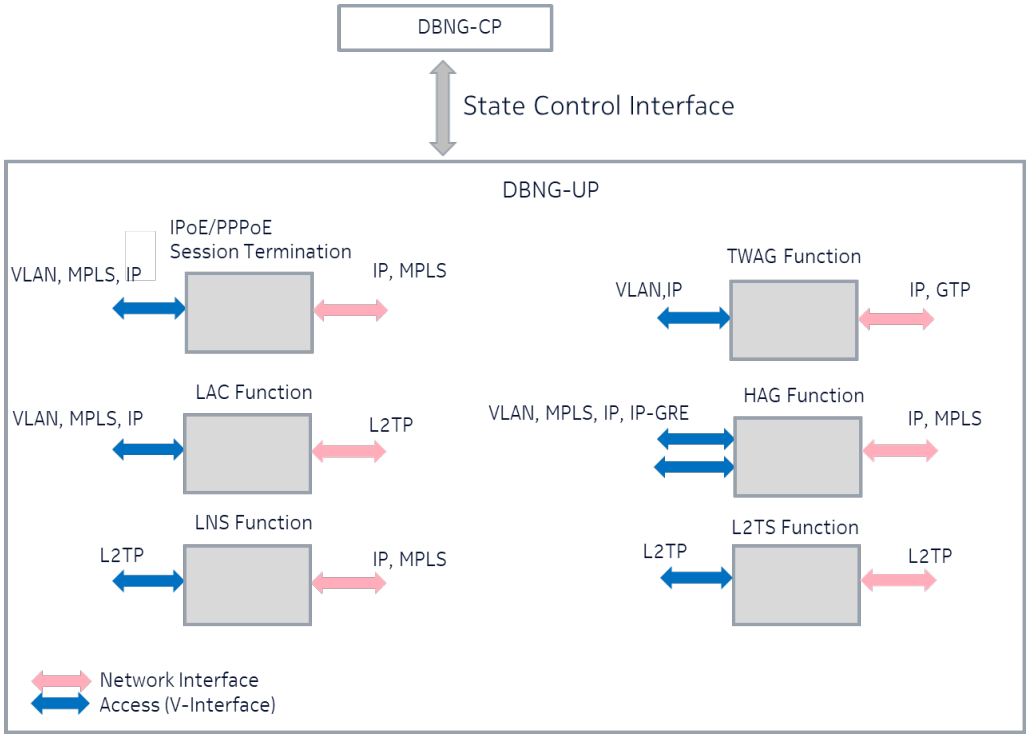

Figure 8: Example of User Plane combinations

The basic traffic detection and forwarding rules in the upstream direction (e.g. access to network) and the downstream direction (e.g. network to access) follows the same pattern and fundamentally consists of session identification followed by one or more actions. Figure 9 and Figure 10 are logical representation of DBNG-CP sending directives to DBNG-UP, instructing the DBNG-UP to install basic forwarding state for fixed L2 access (e.g. access from DSLAM or OLTs over Ethernet).

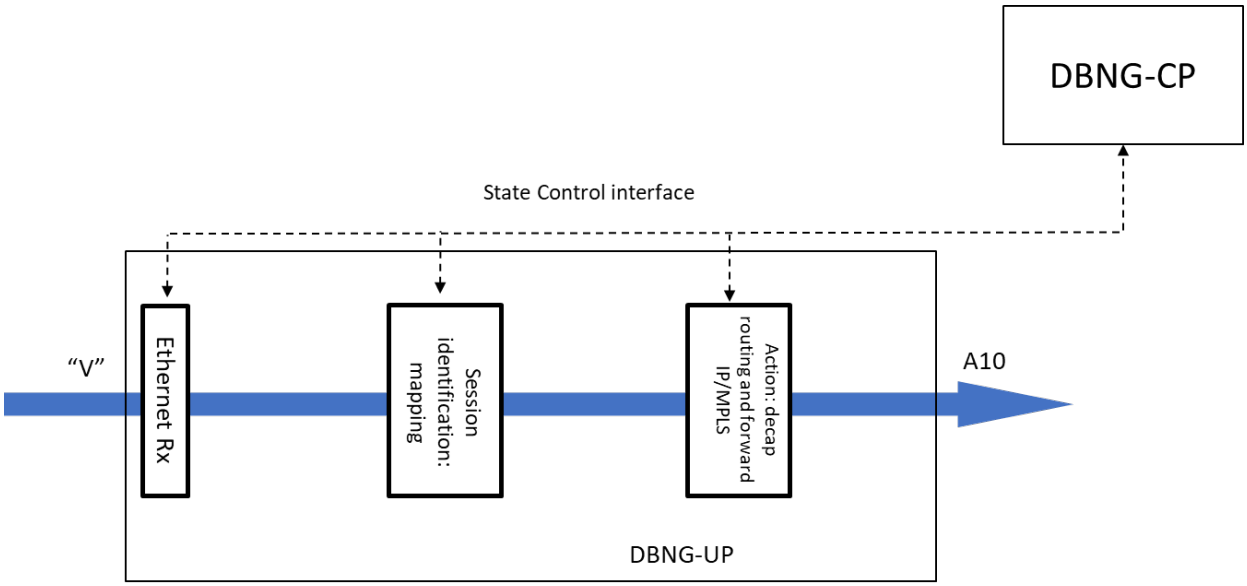

Figure 9: State Control Interface for Access to Network direction

Direction Upstream - Access to Network:

- Session-identification: Port/VLAN-Tag(s) + Subscriber-MAC
- Action: Remove encapsulation, IP FIB lookup, Forward to network.

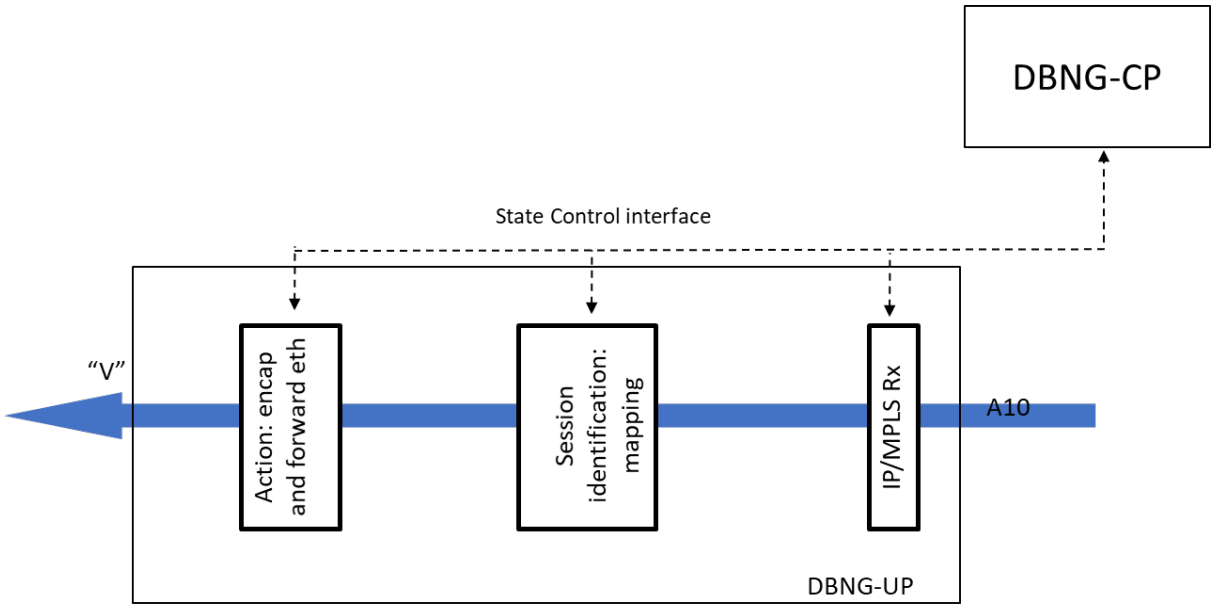

Figure 10: State Control Interface for Network to Access direction

Direction Downstream - Network to Access:

- Session-identification: IP address
- Action: Lookup IP destination address, build encapsulation using Port/VLAN-Tag(s)+subscriber-MAC, Forward to access.

The session state on the DBNG-UP is always controlled by the DBNG-CP i.e. the DBNG-UP just follows the directive from the DBNG-CP to install, modify and delete the session state. In addition to basic forwarding state, the DBNG-CP can also associate, update, and disassociate other related state with the session e.g. state related to:

- Filtering
- SLA management
- Statistics collection
- Credit control
- Traffic mirroring
- Application aware policies

Cases where DBNG-CP would trigger session state change:

1. DBNG-CP triggers a new session state on the DBNG-UP. E.g., when the subscriber successfully authenticates
2. DBNG-CP triggers an update of session state on the DBNG-UP. E.g., triggered by an update from the policy-server.
3. DBNG-CP triggers the deletion of session state. E.g., based on administrative action, session termination or a disconnect-message initiated from the AAA server.

4.2.4 DBNG High level Architecture

In summary, the following are the identified interfaces required for DBNG-CP and DBNG-UP communication.

1. Management Interface (Mi)
2. Control Packet Redirect Interface (CPR interface)
3. State Control Interface (SCi)

Together with the DBNG functions and interfaces, Figure 11 below illustrates a high level architecture of CUPS for a DBNG and the new defined interfaces between the DBNG-CP and DBNG-UP.

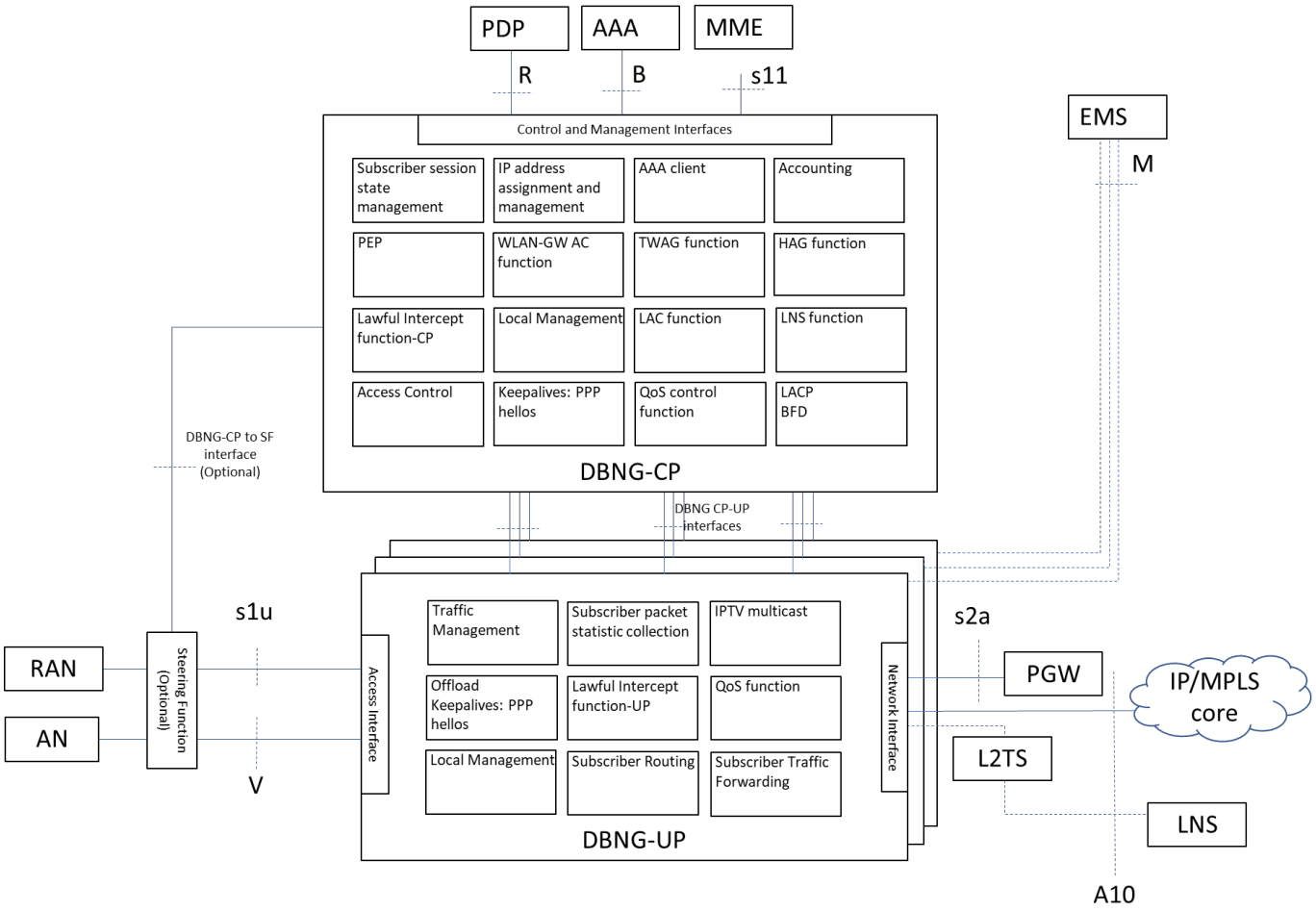

Figure 11: High level architecture of control and user plane separation of a DBNG

4.2.4.1 Steering Function

The separation of control and user plane introduces the option for multiple DBNG-UPs to be under the control of a single DBNG-CP. Multiple DBNG-UPs may be deployed to support the desired network scale, to support different service levels, to provide Multi-Access Edge Compute (MEC) services to a subset of subscribers, or to provide DBNG-UP functions within different network slices. The optional Steering Function provides the capability to steer (direct) customer sessions to the correct DBNG-UP, allowing load balancing of sessions across the available DBNG-UPs and/or to select a specific DBNG-UP for any one session. The Steering Function is deployed on the V interface between the AN and the DBNG-UP.

It is the responsibility of the DBNG-CP (based on local criteria and any relevant policy provided by AAA) to select the correct DBNG-UP for a particular subscriber, and to signal this to the steering function. The selection of DBNG-UP may be performed at session setup and/or for a live session. The following are examples of selection criteria:

- The current load of the DBNG-UP under control of the DBNG-CP.
- The knowledge of service(s) required by the subscriber that are co-located with a subset of DBNG-UPs
- A subscriber group (e.g. an enterprise customer) that may have dedicated DBNG-UP.
- Operational needs such as removing a DBNG-UP from service.
- Performance needs such as to guarantee a subscriber's service level agreement.

4.3 Deployment models

The following section describes different deployment scenarios.

4.3.1 Deployment model: Geographical separation of DBNG-CP and DBNG-UP

The DBNG system can cover the services and subscribers in a broad geographic region. The control plane can be deployed centrally with the user planes deployed in different areas closer to subscribers as shown in Figure 12.

For example, take three areas A, B, and C, each with its own user plane. The three user plane shares one control plane. The control plane can be deployed in a centralized location at a Core Data Center as opposed to the user planes which are deployed at city edge datacenters closer to subscribers. In this design, data centers and edge data centers are selected based on their location and responsibilities.

The centralized control plane communicates with outside subsystems and user planes for control and management. Under the control plane's instruction, users' traffic is forwarded by DBNG-UP to the Internet. The control plane can be virtualized as VNF for its computation intensive workloads, while the user plane may be virtualized for light traffic or stay physical for high traffic.

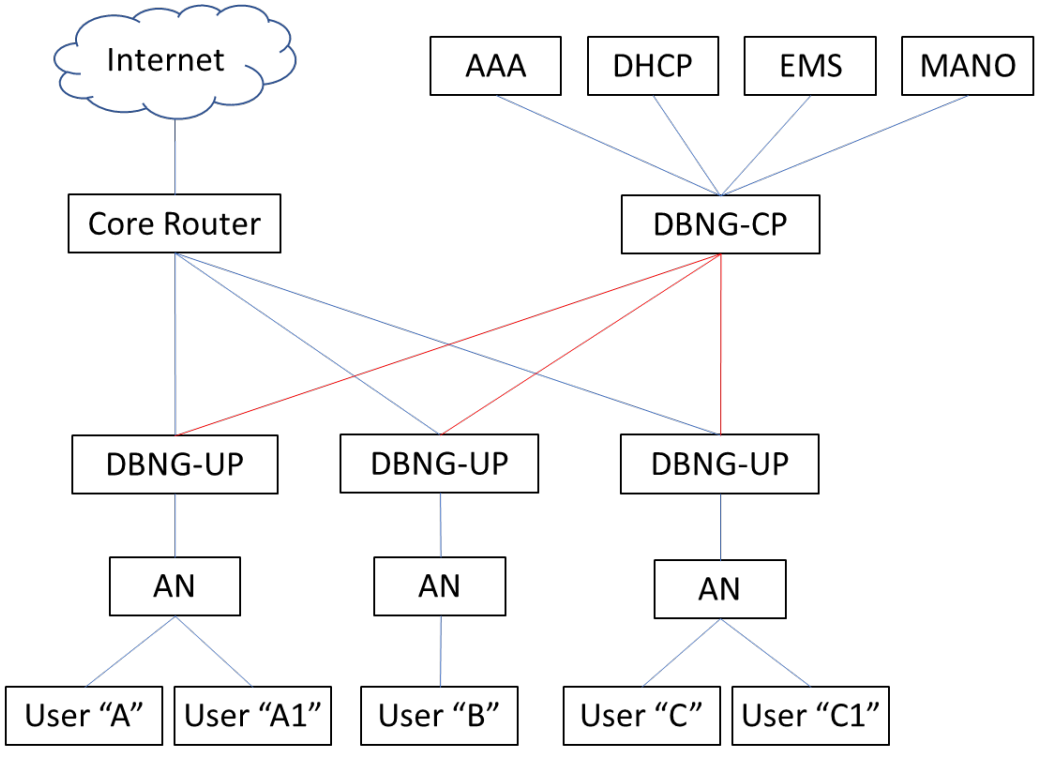

Figure 12: Geographically distributed deployment model

4.3.2 Deployment model: Non-Geographical separation of DBNG-CP and DBNG-UP

Due to scalability and security requirements, the DBNG-CP and DBNG-UP may be placed together at the same central office (CO). In this case, the CO installation does not geographically distribute the DBNG-UP as shown in Figure 13. A Point of Delivery (POD) may consist of multiple DBNG-UPs and a single DBNG-CP. In this deployment model, the same deployment principles described in 4.3.1 apply, but since the DBNG-CP and DBNG-UPs are within the same secured domain certain security requirements can now be removed.

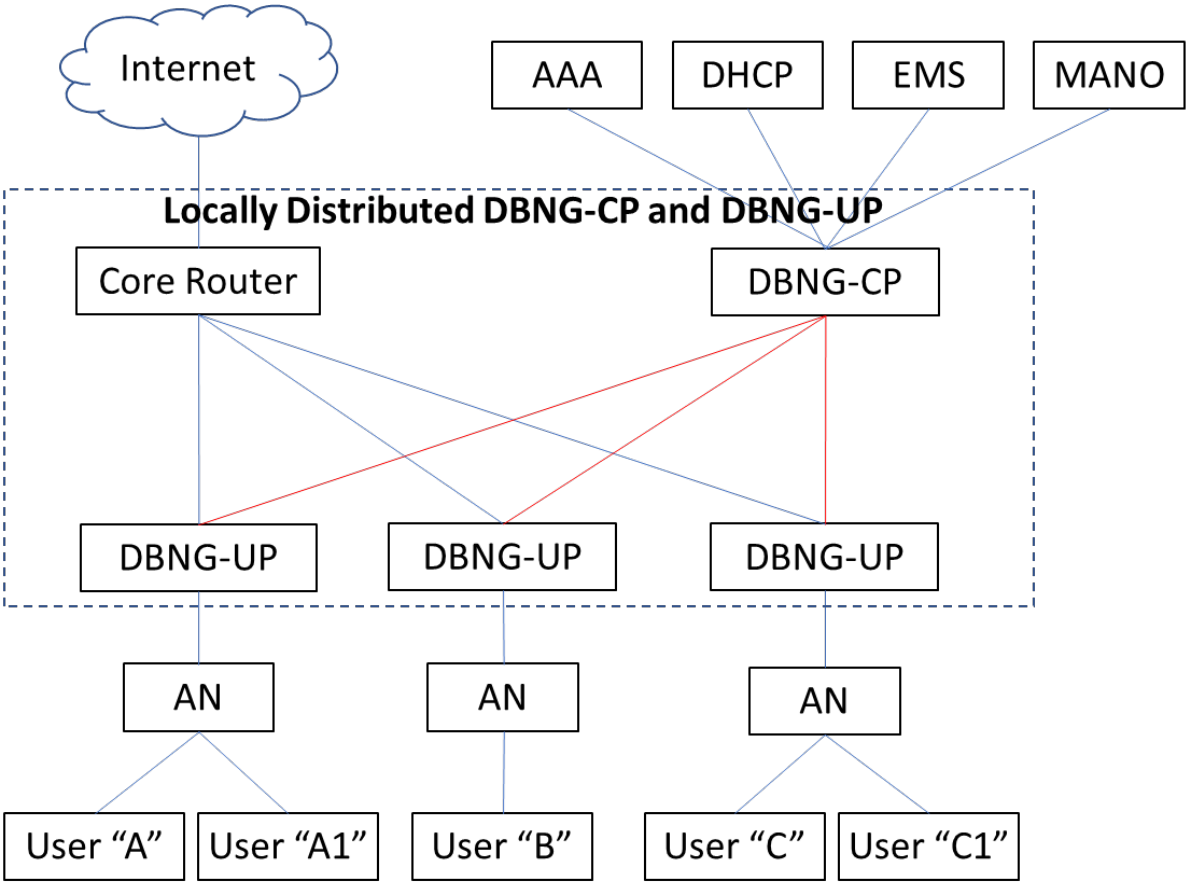

Figure 13: Non-Geographically distributed deployment model

4.4 Call Flows

In this section, the call flows are informative and “session forwarding state” is hereinafter referred to as “session”.

4.4.1 Control Plane and User Plane Association

It is assumed that the two nodes (DBNG-CP and DBNG-UP) are provisioned or otherwise made aware of their partner nodes. E.g., provisioning, configuration, auto-discovery, is outside the scope of the CUPS protocol. A new DBNG-UP must form an association with a DBNG-CP. Afterwards, the DBNG-CP requests to start a generic session with DBNG-UP to program forwarding rules on the DBNG-UP. The forwarding rules instruct the DBNG-UP to redirect control messages over the CPR Interface.

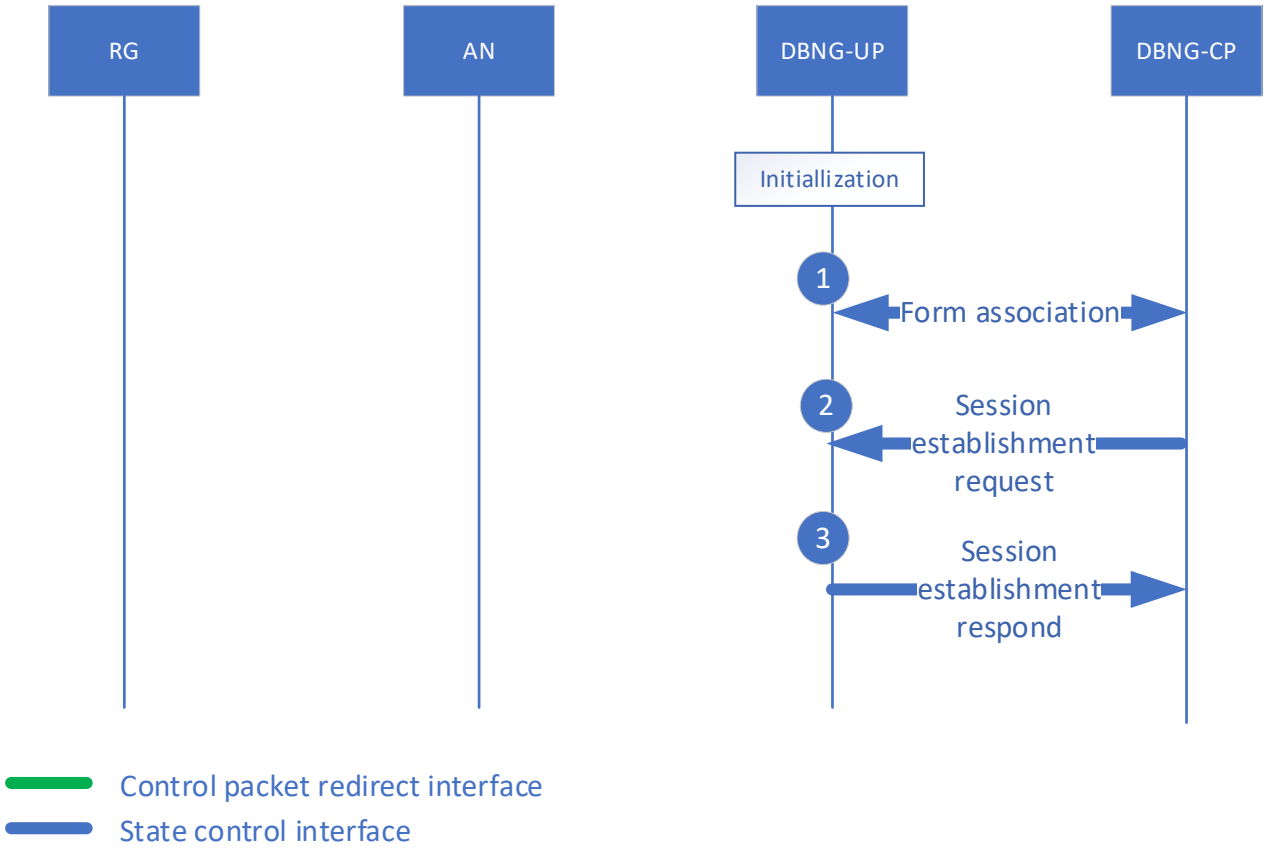

Figure 14: DBNG-CP and DBNG-UP association

1. DBNG-UP and DBNG-CP forms an association. The association can be started by either the DBNG-UP or DBNG-CP. During the association process, the DBNG-UP and DBNG-CP will exchange capabilities information, e.g. types of BNG functions.
2. After the association between DBNG-UP and DBNG-CP is formed, a session establishment request is sent from the DBNG-CP to the DBNG-UP to program the default control packet redirection rules. The control packet redirection rules instructs the DBNG-UP to redirect specific types of control packets to the DBNG-CP through the CPR interface.
3. The DBNG-UP responds to the DBNG-CP session establishment request with either a success or failure.

4.4.2 Initial Control Packet Redirection Rule

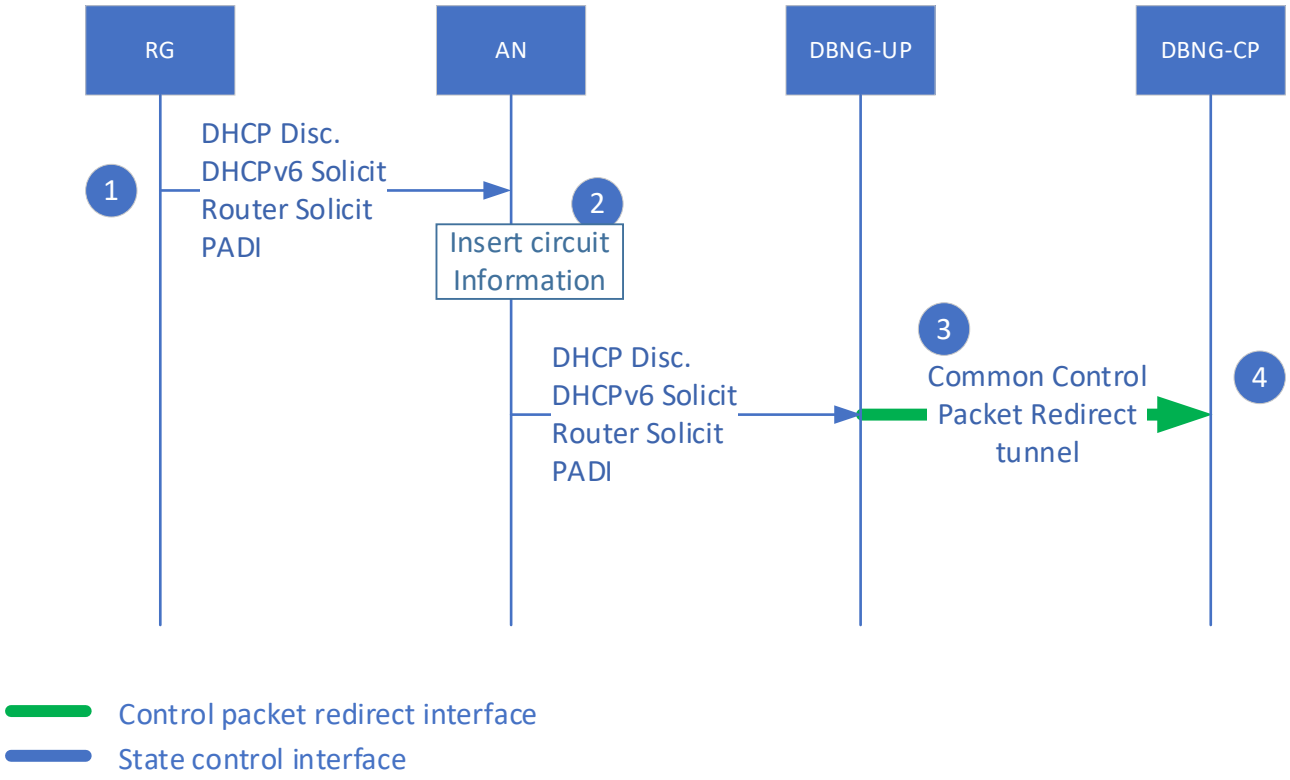

Figure 15: Common control packet redirection rule

1. All new RGs first connecting to the network, send a control message packet. This may include DHCPv4 discovery, PPPoE Auto Discovery Initiation (PADI), DHCPv6 solicit, Router Solicit, or a data trigger packet.
2. The AN inserts circuit information onto the control message which can include: a circuit ID, a remote ID, a Line ID, and/or an interface ID.
3. The DBNG-UP detects these as new control messages that are unrelated to currently established sessions and tunnels these control messages over the CPR Interface. The DBNG-UP must also provide access interface information as metadata (for example port information) to the DBNG-CP because this information might not be within the packet itself.
4. The DBNG-CP receives the control message and its context as metadata, together providing a session context.

4.4.3 IPoE DHCPv4

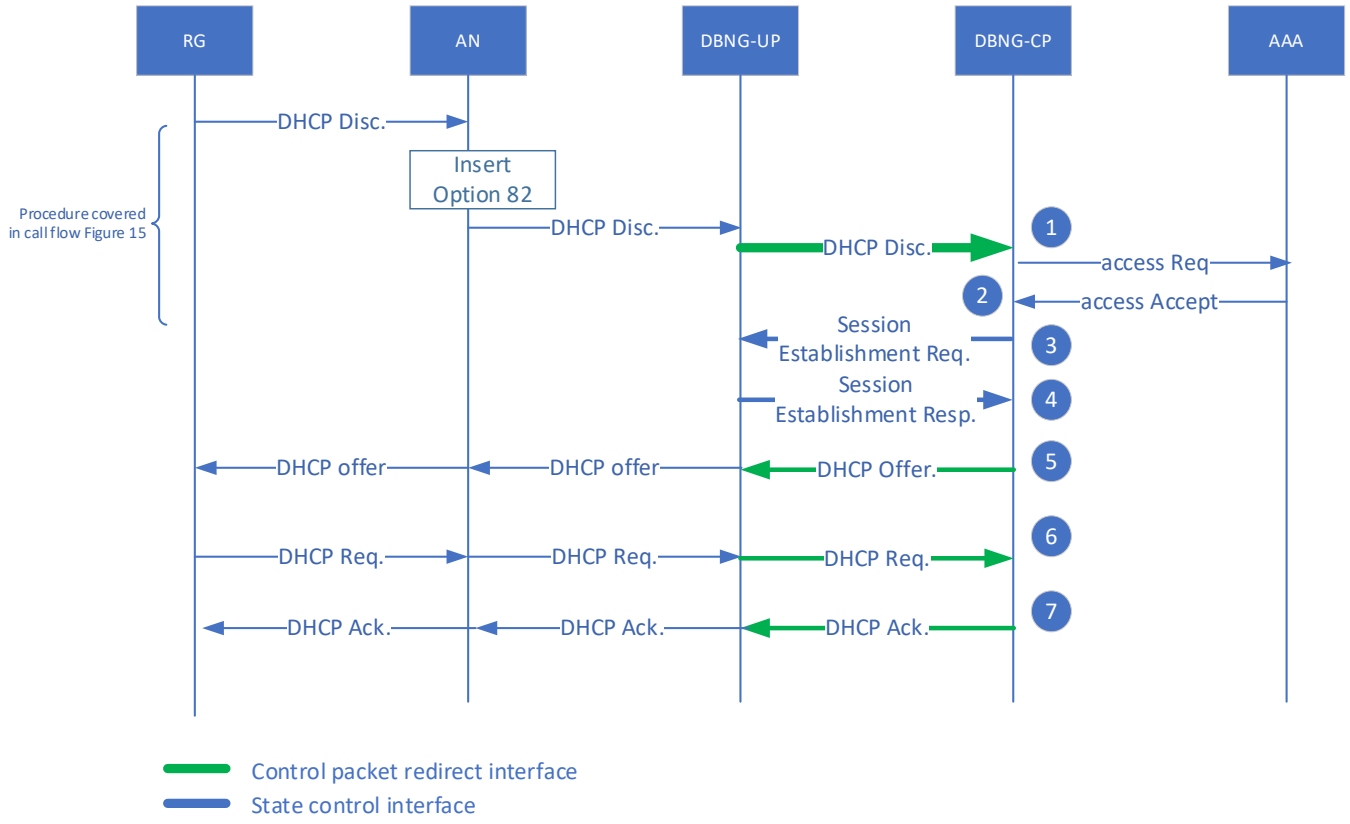

Figure 16: IPoE DHCPv4 call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common CPR rule.

1. The DBNG-CP triggers an Access-Request to authenticate the RG.
2. The AAA successfully authenticates the RG and replies to the DBNG-CP with an Access-Accept.
3. *The DBNG-CP assigns the IP address to the RG which is obtained through either the local address server or returned by AAA as one of the attributes. At this point the DBNG-CP can send a Session Establishment Request to create new packet forwarding states for the data packet. This can update the data plane state.
4. The DBNG-UP sends a Session Establishment Response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscriber's IP data packets.
5. The DHCP Offer from the DBNG-CP is sent back to the RG through the DBNG-UP utilizing the CPR Interface.
6. **The DHCP Request is sent from the RG through the DBNG-UP utilizing a dedicated session control packet redirect tunnel. As noted, if a session has not yet been established, the session must be established at this step.
7. The DHCP process completes by sending the DHCP acknowledgement. The DBNG-CP forwards the DHCP Ack through the dedicated session control packet redirect tunnel back to the RG though the DBNG-UP.

*Note: At this step, it is possible to create a session from the redirected control packet. By doing so, resources are consumed on the DBNG-UP in order to allow individual subscriber control packet management such as blocking, rate limiting, and specific packet filtering. It is also possible to postpone the session

creation. By doing so, additional DBNG-UP resources are not consumed, but individual subscriber control packet management is not possible.

**Note: Subscriber session creation can be performed at any steps prior. This step is the last chance for a session creation in order to avoid subscriber data packets drops. Right after this step, the RG is assigned an address and data packets could be sent immediately.

4.4.4 IPoE DHCPv6

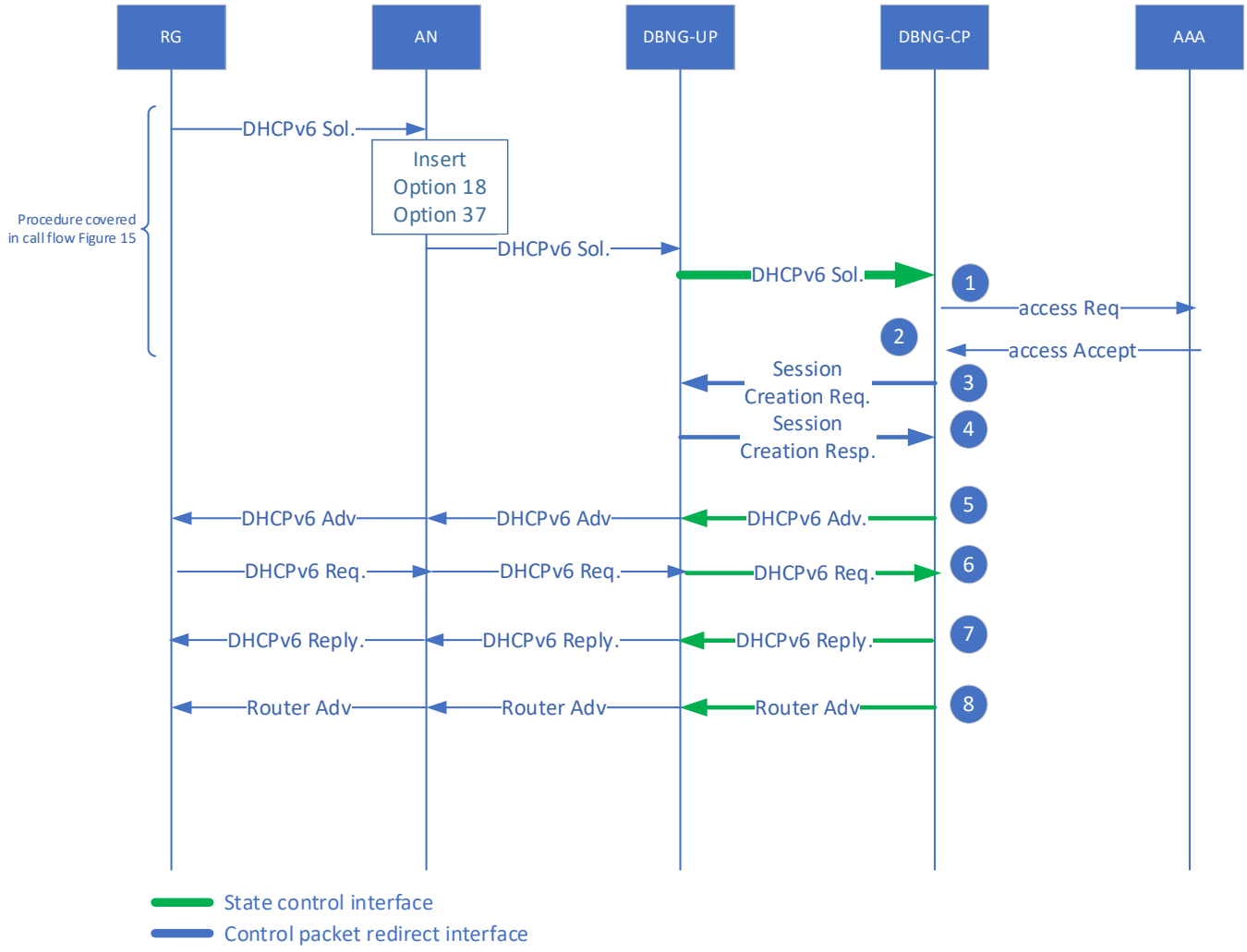

Figure 17: IPoE DHCPv6 call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1. The DBNG-CP triggers an Access-Request to authenticate the RG.
2. The AAA successfully authenticates the RG and replies to the DBNG-CP with an Access-Accept.
3. *The DBNG-CP assigns the IP address to the RG which is obtained through either the local address server or returned by AAA as one of the attributes. At this point the DBNG-CP can send a Session Establishment Request to create new packet forwarding states for the data packet. This updates the data plane state.
4. The DBNG-UP sends a Session Establishment Response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscriber's IP data packets.
5. The DHCPv6 Advertisement from the DBNG-CP is sent back to the RG through the DBNG-UP utilizing the CPR Interface.
6. **The DHCPv6 Request is sent from the RG through the DBNG-UP utilizing a dedicated session control packet redirect tunnel. As noted, if a session has not yet been established, the session must be established at this step.

7. The DHCPv6 process completes by sending the DHCPv6 reply. The DBNG-CP sends the DHCPv6 Reply through the dedicated session control packet redirect tunnel back to the RG though the DBNG-UP.
8. DBNG-CP informs the RG the default gateway Link Local Address (LLA).

*Note: At this step, it is possible to create a session from the redirected control packet. By doing so, resources are consumed on the DBNG-UP in order to allow individual subscriber control packet management such as blocking, rate limiting, and specific packet filtering. It is also possible to postpone the session creation. By doing so, additional resources DBNG-UP are not consumed, but individual subscriber control packet management is not possible.

**Note: Subscriber session creation can be performed at any steps prior. This step is the last chance for a session creation in order to avoid subscriber data packets drops. Right after this step, the RG is assigned an address and data packets could be sent immediately.

4.4.5 IPoE SLAAC

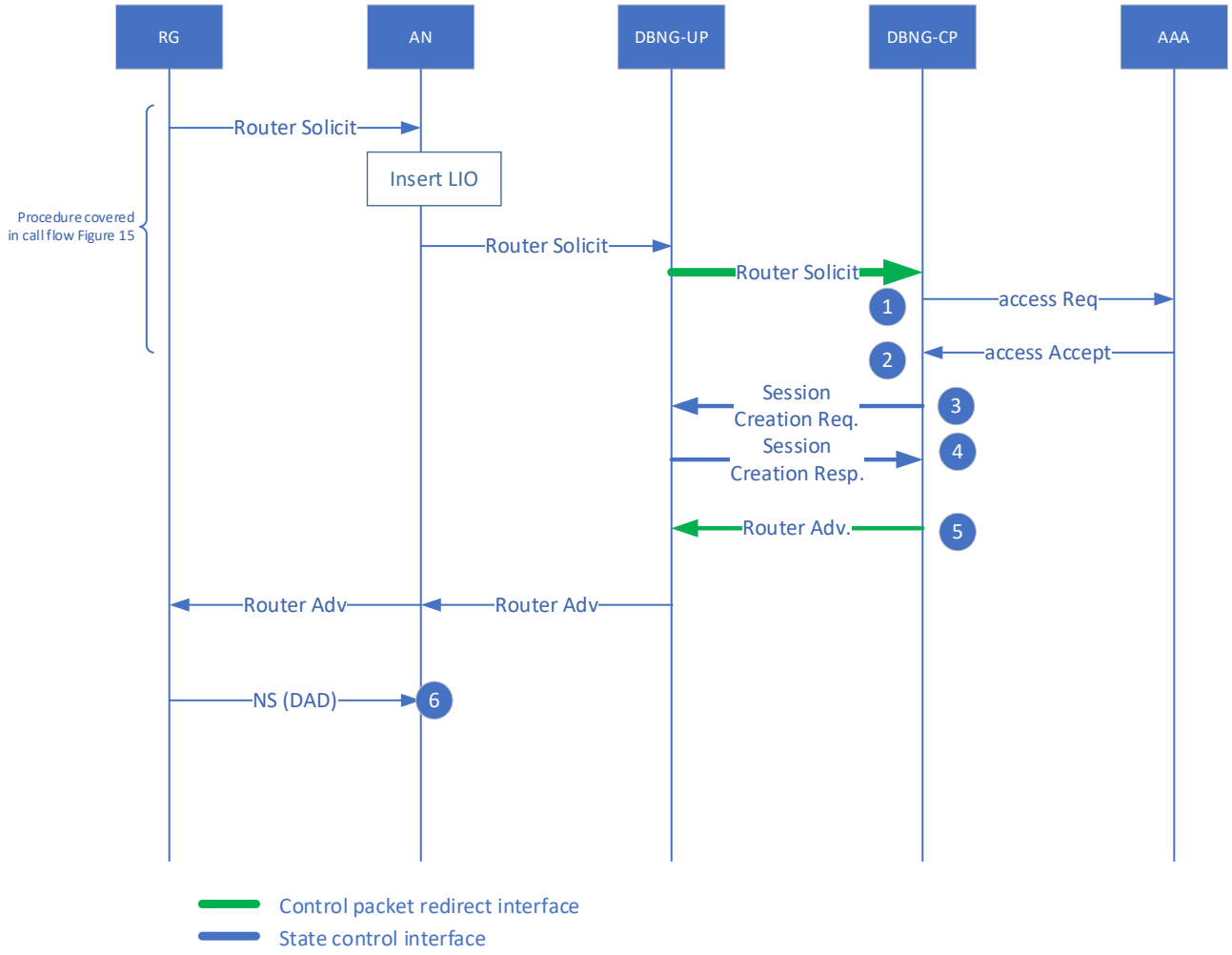

Figure 18: IPoE SLAAC call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1. The DBNG-CP triggers an Access-Request to authenticate the RG.
2. The AAA successfully authenticates the RG and replies to the DBNG-CP with an Access-Accept.
3. The DBNG-CP assigns the IP prefix to the RG which is obtained through either the local address server or returned by AAA as one of the attributes. The DBNG-CP sends a Session Establishment Request to create new packet forwarding states for the data packet. This updates the data plane state.
4. The DBNG-UP sends a Session Establishment Response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscriber's IP data packets.
5. The SLAAC process completes by sending the Router Advertisement back to the RG. The DBNG-CP forwards the RA through the dedicated session control packet redirect tunnel back to the RG though the DBNG-UP.
6. RG sends Neighbor Solicit for Duplicate Address Detection (DAD)

4.4.6 IPoE Data Trigger

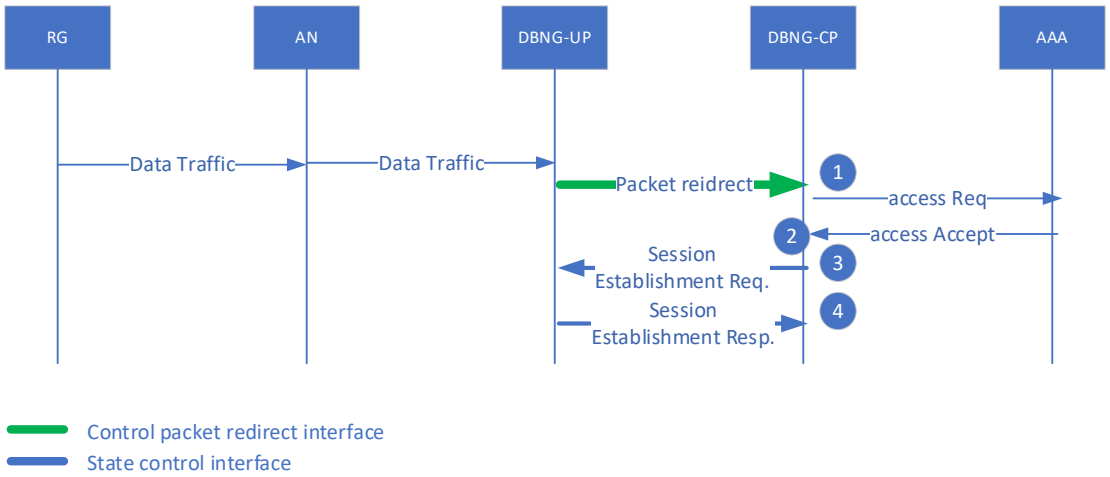

Figure 19: IPoE Data Trigger call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1. A data packet is received from the RG is redirected to the DBNG-CP from the DBNG-UP for authentication.
2. The AAA successfully authenticates the RG based on parameters including IP and MAC, then replies to the DBNG-CP with an Access-Accept.
3. At this point the DBNG-CP can send a session creation request to create new packet forwarding states for the data packet. This updates the data plane forwarding state.
4. The DBNG-UP sends a response back to the DBNG-CP, informing that the forwarding states are installed, and the DBNG-UP is ready to forward the subscriber's IP data packets.

4.4.7 IPoE Dual Stack

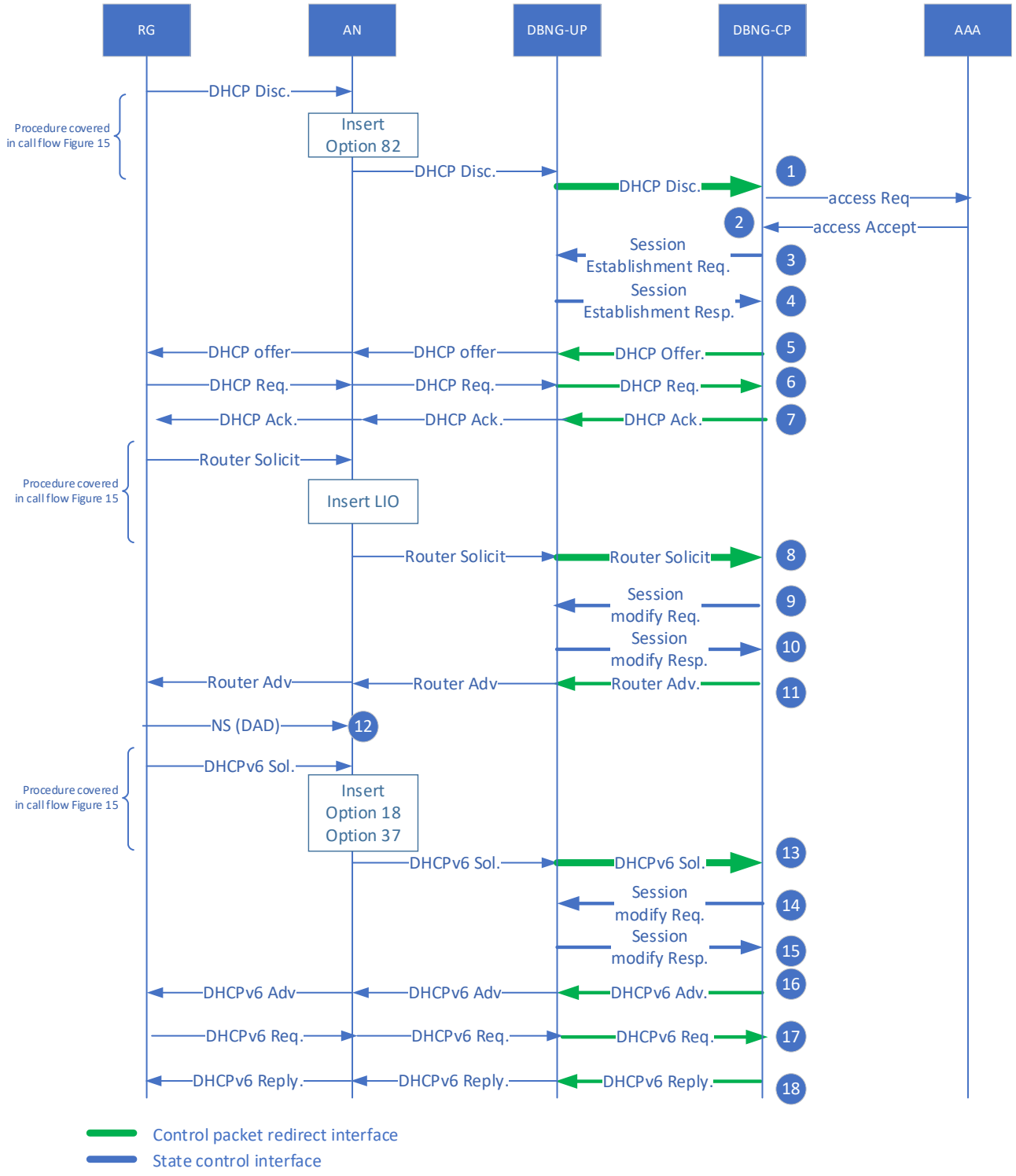

Figure 20: IPoE Dual Stack call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1-7. Follows the same procedure as section 4.4.3 step 1-7.

IPv6 SLAAC configuration:

8. RG initiates a Router Solicit which is redirected through the CPR interface from the DBNG-UP to the DBNG-CP.

9-12: Follows the same procedure as section 4.4.5 step 3-6. However, instead of a Session Create request and respond between the DBNG-CP and DBNG-UP, it is a session modification request and respond.

DHCPv6 negotiation for user's address (PD) configuration;

13. RG initiates a DHCPv6 solicit which is redirected through the CPR interface from the DBNG-UP to the DBNG-CP.

14-18: Follows the same procedure as section 4.4.4 step 3-7. However, instead of a Session Create request and response between the DBNG-CP and DBNG-UP, it is a session modification request and response.

Note: The dual-stack access processes could be concurrent, one before another, or one after another.

4.4.8 IPoE SLAAC and DHCPv6 PD

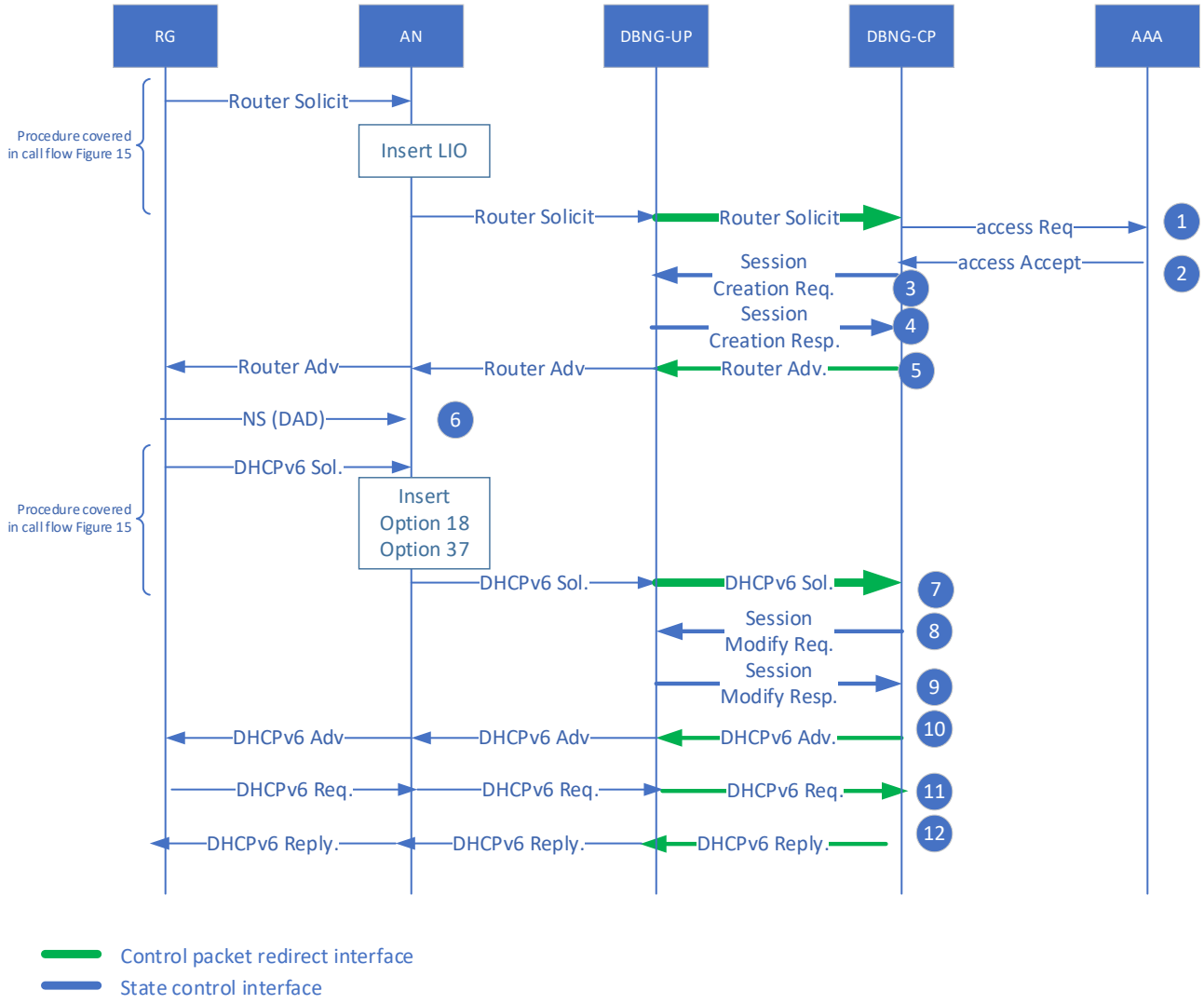

Figure 21: IPoE SLAAC and DHCPv6 PD call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1-6: Follows the same procedure as section 4.4.5 step 1-6.

7. DHCPv6 solicit is initiated from RG, and is sent through AN, DBNG-UP redirects it to DBNG-CP where it responds with DHCPv6 Advertise from the DBNG-CP or DHCPv6 server as a neighboring system;

8-12 Follows the same procedure as section 4.4.4 step 3-7.

4.4.9 PPPoE

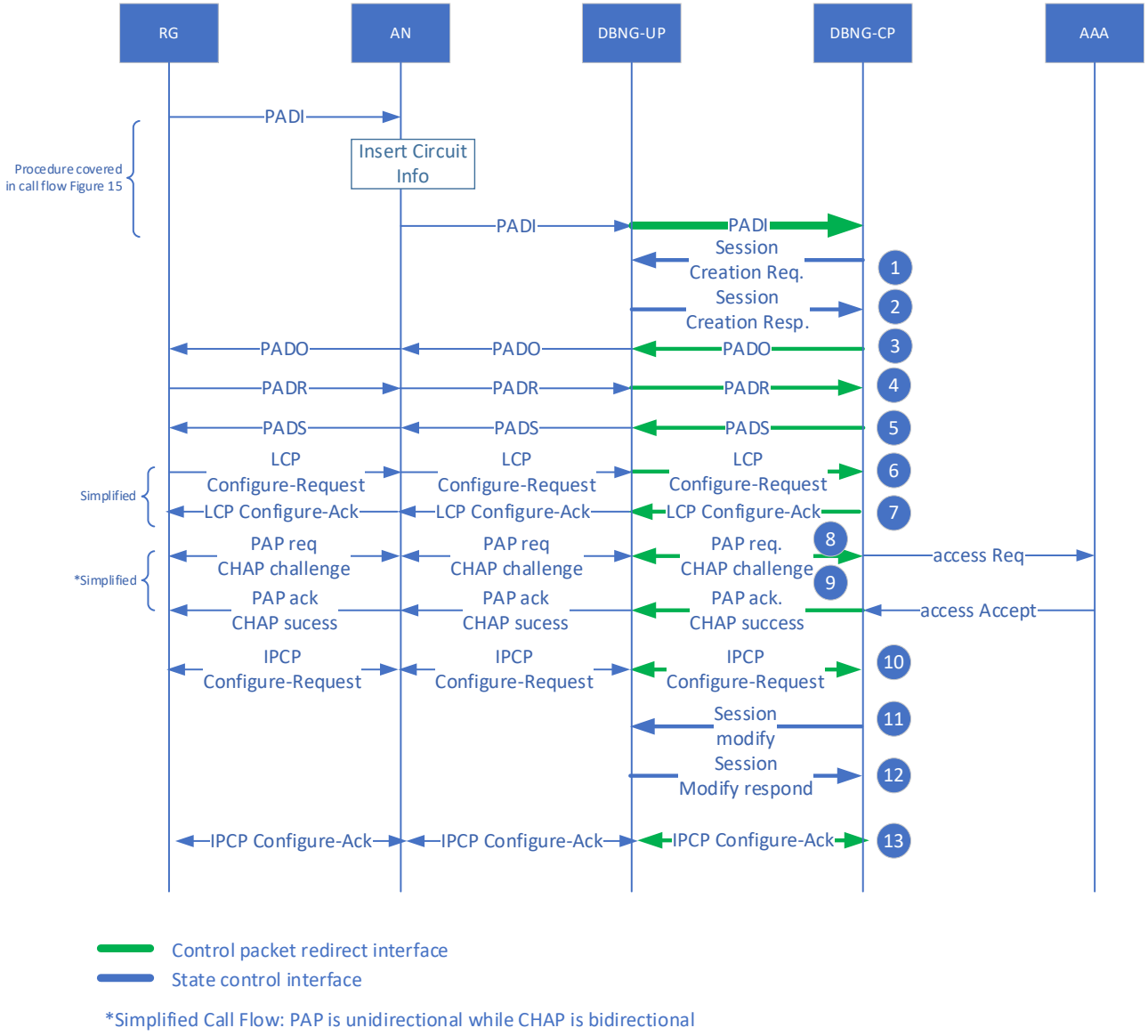

Figure 22: PPPoE call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1. *Upon receiving the first control packet, the DBNG-CP can at this point send a session creation request to create new packet forwarding states for the data packet. This updates the data plane state.
2. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscriber's PPP control packets.
3. The DBNG-CP sends the PADO back to the RG through the DBNG-UP utilizing the CPR interface.
4. The PADR is sent from the RG through the DBNG-UP utilizing the CPR interface.
5. The DBNG-CP sends the PADS back to the RG through the DBNG-UP utilizing the CPR interface.
6. The LCP Configure-Request is sent from the RG through the DBNG-UP utilizing the CPR interface.
7. The DBNG-CP sends the LCP Configure-Ack back to the RG through the DBNG-UP utilizing the CPR interface. The LCP Configure-Ack indicates either a PAP or CHAP authentication challenge.
8. Options:

- Option 1: If the client chooses PAP, the RG sends a PAP request to the DBNG-CP through the DBNG-UP utilizing the CPR Interface. The credentials are sent in the Access-Request to the AAA server.
- Option 2: If CHAP is required, the DBNG-CP initiates a challenge to the RG though the DBNG-UP utilizing the CPR Interface . The RG responds back to the challenge to the DBNG-CP. The challenge response is sent to the AAA server.

9. The AAA successfully authenticates the RG and replies to the RG with PAP/CHAP success.
10. Both DBNG-CP and RG send IPCP Configure-Request for parameter negotiation, utilizing a dedicated session control packet redirect tunnel. The RG is assigned an IPv4 address. Address could be assigned to the RG either through the AAA reply or through a local address server. As noted, if a session has not yet been established, the session must be established at this step.
11. **Once the RG is assigned IP address, the DBNG-CP sends a session modification request (if the session has already been established) or session request (if a session has yet to be established) to create new packet forwarding states for the data packet. The data plane is updated.
12. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscribers IP data packets.
13. The IPCP Configure-Ack is sent from the DBNG-CP to the RG through the DBNG-UP utilizing a dedicated session control packet redirect tunnel.

*Note: At this step, it is possible to create a session from the redirected control packet. By doing so, resources are consumed on the DBNG-UP in order to allow individual subscriber control packet management such as blocking, rate limiting, and specific packet filtering. It is also possible to postpone the session creation. By doing so, additional resources DBNG-UP are not consumed, but individual subscriber control packet management is not possible

**Note: Subscriber session creation can be performed at any steps prior. This step is the last chance for a session creation in order to avoid subscriber data packets drops. Right after this step, the RG is assigned an address and data packets could be sent immediately

4.4.10 PPPoEv6

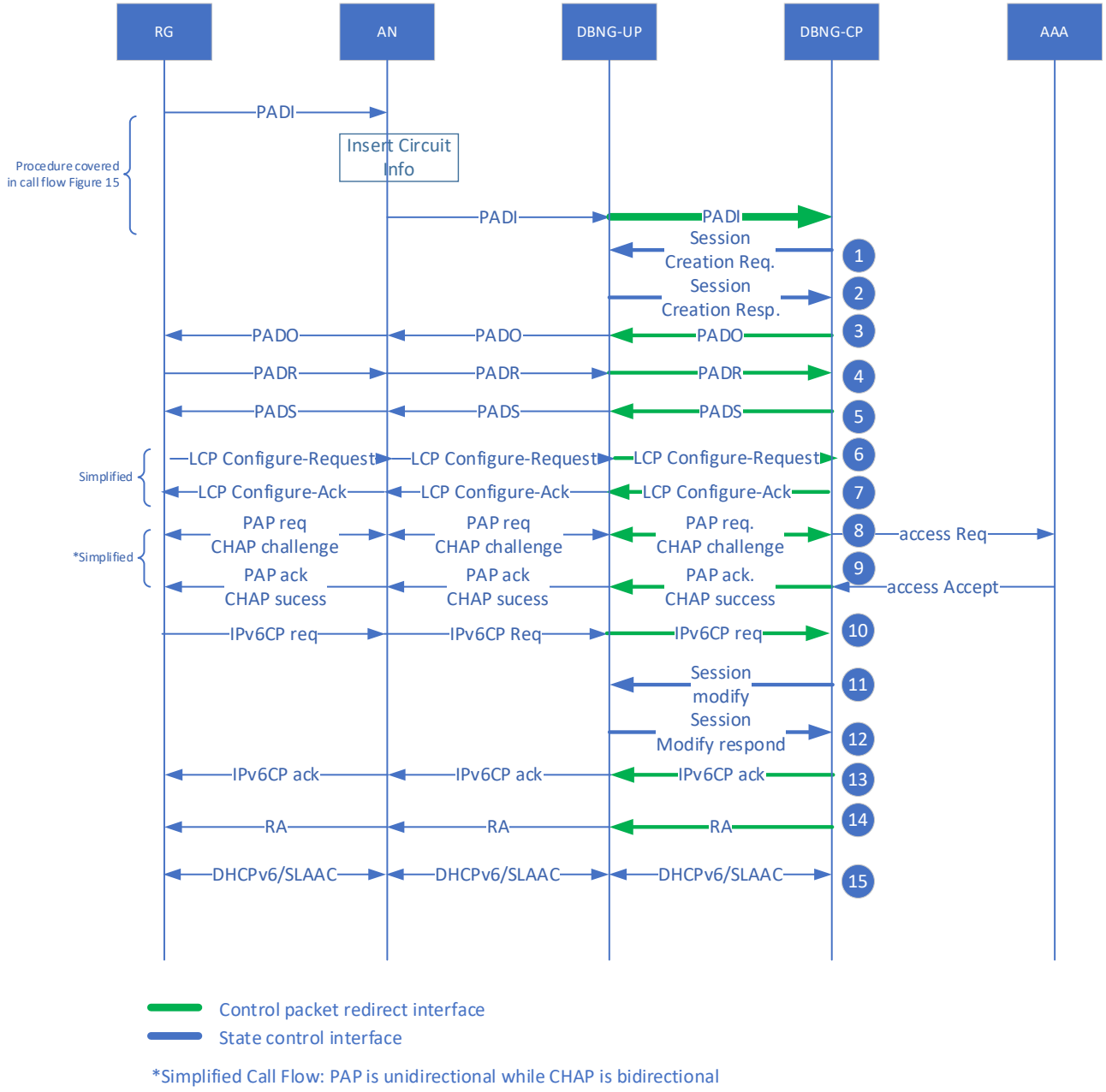

Figure 23: PPPoEv6 call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1. *Upon receiving the first control packet, the DBNG-CP at this point can send a session creation request to create new packet forwarding states for the data packet. This updates the data plane state.
2. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscriber's PPP control packets.
3. After the Session creation request and response, the DBNG-CP sends the PADO back to the RG through the DBNG-UP utilizing the CPR interface.
4. The PADR is sent from the RG through the DBNG-UP utilizing the CPR interface.
5. The DBNG-CP sends the PADS back to the RG through the DBNG-UP utilizing the CPR interface.

6. The LCP Configure-Request is sent from the RG through the DBNG-UP utilizing the CPR interface.
7. The DBNG-CP sends the LCP Configure-Ack back to the RG through the DBNG-UP utilizing the CPR interface. The LCP Configure-Ack indicates either a PAP or CHAP authentication challenge.
8. Options:
    - Option 1: If the client chooses PAP, the RG sends a PAP request to the DBNG-CP through the DBNG-UP utilizing the CPR Interface. The credentials are sent in an Access-Request to the AAA server.
    - Option 2: If CHAP is required, the DBNG-CP initiates a challenge to the RG though the DBNG-UP utilizing the CPR Interface. The RG responds back to the challenge to the DBNG-CP. The challenge response is sent to the AAA server.
9. The AAA successfully authenticates the RG and replies to the RG with PAP/CHAP success.
10. The IPv6CP Configure-Request is sent from the RG through the DBNG-UP utilizing the CPR interface.
11. At this point, the DBNG-CP had obtained the IPv6 addresses and prefixes for the RG either from the local address server or from AAA returned VSAs. The DBNG-CP sends a session modification request to create new packet forwarding states for both control and data packet. The data plane state is updated.
    - Traffic management rules for control packets: redirect DHCPv6 and SLAAC request to the DBNG-CP
    - Traffic management rule for data packets: match data packet and perform forwarding action.
12. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed and the DBNG-UP is ready to forward the subscriber's IP data packets.
13. The DBNG-CP sends the IPv6CP Configure-Ack to the RG through the DBNG-UP utilizing the CPR interface.
14. **As noted, if a session has not yet been established, the session must be established at this step. The DBNG-CP sends an RA to the RG informing the LLA which is described in detail in section 4.4.5.
15. The DBNG-CP responds to the RG DHCPv6. For the subsequent DHCPv6 call flow please refer to section 4.4.4

*Note: At this step, it is possible to create a session from the redirected control packet. By doing so, resources are consumed on the DBNG-UP in order to allow individual subscriber control packet management such as blocking, rate limiting, and specific packet filtering. It is also possible to postpone the session creation. By doing so, additional resources DBNG-UP are not consumed, but individual subscriber control packet management is not possible

**Note: Subscriber session creation can be performed at any steps prior. This step is the last chance for a session creation in order to avoid subscriber data packets drops. Right after this step, the RG is assigned an address and data packets could be sent immediately

4.4.11 PPPoE Dual Stack

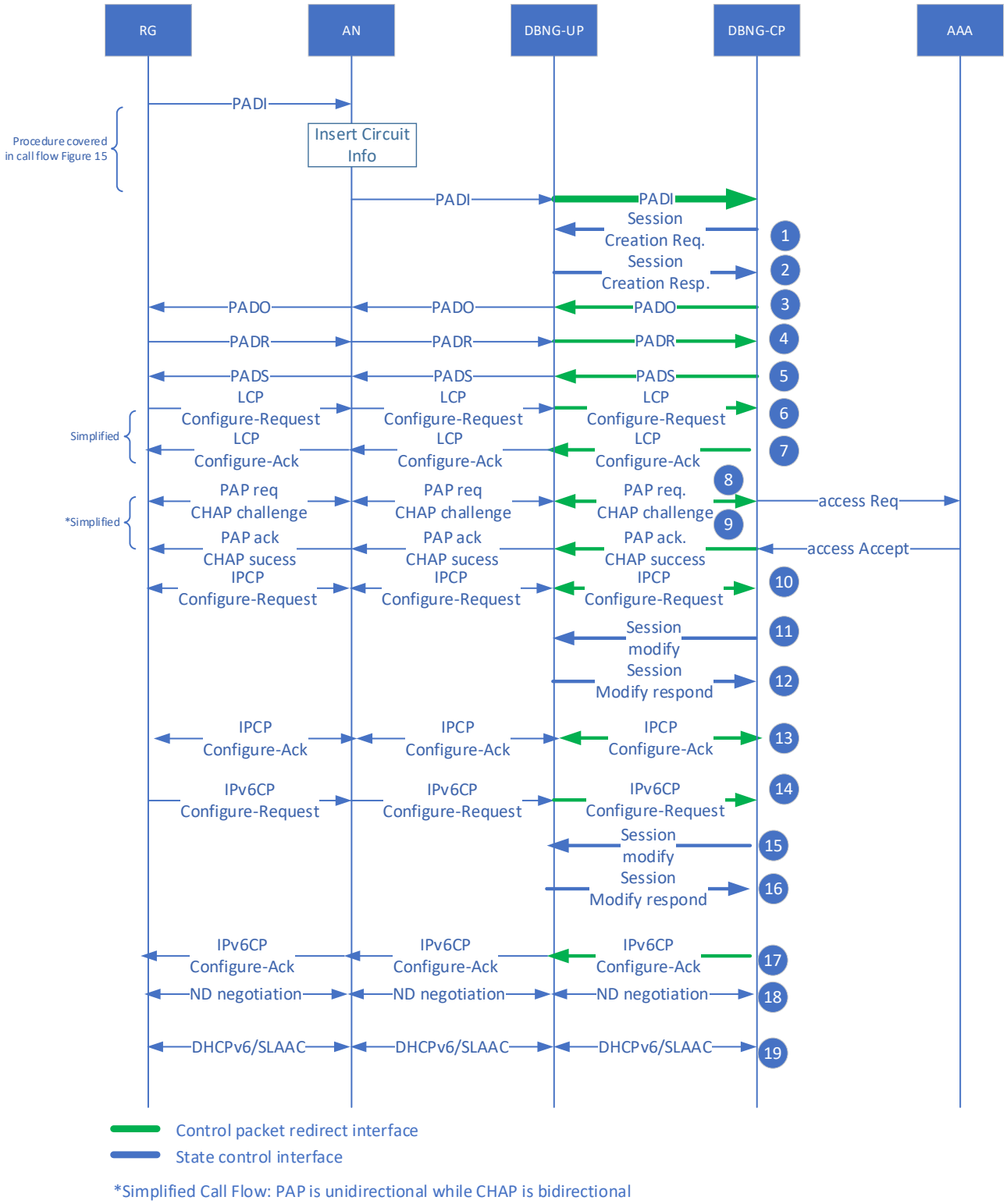

Figure 24: PPPoE Dual Stack call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1-13. Follows the same procedure as section 4.4.9 step 1-13

14-19. Follows the same procedure as section 4.4.10 step 10-15

Note: The dual-stack access processes could be concurrent, one before the other, or one after the other.

4.4.12 LAC

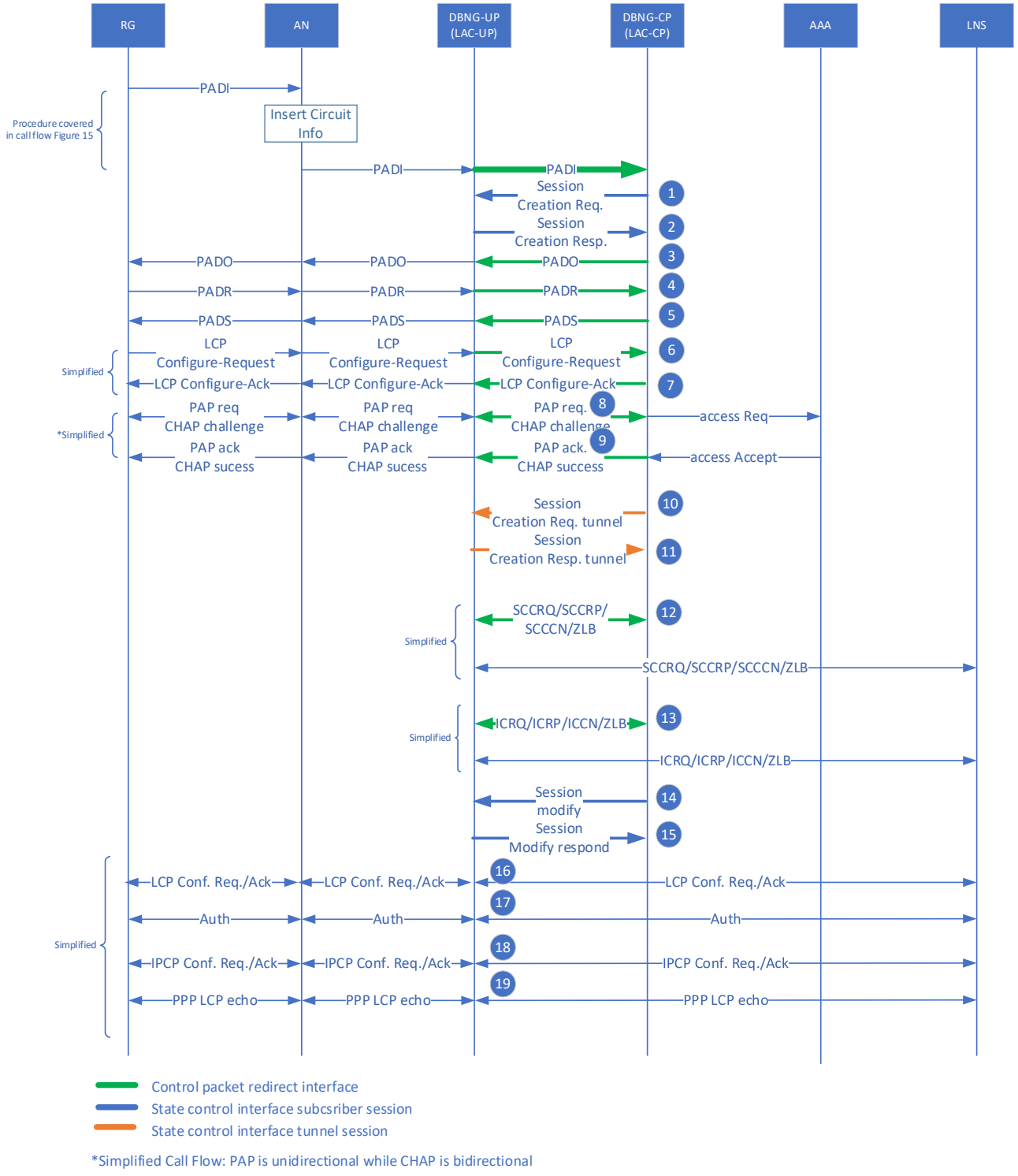

Figure 25: LAC call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1. *Upon receiving the first control packet, the DBNG-CP can at this point send a session creation request to create new packet forwarding states for the data packet. This updates the data plane state.
2. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscriber's PPP control packets.
3. The DBNG-CP sends the PADO back to the RG through the DBNG-UP utilizing the CPR interface.
4. The PADR is sent from the RG through the DBNG-UP utilizing the CPR interface.
5. The DBNG-CP sends the PADS back to the RG through the DBNG-UP utilizing the CPR interface.
6. The LCP Configure-Request is sent from the RG through the DBNG-UP utilizing the CPR interface.
7. The DBNG-CP sends the LCP Configure-Ack back to the RG through the DBNG-UP utilizing the CPR interface. The LCP Configure-Ack indicates either a PAP or CHAP authentication challenge.
8. Options:
    - Option 1: If the client chooses PAP, the RG sends a PAP request to the DBNG-CP through the DBNG-UP utilizing the CPR Interface. The credentials are sent in an Access-Request to the AAA server.
    - Option 2: If CHAP is required, the DBNG-CP initiates a challenge to the RG though the DBNG-UP utilizing the CPR Interface. The RG responds back to the challenge to the DBNG-CP. The challenge response is sent to the AAA server.
9. The AAA successfully authenticates the RG and replies to the RG with PAP/CHAP success and that this is a L2TP session
10. DBNG-CP sends a new session establishment message to the DBNG-UP. The DBNG-CP programs the DBNG-UP control packet redirect rules to 1) encapsulate and send the L2TP control message towards the LNS. 2) redirect L2TP control message back to the DBNG-CP. This session is only established on a per-tunnel basis.
11. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the L2TP control packets.
12. The DBNG-CP exchanges Start-Control-Connection-Request (SCCRQ), Start-Control-Connection-Reply (SCCRP), Start-Control-Connection-Connected (SCCCN), and Zero-Length Body (ZLB) to the LNS via the DBNG-UP through the CPR interface
13. The DBNG-CP sends Incoming-Call-Request (ICRQ), Incoming-Call-Reply (ICRP), Incoming-Call-Connected (ICCN), and ZLB to the LNS via the DBNG-UP through the CPR interface
14. **If there is a previous session established, the DBNG-CP sends a session modify request to allow data packet forwarding to the LNS (and control packet). If there are no previous session established, this require a session establishment request message to allow for data packet forwarding to the LNS. This updates the data plane state.
15. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward subscriber's PPP control and data packets.
16. If the LNS cached the LCP Configure-Request and there is no negotiation disagreement, this step can be skipped. If LNS has not cached LCP Configure-Request or the session requires renegotiation, then LCP negotiation takes place.
17. If the LNS had cached authentication information and there is no disagreement on authentication, this step can be skipped. If LCP had not cached authentication information or authentication failed, then a session re-authentication is required.
18. IPCP takes place between the RG and the LNS through the DBNG-UP
19. PPP LCP echo requests/replies are exchanged between the RG and the LNS through the DBNG-UP

*Note: At this step, it is possible to create a session from the redirected control packet. By doing so, resources are consumed on the DBNG-UP in order to allow individual subscriber control packet management such as blocking, rate limiting, and specific packet filtering. It is also possible to postpone the session creation. By doing so, additional resources DBNG-UP are not consumed, but individual subscriber control packet management is not possible

**Note: Subscriber session creation can be performed at any steps prior. This step is the last chance for a session creation in order to avoid subscriber data packets drops. Right after this step, the RG is assigned an address and data packets could be sent immediately

4.4.13 LNS – PPPoEv4

The LAC DBNG-CP and DBNG-UP split is not relevant in the LNS call flow

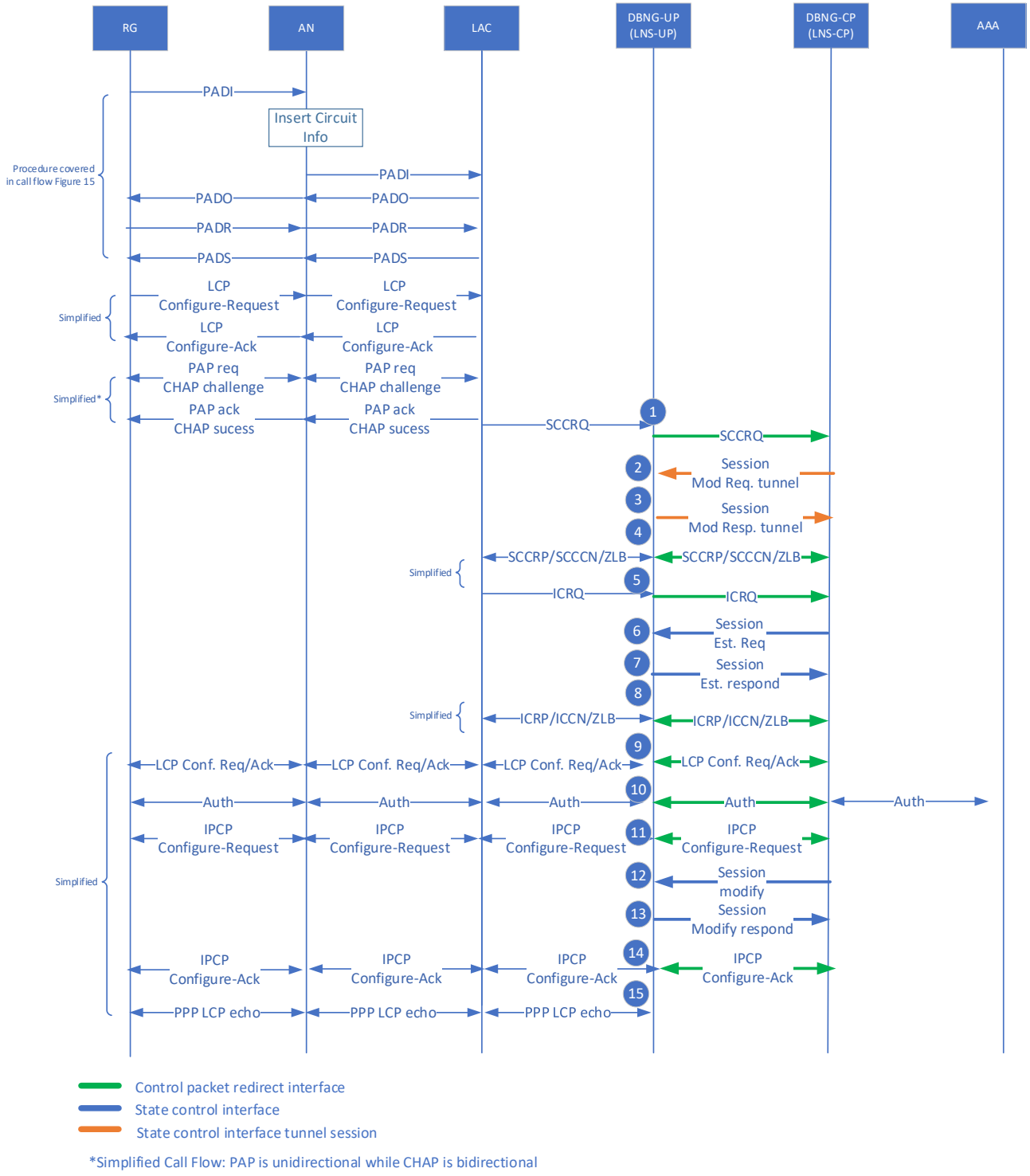

Figure 26: LNS PPPoEv4 call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1. The SCCRQ message is received through the CPR interface following the common packet redirect rule.
2. DBNG-CP sends a session establishment request message to the DBNG-UP. The DBNG-CP programs the DBNG-UP control packet redirect rules to send L2TP control message towards the DBNG-CP to only accept particular tunnels.
3. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the L2TP control packets.
4. The DBNG-CP exchanges SCCRP, SCCCN, and ZLB with the LAC by utilizing the CPR interface
5. The DBNG-CP receives the ICRQ message (including the AVP defined in RFC 5515 [36])
6. *Upon receiving the ICRQ message, the DBNG-CP has the L2TP session ID information. The DBNG-CP can send a session establishment request to the DBNG-UP to ensure only known L2TP session are accepted.
7. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP only accepts L2TP control packet from known sessions.
8. The DBNG-CP exchanges ICRP, ICCN, and ZLB with the LAC by utilizing the CPR interface
9. If the LNS had cached LCP Configure-Request and there is no negotiation disagreement, this step can be skipped. If LCP had not cached LCP Configure-Request or the session requires renegotiation, then LCP negotiation takes place.
10. If the LNS had cached authentication information and there is no disagreement on authentication, this step can be skipped. If LCP had not cached authentication information or authentication failed, then a session renegotiation takes place.
11. Both DBNG and RG sends IPCP Configure-Request for parameter negotiation, utilizing a dedicated session control packet redirect tunnel. The RG is assigned an IPv4 address. Address could be assigned to the RG either through the AAA reply or through a local address server. As noted, if a session has not yet been established, the session must be established at this step.
12. **The DBNG-CP sends a session modify request if there is already an established session to update the data plane state. If there are no prior established sessions, this requires a session establishment request to update the data plane.
13. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward subscriber's PPP control and data packets.
14. The IPCP Configure-Ack is sent from the DBNG-CP to the RG through the DBNG-UP utilizing a dedicated session control packet redirect tunnel.
15. PPP LCP echo requests/replies are exchanged between the RG and the LNS through the DBNG-UP

*Note: At this step, it is possible to create a session from the redirected control packet. By doing so, resources are consumed on the DBNG-UP in order to allow individual subscriber control packet management such as blocking, rate limiting, and specific packet filtering. It is also possible to postpone the session creation. By doing so, additional resources DBNG-UP are not consumed, but individual subscriber control packet management is not possible

**Note: Subscriber session creation can be performed at any steps prior. This step is the last chance for a session creation in order to avoid subscriber data packets drops. Right after this step, the RG is assigned an address and data packets could be sent immediately.

4.4.14 LNS - Dual Stack

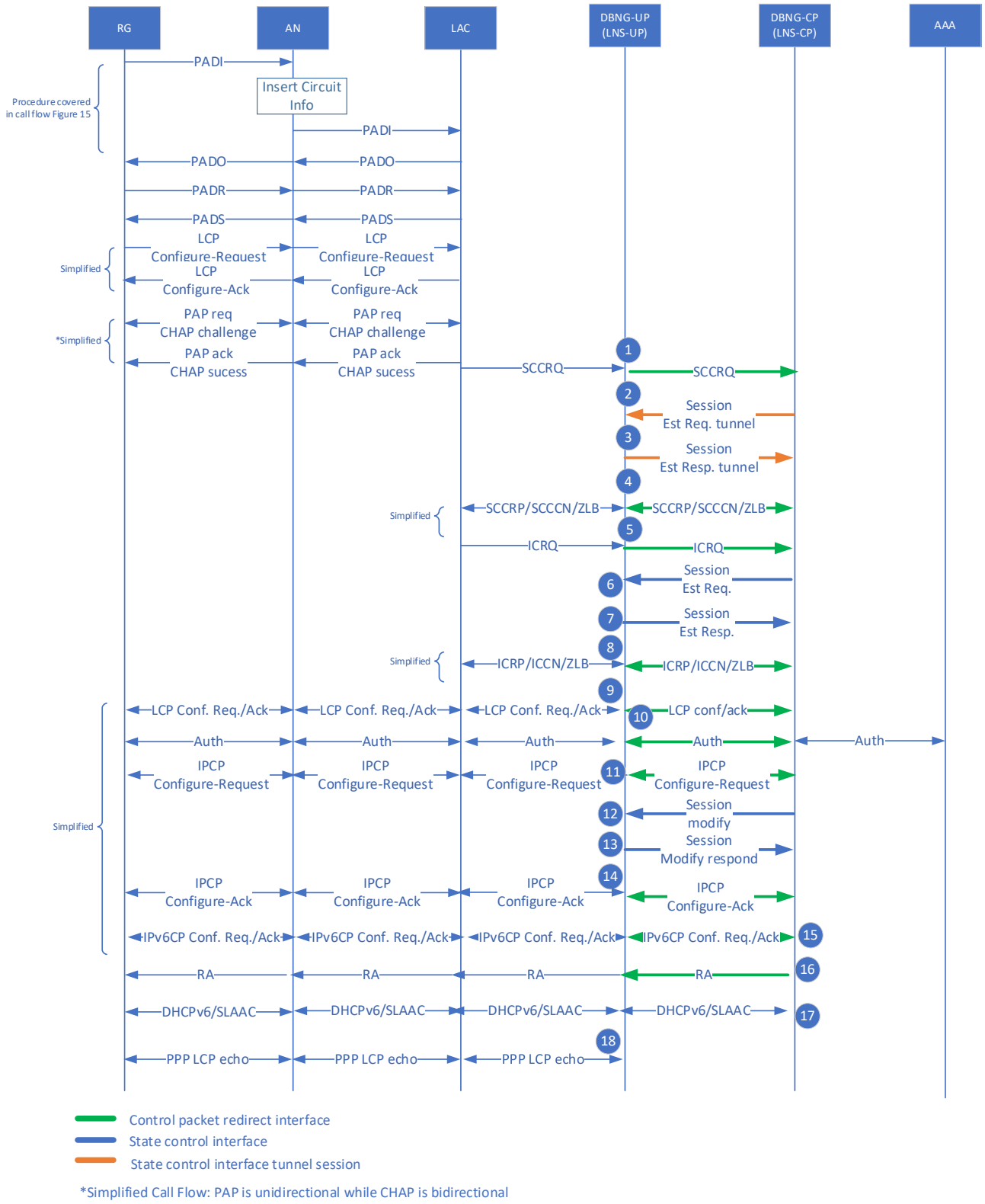

Figure 27: LNS Dual Stack call flow

Procedure 1 to 14 would follow the same LNS procedure outlined in section 4.4.13.

15. The IPv6CP Configure-Request is sent from the RG through the DBNG-UP utilizing the CPR interface. The DBNG-CP sends the IPv6CP Configure-Ack to the RG through the DBNG-UP utilizing the CPR interface.
16. As noted, if a session has not yet been established, the session must be established at this step. The DBNG-CP sends an RA to the RG informing the LLA, for more detail please refer to section 4.4.5.
17. The DBNG-CP responds to the RG DHCPv6. For the subsequent DHCPv6 call flow please refer section 4.4.4.
18. PPP LCP echo requests/replies are exchanged between the RG and the LNS through the DBNG-UP.

4.4.15 Public Wi-Fi Access

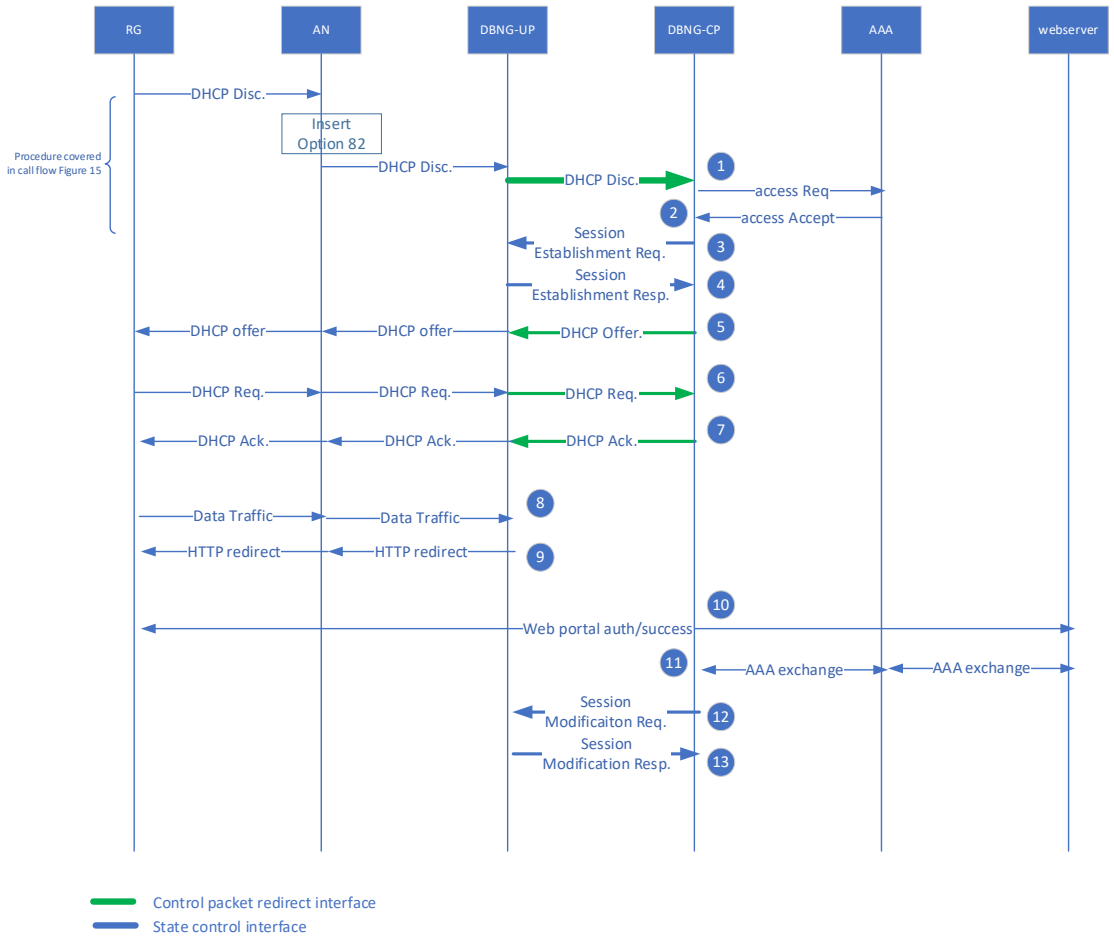

Figure 28: Public Wi-Fi Access call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

1-7: Follows the same procedure as section 4.4.3 step 1-7.

8. As user traffic arrives at the DBNG-UP, the packet is redirected for web authentication.
9. The DBNG must inform RG of HTTP redirection, this can be done by the DBNG-UP or the DBNG-CP. RG then sends the traffic directly to the designated web server for authentication.
10. Subscriber successfully authenticates.
11. AAA updates DBNG-CP to allow subscriber internet access and removes the http redirection rule for the subscriber.
12. If subscriber session has not been established yet, this is the last chance to setup the subscriber session. If a subscriber session has already been established, the session is modified. The DBNG-CP allows the subscriber internet access and removes the HTTP rule from the DBNG-UP.
13. DBNG-UP sends a session modification response to the DBNG-CP.

4.4.16 Public Wi-Fi Layer 3 Access

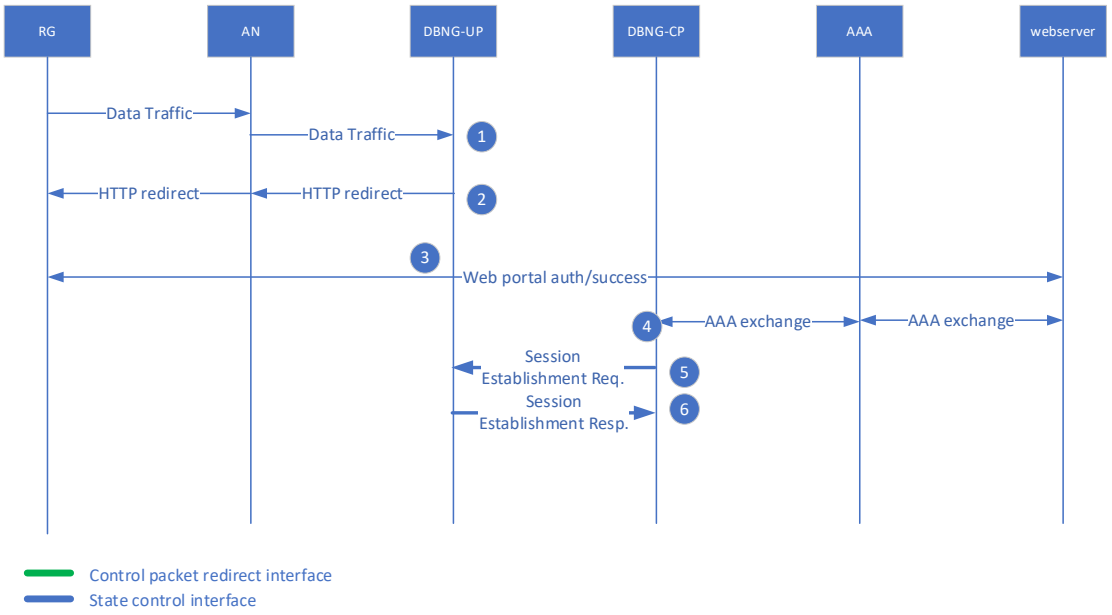

Figure 29: Public Wi-Fi Layer 3 Access call flow

Prior to step 1, call flow in section 4.4.2 covers the generic common control packet redirection rule.

Step 1-6: Follows the same procedure as section 4.4.15 step 8-13.

4.4.17 TWAG Call Flows

The call flow for TWAG follows TR-291 [12] section 11.1 for S2a, where the TWAG and TWAP are integrated into the DBNG, the BBF access is considered as Trusted by the 3GPP network and single-connection mode with Enhanced Packet Core (EPC) access is provided to the UE. The DBNG terminates an S2a interface with the 3GPP PGW;

In this call flow, the TWAG is split up into DBNG-CP and DBNG-UP. Therefore, additional steps are added for DBNG-CP and DBNG-UP communications and packet redirection. Prior to step 1, a common rule would be installed on the DBNG-UP to redirect all control messages (such as DHCP, RS, and DHCPv6) to the DBNG-CP, see section 4.4.2. The procedure related to interaction with an external system stays the same as in TR-291 [12]. This procedure requires the GTP-c and GTP-u to utilize different IP address endpoints.

NOTE: 3GPP S2a signaling already supports that the Fully Qualified Tunnel Endpoint Identifier (F-TEID) for Control Plane can correspond to a different IP address than the S2a-U TWAN F-TEID in a Bearer Context (User Plane).

4.4.17.1 S2a initial attach based on layer 2 trigger: IPv4 based on DHCPv4

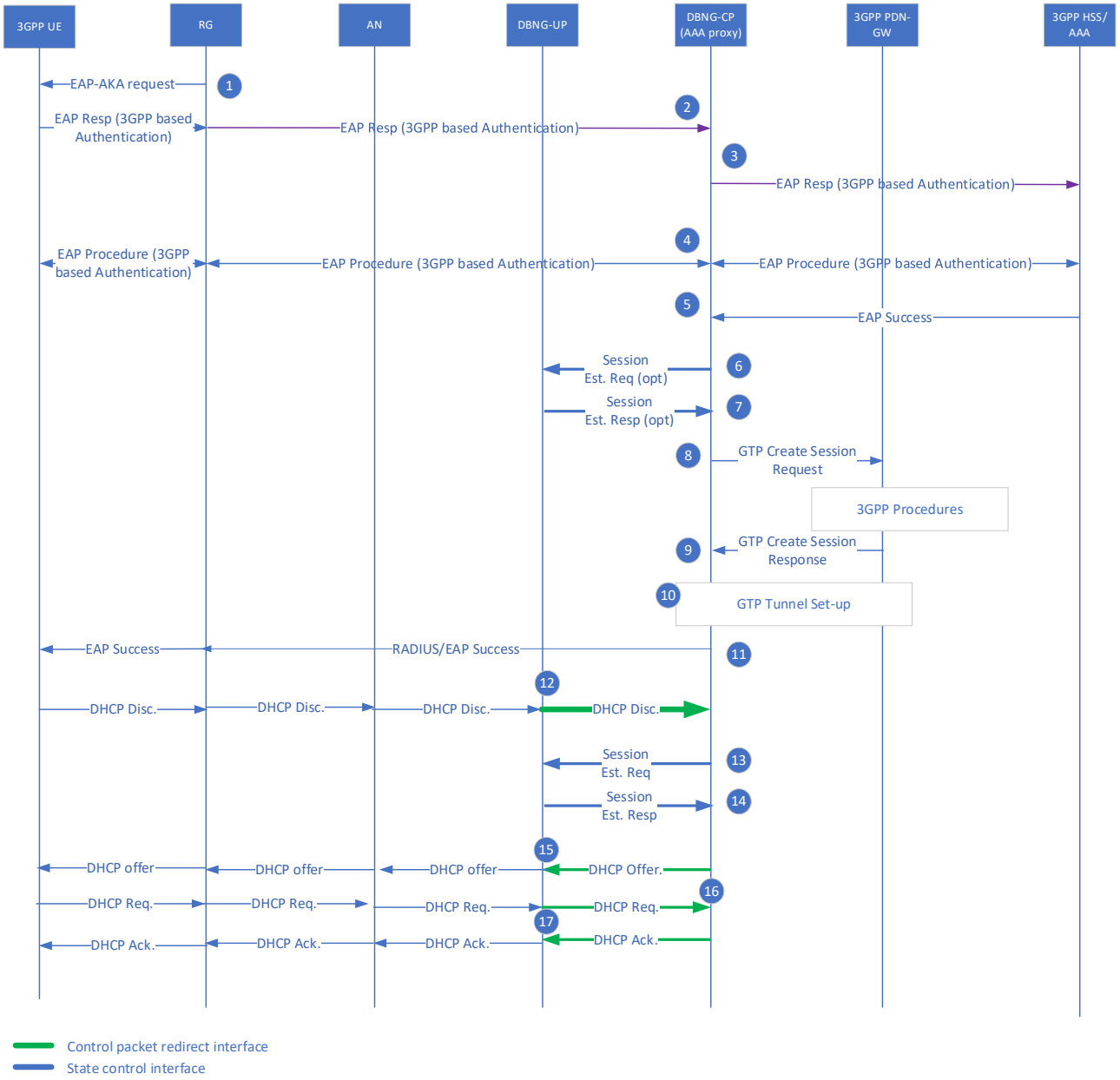

Figure 30: S2a initial attached based on layer 2 trigger: DHCPv4

1. The 3GPP UE attaches to the BBF access network. The RG initiates an EAP request to the 3GPP UE and thus initiates the EAP authentication process (see 3GPP TS 33.402 [25]). During the authentication phase, the RG acts as an 802.1X authenticator, and adds the MAC Address of the 3GPP UE to the RADIUS Request message.
2. The RG forwards the EAP response to the DBNG: the DBNG is invoked as an AAA proxy and DHCP address server for the 3GPP UE.

When the TWAG is deployed in a dedicated router, the DBNG is involved as an AAA proxy and for the 3GPP UE, distinguishing 3GPP UE signaling from fixed device signaling based on Network Access Identifier (NAI).

3. The DBNG-CP forwards the EAP response to the 3GPP AAA. 3GPP procedures between 3GPP AAA server and Home Subscriber Server (HSS) take place as described in TS 23.402 [22] clause 16.2 and 33.402 [25].
4. The DBNG-CP acting as a AAA proxy relays back and forth EAP signaling between the 3GPP AAA server and the RG.
5. Once the 3GPP UE successfully authenticates, the 3GPP AAA server creates an EAP-Success that it embeds into a AAA-Success sent to the DBNG-CP; The 3GPP UE is now authenticated, and the BBF access is considered as trusted by the 3GPP Network.

The rest of the procedure assumes that the DBNG-CP has been instructed by the AAA to provide EPC access (e.g. to establish an S2a GTP tunnel).

6. [Optional]* In the case where the TEID for User plane is assigned by the DBNG-UP, the DBNG-CP initiates a DNBG-UP Control session establishment request to retrieve the TEID for the GTP-u tunnel at DNBG-UP network (PGW) side. (3GPP TS 29.244 [23] section 5.5.3)
7. [Optional]* The DBNG-UP responds with a DNBG-UP Control session establishment response supplying the requested TEID. (3GPP TS 29.244 [23] section 5.5.3)
8. The DBNG-CP sends a GTP-c Create Session Request message to the PDN GW. The DBNG-CP selects the PDN GW and builds the Create Session Request as defined in 3GPP TS 23.402 [22] clause 16.2 8b; 3GPP procedures possibly including a Policy and Charging Rules Function (PCRF) take place. As a result, an IP address is allocated to the UE. It must be noted that the GTP-c and GTP-u for S2a can utilize two different IP endpoints.
9. The PDN GW returns a Create Session Response, including the IP address allocated for the 3GPP UE.
10. Both DBNG-CP and PGW finishes exchanging information to establish the GTP-u tunnel.
11. The DBNG-CP proxies the RADIUS Success (EAP Success) message to the RG through the CPR interface. The RG sends the EAP Success to the 3GPP UE. The 3GPP UE is now authenticated, and the BBF access is considered as trusted by the 3GPP Network.
12. The 3GPP UE sends a DHCP Discovery message and is redirected to the DBNG-CP through the DBNG-UP.
13. The DBNG-CP provides the DBNG-UP with packet forwarding rules based on the DHCP discovery packet (which could include the encapsulation, MAC, and VLANs) and on the GTP-u F-TEID and QoS requirements received from the PDN GW in Create Session Response. These rules include the request to forward DHCP signaling from the UE to the DBNG-CP. They are sent in a session establishment request unless a session establishment request has been used in step 6, in which case a session modification request would be used.
    NOTE: The DBNG-CP is responsible of the charging interface, if any.
14. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscribers IP data packets
15. The DBNG-CP sends a DHCP offer including the IPv4 Address allocated by the PDN GW to the 3GPP UE via the CPR interface.
16. The 3GPP UE sends a DHCP request message and is redirected to the DBNG-CP through the DBNG-UP via the CPR interface.
17. The DBNG-CP sends a DHCP ack through the CPR interface.

Note: The procedure for accounting message exchange used for charging purposes is not included in this flow.

Note*: TEID allocation can be done by the DBNG-CP function (3GPP TS 29.244 [23] section 5.5.2) or optionally by the DBNG-UP function (3GPP TS 29.244 [23] section 5.5.3)

4.4.17.2 S2a initial attach based on layer 2 trigger: IPv6 prefix based on SLAAC

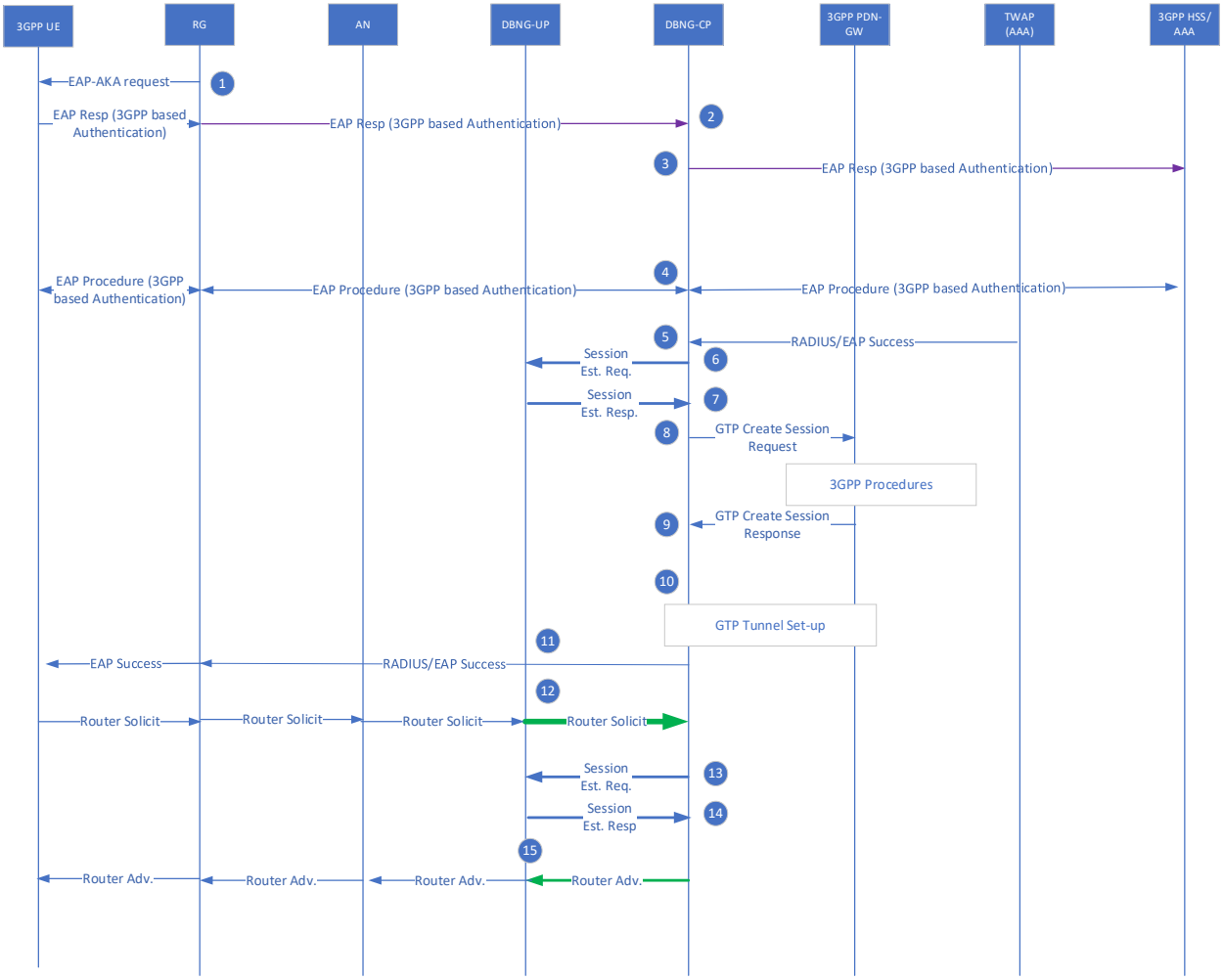

Figure 31: S2a initial attached based on layer 2 trigger: SLAAC

Procedure 1 to 11 would follow the same DHCPv4 procedure outlined in section 4.4.17.1

12. The 3GPP UE sends a router solicit message and is redirected to the DBNG-CP through the DBNG-UP.
13. The DBNG-CP provides the DBNG-UP with packet forwarding rules based on the router solicit packet (which could include the encapsulation, MAC, and VLANs) and on the GTP-u F-TEID and QoS requirements received from the PDN GW in Create Session Response. These rules include the request to forward router solicits from the UE to the DBNG-CP. They are sent in a session establishment request unless a session establishment request has been used in step 6, in which case a session modification request would be used.
    NOTE: The DBNG-CP is responsible of the charging interface, if any.
14. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscribers IP data packets
15. The DBNG-CP sends a router advertisement including the IPv6 prefix allocated by the PDN GW to the 3GPP UE via the CPR interface.

Note: The procedure for accounting message exchange used for charging purposes is not included in this flow.

4.4.17.3 S2a initial attach based on layer 3 trigger: IPv4 based on DHCPv4

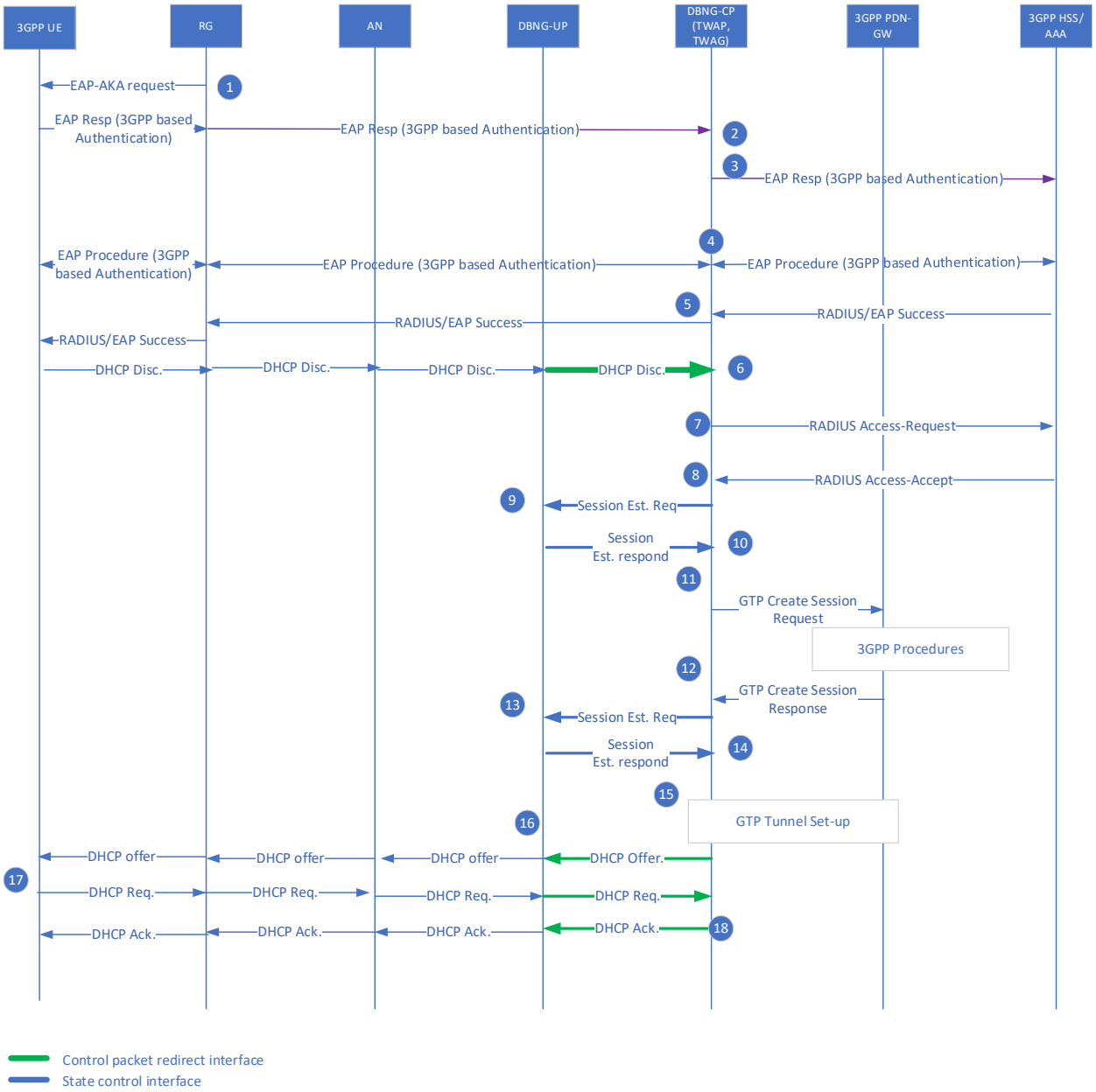

Figure 32: S2a initial attached based on layer 3 trigger: DHCPv4

1. The 3GPP UE attaches to the BBF access network. The RG initiates an EAP request to the 3GPP UE and thus initiates the EAP authentication process (see 3GPP TS 33.402 [25]). During the authentication phase, the RG acts as an 802.1X authenticator, and adds the MAC Address of the 3GPP UE to the RADIUS Request message. The DBNG is invoked as an AAA proxy and address server for the 3GPP UE.
2. When the DBNG is deployed as a dedicated router, the DBNG acts as an AAA proxy and for the 3GPP UE, distinguishing 3GPP UE signaling from fixed device signaling based on NAI. During the

authentication phase, the RG acts as an 802.1X authenticator, and adds the MAC Address of the 3GPP UE to the RADIUS message sent to the TWAG.

3. The DBNG-CP forwards the EAP response to the 3GPP AAA. 3GPP procedures between 3GPP AAA server and HSS take place as described in 3GPP TS 23.402 [22] clause 16.2 and 33.402 [25].
4. The DBNG-CP acting as a TWAP relays back and forth EAP signaling between the 3GPP AAA server and the RG.
5. Once successfully authenticated, the 3GPP AAA server creates an EAP-Success that it embeds into a AAA-Success sent to the DBNG-CP; The 3GPP UE is now authenticated, and the BBF access is considered as trusted by the 3GPP Network.
6. The 3GPP UE sends a DHCP Discover message including the MAC Address. The RG Relays the DHCP Discover message to the DBNG-CP through the DBNG-UP.
7. The DBNG-CP sends a RADIUS Access-Request to the AAA, including the MAC Address. The TWAG makes use of the MAC Address, which is stored during the authentication phase of the 3GPP UE, for correlating the information obtained from the 3GPP Domain during the authentication phase (Step 2) with the IP session.
8. The AAA responds with a RADIUS Access-Accept to the DBNG-CP, including an indication of the need to establish an S2a connection between the DBNG-UP and the 3GPP PDN GW. TWAP also provides information retrieved from the 3GPP Domain at Step 1, such as the APN, the selected PLMN Id and the 3GPP IMSI.

Note: Steps 7 and 8 may be avoided if the DBNG is a RADIUS proxy during the 3GPP UE authentication performed during Step 2.

9. [Optional]* In the case where the TEID for User plane is assigned by the DBNG-UP, the DBNG-CP must initiate a session establishment request to retrieve the TEID for the GTP-u tunnel at its network side.
10. [Optional]* The DBNG-UP responds with a session establishment response supplying the TEID for the PGW GTP-u tunnel to use.
11. If the DBNG-CP is instructed by the AAA to establish an S2a GTP tunnel, the DBNG-CP sends a Create Session Request message to the PDN GW. The DBNG-CP selects the PDN GW and builds the Create Session Request as defined in 3GPP TS 23.402 [22] clause 16.2 8b; 3GPP procedures possibly including a PCRF take place. As a result, an IP address is allocated to the UE. It must be noted that the GTP-c for S2a and GTP-u can utilize two different IP endpoints.
12. The PDN GW returns a Create Session Response, including the IP address allocated for the 3GPP UE.
13. The DBNG-CP provides the DBNG-UP with packet forwarding rules based on the DHCP discovery packet at step 6 (which could include the encapsulation, MAC, and VLANs) and on the GTP-u F-TEID and QoS requirements received from the PDN GW in Create Session Response. These rules include the request to forward DHCP signaling from the UE to the DBNG-CP. They are sent in a session establishment request unless a session establishment request has been used in step 6, in which case a session modification request would be used.
    NOTE: The DBNG-CP is responsible of the charging interface, if any.
14. The DBNG-UP sends a response back to the DBNG-CP, informing that the states are installed, and the DBNG-UP is ready to forward the subscribers IP data packets
15. Both DBNG and PGW finishes exchanging information to establish the GTP-u tunnel.
16. The DBNG-CP sends a DHCP offer including the IPv4 Address allocated by the PDN GW to the 3GPP UE via the CPR interface.
17. The 3GPP UE sends a DHCP request message and is redirected to the DBNG-CP through the DBNG-UP via the CPR interface.
18. The DBNG-CP sends a DHCP ack through the CPR interface

Note: The procedure for accounting message exchange used for charging purposes is not included in this flow.

Note*: TEID allocation can be done by the DBNG-CP function (3GPP TS 29.244 [23] section 5.5.2) or optionally by the DBNG-UP function (3GPP TS 29.244 [23] section 5.5.3)

4.4.18 Hybrid Access Gateway

The call flow covers Hybrid Access Gateway L3 Network-based Tunneling in both TR-348 [16] and TR-378 [17].

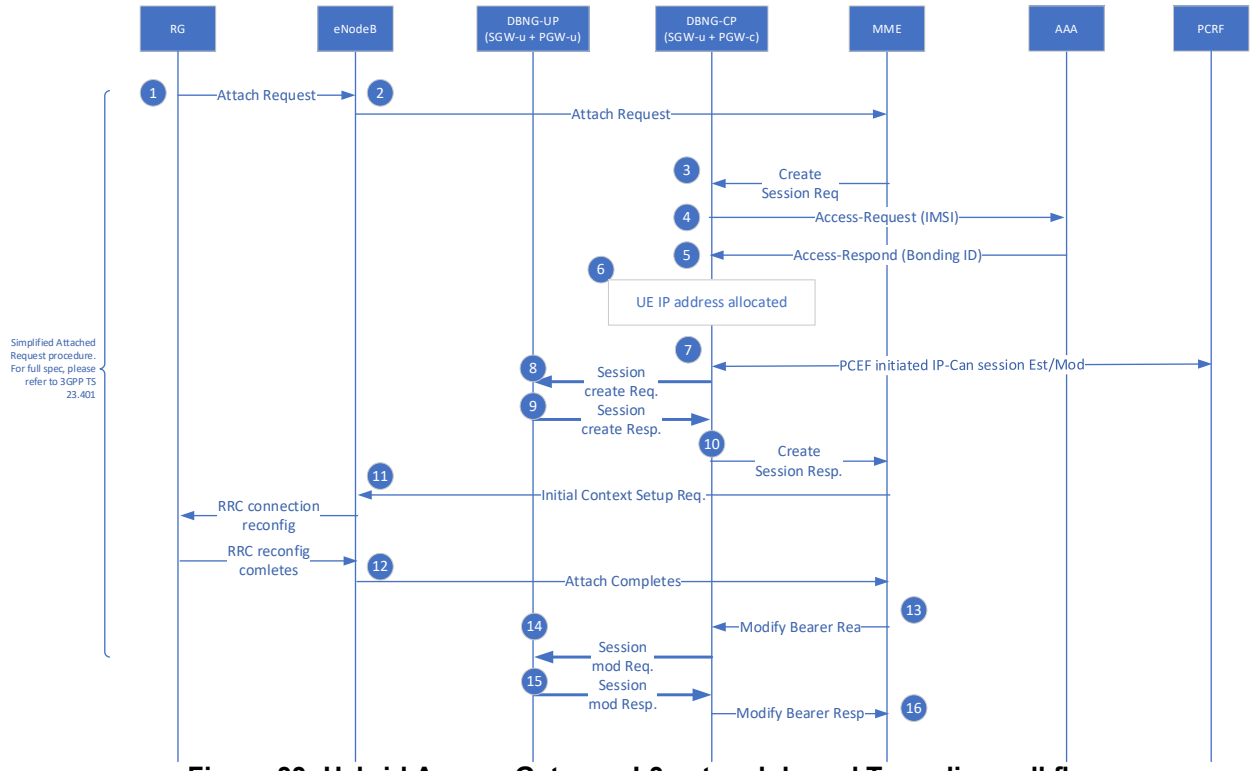

Figure 33: Hybrid Access Gateway L3 network-based Tunneling call flow

The above CPE attach procedure is simplified, for full attachment procedure, refer to 3GPP TS 23.401 [21]. The HAG is a BBF defined element in TR-348 [16] where PGW, SGW, and MS-BNG are integrated into a single element that can serve both wireline and wireless access. For some deployment cases, it is possible for only the PGW and MS-BNG to be integrated into the HAG. The HAG in the call flow procedure is split between the DBNG-CP and DBNG-UP.

The Hybrid CPE (HCPE) can start with either the wireless or wireline connection. To bond the two connections, a policy or a local configuration is required. As an example, a RADIUS attribute named Bonding ID returned by the AAA.

- For wireline: during the DHCP or PPPoE authentication process the AAA server returns the RADIUS attribute: Bonding ID.
- For wireless: during the create session request procedure, the DBNG-CP sends an Access-Request to the AAA server which returns the RADIUS attribute: Bonding ID.

Utilizing the bonding ID, the DBNG-CP can correlate the wireline and wireless session as a single hybrid session. Regardless of the connection sequence, wireline or wireless, the DBNG-CP can identify the two connections as a single hybrid session.

Additional parameters might be required to load-balance traffic among wireline and wireless access. However, it is important to note that the HAG integration is transparent to other 3GPP components (MME, eNodeB, and PCRF).

Key information regarding load-balancing as documented in TR-378 [17]:

- Downstream:
  - QoS or policy control on the HAG can be provided by local policies or via RADIUS
- Upstream:
  - RG traffic load balancing is provided by a pre-defined policy.

This diagram depicts the case where the RG connects to Core over LTE first and then over Wireline

1. The Hybrid RG initiates an Attach Request to the eNodeB including a request for a PDN connection in an ESM container. This takes place as defined in step 1 of Figure 5.3.2.1 within 3GPP TS 23.401 [21]
2. The eNodeB forwards the Attach Request to the MME. This takes place as defined in step 2 of 3GPP TS 23.401 [21] Figure 5.3.2.1. The MME may carry out security features and retrieve subscription data as defined in step 3 to 11 of 3GPP TS 23.401 [21] Figure 5.3.2.1.
3. MME identifies the DBNG (HAG) to host the subscriber session as a PGW, where the SGW is also co-located: if it has received one in the subscription data from HSS it uses it, otherwise it selects one using the APN in the subscription data and as defined in 3GPP TS 23.401. The MME sends a session request to the DBNG-CP (acting as both the SGW and PGW from MME viewpoint). This takes place as defined in steps 12 to 13 of 3GPP TS 23.401 [21] Figure 5.3.2.1.
4. The DBNG-CP sends an Access-Request to the AAA server. The Request contains the subscriber IMSI.
5. The AAA server returns the bonding ID for the subscriber session. The AAA might contain other attributes which contains QoS parameter for load-balancing downstream.
6. DBNG-CP selects a DBNG-UP and allocates an IP address for the Hybrid RG
7. *[optional] QoS parameter might be provided by the PCRF to the DBNG-CP through the Gx interface.
8. DBNG-CP requests a session establishment from the DBNG-UP. The DBNG-UP could be used to provide the TEID for the GTP-u tunnel.
9. The DBNG-UP responds to the session establishment request.
10. The DBNG-CP sends a create session response back to the MME. This takes place as defined in steps 15 to 16 of 3GPP TS 23.401 [21] Figure 5.3.2.1;
11. The MME sends the NAS attach accept back to the HCPE through the eNodeB via DBNG-CP and DBNG-UP: the NAS attach accept is sent within a S1-AP Initial Context Setup Request as defined in steps 17 of 3GPP TS 23.401 [21] Figure 5.3.2.1.
12. The eNodeB forwards the Attach complete message to the MME through the DBNG-UP and DBNG-CP.
13. The MME sends a modify bearer request to the DBNG-CP. This informs the DBNG-CP the TEID that the eNodeB intends to use.
14. The DBNG-CP sends modify the session to update the DBNG-UP with known information for both uplink and downlink (TEID, RG IP, and the bonding ID)
15. The DBNG-UP respond to the session modification to the DBNG-CP
16. The DBNG-CP sends a modify bearer response to the MME.

For subsequent DHCP, SLAAC, or PPPoE wireline connections, please look at section 4.4 for the call flow. The only modification to the call flows of the wireline access is AAA Access-Accept includes the Bonding ID to allow DBNG-CP to bond the existing wireless session with the new wireline session. This is application to:

- DHCP call flow step 2
- DHCPv6 call flow step 2
- SLAAC call flow step 2
- PPPoE call flow step
- PPPoEv6 call flow step 10

Note*: TEID allocation can be done by the DBNG-CP function (3GPP TS 29.244 [23] section 5.5.2) or optionally by the DBNG-UP function (TS 29.244 [23] section 5.5.3)

4.4.19 Lawful Intercept

Note: Lawful Intercept (LI) is governed by local policy and regulations. This TR provides a basic mechanism for the DBNG to perform lawful intercept. The following call flow is an example which can realize Lawful Intercept using various PFCP mechanisms.

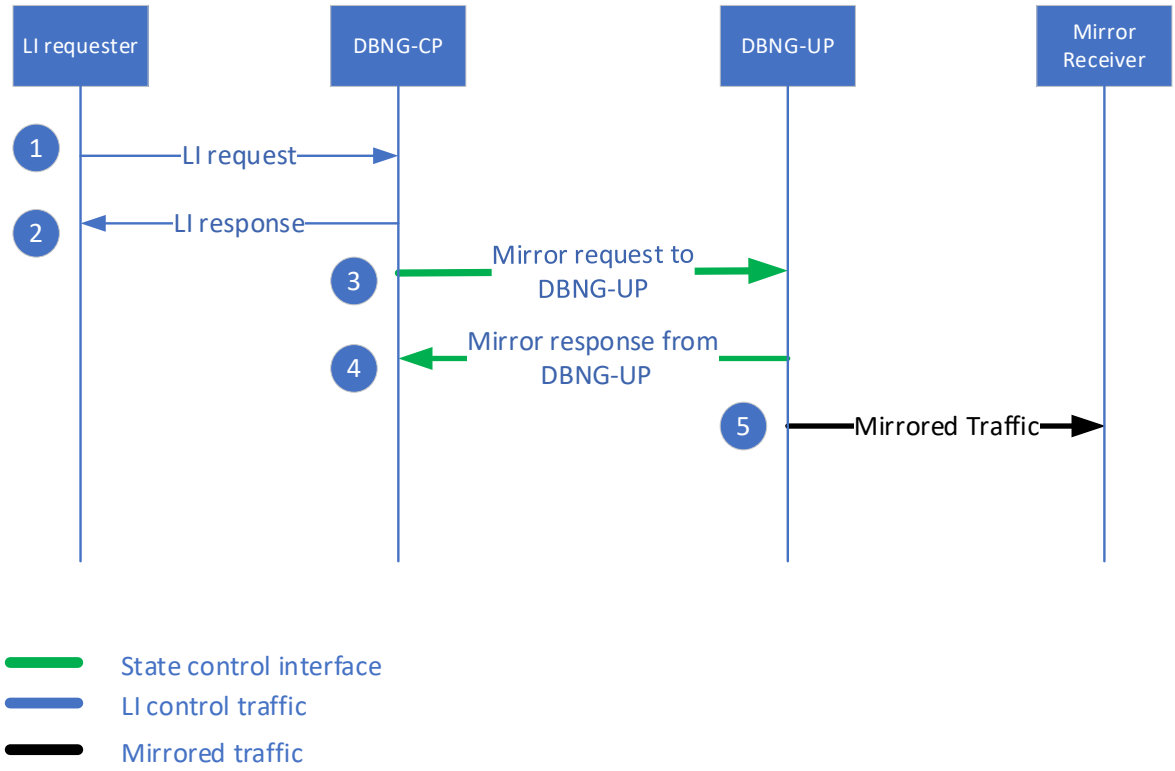

Figure 34: Example of Lawful intercept Request

1. The LI requester (unspecified in this document) contacts the DBNG-CP requesting to mirror traffic for a specific subscriber.
2. DBNG-CP sends back the answer to the LI-requester (note that this may optionally take place after step 4).
3. DBNG-CP performs a lookup for the specific subscriber and identifies the DBNG-UP handling that subscriber. DBNG-CP instructs the identified DBNG-UP and sends a mirror request message to the identified DBNG-UP.
4. DBNG-UP sends a mirror response message to the DBNG-CP.
5. DBNG-UP sends mirrored traffic to the mirror receiver.

If for any reason, the subscriber is moved to a different DBNG User Plane (due to DBNG-UP failure or session steering request) then the subscriber mirror configurations should also be moved accordingly.

5 Technical Requirements

5.1 State Control Interface requirements

The section lists the functional requirements for a CUPS protocol that DBNG-CP and DBNG-UP use to communicate and maintain the required functions and services. Note that throughout this section terms 'SCi protocol', 'CUPS protocol' and 'protocol' are used interchangeably and refers to the protocol used over the State Control Interface.

[R-1] The State Control Interface MUST support the communication of traffic detection and matching forwarding rules to allow the handling of subscriber traffic over the V-interface.
[R-2] The State Control Interface protocol MUST support the communication of forwarding rules to allow the handling of subscriber traffic over the V-interface.
[R-3] The State Control Interface MUST support the communication of traffic detection and matching forwarding rules to allow the handling of subscriber traffic over the A10 interface. For example, Ethernet, MPLS, L2TP, and GTP.
[R-4] The State Control Interface protocol MUST support the communication of forwarding rules to allow the handling of subscriber traffic over the A10 interface. For example, Ethernet, MPLS, L2TP, and GTP.
[R-5] The protocol MUST enable the DBNG to support all the functions and services supported by a single node-based MS-BNG as documented in Table 1.
[R-6] The protocol MUST support the multiple access technologies used by functions and services required by Table 1.
[R-7] The protocol MUST provide reliable communication between the DBNG-CP and the DBNG-UP entities of the DBNG.

To fulfill MS-BNG functionality, DBNG-CP and DBNG-UP form associations. It is possible for each association to support a different subsets of functions. The protocol should be able to exchange information on supported features.
[R-8] The protocol MUST be extensible, e.g., allow introduction of the new information elements in a backward compatible manner.

[R-9] The protocol MUST be able to monitor reachability and liveliness of the entities in the association.
[R-10] The protocol MUST support the use of redundant DBNG-CPs in the association.

Security and privacy are critical for the CUPS protocol. The following are detailed requirements to ensure secure communication and minimize the risk of attacking DBNG-CP and/or DBNG-UP.
[R-11] It MUST be possible to encrypt data exchanged by the protocol.
[R-12] It MUST be possible to authenticate the source of data exchanged by the protocol.

[R-13] The protocol MUST be able to convey rules to DBNG-UP to determine types of control packets to be re-directed to DBNG-CP.
[R-14] The SCi protocol MUST support capabilities determination between the DBNG-CP and DBNG-UP.
[R-15] The SCi protocol MUST be able to support a DBNG-CP to:
- add subscriber framed/network/host routes on a DBNG-UP
- update subscriber framed/network/host routes on a DBNG-UP
- delete subscriber framed/network/host routes on a DBNG-UP

[R-16] For all of the access types documented on fourth column of **Table 2**, the SCi protocol MUST support a DBNG-CP to:
- add subscriber session forwarding states on DBNG-UP(s).
- update subscriber session forwarding states on DBNG-UP(s).
- delete subscriber session forwarding states on DBNG-UP(s).

[R-17] The SCi protocol MUST be able to support session status synchronization between a DBNG-CP and a DBNG-UP.

[R-18] The SCi MUST be able to support a DBNG-CP to selectively apply lawful interception on DBNG-UP(s).

As specified in [R-1], a MS-BNG MUST support a variety of access types: fixed wireline, fixed wireless, and hybrid. Therefore, the DBNG-UP must be just as flexible in supporting the access types. To accomplish this, the DBNG-CP is responsible to program DBNG-UP forwarding information. The programming of forwarding states simply consists of:

1) Find the subscriber and match on packet types (**matching criteria**)
2) Perform one or more actions. (perform **action)**

The match and action rules would provide platform independent abstraction to derive data-path state and processing by the DBNG-UP. Table 5 shows examples of DBNG-CP using a CUPS protocol instructing the DBNG-UP to install traffic detection and forwarding rules on the DBNG-UP.

Table 5: Examples of traffic detection and traffic forwarding rules

Access Types	Upstream (access to network)		Downstream (network to access)	
	Match	**Action**	**Match**	**Action**
PPPoE single stack	Port ETH header Session ID IPv4	Remove ETH + PPPoE Apply QoS and Filter(s) Forward to network	IPv4	Encap. ETH + PPPoE Apply QoS and Filter(s) Forward to access
PPPoE dual Stack	Port ETH header Session ID IPv4 IPv6 NA/PD IPv6 SLAAC	Remove ETH + PPPoE Apply QoS and Filter(s) Forward to network	IPv4 IPv6 NA/PD IPv6 SLAAC	Encap. ETH + PPPoE Apply QoS and Filter(s) Forward to access
IPoE single stack	Port ETH header IPv4	Remove ETH Apply QoS and Filter(s) Forward to network	IPv4	Encap. ETH Apply QoS and Filter(s) Forward to access
IPoE dual Stack	Port ETH header IPv4 IPv6 NA/PD IPv6 SLAAC	Remove ETH encap. Apply QoS and Filter(s) Forward to network	IPv4 IPv6 NA/PD IPv6 SLAAC	Encap. ETH Apply QoS and Filter(s) Forward to access
Public Wi-Fi	Port GRE tunnel ETH header IP	Remove GRE/ETH Apply QoS and Filter(s) Forward to network	IP	Encap. ETH/GRE Apply QoS and Filter(s) Forward to access
TWAG	Port ETH header IP	Remove ETH Encap. GTP Apply QoS and Filter(s)	GTP	Remove GTP Encap. ETH Apply QoS and Filter(s)

		Forward to network		Forward to access
HAG	Port ETH header IP	Remove ETH Apply QoS and Filter(s) Forward to network	IP	Encap. ETH Apply QoS and Filter(s) Forward to access
	GTP	Remove GTP Apply QoS and Filter(s) Forward to network		Encap. GTP Apply QoS and Filter(s) Forward to s1u

Supporting data forwarding for different types of access, as shown in Table 5, can be represented by a list of matching criteria and action rules. The traffic detection and forwarding rules can be combined to accomplish the following:

- Flexible to cover all different access types for current MS-BNG deployments
- Flexible to cover the A10 transport protocol as specified on Table 3 used for current MS-BNG deployments.
- Extensible to handle future types of access and transport protocols
    - Covering future types of access and transport SHOULD NOT require versioning

[R-19] The CUPS protocol MUST be able to signal a set of packet matching rules and set of actions for each individual subscriber session from the DBNG-CP to the DBNG-UP.
Note: the method of how rules and actions are signaled is up to the protocol, for example, expressing the relationship between the set of rules and actions is protocol specific.

A native MS-BNG function includes subscriber accounting, to account for both time and volume usage per subscriber. It is expected that the DBNG architecture will provide the equivalent capability. Based on the accounting function, service provider can offer services such as monthly flat rate or credit based broadband access. Credit control refers to subscriber utilizing monetary means to exchange credits in the form of time, data volume, or a combination of both for broadband service. The DBNG-UP would be instructed to monitor the subscriber usage. As the credits are exhausted, the DBNG-UP would inform the DBNG-CP, followed by a subsequent action including, degrading the service, redirecting to a web portal, or stopping the service entirely.

Accounting is the ability to report periodic or upon demand the subscriber usage based on time and data. The accounting record can also contain the amount of time and/or volume consumed by the subscriber.
[R-20] The CUPS protocol MUST be able to perform credit control for usage monitoring and reporting.

As specified in TR-178 [10] section 7.1.4 and 7.1.6, MS-BNG has a variety of QoS mechanisms such as scheduling, traffic shaping, and traffic policing. The DBNG is expected to provide the same set of QoS mechanisms. The CUPS protocol must provide means for the DBNG-CP to communicate QoS parameters to the DBNG-UP.
[R-21] The CUPS protocol MUST be able to set and modify QoS policy per subscriber session.

A MS-BNG that is also acting as a PE (as per TR-178 [10]) may have multiple virtual networks to which a subscriber may be connected.
[R-22] The SCi MUST support the identification of virtual network to which the subscriber should be connected.

[R-23] The SCi MUST support the communication of an action rule with a recursive lookup.
[R-24] The SCi protocol MUST support the ability to request and confirm the offload of PPP keep-alive generation and processing including the generation and response to LCP Echo-Request and the processing of LCP Echo-Reply messages from the DBNG-CP to the DBNG-UP on a per session basis.

[R-25] The SCi protocol MUST support the ability to disable offload of PPP keep-alive generation and processing including the generation and response to LCP Echo-Request and the processing of LCP Echo-Reply messages on a per session basis.
[R-26] The SCi protocol MUST support the ability to negotiate the presence of the PPP keep-alive generation and processing capability including the generation and response to LCP Echo-Request and the processing of LCP Echo-Reply messages offloaded to the DBNG-UP.

5.2 Requirements to support Control packet redirect interface

The CPR Interface is an interface between DBNG-CP and DBNG-UP. It is used to tunnel control packets between the V or the A10 interface to the DBNG-CP via the DBNG-UP.

[R-27] Subscriber control messages to and from RGs MUST be tunneled between DBNG-CP and DBNG-UP through the CPR interface.
[R-28] The DBNG-CP MUST be able to communicate rules to the DBNG-UP to match specific control packet types and forward these to the DBNG-CP over a specified tunnel when no subscriber session context exists on the DBNG-UP
[R-29] The DBNG-UP MUST pass access interface information (e.g. port or virtual-port on which the control traffic is received) together with the tunneled subscriber control packet to the DBNG-CP where applicable. e.g. control packets: DHCP, PPP, RA, data-trigger
[R-30] The DBNG-CP MUST pass access interface information (e.g. port or virtual-port on which the control traffic is received) together with the tunneled control packet to the DBNG-UP where applicable.
[R-31] The DBNG-CP MUST be able to signal the DBNG-UP to update the forwarding action matching specific control messages from the V interface per subscriber
[R-32] The DBNG-CP MUST be able to send control packets to the A10 interface through the DBNG-UP
[R-33] The DBNG-CP MUST be able to signal the DBNG-UP to update the forwarding action matching specific control messages from the A10 interface per subscriber

The selection and redirection of messages to the DBNG-CP must be flexible in accommodating the many types of services provided by the DBNG. E.g. some subscribers connect to the internet using PPPoE, IPTV multicast services through DHCP, and only enterprise customers are using data-trigger service.
[R-34] The CUPS protocol MUST allow the DBNG-CP to signal DBNG-UP to redirect only specific control packets per match criteria. e.g. match criteria could be a granular as per subscriber or as general as per DBNG-UP node

Subscriber control packets are rate limited to protect the DBNG-CP. The DBNG treats subscribers individually. E.g. rate limiting malicious users from the rest of the subscribers, rate limit data-trigger subscriber redirected packets, and prioritize control messages for authenticated subscriber vs. yet to be authenticated subscriber. Unnecessary control packets are be filtered out at the DBNG-UP before reaching the CPR interface.
[R-35] The CUPS protocol MUST allow the DBNG-CP to signal the DBNG-UP the priority of specific control messages per match criteria. E.g., match criteria could be as granular as per subscriber or as general as per DBNG-UP node.
[R-36] The DBNG-UP MUST be able to perform rate limiting on the control packets per subscriber or as general as per DBNG-UP node.
Note: control packets include data-trigger packets.

5.3 Management Interface requirements

The Management interface on DBNG-CP and DBNG-UP provides two main functions: configuration and operational state retrieval of DBNG-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. XML was designed to be self-descriptive and is human-readable.

[R-37] The Management Interface MUST support transactional configuration from DBNG-CP to DBNG-UPs based on YANG data model

Operational data can either be streamed (published) at configured cadence or on-change/event. With on-change/event, data is streamed only when a change in the data occurs. Operational data can be transported using different protocols and in different encoding formats.

[R-38] The Management Interface MUST support operational state retrieval based on YANG data model
[R-39] The Management Interface MUST support operational state retrieval in XML via NETCONF
[R-40] The Management Interface SHOULD support operational state retrieval in JSON via RESTCONF
[R-41] The Management Interface MUST support publishing of state information at configurable cadence or on-event based on YANG data model
[R-42] The Management Interface MUST support publishing of state information in XML via NETCONF
[R-43] The Management Interface SHOULD support publishing of state information in JSON via RESTCONF

5.4 Disaggregated MS-BNG control plane requirements

DBNG-CP is responsible for the wireline access subscriber management as well as its address management, and user plane management. It usually resides in virtualized machines due to being computationally intensive and could be scaled in the cloud infrastructure such as NFVI etc.

[R-44] The DBNG-CP MUST support IPv4/IPv6 address pool management;
[R-45] The DBNG-CP MUST support IPv4/IPv6 address prefix and prefix length allocation
[R-46] The DBNG-CP MUST support resource and state management of DBNG-UP;
[R-47] The DBNG-CP MUST support association and disassociation with DBNG-UP;

In section 4.4.3, in step 3, after the subscriber have successfully authenticated, the DBNG-CP would assign an IP address to the subscriber. It is possible for the DBNG-CP to either have pre-allocated a static IP for the subscriber or dynamic assign the next IP address available for the subscriber. This is applicable to all call flows in section 4.4.

[R-48] The DBNG-CP MUST be able to support static address prefix allocation on behalf of DBNG-UP(s) before subscriber access and subscriber traffic packets arrive.
[R-49] The DBNG-CP MUST be able to support dynamic address prefix allocation on behalf of DBNG-UP upon subscriber access control procedure.

[R-50] A DBNG-CP that supports communication with a Steering Function MUST implement a DBNG-UP Selection Function as per requirements [R-51] to [R-54].
[R-51] Where the DBNG-CP implements a DBNG-UP Selection Function, the DBNG-UP Selection Function MUST select the DBNG-UP that is to serve a newly connecting subscriber.
[R-52] Where the DBNG-CP implements a DBNG-UP Selection Function, the DBNG-UP Selection Function MUST identify required changes in serving DBNG-UP for an established subscriber.
[R-53] Where the DBNG-CP implements a DBNG-UP Selection Function, the DBNG-UP Selection Function MUST signal the target DBNG-UP to the Steering Function.

Note: The exact mechanism by which the DBNG-UP Selection Function signals the Steering Function is not defined here, but it is expected that this may be based on communicating the requirement via an SDN controller.

[R-54] Where the DBNG-CP implements a DBNG-UP selection Function, the DBNG-UP Selection Function MUST be able to identify the DBNG-UP which will serve a specific subscriber based on policy. The policy may take into account the following criteria:
- Subscriber policy information from AAA.
- Current load of the DBNG-UP elements.
- DBNG-UP that are not available (such as undergoing maintenance).
- DBNG-UP to which the subscriber cannot be connected (for network topology reasons).
- Network performance (such as latency) between the subscriber and the DBNG-UP.
- Placement of other subscribers with common attributes such as IP Subnet.

[R-55] The DBNG-CP MUST support PPP keep-alive processing, including the generation and response to LCP Echo-Request and the processing of LCP Echo-Reply messages, and BFD (RFC 5880 [37] and RFC 5881 [38])

[R-56] The DBNG-CP MUST support NETCONF for integration with EMS

[R-57] The DBNG-CP SHOULD support RESTCONF for integration with EMS

[R-58] The DBNG-CP MAY support SNMP for integration with EMS

5.5 Disaggregated MS-BNG user plane requirements

DBNG-UP is responsible for routing, forwarding subscriber data, and terminating subscriber L2 data traffic. Apart from subscriber data termination and forwarding, user plane runs as gateway between the user and the control plane. It could reside in dedicated devices which are designed specifically for forwarding performance or in virtual machines.

[R-59] The DBNG-UP SHOULD support network management interfaces to the operator's EMS.

[R-60] The DBNG-UP MUST support V-interface encapsulations

[R-61] The DBNG-UP MUST support A10 interface encapsulations

[R-62] The DBNG-UP MAY support the offload of PPP keep-alive generation and processing including the generation and response to LCP Echo-Request and the processing of LCP Echo-Reply messages.

[R-63] In the case that the DBNG-UP supports PPP offload as per [R-62], this MUST be supported on a per session basis.

5.6 Disaggregated MS-BNG functional requirements

[R-64] The DBNG MUST support cold standby for redundant DBNG-CPs.

[R-65] The DBNG MUST support cold standby for redundant DBNG-UPs.

[R-66] The DBNG SHOULD support warm standby for redundant DBNG-CPs.

[R-67] The DBNG SHOULD support warm standby for redundant DBNG-UPs.

[R-68] The DBNG MAY support hot standby for redundant DBNG-CPs.

[R-69] The DBNG MAY support hot standby for redundant DBNG-UPs.

6 PFCP CUPS protocol

PFCP is the selected CUPS protocol for the DBNG SCi and is used to program subscriber forwarding state and control packet redirection rules. PFCP is a 3GPP protocol standardized since 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 messages types: node messages and session messages. Node messages are mainly used to form association between DBNG-CP and DBNG-UP. Session messages are mainly used to program the subscriber forwarding state. Both node and session messages utilize information elements (IEs) for communication between DBNG-CP and DBNG-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 various MS-BNG use cases.

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”.

6.1 PFCP messages

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

6.1.1 PFCP node messages

PFCP node message includes:

- Association Setup: Used to signal node level information such as capabilities
- Association Update: Used to signal a change of node level information, e.g. due to reconfiguration or an upgrade.
- Association Release: Used to remove a node from the DBNG function.
- Heartbeat: Used to detect unexpected failures

6.1.2 PFCP session messages

PFCP session messages are divided into the following 4 message types:

- Session Establishment: programs subscriber forwarding state, typically used when a subscriber initiates a connection to the DBNG.
- Session Modification: updates subscriber forwarding state, typically used to update subscriber attributes which can be triggered by a RADIUS CoA
- Session Deletion: removes a subscriber forwarding state, typically used when a subscriber terminates the broadband session or logs off the network.
- Report Session: reports information about the session, allows the DBNG-UP to report subscriber session information to the DBNG-CP. PFCP also supports DBNG-CP querying the DBNG-UP as well.

Within Session Establishment, Session Modification, and Session Deletion, rules are used to program the subscriber forwarding state:

- Packet Detection Rule (PDR) is a rule that contains a selection of the objects below
- Packet Detection Identifier (PDI) specifies the matching criteria for packets
- Forward action Rule (FAR) specifies the action (e.g. forward/drop/mirror) to be taken based on the matching PDI.

- QoS Enforcement Rule (QER) specifies the QoS treatment based on the matching PDI.
- Usage Reporting Rule (URR) specifies the usage reporting and charging rule based on the matching PDI.

6.1.3 PFCP information elements

Information Elements are encoded as TLVs. Each PFCP session may use individual IEs or grouped IEs (IE that contains other IEs) for DBNG-CP and DBNG-UP communication.

6.2 General PFCP information exchanges for a subscriber session

For the MS-BNG use cases, this document separates PDRs into two categories.

A. PDRs to match on subscriber control packets
   - Typically require a minimum of two PDRs
     1. To redirect control packets from access to the DBNG-CP through the CPR Interface
     2. To redirect control packets from DBNG-CP back to access through the CPR Interface. Control packets can include: DHCP, PPP discovery, and router solicits

B. PDRs to match on subscriber data packets
   - Again, typically require a minimum of two PDRs
     1. To forward traffic upstream by matching on data packets arriving from the access and forwarding the packets to the network interface
     2. To forward traffic downstream by matching on IP packets from the network interface and forwarding the packets back to the subscriber.

Therefore, a typical subscriber session would require at least 4 PDRs.

6.2.1 General PFCP rules for control packet redirection

For redirecting control packets from the DBNG-UP to the DBNG-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 6.2.3.
- FAR – Specify the forwarding action and the destination for the redirected control packet. The control messages are encapsulated for tunneling.
- For more information on:
  - Traffic endpoint see section 6.5.5.5 and 6.5.6.3
  - Filter see section 6.2.3

A typical template is shown in **Table 6** below for control packet redirection from the DBNG-UP to the DBNG-CP through the CPR Interface.

Table 6: Example of a PDR for Control Packet Redirection from DBNG-UP to DBNG-CP

Direction	PDR	FAR

Control packet from the RG to DBNG-CP	PDR ID
	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 DBNG-CP to the DBNG-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.
- For more information on:
    - Traffic endpoint see section 6.5.5.5 and 6.5.6.3

From the attributes above, a typical template is shown in Table 7 below for control packet redirection from the DBNG-CP to the DBNG-UP through the CPR interface.

Table 7: Example of a PDR for Control Packet redirection from DBNG-CP to DBNG-UP

Direction	PDR	FAR

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

6.2.2 General PFCP rules for data packet forwarding

For the upstream direction, data packets from the subscriber are routed through the network 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. Detail is section 6.2.3
- FAR – Specify the forwarding action and the destination for the data packet.
- For more information on:
    - Traffic endpoint see section 6.5.5.5 and 6.5.6.3
    - BBF Outer Header removal see section 6.6.4

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

Table 8: Example of a PDR for upstream data packet forwarding through the DBNG-UP

Direction	PDR	FAR

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

***Bolded text indicates BBF PFCP extension**

For the downstream direction, IP packets are routed form the network to the DBNG-UP and are forwarded back to the subscriber, 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 control packet.

- For more information on:
  - Traffic endpoint see section 6.5.5.5 and 6.5.6.3
  - BBF Outer Header creation see section 6.6.3

Below in Table 9, a typical template for downstream data packet forwarding is shown. Traffic is forwarded from the network core through the DBNG-UP and then to the subscriber.

Table 9: Example of a PDR for downstream data packet forwarding through the DBNG-UP

Direction	PDR	FAR

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

***Bolded text indicates BBF PFCP extension**

6.2.3 General Information PFCP Filter IEs

Filters are required when a sub-flow of a traffic endpoint needs to be further separated. Matching on a sub-flow, can be done at Layer 2, Layer 3, or both. For Layer 2, IE Ethernet Packet Filter is used and for Layer 3, IE Service Data Filter (SDF) is used. Both types of filter are well defined in 3GPP TS 29.244 [23]. To cover the wireline case, further extensions are required on Ethernet Packet Filter IE, see section 6.5.5.2

6.3 PFCP use case and information exchanges

This section describes the information exchange required to cover different MS-BNG use cases. IEs that are extended by BBF are highlighted in **bold.**

6.3.1 Use case: Default control packet redirection

As shown in the call flow diagram in section 4.4.2, the DBNG-CP and DBNG-UP forms an association using PFCP Association Setup messages. During the association setup, the DBNG-UP informs the DBNG-CP of DBNG function(s) support. Based on this information, the DBNG-UP is instructed to program a default forwarding rule to redirect all control packets from unknown subscribers to the DBNG-CP. To indicate the support of DBNG function(s) a new extension is required:

- **BBF UP Function Features:** A BBF IE extension for capability flag. Please see new extension in section 6.5.1

6.3.1.1 PFCP control packet redirection rule

Control packet redirection PFCP rules follow the general description highlighted in section 6.2.1. Filters rules would be required to match a control packet including: DHCPv4 and PPPoE. A new extension is required to tunnel control packet along with attached meta data to the DBNG-CP:

- **BBF Outer Header Creation:** A BBF IE extension to insert the logical port information as an Network Service Header (NSH) to the subscriber control packet when redirected to the DBNG-CP. Details of this new extension is in section 6.6.3

6.3.2 Use case: IPoE

For IPoE using DHCPv4, DHCPv6, or SLAAC address request. The data forwarding rules are split between control packet forwarding and data traffic forwarding. Control packets, DHCP, DHCPv6, and router solicit packets must be redirected through the CPR Interface to DBNG-CP for address assignment. And subscriber IPoE data traffic is forwarded through the User Plane.

6.3.2.1 PFCP Control Packet redirection rule

Control packet redirection PFCP rules follow the general description highlighted in section 6.2.1. Filter rules are required to match on DHCP, DHCPv6, or ICMPv6 control packets only. Further extensions are required on Traffic Endpoint support IPoE use case:

- **Traffic-Endpoint IE extensions required:** Ethernet header information such as C-Tag, S-Tag, and the logical port where the control packet is coming from. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3

6.3.2.2 PFCP Data Packet Forwarding rule

Data packet forwarding PFCP rules follow the general description highlighted in section 6.2.2. Below are further extensions are required to support IPoE use case for data forwarding:

- **BBF Outer Header Creation:** BBF extended IE to construct the Ethernet header for packet forwarding to the subscriber. Details of the extension are in section 6.6.3
- **BBF Outer Header Removal**: BBF extended IE to remove the Ethernet header from data packets before forwarding to the network interface. Details of the extension are in section 6.6.4
- **Traffic-Endpoint IE extensions required:** Ethernet header information such as C-Tag, S-Tag, and the logical port where the control packet is coming from. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3

6.3.3 Use case: PPPoE

For PPPoE, data forwarding rules are split between control packet redirection and data packet forwarding. Only control packets such as PPP discovery, link control, and network control packets should be redirected to the CPR Interface while PPPoE data traffic should be routed through the network interface.

6.3.3.1 PFCP Control Packet redirection rule

PFCP Control packet redirection PFCP rules follow the general description highlighted in section 6.2.1. Filter rules would match on PPP control message such as discovery, LCP, and NCP. For PPPoEv6, DHCPv6 and Router Solicit messages should also be redirected to the DBNG-CP. Further extensions are required to support PPPoE use case:

- **Ethernet packet filter IE extension required**: Specifies PPP attributes such as the PPP protocol type. Details of the extension are in section 6.5.5.3
- **Traffic-Endpoint IE extensions required**: Ethernet header information such as C-Tag, S-Tag, PPPoE session ID, and the logical port where the control packet is coming from. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3

6.3.3.2 PFCP Data Packet Forwarding rule

Data packet forwarding PFCP rules follow the general description highlighted in section 6.2.2. Further extensions required to support PPPoE use case for data forwarding:

- **BBF Outer Header Creation:** BBF extended IE to construct the PPPoE header for packet forwarding to the subscriber. Details of the extension are in section 6.6.3
- **BBF Outer Header Removal**: BBF extended IE to remove the PPPoE header from data packets before forwarding to the network interface. Details of the extension are in section 6.6.4
- **Ethernet packet filter IE extension required:** Specified PPP attributes such as the PPP protocol type. Details of the extension are in section 6.5.5.3
- **Traffic-Endpoint IE extensions required**: Ethernet header information such as C-Tag, S-Tag, PPPoE session ID, and the logical port where the control packet is coming from. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3
- **PPP LCP Connectivity IE:** An IE to specify the LCP echo hello properties. Note, upon failure, a PFCP session report is sent from the DBNG-UP to the DBNG-CP informing of the inactivity.
- **MTU:** An IE used to enforce the MRU specified by the CPE

6.3.4 Use Case: L2TP LAC

The call flow for LAC subscriber will initially follow the same PPPoE procedure as specified in section 6.3.3, authentication will inform the DBNG-CP that the subscriber requires an L2TP tunnel to the LNS. A PFCP session is established for the L2TP tunnel. Afterward when the L2TP tunnel and session are established, the PPPoE session would be tunneled to the LNS. Therefore, the PFCP sessions are as follows:

1. An initial PFCP session to allow PPPoE procedure follows the control packet forwarding rule listed in section 6.2.1. After authentication, the DBNG-CP identifies that the subscriber requires an LNS connection. The LAC will need to determine:
    - If a new L2TP tunnel is required for the L2TP session, section 6.3.4.1 outline the PFCP information exchange to allow for L2TP tunnel setup.
    - Or If an existing L2TP tunnel can be reused, then move to step 2)
2. The subscriber PFCP session is modified to forward both PPP control and data packets to the LNS. See section 6.3.4.2

6.3.4.1 PFCP session for L2TP tunnel setup

Each L2TP tunnel setup would require an individual PFCP session to forward L2TP control messages between DBNG-CP and DBNG-UP. The PFCP rules to redirect L2TP tunnel setup control messages follow the general description highlighted in section 6.2.1, instead of forwarding control message to access ports, L2TP control messages are forwarded to the network core instead. L2TP control messages from specific tunnels are redirected from the network core to the DBNG-CP. Further extensions are required on Traffic Endpoint to support L2TP tunnel signaling:

- **Traffic-Endpoint IE extensions required:** For the DBNG-UP to DBNG-CP direction, matching L2TP control messages based on tunnel ID and allowing DBNG-UP to select the IP address for the L2TP tunnel. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3
- **L2TP type**: Used to match on L2TP control messages.

6.3.4.2 PFCP update for L2TP session

The PFCP rule in section 6.3.3.1 will continue to redirect PPPoE discovery control packets to the local LAC-CP. Other PPP control packets, previously redirected to the LAC DBNG-CP, are updated to be forwarded to the LNS instead, specified in section 6.3.4.1. Both PPP control and data packet forwarding PFCP rules to the LNS follow the general description highlighted in section 6.2. Further extensions are required on Traffic Endpoint to forward PPP packets to the L2TP tunnel:

- **BBF Outer Header Creation:** BBF extended IE to construct the Ethernet downstream and creating the L2TP header upstream. Details of the extension are in section 6.6.3
- **BBF Outer Header Removal:** BBF extended IE to remove the Ethernet header in the upstream direction and removing the L2TP header in the downstream direction. Details of the extension are in section 6.6.4

- **Ethernet packet filter IE extension required**: Specifies PPP attributes such as the PPP protocol types. Details of the extension are in section 6.5.5.3
- **Traffic-Endpoint IE extensions required**: For upstream, Ethernet header information such as C-Tag, S-Tag, and the logical port where the control packet is coming from. And for downstream, match on specific session within a L2TP tunnel. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3
- **L2TP type:** Identify to only match on L2TP data messages.

6.3.5 Use Case: L2TP LNS

After DBNG-UP and DBNG-CP association, a default PFCP rule is installed to redirect new L2TP control message for tunnel setup from DBNG-UP to DBNG-CP. Upon completion of PPP authentication, a PFCP session can be installed for control message and data packets forwarding. Authentication can be sped up with standard L2TP LCP and authentication proxy. Therefore, the PFCP sessions are as follows:

1. A PFCP session start for specific L2TP tunnels, described below in section 6.3.5.1
2. Individual PFCP session for each subscriber L2TP session, described in section 6.3.5.2 and 6.3.5.3

6.3.5.1 PFCP session for L2TP tunnel setup

Individual PFCP session is used to redirect L2TP control packets from the DBNG-UP to DBNG-CP. The PFCP rules to redirect L2TP tunnel setup control messages follow the general description highlighted in section 6.2.1. Further extensions are required on Traffic Endpoint to support L2TP tunnel control signaling:

- **Traffic-Endpoint IE extensions required**: For the DBNG-UP to DBNG-CP direction, matching L2TP control messages based on tunnel ID and tunnel IP address. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3
- **L2TP type:** Used to match on L2TP control messages.

6.3.5.2 PFCP Control Packet redirection rule

L2TP data packets are split into two categories, one is for PPP control and the other is subscriber data traffic. Control packet redirection PFCP rules follow the general description highlighted in section 6.2.1. L2TP data packet containing PPP control message must be redirected to the DBNG-CP for processing. Further extensions are required on Traffic Endpoint and Ethernet Filter to support L2TP use case:

- **Ethernet packet filter IE extension required:** Redirects PPP control messages within the L2TP data packet only. Details of the extension are in section 6.5.5.3
- **Traffic-Endpoint IE extensions required:** To match on specific session within a L2TP tunnel. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3
- **L2TP type:** Used to match on L2TP data messages.

6.3.5.3 PFCP Data Packet Forwarding rule

This rule is programmed after authentication. Data packet forwarding PFCP rules follows the general description highlighted in section 6.2.2. Further extensions are required to support LNS use case for data forwarding:

- **BBF Outer Header Creation:** BBF extended IE to construct both L2TP and PPP header downstream. Details of the extension are in section 6.6.3
- **BBF Outer Header Removal:** BBF extended IE to remove the both L2TP and PPP header in the upstream direction. Details of the extension are in section 6.6.4
- **Traffic-Endpoint IE extensions required:** for upstream to match on specific L2TP tunnel ID and the session ID. For downstream match on the subscriber IP address information. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3
- **L2TP type:** Use to match on L2TP data messages.

- **PPP LCP Connectivity IE:** An IE to specify the LCP echo hello properties. Note, upon failure, a PFCP session report is sent from the DBNG-UP to the DBNG-CP informing of the inactivity.
- **MTU:** Used to enforce the MRU specified by the CPE

6.3.6 Use Case: TWAG

In all layer 2 and layer 3 models, the DBNG-UP can optionally decide the TEID for the DBNG-CP to use. There are two ways for DBNG-UP to select TEID range and inform the DBNG-CP.

1) During association the DBNG-UP can pass the range of TEID for DBNG-CP to use
2) During PFCP session establishment, the DBNG-CP request a TEID from the DBNG-UP to use.

Both options are covered in section 6.3.6.1. Afterwards, the PFCP session will update the DBNG-UP (or if there are no PFCP session establish a PFCP session) to redirect control traffic to the DBNG-CP and to forward data traffic to the EPC core through a GTP encapsulation.

6.3.6.1 DBNG-UP TEID assignment (optional)

Option 1) If the DBNG-UP has a TEID range for DBNG-CP to use to establish a tunnel to the 3GPP PGW, during the PFCP association procedure, the DBNG-UP must utilize IE User Plane IP resource information to specify the TEID range. For details of the IE can be found in 3GPP TS 29.244 [23] section 8.2.82.

Option 2) The DBNG-CP establish a PFCP session with the DBNG-UP and request for a TEID. The PDR will request for TEIDs from the DBNG-UP. The DBNG-UP will respond with a list of TEIDs for the DBNG-CP in a session respond message.

6.3.6.2 PFCP Control Packet redirection rule

For upstream: From step 8 of the layer 2 trigger initial attached call flow in section 4.4.17.1 and step 12 of the layer 3 trigger initial attached call flow in section 4.4.17.3, the PDN GW would have assigned the DBNG-CP an IP address and/or IPv6 SLAAC prefix for the subscriber. DHCP and RS control packets from the subscriber access interface are redirected to the CPR Interface following the general description highlighted in section 6.2.1. Further extensions are required on Traffic Endpoint to support the TWAG use case:

- **Traffic-Endpoint IE extensions required**: Ethernet header information such as C-Tag, S-Tag, and the logical port where the control packet is coming from. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3

6.3.6.3 PFCP Data Packet Forwarding rule

Data packet forwarding PFCP rules follow the general description highlighted in section 6.2.2. Further extensions are required to support TWAG use case for data forwarding:

- **BBF Outer Header Removal**: BBF extended IE to remove the Ethernet header from data packets before forwarding to the EPC. Details of the extension are in section 6.6.4
- **Traffic-Endpoint IE extensions required**: Ethernet header information such as C-Tag, S-Tag, and the logical port where the control packet is coming from. Detailed information of the extension is in section 6.5.5.5 and 6.5.6.3

6.4 BBF PFCP Information Element Summary

BBF PFCP IE type values are specified in the Table 10. Table 10 is an applicability table for each broadband use case. "Yes" indicates that the IE indicated in column 2 MUST be included for that particular use case. "No" indicates that the IE indicated in column 2 MUST NOT be included for that particular use case. "Opt" means the IE can provide more specific matching information for the PFCP session and MAY be included for that particular use case.

Table 10: BBF extended Information Element Types and applicability

IE Type value (Decimal)	Information Elements	Section	Use Case								
			CP and UP Association	Default CPR	PPPoE	IPoE	LAC tunnel	LAC subscriber session	LNS tunnel	LNS subscriber session	TWAG
32768	BBF UP Function Features	6.6.1	Yes	No	No	No	No	No	No	No	No
32769	Logical Port	6.6.2	No	No	Yes	Yes	No	Yes	No	No	Yes
32770	BBF Outer Header Creation	6.6.3	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
32771	BBF Outer Header Removal	6.6.4	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
32772	PPPoE Session ID	6.6.5	No	No	Yes	No	No	Yes	No	No	No
32773	PPP protocol	6.6.6	No	Opt	Yes	No	No	Yes	No	Yes	No
32774	Verification Timers	6.6.7	No	No	Yes	No	No	No	No	Yes	No
32775	PPP LCP Magic Number	6.6.8	No	No	Yes	No	No	No	No	Yes	No
32776	MTU	6.6.9	No	No	Yes	No	No	No	No	Yes	No
32777	L2TP Tunnel Endpoint	6.6.10	No	Opt	No	No	Yes	Yes	Yes	Yes	No
32778	L2TP Session ID	6.6.11	No	No	No	No	No	Yes	No	Yes	No
32779	L2TP Type	6.6.12	No	Opt	No	No	Yes	Yes	Yes	Yes	No
32780	PPP LCP Connectivity	6.5.7	No	No	Yes	No	No	No	No	Yes	No
32781	L2TP Tunnel	6.5.8	No	Opt	No	No	Yes	Yes	Yes	Yes	No

6.5 PFCP Grouped IE extensions

This section highlights extensions required on grouped IE such as PDR, PDI, FAR, to cover DBNG 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 use case specified in Table 10.

6.5.1 PFCP Association Setup Request

In the case where the DBNG-UP requests the association setup, the DBNG-UP would include IE "BBF UP Function Features" to notify the DBNG-CP of its functional support.

Table 11: BBF extended Information Element(s) in a PFCP Association Setup Request

Information element	P	Condition / Comment	IE Type
BBF UP Function Features	C	This IE MUST be present if the DBNG-UP function sends this message and the DBNG-UP function supports at least one DBNG-UP feature defined in this IE. When present, this IE MUST indicate the features the BBF UP Function supports.	**BBF UP Function Features** Details in section 6.6.1

6.5.2 PFCP Association Setup Response

In the case where the DBNG-CP request the association setup, the DBNG-UP would respond with this IE “BBF UP Function Features” to notify the DBNG-CP of its functional support.

Table 12: BBF extended Information Element(s) in a PFCP Association Setup Response

Information element	P	Condition / Comment	IE-Type
BBF UP Function Features	C	This IE MUST be present if the DBNG-UP function sends this message and the DBNG-UP function supports at least one DBNG-UP feature defined in this IE. When present, this IE MUST indicate the features the BBF UP Function supports.	**BBF UP Function Features** Details in section 6.6.1

6.5.3 PFCP Association Update Request

In the case where the DBNG-UP request the association setup, the DBNG-UP would include IE “BBF UP Function Features” to notify the DBNG-CP of its functional support.

Table 13: BBF extended Information Element(s) in a PFCP Association Update Request

Information element	P	Condition / Comment	IE Type
BBF UP Function Features	C	This IE MUST be present if the DBNG-UP function sends this message and the DBNG-UP function supports at least one DBNG-UP feature defined in this IE. When present, this IE MUST indicate the features the BBF UP Function supports.	**BBF UP Function Features** Details in section 6.6.1

6.5.4 PFCP Association Update Response

In the case where the DBNG-CP request the association setup, the DBNG-UP would respond with this IE “BBF UP Function Features” to notify the DBNG-CP of its functional support.

Table 14: BBF extended Information Element(s) in a PFCP Association Update Response

Information element	P	Condition / Comment	IE-Type
BBF UP Function Features	C	This IE MUST be present if the DBNG-UP function sends this message and the DBNG-UP function supports at least one DBNG-UP feature defined in this IE. When present, this IE MUST indicate the features the BBF UP Function supports.	**BBF UP Function Features** Details in section 6.6.1

6.5.5 PFCP Session Establishment Request

In the case where PPP LCP connectivity is required for the subscriber session, this IE is included in the PFCP session establishment request message.

Table 15: BBF extended Information Element(s) in a PFCP Session Establishment Request

Information element	P	Condition / Comment	IE Type
PPP LCP connectivity	C	This IE MUST be present if periodic LCP echo hello is required.	**PPP LCP connectivity** Details in section 6.5.7

6.5.5.1 Create PDR

The create PDR grouped IE should include BBF Outer Header Removal to remove various wireline encapsulations.

Table 16: BBF extended Create PDR IE(s) within PFCP Session Establishment Request

Octet 1 and 2	Create PDR IE Type = 1(decimal)		
Octets 3 and 4	Length = n		
Information element	**P**	**Condition / Comment**	**IE Type**
BBF Outer Header Removal	C	This IE MUST be present if the DBNG-UP function is required to remove header(s) from the packets matching this PDR.	**BBF Outer Header Removal** Details in section 6.6.3

6.5.5.2 PDI

The PDI IE should include L2TP type IE in the case of supporting L2TP subscribers.

Table 17: BBF extended PDI IE within PFCP Session Establishment Request

Octet 1 and 2	PDI IE Type = 2 (decimal)		
Octets 3 and 4	Length = n		
Information element	**P**	**Condition / Comment**	**IE Type**
L2TP type	C	This IE MUST be present if identification of the L2TP type control or data is required.	**L2TP type** Details in section 6.6.12

6.5.5.3 Ethernet Packet Filter

The table below is the 3GPP defined Ethernet Packet Filter IE. Details of this grouped IE can be found in 3GPP TS 29.244 [23]. The IE is used to match on sub flow of a traffic endpoint.

Table 18: BBF extended Ethernet Packet Filter IE(s) within PFCP Session Establishment Request

Octet 1 and 2	Ethernet Packet Filter IE Type = 132 (decimal)		
Octets 3 and 4	Length = n		
Information element	**P**	**Condition / Comment**	**IE Type**
PPP Protocol	C	If present, this IE MUST identify the PPP protocol to match for the incoming packet. (see section 6.6.6 for IE details)	**PPP Protocol** Details in section 6.6.6

6.5.5.4 Forwarding Parameters

The Forwarding Parameters IE in FAR can include the BBF Outer Header Creation IE and The MTU IE. The BBF Outer Header Creation is used to encapsulate the subscriber data packet in various wireline encapsulations. The MTU IE is primarily used in the case of PPPoE.

Table 19: BBF extended 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**
BBF Outer Header Creation	C	This IE MUST be present if the DBNG-UP function is required to add outer header(s) to the outgoing packet.	**BBF Outer Header Creation** Details in section 6.6.3
MTU	C	This IE MUST be present to enforce an MTU on outgoing packets. In the case of PPPoE, this may be based on negotiated MRU value	**MTU** Details in section 6.6.9

6.5.5.5 Create Traffic Endpoint

The table below is the 3GPP defined Create Traffic Endpoint IE. Details of this grouped IE can be found in 3GPP TS 29.244. The grouped IE traffic endpoint already contains a list of IEs to specify properties of the endpoint including the GTP tunnel TEID or the subscriber IP address. To cover the wireline case, further extensions are required to describe the endpoint.

Table 20: 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**
Reused 3GPP IEs below			
MAC address	C	If present, this IE MUST be used to identify the MAC address of the traffic endpoint. (see 3GPP TS 29.244 [23] for IE details)	MAC address
C-Tag	C	If present, this IE MUST be used to identify the customer VLAN Tag of the traffic endpoint (see 3GPP TS 29.244 [23] for IE details)	C-Tag
S-Tag	C	If present, this IE MUST be used identify the service VLAN Tag of the traffic endpoint (see 3GPP TS 29.244 [23] for IE details)	S-Tag
BBF Extended IEs below			
Logical Port	C	If present, this IE MUST be used to provide an opaque value obtained from the NSH header to indicate the logical port for the subscriber. (see section 6.6.2 for IE details)	**Logical port** Details in section 6.6.2
PPPoE Session ID	C	If present, this IE MUST be used to identify the PPPoE session ID of the subscriber. (see section 6.6.5 for IE details)	**PPPoE Session ID** Details in section 6.6.5
L2TP tunnel	C	If present, this IE MUST be present if a L2TP tunnel is required. (see section 6.5.8 for IE details)	**L2TP Tunnel** Details in section 6.5.8

6.5.6 PFCP Session Modification Request

In the case where PPP LCP connectivity is required for the subscriber session, this IE is included in the PFCP session establishment modification message.

Table 21: BBF extended Information Element(s) in a PFCP Session Modification Request

Information element	P	Condition / Comment	IE Type
PPP LCP connectivity	**C**	This IE MUST be present if periodic LCP echo hello is required.	**PPP LCP connectivity** Details in section 6.5.7

6.5.6.1 Update PDR

The Update PDR grouped IE should include BBF Outer Header Removal to remove various wireline encapsulations.

Table 22: BBF extended Update PDR IE(s) within PFCP Session Modification Request

Octet 1 and 2	Update PDR IE Type = 9 (decimal)		
Octets 3 and 4	Length = n		
Information element	**P**	**Condition / Comment**	**IE Type**
BBF Outer Header Removal	C	This IE MUST be present if the DBNG-UP function is required to remove header(s) from the packets matching this PDR. This IE MUST be present if it needs to be changed.	**BBF Outer Header Removal** Details in section 6.6.4

6.5.6.2 Update Forwarding Parameters

The Update forwarding Parameters IE in FAR can include the BBF Outer Header Creation IE and the MTU IE. The BBF Outer Header Creation IE is used to encapsulate the subscriber data packet in various wireline encapsulation. The MTU IE is primarily used in the case of PPPoE.

Table 23: BBF extended Update Forwarding Parameters IE(s) in FAR

Octet 1 and 2	Update Forwarding Parameters IE Type = 11 (decimal)		
Octets 3 and 4	Length = n		
Information element	**P**	**Condition / Comment**	**IE Type**
BBF Outer Header Creation	C	This IE MUST be present if the DBNG-UP function is required to add outer header(s) to the outgoing packet. This IE MUST only be provided if it is changed.	**BBF Outer Header Creation** Details in section 6.6.3
MTU	C	This IE MUST be present to enforce an MTU on outgoing packets. In the case of PPPoE, this may be based on negotiated MRU value. This IE MUST only be provided if it is changed.	**MTU** Details in section 6.6.9

6.5.6.3 Update Traffic Endpoint IE

The Update Traffic Endpoint IE require addition IEs such as MAC address and BBF extended IE such as PPPoE session ID to be able to match more wireline encapsulations.

Table 24: BBF extended update Traffic Endpoint IE(s) within PFCP Session Modification 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**
Reused 3GPP IEs below			
MAC address	C	If present, this IE MUST be used to identify the MAC address of the traffic endpoint and needs to be changed. (see 3GPP TS 29.244 [23] for IE details) This IE MUST only be provided if it is changed.	MAC address
C-Tag	C	If present, this IE MUST be used to identify the customer VLAN Tag of the traffic endpoint and needs to be changed (see 3GPP TS 29.244 [23] for IE details) This IE MUST only be provided if it is changed.	C-Tag
S-Tag	C	If present, this IE MUST be used to identify the service VLAN Tag of the traffic endpoint and needs to be changed (see 3GPP TS 29.244 [23] for IE details) This IE MUST only be provided if it is changed.	S-Tag
BBF Extended IEs below			
Logical Port	C	If present, this IE MUST be used to provide an opaque value obtained from the NSH header to indicate the logical port for the subscriber and needs to be changed. (see section 6.6.2 for IE details)	**Logical port** Details in section 6.6.2
PPPoE Session ID	C	If present, this IE MUST be used to identify the PPPoE session ID of the subscriber and needs to be changed. (see section 6.6.5 for IE details)	**PPPoE Session ID** Details in section 6.6.5
L2TP tunnel	C	If present, this IE MUST be used to identify if L2TP tunnel is required and needs to be changed. (see section 6.5.8 for IE details)	**L2TP tunnel** Details in section 6.5.8

6.5.7 PPP LCP Connectivity

The table below is a new BBF specified grouped IE used to specify PPP LCP connectivity check parameters.

In the case where LCP echo hello is offloaded on the DBNG-UP, the LCP echo hellos MUST not be redirected to the DBNG-CP.

Table 25: PPP LCP Connectivity

Octet 1 and 2	PPP LCP Connectivity IE Type = 32780		
Octets 3 and 4	Length = n		
Octets 5 and 6	Enterprise ID 3561		
Information elements	**P**	**Condition / Comment**	**IE Type**
Traffic Endpoint ID	M	Identifies the context on which connectivity verification must be performed.	Traffic Endpoint ID
Verification Timers	C	This IE MUST be used to indicate the frequency and number of retries for verification messages. If this IE is not present, no periodic verification is started.	**Verification Timers** Details in section 6.6.7
PPP LCP Magic Number	C	If present this IE MUST be used to indicate which magic number to use when generating keepalives and which magic number to verify incoming keepalives against.	**PPP LCP Magic Number** Details in section 6.6.8

6.5.8 L2TP Tunnel

In the case where L2TP tunnel required for the subscriber session, this IE is included.

Table 26: L2TP Tunnel

Octet 1 and 2	L2TP Tunnel IE Type = 32781		
Octets 3 and 4	Length = n		
Octets 5 and 6	Enterprise ID 3561		
Information elements	**P**	**Condition / Comment**	**IE Type**
L2TP tunnel endpoint	C	If present, this IE MUST be used to identify the L2TP tunnel ID and IP information. (see section 6.6.10 for IE details)	**L2TP Tunnel Endpoint** Details in section 6.6.10
L2TP Session ID	C	If present, this IE MUST be used to identify the L2TP session ID. (see section 6.6.11 for IE details)	**L2TP session ID** Details in section 6.6.11

6.6 BBF PFCP IE extensions

This section highlights required IE extensions to cover MS-BNG use cases. Please refer to 3GPP TS 29.244 [23] section 8.1.1 for further information vendor specific extensions. Below is the 3GPP specified IE format for Vendor Specific IE.

Figure 35 depicts the format of a vendor-specific Information Element, which content is not specified and the IE Type value MUST be within the range of 32768 to 65535. From m to (m+4) are octets which can be defined by BBF for future uses.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = xxx (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID							
7 to (n+4)	IE specific data or content of a grouped IE							
m to (m+4)	These octet(s) is/are present only if explicitly specified							

Figure 35: 3GPP Vendor-Specific Information Element Format Reference

6.6.1 BBF UP Function Features

The BBF UP Function Features IE indicates the features supported by the DBNG-UP function and MUST be coded as depicted in Figure 36.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32768							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	Supported-Features							
9 to 10	Additional Supported-Features 1							
11 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 36: BBF UP Function Features

The BBF UP Function Features IE takes the form of a bitmask where each bit set indicates that the corresponding feature is supported. Undefined bits MUST be set to zero by senders and MUST be ignored by the receiver.

Supported-Features

When present, MUST be encoded as Table 27 which specifies the features defined on the DBNG-UP.

Table 27: BBF UP Function Features

Feature Octet / Bit	Feature	Description
7/1	PPPoE	Informs the DBNG-CP that the DBNG-UP supports PPPoE
7/2	IPoE	Informs the DBNG-CP that the DBNG-UP supports IPoE
7/3	LAC	Informs the DBNG-CP that the DBNG-UP supports LAC
7/4	LNS	Informs the DBNG-CP that the DBNG-UP supports LAC
7/5	LCP keepalive offload	Informs the DBNG-CP that the DBNG-UP supports PPP LCP echo

Note: For IPoE, PPPoE, LAC, and LNS, both IPv4 and IPv6 are supported

6.6.2 Logical Port

The Logical Port IE MUST be encoded as Figure 37.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32769							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to n+4	logical-port-id							

Figure 37: Logical Port

Logical-port-id

Encode a logical-port-id, which is an opaque value to indicate the logical port on which Ethernet traffic is received. This should not contain S-Tag or C-Tag values, which are signaled more explicitly in PFCP described in 3GPP TS 29.244 [23].

6.6.3 BBF Outer Header Creation

The BBF Outer Header Creation indicates a header is to be added to the packet before forwarding and MUST be coded as depicted in Figure 38. The BBF Outer Header also contains parameters to construct the header. This IE can be used in combination with the Outer Header Creation IE. If both are present, both headers are added, the 'Outer Header Creation IE' will be the top header and "BBF Outer Header" will be the next (lower) header.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32770							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	BBF Outer Header Creation Description							
9 to 10	Tunnel ID							
11 to 12	Session ID							
13 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 38: BBF Outer Header Creation

BBF Outer Header Creation Description

When present, MUST be encoded as specified in Table 28. It takes the form of a bitmask where each bit indicates the outer header to be created in the outgoing packet. Undefined bits MUST be zeroed on transmission and MUST be ignored by the receiver.

Table 28: BBF Outer Header Creation Description

Octet/bit	Outer Header to be created in the outgoing packet
7/1	CPR-NSH
7/2	Traffic-Endpoint
7/3	L2TP
7/4	PPP

Note: At least one bit of the Outer Header Creation Description field MUST be set to 1.

- CPR-NSH: An NSH header defined in RFC 8300 [41] will be attached to the control packet, which contains meta data for the logical port. The NSH encapsulated control packet tunneled over a GTP-u tunnel utilizing the IE Outer Header Creation. For more information on NSH, please look at section 6.6.3.1.
- Traffic-Endpoint: The header creation for the packet will be based on the IE Linked Traffic Endpoint within the same FAR. Further detail:
  - This is used for layer 2 traffic forwarding. The traffic endpoint specified must contain a logical port and a MAC address. Optionally, the traffic endpoint can also contain S-Tag, C-Tag and PPPoE Session ID. Note: The Linked Traffic Endpoint always refer to traffic endpoint that flows in the opposite direction, therefore the source and destination MAC address must always be swapped when reconstructing the Ethernet header.
- L2TP – Creates the L2TP header with indicated tunnel ID and session ID. For LAC, this is used to encapsulate the PPP packet with a L2TP header before forwarding to LNS. For LNS, this is used in combination with PPP to encapsulate the IP packet with both PPP and L2TP before forwarding to the LAC.
- PPP – Creates the PPP data packet header.

Tunnel ID

Indicates the L2TP Tunnel ID

Session ID

Indicates the L2TP Session ID

6.6.3.1 NSH header information

In order to signal the logical port and the local DBNG-UP port MAC, Ethernet packets will be encapsulated using an MD-type 2 NSH header as defined in RFC 8300 [41]. This header is shown in Figure 39.

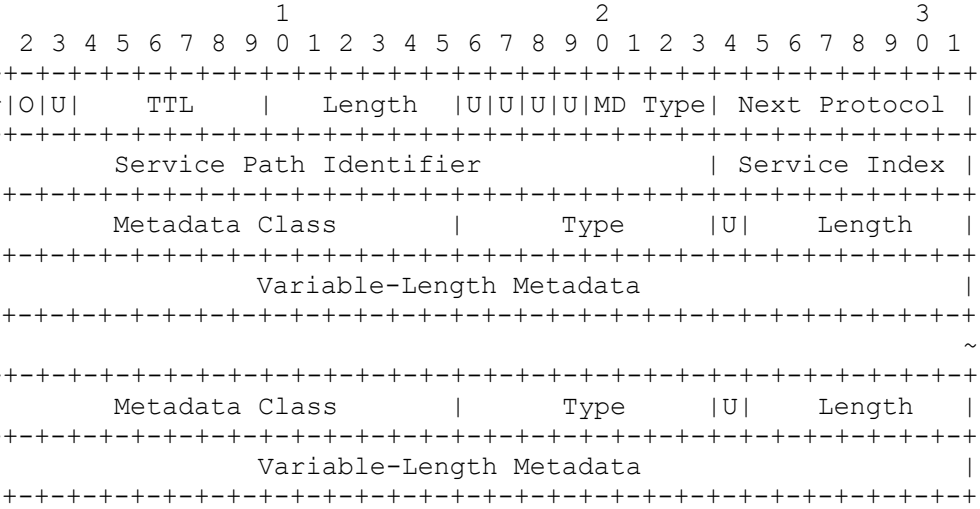

Figure 39: NSH header information

Where OAM MUST be set to 0, TTL MUST be set to 1, MD Type MUST be set to 2 and Next Protocol MUST be set to 0x3 (Ethernet). Service Path Identifier is initially not used and MUST be set always to 0, Service Index MUST be set to 255. Version and (NSH) length are per RFC 8300 [41].

Specific Metadata types and information:

- Metadata Class = 0x0200
- Logical port (Type=0, Length=N): an opaque byte string identifying an access context on a DBNG-UP (e.g. port, lag, Ethernet tunnel, …)
- MAC (Type=1, Length=6): The local DBNG-UP MAC associated with the logical port

6.6.4 BBF Outer Header Removal

The BBF Outer Header Removal IE MUST be encoded as Figure 40:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32771							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7	BBF Outer Header Removal Description							
8 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 40: BBF Outer Header Removal

BBF Outer Header Removal Description

This field MUST be an 8-bit unsigned integer and indicates which headers need to be removed from an incoming packet. The values are as defined as follows:

Table 29: 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

- Ethernet: Removes the Ethernet header including S-Tags and C-Tags.
- PPPoE / Ethernet: Removes the PPP header and Ethernet header including S-Tags and C-Tags.
- PPP / PPPoE/ Ethernet: Removes the PPP header, the PPPoE header, and the Ethernet header including S-Tags and C-Tags.
- L2TP: Removes only the L2TP header
- PPP/L2TP: Removes the PPP and the L2TP header together.

6.6.5 PPPoE Session ID

The PPPoE Session ID IE MUST be encoded as Figure 41.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32772							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	PPPoE Session ID							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 41: PPPoE Session ID

PPPoE Session ID

Encode a PPPoE Session ID as specified in RFC 2516 [29].

6.6.6 PPP Protocol

The PPP Protocol IE MUST be encoded as Figure 42.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32773							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7	Spare					control	data	specific
8 to 9	protocol							
10 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 42: PPP Protocol

Exactly one flag MUST be set in octet 7. If more than one bit is set, this is an error and is handled according to 3GPP TS 29.244 [23] section 7.6

specific

Indicates a specific protocol value must be matched, further specified in the IE

data
Indicates any protocol value where the most significant bit equals zero, as per RFC 1661.

control
Indicates any protocol value where the most significant bit equals one, as per RFC 1661.

protocol
Octets “8 to 9” are only present if the specific bit is set and encode a valid PPP protocol value as assigned by IANA.

Spare bits MUST be set to zero by senders and MUST be ignored by the receiver.

6.6.7 Verification Timers

The Verification Timers IE MUST be encoded as Figure 43.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32774							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	interval							
9	count							
10 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 43: Verification Timers

interval
Specify an unsigned 16-bit interval in 10 milli-seconds that indicates how frequent the verification procedure is started.

count
Specifies an unsigned 8-bit integer on how many unanswered consecutive keepalive messages should be sent before connection is considered down.

6.6.8 PPP LCP Magic Number

The PPPoE LCP Magic Number IE MUST be encoded as Figure 44.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32775							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 10	Tx Magic Number							
11 to 14	Rx Magic Number							
15 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 44: PPP LCP Magic Number

Tx Magic Number
Encode a PPP LCP Magic Number as defined in RFC 1661 [27]. This is the magic number used when transmitting LCP keepalive messages.

Rx Magic Number

Only present if length >=10 and encode a PPP LCP Magic Number as defined in RFC 1661 [27]. When present, received LCP keepalive messages need to verify against this magic number. When not present (length < 10), magic numbers are not verified.

6.6.9 MTU

This IE MUST be encoded as indicated in Figure 45.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32776							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	MTU value							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 45: MTU

MTU

The MTU MUST be encoded as an unsigned 16-bit integer value. Packets exceeding the MTU must either be fragmented (IPv4 without DF bit set RFC 791 [26]) or answered with an ICMP/ICMPv6 “Packet Too Big” error code (IPv4 with DF bit set RFC 791 [26], IPv6 RFC4443 [35]). MTU is applied on IP level, before any outer header or Ethernet encapsulation. A UP may apply a lower MTU if the associated forwarding construct requires so.

Note: The system MUST have a mechanism to control the rate of sending of ICMP Error Messages.

6.6.10 L2TP Tunnel Endpoint

This IE MUST be encoded as Figure 46.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32777							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7						CH	v6	v4
8 to 9	Tunnel ID							
10 to 13	IPv4 Address							
14 to 29	IPv6 Address							
30 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 46: L2TP Tunnel Endpoint

Flags v4, v6, and CH are mutually exclusive.

v4

Indicates an IPv4 address is included

v6

Indicates an IPv6 address is included

CH

Indicates no IP is included and the DBNG-CP function sets the CHOOSE (CH) bit to 1 if the DBNG-UP function supports the allocation of L2TP tunnel IP address and the DBNG-CP function requests the DBNG-UP function to assign the L2TP tunnel IP to the Traffic Endpoint.

Tunnel ID
Specifies the L2TP tunnel ID to match

IPv4 address
Specifies the L2TP IPv4 local terminating address

IPv6 address
Specifies the L2TP IPv6 local terminating address

6.6.11 L2TP Session ID

This IE MUST be encoded as specified in Figure 47.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32778							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	L2TP Session ID							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 47: L2TP Session ID

L2TP session ID
Specifies the L2TP session ID to match

6.6.12 L2TP type

This IE MUST be encoded as specified in Figure 48.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32779							
3 to 4	Length = n							
5 to 6	Enterprise ID 3561							
7 to 8	Spare							T
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 48: L2TP type

T
Identifies the l2tp type, 0 means l2tp data and 1 means l2tp control (RFC 2661 [30])

Spare bits MUST be set to zero by senders and MUST be ignored by the receiver.

Annex A: Use Cases

A.1 Multi-access MS-BNG CUPS use case

Since TR-101 [4], the MS-BNG has evolved beyond basic broadband wireline access. The MS-BNG has enabled broadband services to be served over multiple access types which includes, fixed line users, hybrid access, and even public Wi-Fi. Figure 49 depicts a multiple server MS-BNG serving multiple access. Each "box" below represents a single physical network element. The redundancy mechanism within a single physical network element is out of the scope of this use case.

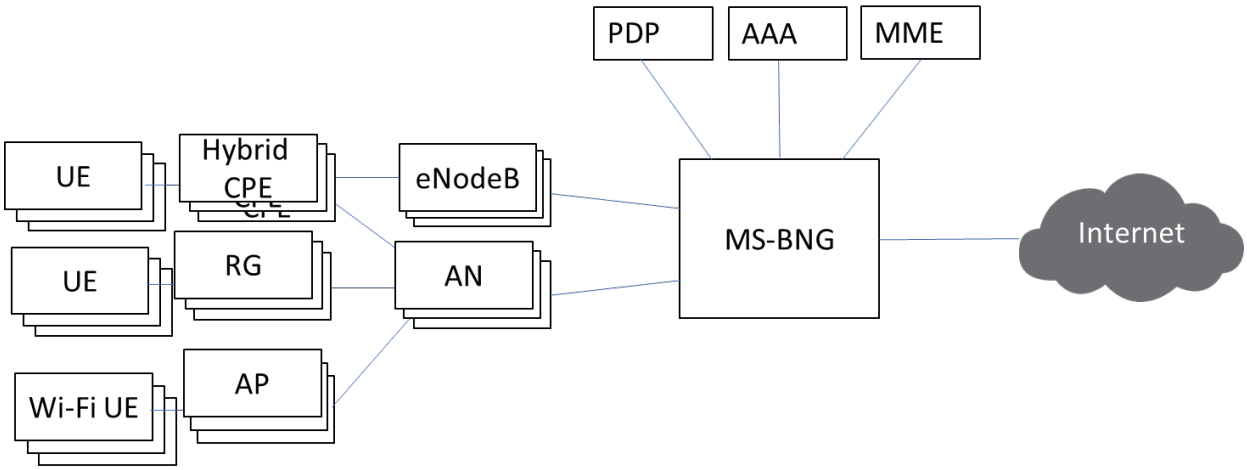

Figure 49: Multi-access MS-BNG

As subscribers scale and bandwidth scale increased, traditionally, this required introducing a new MS-BNG into the network. The new MS-BNG is a separate entity and requires separate commissioning.

BNG control and user plane separation addresses:

- Supporting increase of subscribers
- Supporting new types of subscribers connecting to the multi-access MS-BNG for broadband services enabled by new access technologies.

BNG CUPS simplifies in scaling up both subscribers and bandwidth. The CUPS architecture must allow the service provider to either an increase the scaling of DBNG-CP for subscriber independent of the DBNG-UP. And vice versa, as more bandwidth is required, the DBNG-UP can be increased independent of the DBNG-CP. Please note that although DBNG-CP and DBNG-UP scaling can be increased independently, increase of either element requires a proportional increase of the other. The DBNG-CP provides a single point of management for all User Plane instances. The DBNG architecture shown in Figure 50 must continue to offer the same number of functions as today's MS-BNGs deployed in production networks.

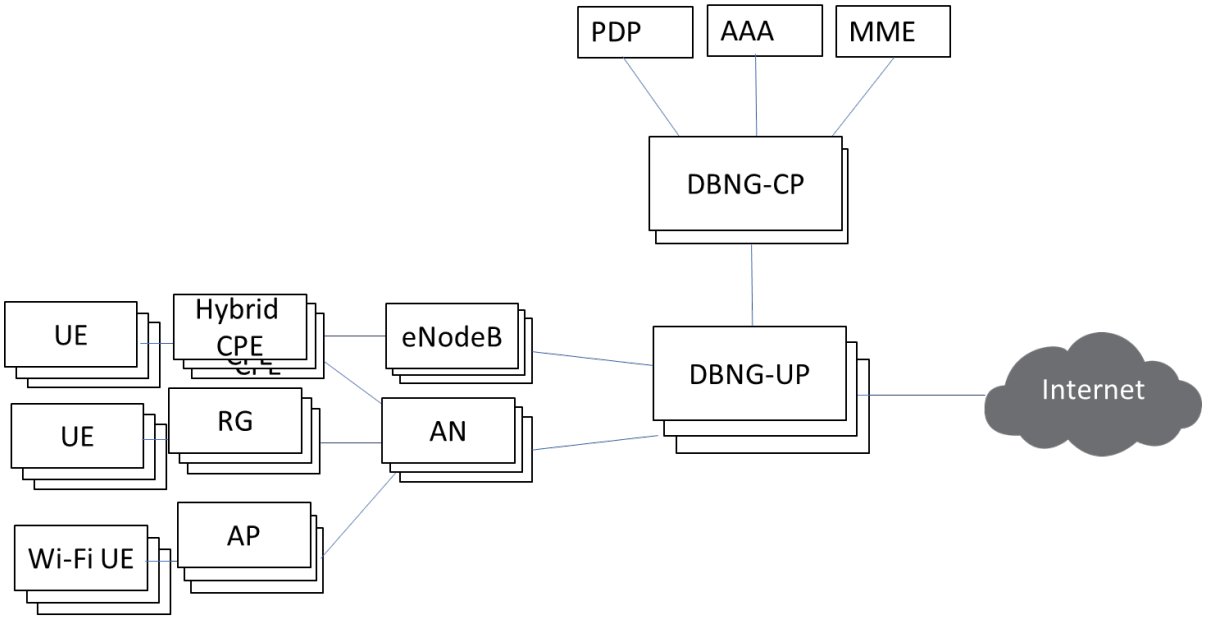

Figure 50: Multi-access DBNG

A.2 Wireline-Access disaggregated MS-BNG use case

From the perspective of wireline access services, it consists of residential subscriber access service and enterprise access service. Residential subscriber access services include HSI, IPTV multicast, VoIP, IMS (TR-69 [3]), and enterprise subscriber access service is usually a leased line service. The subscriber dials up through the access network, and MS-BNG User Plane redirects the access control packets to MS-BNG Control Plane which authenticates the subscriber and creates subscriber forwarding entries upon which MS-BNG User Plane forwards the subscriber data traffic. Usually after the completion of the subscriber access procedure, MS-BNG needs to do network address translation for the subscriber, both native IP and MPLS VPN could be the underlying technologies for MS-BNG network-side data traffic forwarding.
The typical wireline access service scenarios include IPTV multicast, CGN, L2TP, and LI with access types of PPPoE, L2/L3 IPoE, dual-stack IPoE, L2-line, L3-line, L2TP, L2VPN（VLL/VPLS), and etc.
Address management will require special considerationwhen the MS-BNG control plane and use plane function are separated.

A.3 Data-trigger service use case

This type of service is common amongst enterprise customers who are provided static IP address. These static IP addresses are statically configured on CPE. Therefore, DHCP or PPPoE address request is not required. In this use case, the MS-BNG will verify the subscriber based on the data packet (e.g Ethernet and IP header) and optionally other physical attributes (e.g. NAS port and NAS port ID). For this document, this use case will be referred to as data-trigger service where the DBNG-CP verification is triggered by the subscriber data packet. In the DBNG case, the subscriber data packet is the control packet and will be redirected by the DBNG-UP to the DBNG-CP for verification.

A.4 Wholesale Retail model with L2TP use case

As shown in Figure 51, the RG initiates PPPoE negotiation with the DBNG-CP, where the DBNG-CP cannot determine if the user should be terminated locally or tunnel through L2TP until authorization. The PPPoE packets are sent by the DBNG-UP to the DBNG-CP via the general CPR interface (tunnel). Once the DBNG-UP and DBNG-CP complete PPP LCP and PPP authentication, it is determined that this particular subscriber **session** is to be tunneled through L2TP. The DBNG-CP must initiate a L2TP tunnel/session with

the LNS, via the A10 interface. The DBNG-CP initiates the SCCRQ via the (subscriber-specific) packet redirect tunnel to the DBNG-UP, which would forward the packet out the A10 interface. Similarly, remaining SCCRP, SCCCN, ICRQ, ICRP, ICCN control packets are exchanged between the DBNG-CP through the DBNG-UP towards the LNS (via the A10). It should be noted that at any point in time, the session forwarding state can be updated for example due to bandwidth changes as specified in RFC 5515 [36]. Upon tunnel set-up completion, the DBNG-CP must be able to signal an update to the DBNG-UP to forward all packets from the RG directly to the A10 (via the DBNG-UP) without DBNG-CP involvement. The remaining, PPP NCP, LCP echo requests/responses, ND, RA, DHCPv6, etc. are all forwarded without DBNG-CP involvement. It is important that a single subscriber can have more than one PPPoE service, only some of which are offered by retailers. Therefore, not all PPPoE sessions are to be redirected to the LNS.

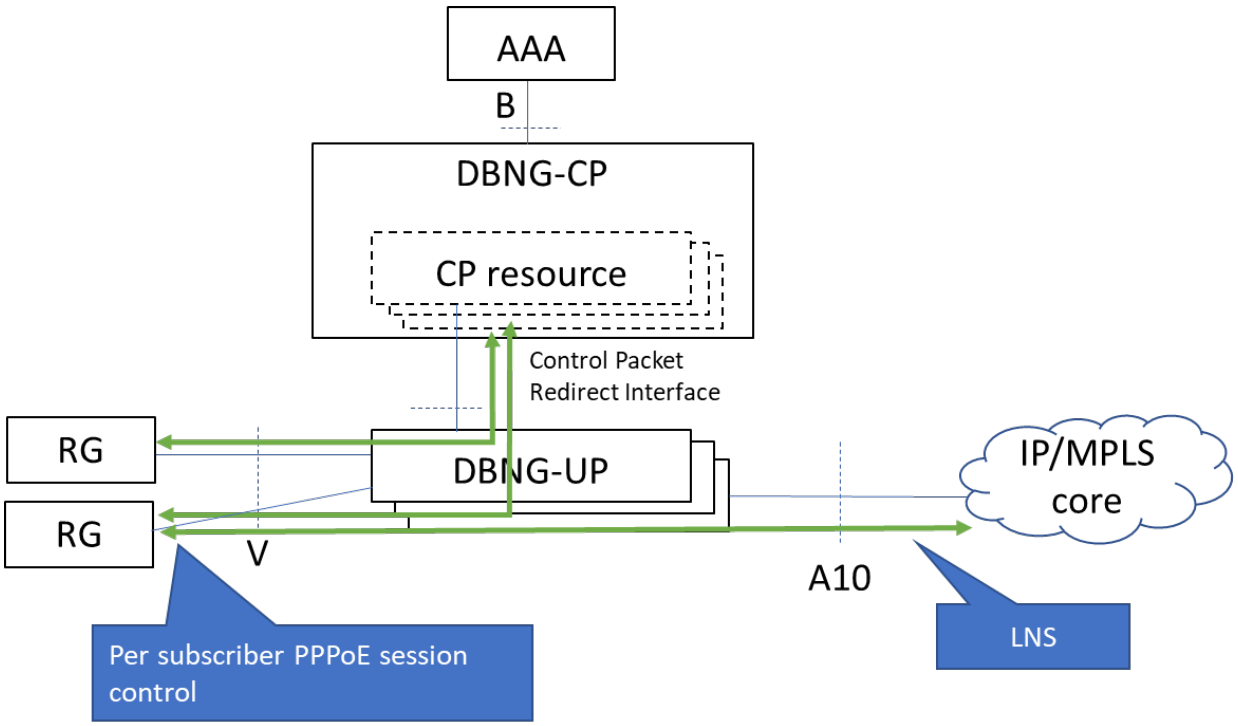

Figure 51: L2TP deployment model

End of Broadband Forum Technical Report TR-459