Working Text

Draft
CONTRIB-21341

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

Revision: 0.09
Revision Date: Nov 2019

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Working Text is a draft, is subject to change, and has not been approved by members of the Forum. This Working Text is copyrighted by the Broadband Forum, and portions of this Working Text may be copyrighted by Broadband Forum members. This Working Text is for use by Broadband Forum members only. Advance written permission by the Broadband Forum is required for distribution of this Working Text in its entirety or in portions outside the Broadband Forum.

Intellectual Property

Recipients of this document 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 Working Text if it were to be adopted as a Technical Report, and to provide supporting documentation.

Terms of Use

This Working Text (i) is made available to non-members for internal study purposes only, (ii) may be implemented by Broadband Forum members in a product or service made commercially available, and (iii) may only be copied and distributed internally for the purpose of exercising Broadband Forum membership rights and benefits.

Confidentiality

All materials submitted for possible incorporation into Technical Reports or other work product shall be regarded as confidential until such time as the Technical Report or other work product in question is publicly released. In the event that any material, or portion of any material, is not included in the Technical Report or other work product in question, or if such Technical Report or other work product is never publicly released, such material shall remain confidential until such time, if ever, as the submitter makes the same publicly available, or it otherwise becomes publicly disclosed other than by a breach of a Member's obligations under this Confidentiality Policy. Member representatives shall have access to confidential materials in such manner as may from time to time be provided in Broadband Forum's procedural rules, and shall not copy or further distribute such materials, except internally, to the extent necessary to exercise their participation rights as Members.

THIS Working Text IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS Working Text SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS Working Text.

The text of this notice must be included in all copies of this Working Text.

Revision History

Revision Number	Revision Date	Revision Editor	Changes
0.01	Mar 2019	Kenneth Wan, Nokia	Added CONTRIB-21317 Added CONTRIB-21318 Added CONTRIB-21319 Added CONTRIB-21320 Added CONTRIB-21321 Added CONTRIB-21322 Added CONTRIB-21323
0.02	May 2019	Kenneth Wan, Nokia	Added CONTRIB-21266 Added CONTRIB-21363 Added CONTRIB-21364
0.03	Jun 2019	Kenneth Wan, Nokia	Added CONTRIB-21412
0.04	Aug 2019	Kenneth Wan, Nokia	Added CONTRIB-21403 Added CONTRIB-21415 Added CONTRIB-21369 Added CONTRIB-21367 Added CONTRIB-21413 Added CONTRIB-21445
0.05	Aug 2019	Kenneth Wan, Nokia	Added CONTRIB-21496 Added CONTRIB-21572 Added CONTRIB-21569 Added CONTRIB-21597 Added CONTRIB-21595
0.06	Sep 2019	Kenneth Wan, Nokia	Added CONTRIB-21645 Added CONTRIB-21595 Added CONTRIB-21533 Added CONTRIB-21618 Added CONTRIB-21366 Added CONTRIB-21610 Added CONTRIB-21423
0.07	Oct 2019	Kenneth Wan, Nokia	Added CONTRIB-21756 Added CONTRIB-21760 Added CONTRIB-21758 Added CONTRIB-21764 Added CONTRIB-21765 Added CONTRIB-21766 Added CONTRIB-21767
0.08	Nov 2019	Kenneth Wan, Nokia	Added CONTRIB-21799 Added CONTRIB-21780 Added CONTRIB-21768 Added CONTRIB-21769 Added CONTRIB-21801 Added CONTRIB-21803 Added CONTRIB-21780 Added CONTRIB-21805 Added CONTRIB-21084
0.09	Nov 2019	Kenneth Wan, Nokia	Revision number change

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

Editor: Kenneth Wan, Nokia

Work Area Director(s): David Sinicrope, Ericsson

Project Stream Leader(s):

Table of Contents

Table of Figures

Table of Tables

Executive Summary

The summary section provides a brief overview of the purpose, scope, and contents of the Working Text.

1 Purpose and Scope

The Purpose and Scope sections MUST be included in the Working Text in some form.

> **Note:** Each new section with Heading 1 style begins on a new page.

1.1 Purpose

This Working Text specifies the architecture and requirements for a control and user plane separation of a disaggregated BNG. The architecture will consist of separating BNG functions either to the control plane or user plane and defining the interfaces associated to a disaggregated BNG. Requirements on interfaces and protocols will ensure interoperability between various types of control planes and user planes deployments. From the interface and protocol identified, high level information models will be defined. Use cases and deployment scenarios will be also be captured in this working text. The goal is to ensure that even with BNG control plane and user plane separated, the same broadband service offerings are provided. In addition, new capabilities such as independent user plane and control plane scaling, independent control and user plane life cycle management, and 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 information exchange:

- Session Types:
  - TR-146 (PPPoEv4 and PPPoEv6, IPoEv4 and IPoEv6)
- Access side interfaces and protocols
  - TR-25 V-interface (context LAC, LNS, PTA)
  - TR-101 V-interface (PPPoE, 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)
  - WT-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, PDP
  - TR-300 Accounting and charging
  - WT-378 S11 (GTP-c),
- QoS functions
  - TR-59 DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services
  - TR-101 Migration to Eth 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 Eth 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
  - Multicast IPTV 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 BNG control plane and user plane separation
- Deployment models for BNG control plane and user plane separations
- Create an architectural reference picture of the functional blocks in the BNG, showing disaggregated control plane and user plane with their respective interfaces. A high-level network architecture to support BNG control plane and user plane disaggregation
  - Specify interface(s) between BNG control plane and user plane
- Functional requirements of both the control plane and user plane (with references to appropriate TR/WTs)
  - Includes both control plane and user plane resiliency
- Specify a protocol for control plane and user plane separation for each of the defined interface.
- To define information model exchanged between control plane and user plane interfaces
- Subscriber Management
- Policy Management
- Accounting
- Management architecture of user planes from the control plane

Out of scope:

- Further disaggregation of BNG functions beyond control plane and user plane separation.
  - 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. In addition, requirements for protocol extension are within scope of this project.
- TR 317, as the architecture is more aligned with RG architecture than the BNG.
- 3GPP have already produce technical specifications on PGW control plane and user plane separation. This project will reuse 3GPP PGW defined TS and reuse 3GPP PGW CUPS TS.

2 References and Terminology

2.1 Conventions

In this Working Text, 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 [5].

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

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

Document	Title	Source	Year
[1] TR-069 Amendment 4	CPE WAN Management Protocol	BBF	2011
[2] TR-101 Issue 2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[3] G.992.1	ADSL Transceivers	ITU-T	1998
[4] 802.3	CSMA/CD access method and physical layer specifications	IEEE	2005
[5] RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997

Note: Each cell in column 1 is a Numbered Reference (Paragraph→Bullets and Numbering). BBF documents should be listed first. Within the SDO group, documents should be listed alphabetically. Use the Insert Row command to add rows as appropriate. To reference within the body of the Working Text, use the command Insert→Cross-reference.

2.3 Definitions

The following terminology is used throughout this Working Text.

ACS Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.

ATSC Advanced Television Systems Committee. Digital television standards, primarily adopted in North America.

CPE Customer Premises Equipment.

WLAN Wireless Local Area Network.

Working Instance An instance of DBNG, whether CP or DBNG-UP, that maintains both the current configuration and operational state.

Protecting Instance An instance that has been assigned to a particular working instance or a group of working instances.

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.

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.

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.

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)

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.

2.4 Abbreviations

This Working Text uses the following abbreviations:

BNG	Broadband Network Gateway
CPRi	Control Packet Redirect interface
CPE	Customer Premises Equipment
CUPS	Control and User Plane separations
DBNG	Disaggregated BNG
DBNG-CP	Disaggregated BNG Control Plane
DBNG-UP	Disaggregated BNG User Plane

HAG	Hybrid Access Gateway
Mi	Management interface
SCi	State Control interface
TR	Technical Report
WA	Work Area
WLAN	Wireless Local Area Network
WT	Working Text

3 Working Text Impact

3.1 Energy Efficiency

Energy Efficiency maybe impacted migrating from standalone BNG to DBNG. DBNG allows dynamical 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 a deployment factors such as power per node, geo dispersion of user plane, and user 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 is out-of-scope for this document.

3.2 Security

This section MUST be included.

This section will discuss the relevant security issues pertaining to this Working Text. References to other sections of the Working Text may be included here.

If the Working Text has no impact on Security, the following statement may be used: WT-459 has no impact on security.

3.3 Privacy

This section MUST be included.

This section will discuss any ways the Working Text affects privacy.

If the Working Text has no impact on Privacy, the following statement may be used: WT-459 has no impact on energy privacy.

4 Introduction

Editor's note: introduce function definition (or mapping) or what functions goes where. Ex, where does routing live.

BNG is an essential device that grants subscribers access to the internet. It provides critical subscriber management functions, such as: authentication, IP address assignment, bandwidth allocation, and accounting. The BNG is also a multi-access edge device terminating services from access types including: fixed wireline, fixed wireless, public Wi-Fi, and hybrid access.

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

- Over-utilizing a BNG
- Under-utilizing a BNG
- Operation challenge in managing and maintaining a geographically distributed BNG deployment
- Service provisioning across all BNGs and time to market new services

The Disaggregated BNG (DBNG) tackle these challenges by separates the subscriber management control plane (CP) and user plane (UP). DBNG allows individual scaling of the control plane the user plane to keep up with subscriber growth and subscriber bandwidth demands. The CUPS architecture also simplifies operations by maintaining a single user interface on the CP to manage all UPs.

This TR provides the architecture, requirements, and call flows of a DBNG. In addition, DBNG state control interface utilizes 3GPP defined Packet Forwarding Control Protocol (PFCP) for programming subscriber forwarding state. Section 6 provides the PFCP information exchanges for typical BNG use cases and PFCP IE extensions required to support wireline use cases.

4.1 BNG Functional Architecture

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

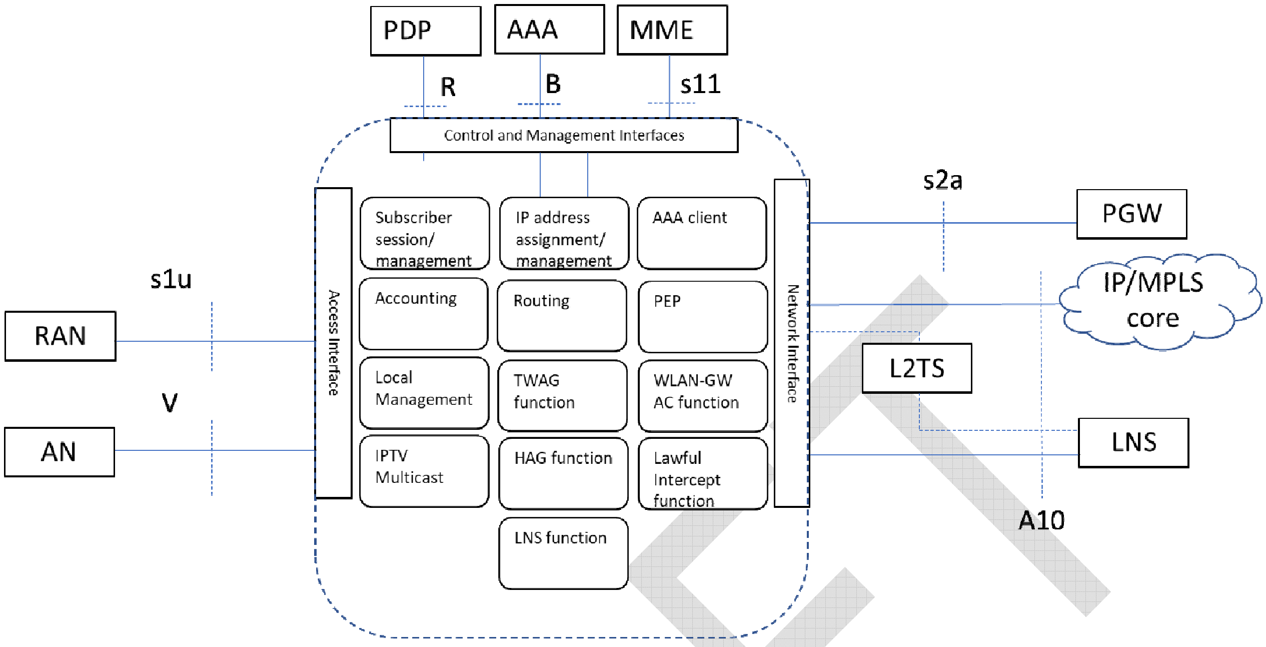


Figure 1: Functions and interfaces of a BNG

4.1.1 BNG Functions

BNG provide subscriber management by utilizing different functional blocks: AAA authentication, IP address assignment, policy enforcement, and accounting. With these functional blocks the BNG offers subscriber managed broadband service. The BNG further integrate other functional blocks to provide enhanced broadband service such as TWAG and HAG. Table 1 lists the functional blocks within the BNG:

Functions	TR	TR function support
Subscriber session termination	TR-145, TR-25	IPoE and PPPoE session L2TP LAC session
IP address assignment and management	TR-101, TR-177, TR-178, TR-187, TR-341	IP address/prefix assignment through DHCPv4, DHCP6, SLAAC, PPPoE, DHCPv6oPPPoE, and SLAACoPPPoE
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	TR-101, TR-177, TR-	Subscriber filters and QoS rules

Point	178, TR-187, TR-134, TR-300, TR-341	
Multicast IPTV	TR-101, TR-177, TR-178, TR-187, TR-134, TR-300	Subscriber IGMP/MLD processing
WLAN-GW AC function	TR-321	Access controller for AP management
TWAG function	TR-291	Hands off broadband access to 3GPP
HAG function	TR-384	Hybrid access
Routing	TR-101, TR-177, TR-178, TR-187	IGP, BGP, MPLS, PIM
Lawful Intercept	TR-178	Mirroring
Local Management		Local User Interface

Table 1: Functional Blocks of a BNG

4.1.2 BNG Interfaces

The following interfaces are defined in BBF various TRs:

- V-interface: Defined in TR-101 as the Ethernet interface between the Access Node and the Broadband Network Gateway (BNG). Further, it provides the following capabilities: traffic aggregation, class of service distinction, and user isolation and traceability
- A10-interface: Defined in TR-25 as the interface between the Regional Broadband network and the network service provider POPs.
- R-interface: Defined in TR-134 as the interface between the Policy Enforcement Point and the Policy Decision Point. The Policy Enforcement Point is a function integrated into the BNG.
- B-interface: Defined in TR-134 as the interface between the Policy Enforcement Point and the AAA server. The PEP is a function integrated in the BNG, where it can receive/activate/modify/delete policies from AAA server.
- s1u: Defined in TR-378, the interface between the eNodeB to HAG as per 3GPP TS23.002
- s11: Defined in TR-378, interface from the 3GPP MME to the HAG.
- s2a: Defined in TR-291, as the reference point between the Trusted WLAN Access Gateway (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 BNG terminates various access types such as broadband and mobile connection. Table 2 specifies the access interface cross referenced to relevant TR and the protocol stacks by the BNG function.

Interface	TR	Protocol Stack	TR defined function with respect to the access interface
V	TR-25, TR-101	IPoEv4, PPPoEv4	Ethernet based BNG terminates PPPoE and IPoEv4 sessions. And PPPoE for LAC.
V	TR-177	IPoEv6	Based on TR-101, the BNG terminates IPoEv6 sessions
V	TR-178	PPPoEv4, IPoEv4,	Based on TR-101, the MS-BNG terminates IPoMPLS

		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 WiFi 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, terminates PPPoE, GTP, and IPoE sessions

Table 2: BNG access interfaces

The network interface on the BNG connects subscriber IPoE or PPPoE session to the network core in most cases providing broadband services. As highlighted in the diagram, the network interface also provides connectivity to wholesaler service via L2TP or via MPLS. In addition, broadband service can also be connected to the 3GPP core network. Table 3 specifies the network interface cross referenced to relevant TR and the protocol stacks by the BNG function.

Interface	TR	A10 protocol stack	TR defined function with respect to the network interface
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 provide trusted access to the 3GPP SGW

Table 3: BNG network interfaces

BNG manages subscribers through control and management message exchanges with external elements. Typically, this includes AAA server, policy server, Accounting servers. Table 4 specify the control and management interface cross referenced to relevant TR and the protocol stacks by the BNG function.

Interface	TR	A10 protocol stack	TR defined function with respect to the control and management interface
R	TR-134, TR-300	RADIUS, Diameter	Policy policy control frame work
B	TR-134	RADIUS, Diameter	AAA service
S11	TR-378	GTP-c	Session creation and management

Table 4: BNG control and management interfaces

4.2 DBNG Functional Architecture

Utilizing the baseline BNG illustration, the BNG interfaces and functional blocks are further separated between the control plane and user plane. This document defines the functional architecture of DBNG as in Figure 2 which separates BNG function among control plane and user plane respectively.

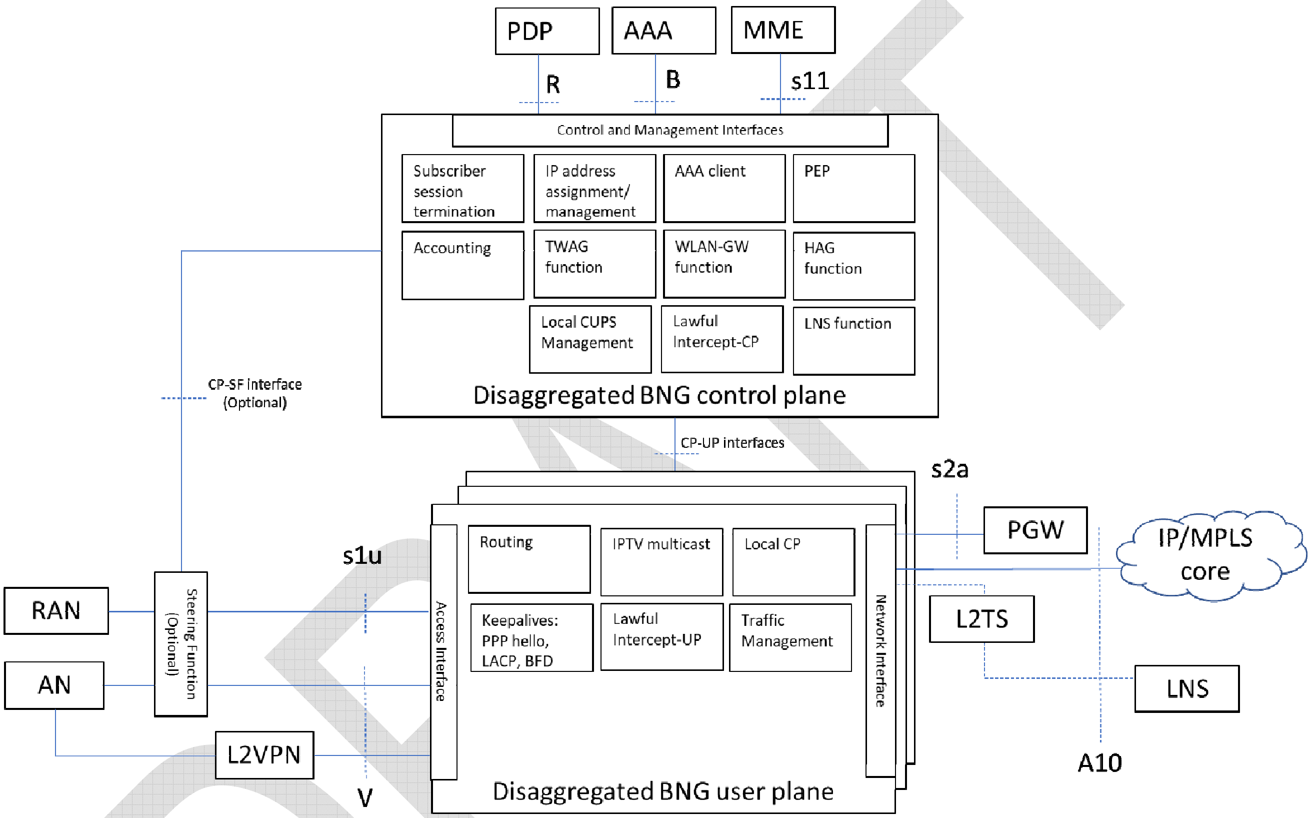


Figure 2: BNG functions separating into Control Plane and User Plane

EDITOR’s NOTE: a routing function must be added to the DBNG-CP. The routing functions in both planes must be described in detail based on the support/deployment scenarios.

Also, a combination of all the functions of the control plane (CP) referred to as disaggregated CP (DBNG-CP). Similarly, a combination of user plane (UP)-specific functions to as disaggregated UP (DBNG-UP).

4.2.1 DBNG-CP Functions

The BNG control plane terminates signaling protocol such as PPPoE, performs authentication via AAA servers and assign IP address to the subscriber. After the BNG establishes a subscriber session, accounting updates are sent periodically to an accounting server. Therefore, the following BNG functions which resides in the control plane:

- Subscriber session termination
    - Both PPPoE and IPoE (which contains DHCPv4, DHCPv6, and SLAAC) are control plane related functions.
- AAA client:
    - Control message exchange with AAA servers
    - The DHCP and PPPoE initial message will trigger authentication with the AAA server
- IP address assignment/management
    - Utilizing PPPoE and IPoE session to assign IPv4 address, IPv6 address, or IPv6 prefix are control plane related functions. After the address assignment is completed the control plane will signal forwarding rules to the user plane
- Accounting: subscriber usage information are exchanged with accounting servers
- PEP
    - After receiving the policies from a PDP, the control plane as the enforcement will push these policies onto the user plane.

In addition, TR-291, TR-321, and TR-384 integrate further functions into the BNG control plane.

- TWAG: As explained in TR-291 performs wireline authentication with an IPoE subscriber. After a successful authentication, the BNG TWAG function will signal the PGW to create a GTP tunnel. After the tunnel setup is complete, the address assignment is also completed by the BNG. The BNG authentication/addressing function and the TWAG signaling are all control plane processing. After the address assignment is completed the control plane will signal forwarding rules to the user plane.
- WLAN GW: As explained in TR-321, the access controller is integrated into the BNG. Prior to address assignment, the end device performs EAP authentication with the AC. After a successful authentication, the BNG will assign an IP address for the end device. The authentication of the AC and address assignment of the BNG re all control plane processing. After the address assignment is completed the control plane will signal forwarding rules to the user plane.
- HAG: As explained in TR-384, the hybrid access consists of a broadband connection and a 3GPP connection. The broadband connection is provided through traditional BNG functions. The 3GPP connection follows 3GPP procedures where the eNodeB establishes tunnels to the HAG using procedure defined in TR29.274. 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 control plane function:

- Lawful intercept control plane function that receive instruction from a lawful intercept mediation element and instructs the DBNG-UP mirroring actions.
- Local CUPS management, a human user interface that allows management of a DBNG-CP and its many DBNG-UPs.
- 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).

4.2.1.1 DBNG-CP Interfaces

The northbound interfaces: R, B, and S11 are management and control related belongs to the DBNG-CP.

4.2.2 DBNG-UP Functions

On the DBNG-UP, once the control completes authentication and address assignment, the DBNG-UP would create state related to forwarding and SLA management for the subscriber session on the DBNG-UP. The DBNG-UP performs forwarding, traffic management, and policy enforcement on the subscriber traffic. Therefore, the following BNG function are part of the user plane:

- Traffic Management: follows the instruction from the DBNG-CP on forwarding and related state for each subscriber session. For example, forwarding rules, filtering rules, and qos rules.

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

- IPTV: where IGMP and MLD request are processed locally to provide the fastest channel change time.
- Routing: to react to network faults and topology changes
- Keepalive messages: such as BFD and PPPoE echo hello which scales better on the local DBNG-UP.
- Lawful Intercept: the user plane component of lawful intercept where mirrored packet must adhere to local country standard LI format.
- Local control plane that process all the messages mentioned: IGMP, MLD, IGP, BGP, keepalives.

4.2.2.1 DBNG-UP Interfaces

The access interface (V) and network interface (A10) that forwards subscriber data traffic belongs to the BNG user plane.

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 user interface for configuration shown in Figure 3. The DBNG-CP will manage its associated DBNG-UPs and is responsible for pushing configuration and retrieving operational state and status from the DBNG-UPs. For reference, this is similar to “config” and “show” commands of the traditional BNG. Some examples of the configuration 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, therefore, traditional BNG proprietary internal representation of system resources and hardware resources and their exact physical configuration is transparent to the DBNG-CP. The management interface would be used to communication system resource information.

The management interface includes these functionalities: exchange DBNG-UP resources’ information, resource constructs such as cards, ports, and or interface.

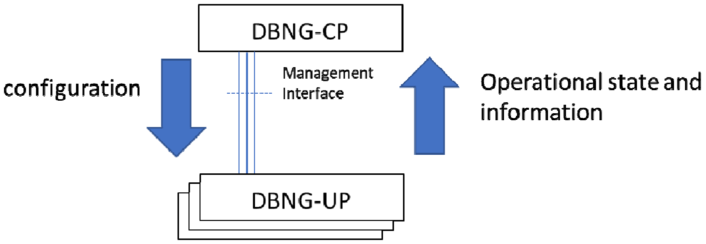


Figure 3: Management Interface

4.2.3.2 Control Packet Redirection Interface

A separate interface is required to exchange control messages from the V interface to the control plane. Figure 4 below shows a flow diagram provides an example of the control messages that are exchanged between the BNG-UP and BNG-CP.

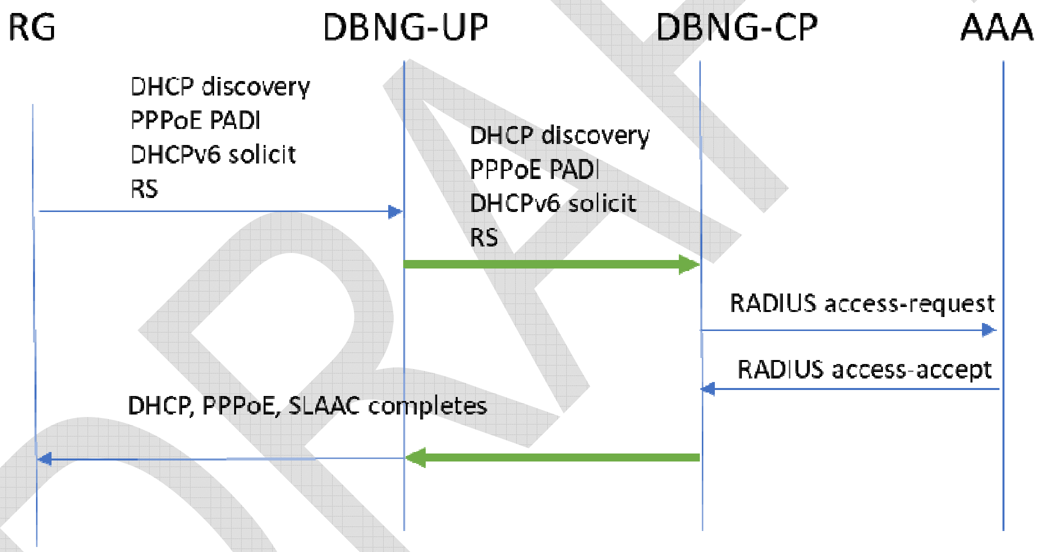


Figure 4: Example of Control and User Plane control message exchange

From the flow diagram in Figure 4 above, it shows that an in-band signaling channel between the DBNG-UP and DBNG-CP is necessary to trigger subscriber authentication. The DBNG-UP and DBNG-CP separated would be connected over a network. Therefore, control packets would be sent over a tunnel. Figure 5 below illustrates the requirement of a control packet redirect interface.

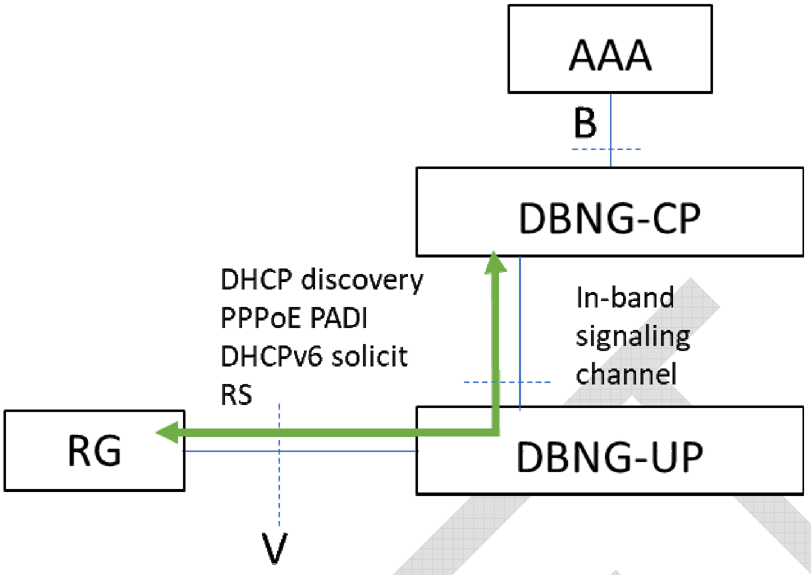


Figure 5: Control Packet Redirect Interface

With DBNG, the DBNG-CP and the DBNG-UP each become a separate network function, control plane function and user plane function. The network separation between BNG-CP and DBNG-UP can vary between a small layer 2 domain to a layer 3 multi hop data centers.

A subscriber session typically starts with control messages for subscriber access, which may include requesting one or more address. 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 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 logging on to the network).

Since the DBNG-CP is decoupled from the DBNG-UP, the DBNG-CP has no access circuit information (ex. VLAN tags, MPLS label, and etc). Therefore, the DBNG-UP would need to send the access circuit information to the DBNG-CP as meta data.

4.2.3.3 State control Interface

Once the subscriber has successfully authenticated, the DBNG-CP will require another interface to install traffic forwarding rules and related states to the DBNG-UP as shown in Figure 6. The traffic rules will require 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.

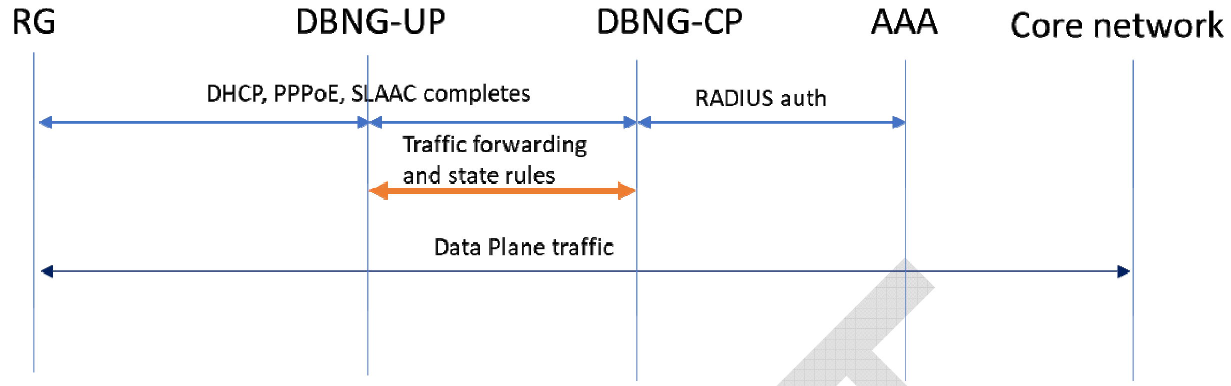


Figure 6: Example of Control Plane pushing forwarding rules to the User Plane

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

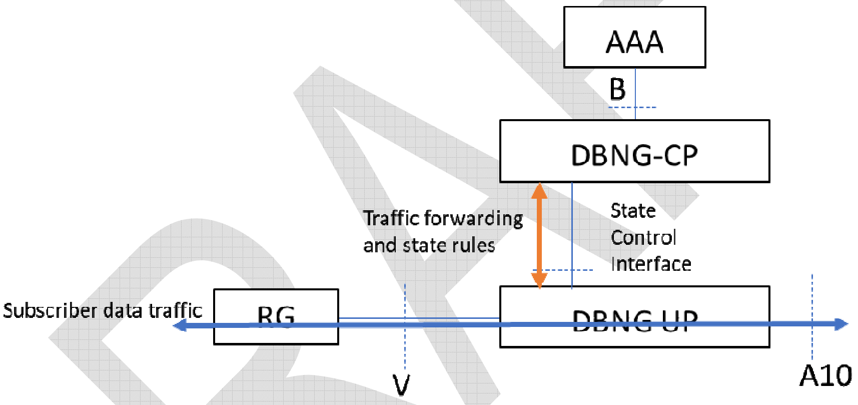


Figure 7: State control Interface

Since BNG can support different access types and protocol on the V interface, the traffic detection and forwarding rules must be flexible. Figure 8 below shows the different user plane combination with respect to the BNG function as describe in their respective TRs.

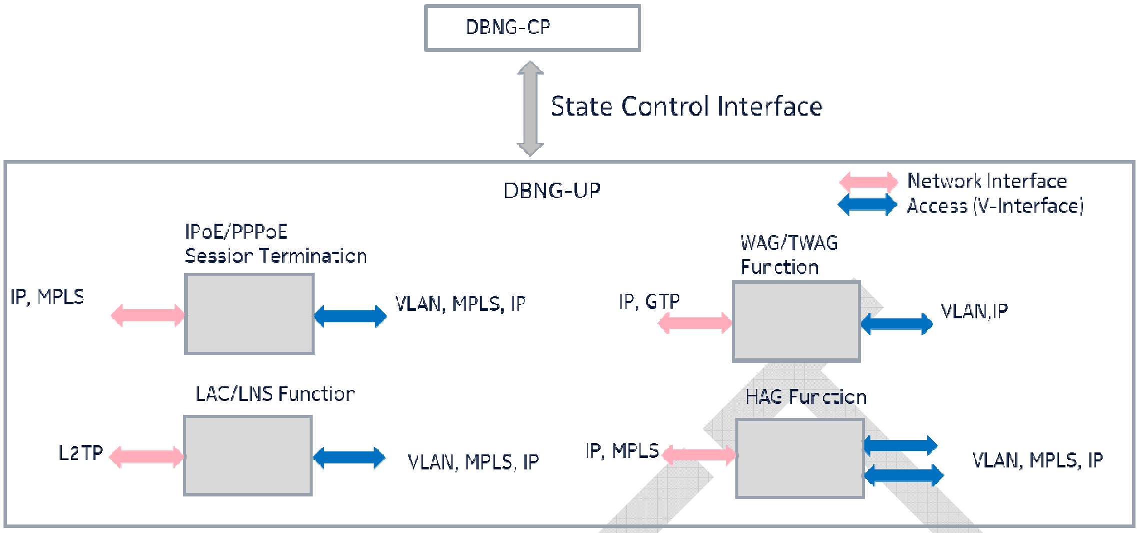


Figure 8: Example of User Plane combinations

The basic traffic detection and forwarding rules in upstream direction (i.e. access to network) and downstream direction (i.e. 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 (i.e. access from DSLAM or OLTs over Ethernet).

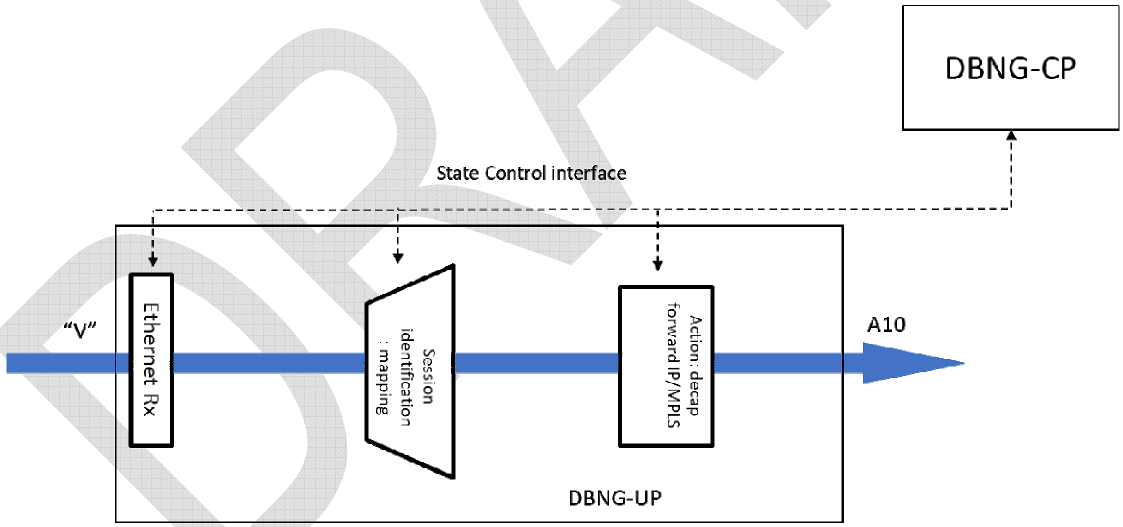

DBNG-CP
State Control interface
"V"
Ethernet Rx
Session identification : mapping
Action: decap forward IP/MPLS
A10
DBNG-UP

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.

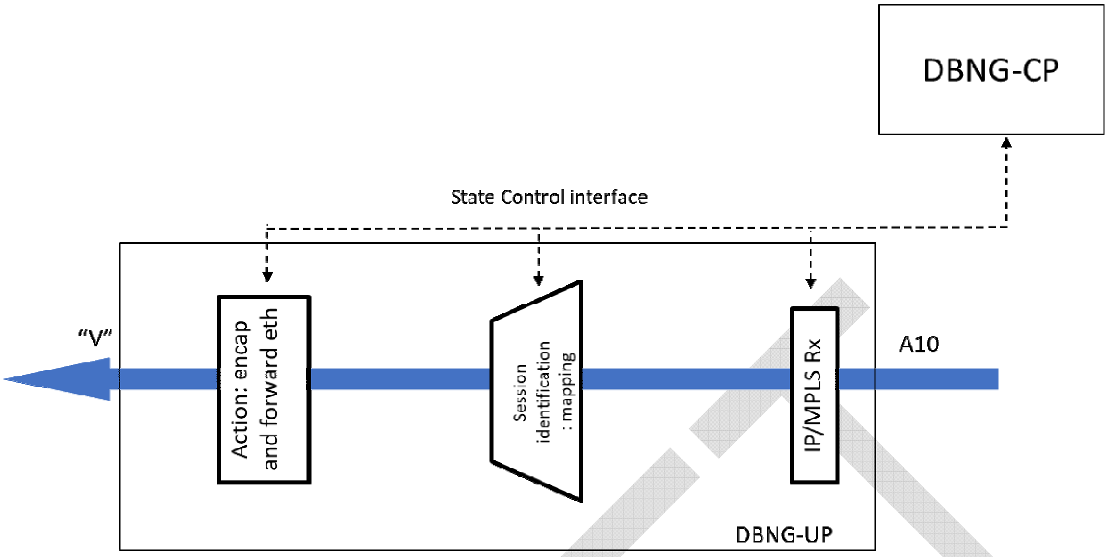

DBNG-CP
State Control interface
"V"
Action: encap and forward eth
Session identification : mapping
IP/MPLS Rx
A10
DBNG-UP

Figure 10: State Control Interface for Network to Access direction

Direction Downstream - Network to Access:

Session-identification: IP address
Action: lookup IP DA, 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 the 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
. Traffic Steering
. Application aware policies

The DBNG-CP would trigger session state cases:

1. DBNG-CP triggers a new session state on the DBNG-UP. i.e. When the subscriber successfully authenticates
2. DBNG-CP will trigger update of session state on the DBNG-UP. i.e. Triggered by an update from the policy-server.
3. DBNG-CP triggers the deletion of session state. i.e. Based on administrative action, session termination or a disconnect-message initiated from the AAA server.

4.2.4 High level architecture of the disaggregated BNG

In summary the following are the identified interface classes required for DBNG-CP and DBNG-UP communication.

1. Management Interface (Mi)
2. Control Packet Redirect Interface (CPRi)

3. State Control interface (SCi)

The architectural model of CUPS, defined three interfaces that applications comprising the DBNG-CP and the DBNG-UP use to support operation, management, and maintenance of these applications:

- control packet redirect;
- state control;
- management.

Together with the disaggregated BNG function and interfaces, Figure 11 below illustrates a high level architecture of control and user plane separation for a disaggregated BNG which elaboration on the interfaces between the CP and UP.

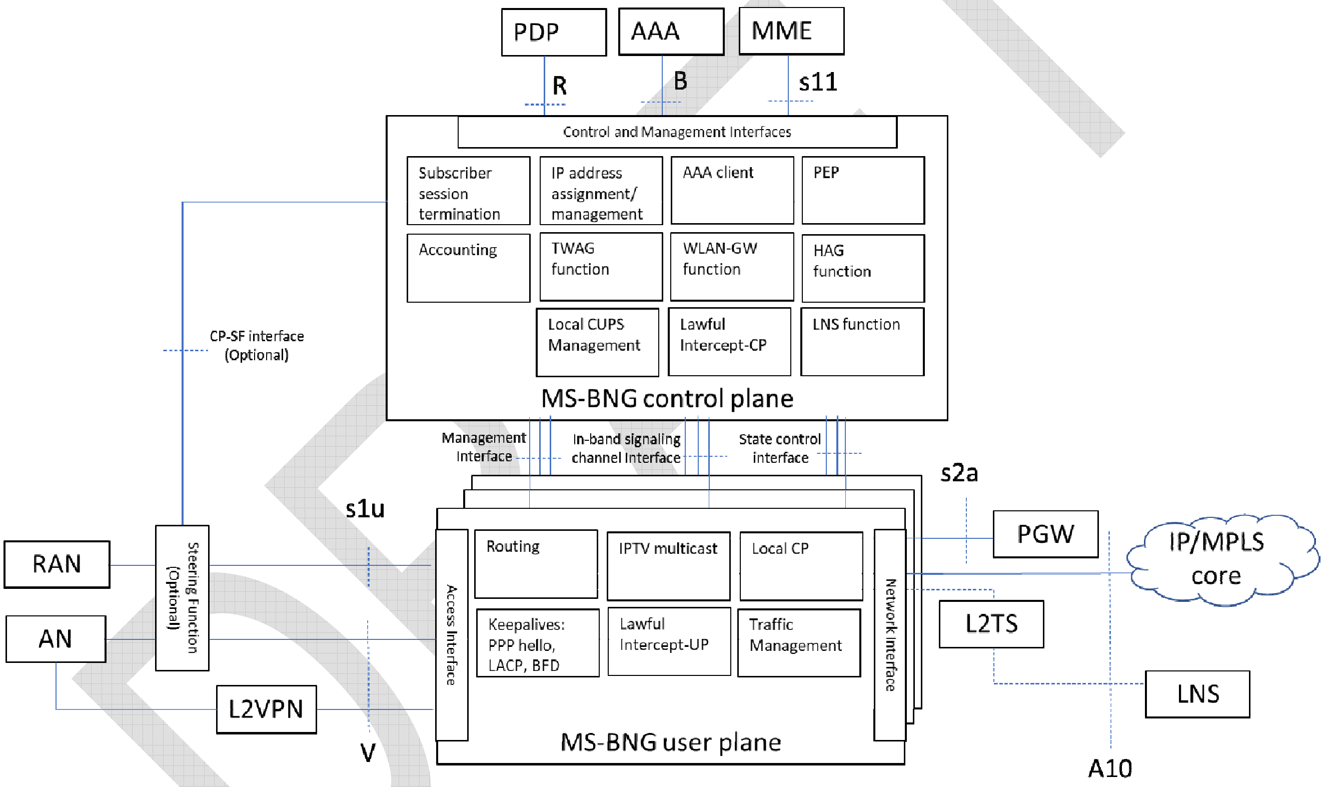


Figure 11: High level architecture of control and user plane separation of a disaggregated BNG

4.2.4.1 Steering Function

The separation of control and user plane introduces the option for multiple DBNG-UP to be under the control of a single DBNG-CP. Multiple DBNG-UP 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-UP 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 upon 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 example 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-UP
- The subscriber group (eg 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 subscribers service level agreement.

4.3 Deployment models

4.3.1 DBNG-CP and DBNG-UP resides within an area

In this deployment scenario, a single DBNG system is deployed in a subscriber intensive area. The control plane is deployed in one central office or data center while multiple user planes are distributed across sub-areas. The user planes specifically could reside in multiple central offices or edge data centers within this area. Since the control plane is computationally intensive, a virtualized control plane acting as a VNF can meet the requirements of flexibility and computation performance. On the other hand, the user plane depending on traffic can either be virtualized or utilize physical hardware. The virtualized user plane with high flexibility can be suitable for light traffic, while high-performance hardware is needed for high traffic forwarding performance.

In order to fulfill the functions of a BNG, the control plane needs to communicate with outside systems such as a AAA (Radius/Diameter) server and many others in the management network. In addition, the control plane has three interfaces with the user plane separated by their traffic categories: Service Interface, Control Interface, and Management Interface whose functions have been identified in section 4.2.1.1.

4.3.2 DBNG-CP and DBNG-UP resides in separate areas

(editors note: Discuss on call to remove. 4.3.2 and 4.3.1 and be merged because DBNG is the separation of CP and UP doesn't really matter the distance)
It's feasible and reasonable to deploy one DBNG system to cover the services and subscribers across multiple areas which are otherwise less intensive. The control plane can be deployed centrally with the user planes deployed in different areas close to subscribers as shown in Figure x.

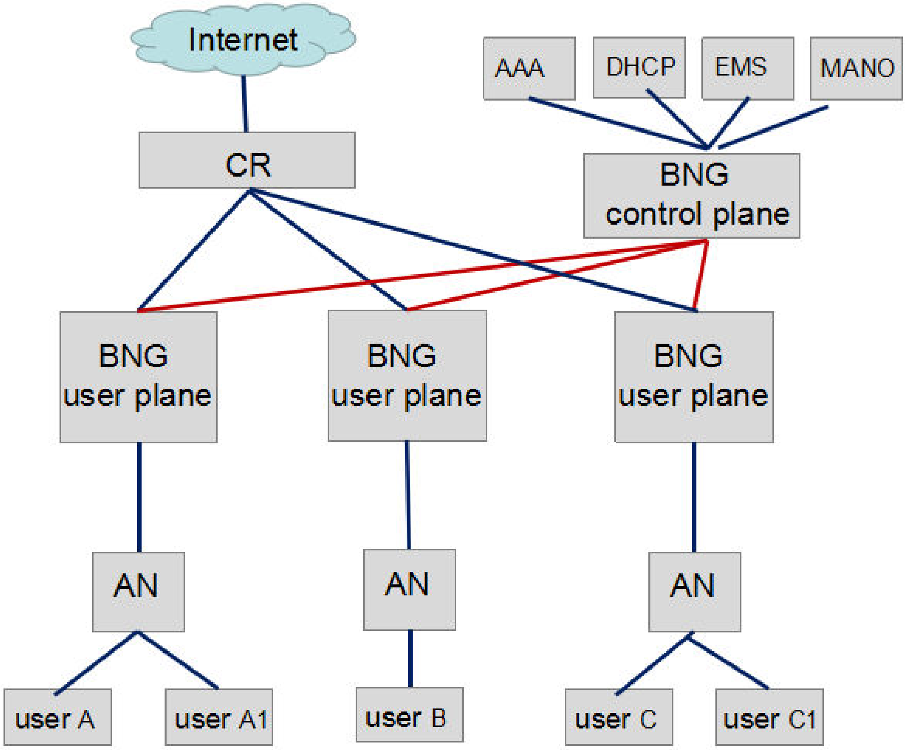


Figure 12: Geographically distributed User Plane deployment model

Take three areas A, B. and C for example. Here three user planes are placed with one shared control plane. The control plane is usually deployed in a Core Data Center such as in a provincial datacenter with user planes in edge Date Centers such as city datacenters. In this Data Centers design, we have core data centers and edge data centers according to their location and responsibility. Core data centers are often planned in province capitals for control and management, while edge data centers are in cities or towns for easy service access.

In this scenario, a centralized control plane interfaces to the subsystems outside and communicate with all these user planes for control and management. Under the control plane's control, the corresponding traffic is forwarded by DBNG-UP to the Internet. As described above, the control plane is virtualized as VNF for its computation intensive workloads, while the user plane could ether be virtualized for light traffic or stay physical for high traffic.

The transport latency resulting from the distance between the two planes across multiple areas here could reach such a range that the routing control should reside in the user planes.

4.4 Call flows

4.4.1 Control Plane and User Plane association

Pre-condition to form association is outside the scope of this call flow. 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 instructs the DBNG-UP to redirect control messages over the control packet redirect interface.

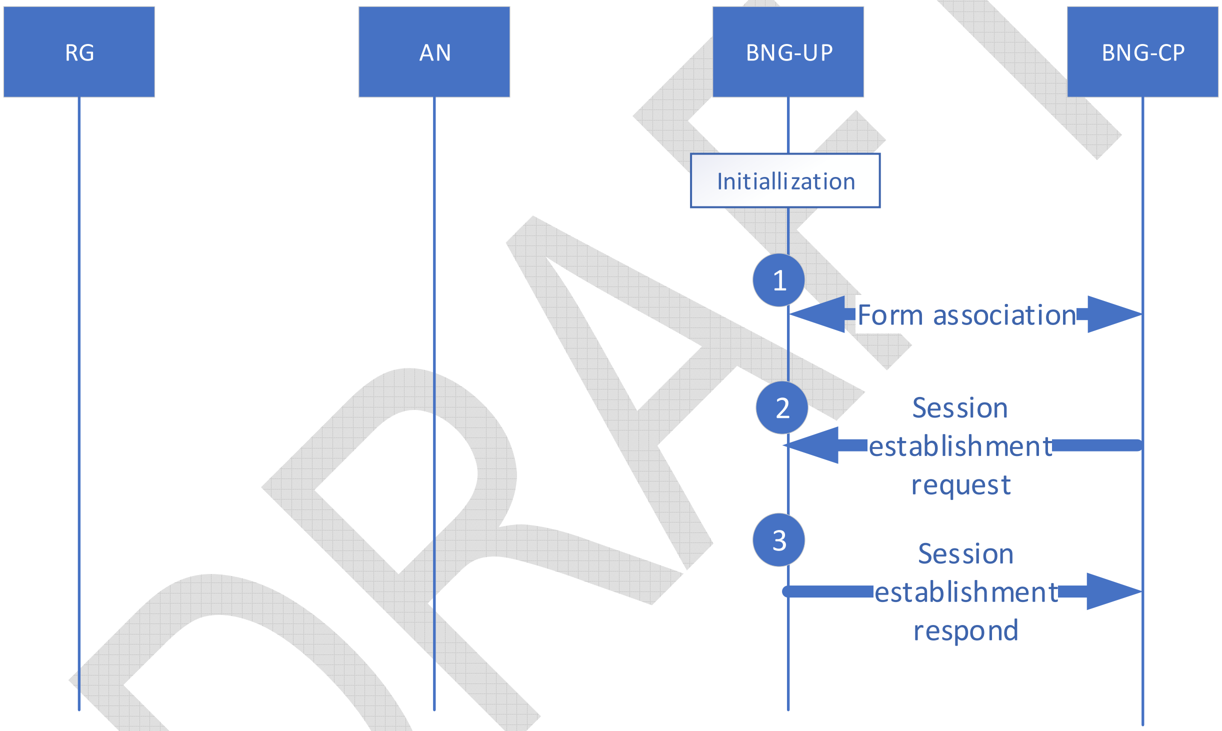


Figure 13: DBNG-CP and DBNG-UP association

4.4.2 Initial control packet redirection rule

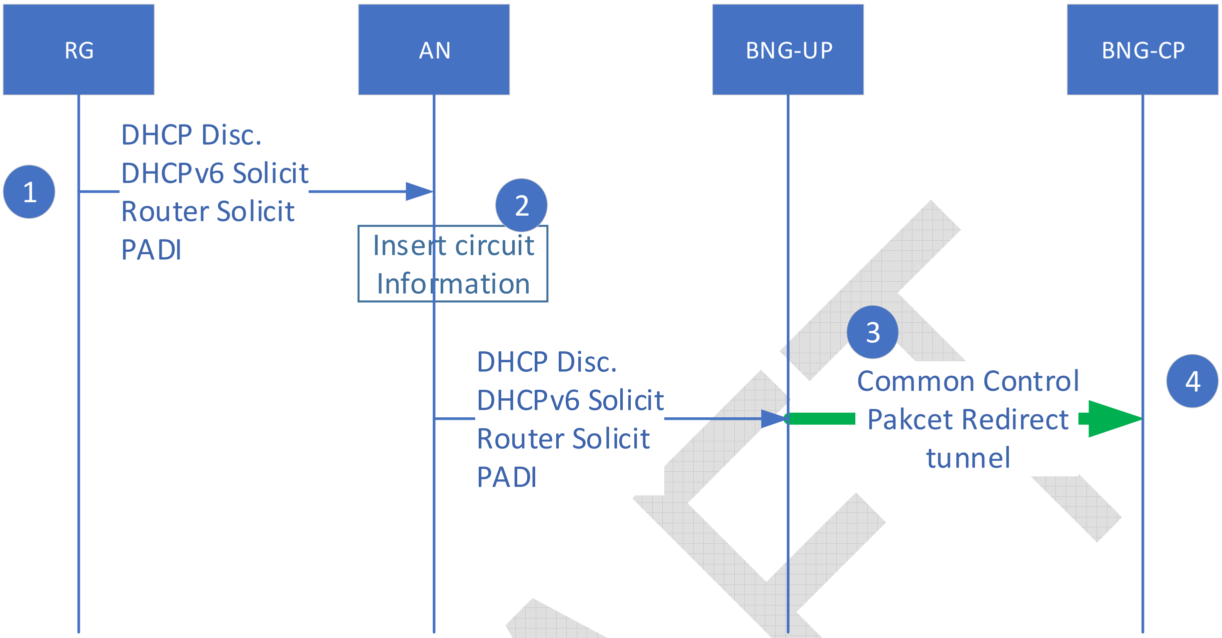


Figure 14: Common control packet redirection rule

1. All new RGs connecting to the network sends a control message including, DHCPv4 discovery, PPPoE PADI, DHCPv6 solicit, or Router Solicit
2. The AN insert circuit information onto the control message which includes: circuit ID, remote ID, Line ID, and/or interface ID.
3. The BNG-UP detects these as new control message unrelated to current established session and tunnel these control messages over the Control Packet Redirect Interface. The DBNG-UP must also provide access interface information as metadata to the BNG-CP information because this information might not be within the packet itself.
4. The BNG-CP receives the control message and its context (port, VLAN, and etc), together providing a session context.

4.4.3 DHCPv4 Call Flow

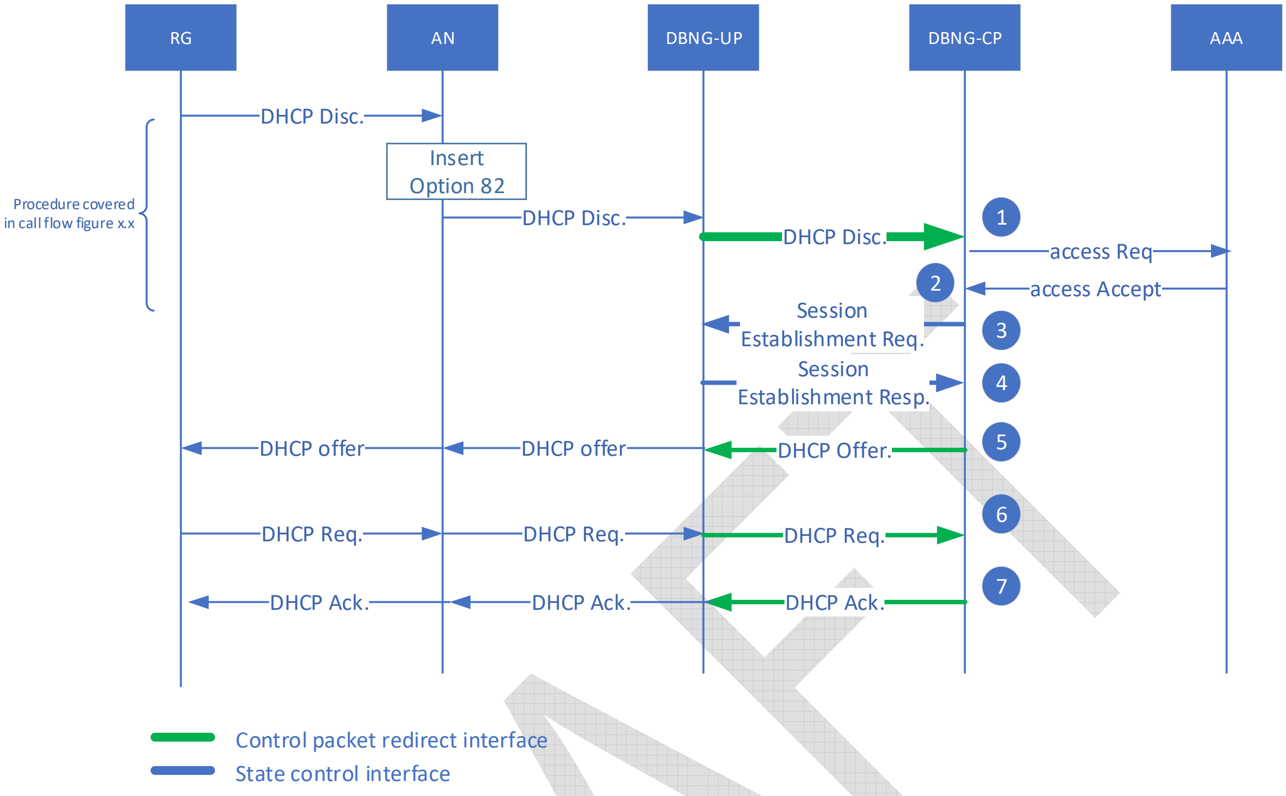


Figure 15: DHCPv4 call flow

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 reply to the DBNG-CP with an access accept.
3. *The DBNG-CP knows the IP address to be assigned to the RG, either obtained through the local address server or from a AAA returned attribute. 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 state.
4. 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.
5. The DHCP Offer from the DHCP server is sent back to the RG through the DBNG-UP utilizing the control packet redirect 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 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 would be sent immediately

4.4.4 DHCPv6 Call Flow

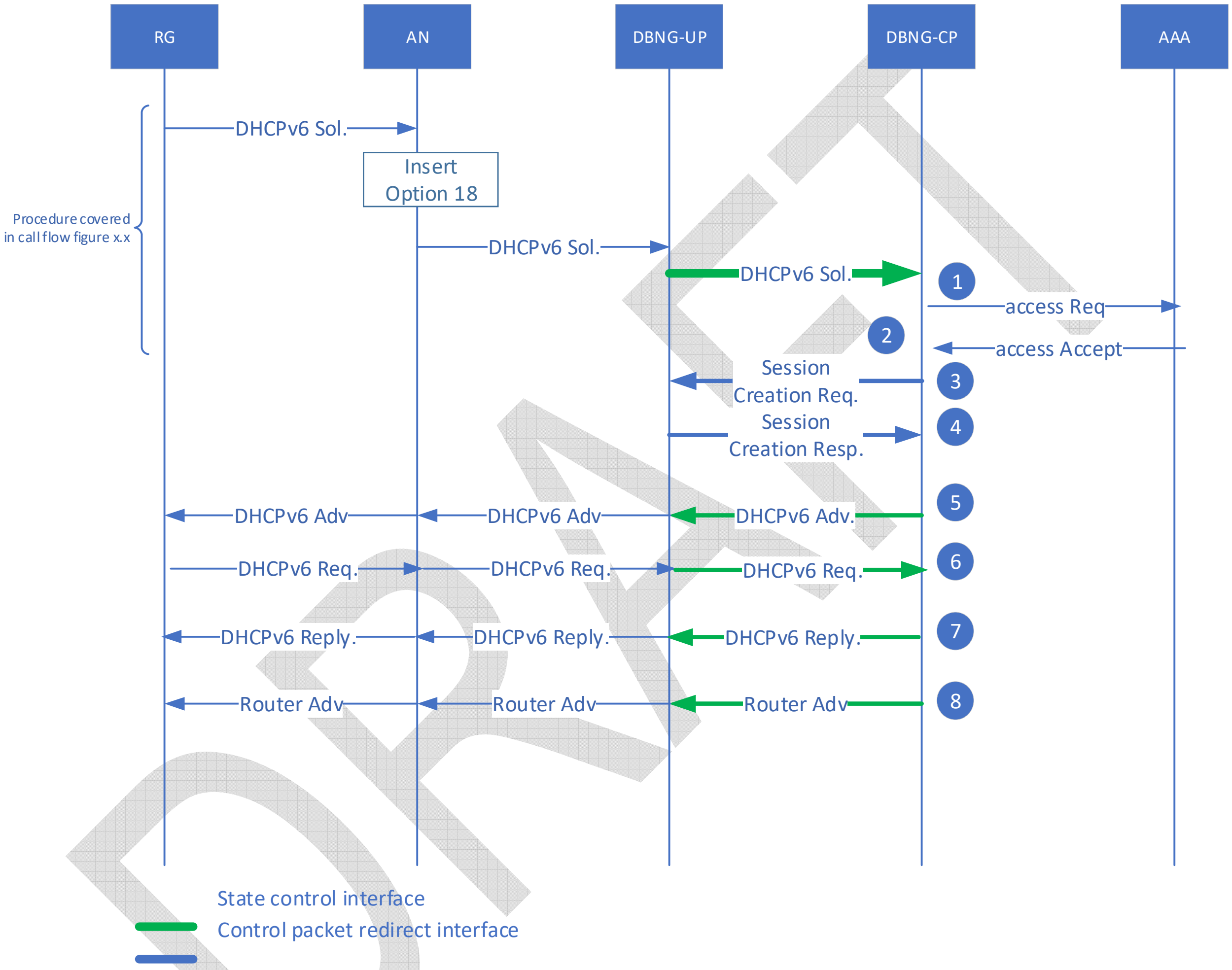


Figure 16: DHCPv6 call flow

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 reply to the DBNG-CP with an access accept.
3. *The DBNG-CP knows the IP address and/or prefix to be assigned to the RG, either obtained through the local address server or from a AAA returned attributes. 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 state.
4. 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.
5. The DHCPv6 Advertisement from the DHCPv6 server is sent back to the RG through the DBNG UP utilizing the control packet redirect 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 forwards 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 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 would be sent immediately

4.4.5 SLAAC Call Flow

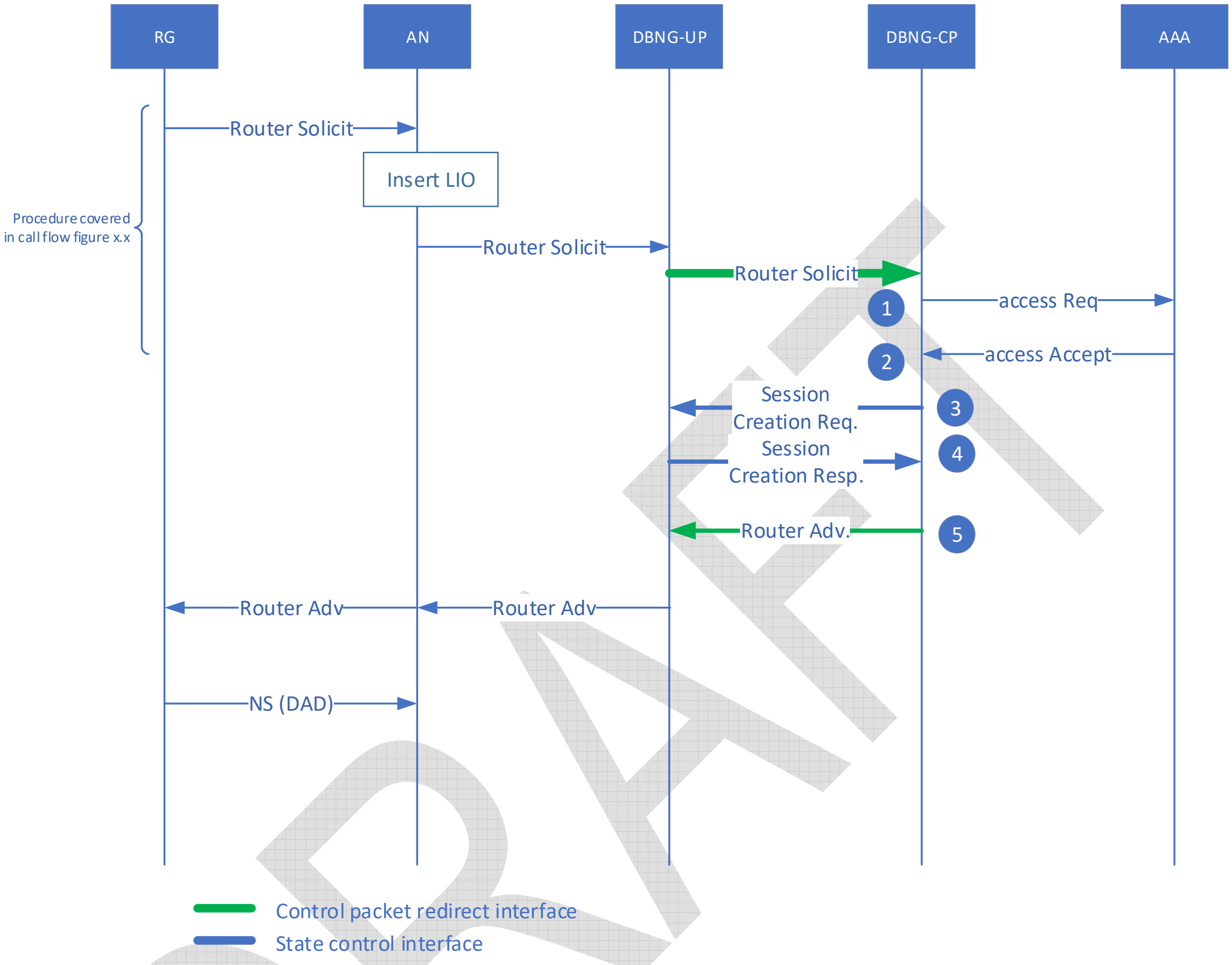


Figure 17: SLAAC call flow

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 reply to the DBNG-CP with an access accept.
3. The DBNG-CP knows the IP prefix to be assigned to the RG, either obtained through the local address prefix server or from a AAA returned attributes. The DBNG-CP sends a session creation request to create new packet forwarding states for the data packet. This updates the data plane state.
4. 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.
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

4.4.6 PPPoE Call Flow

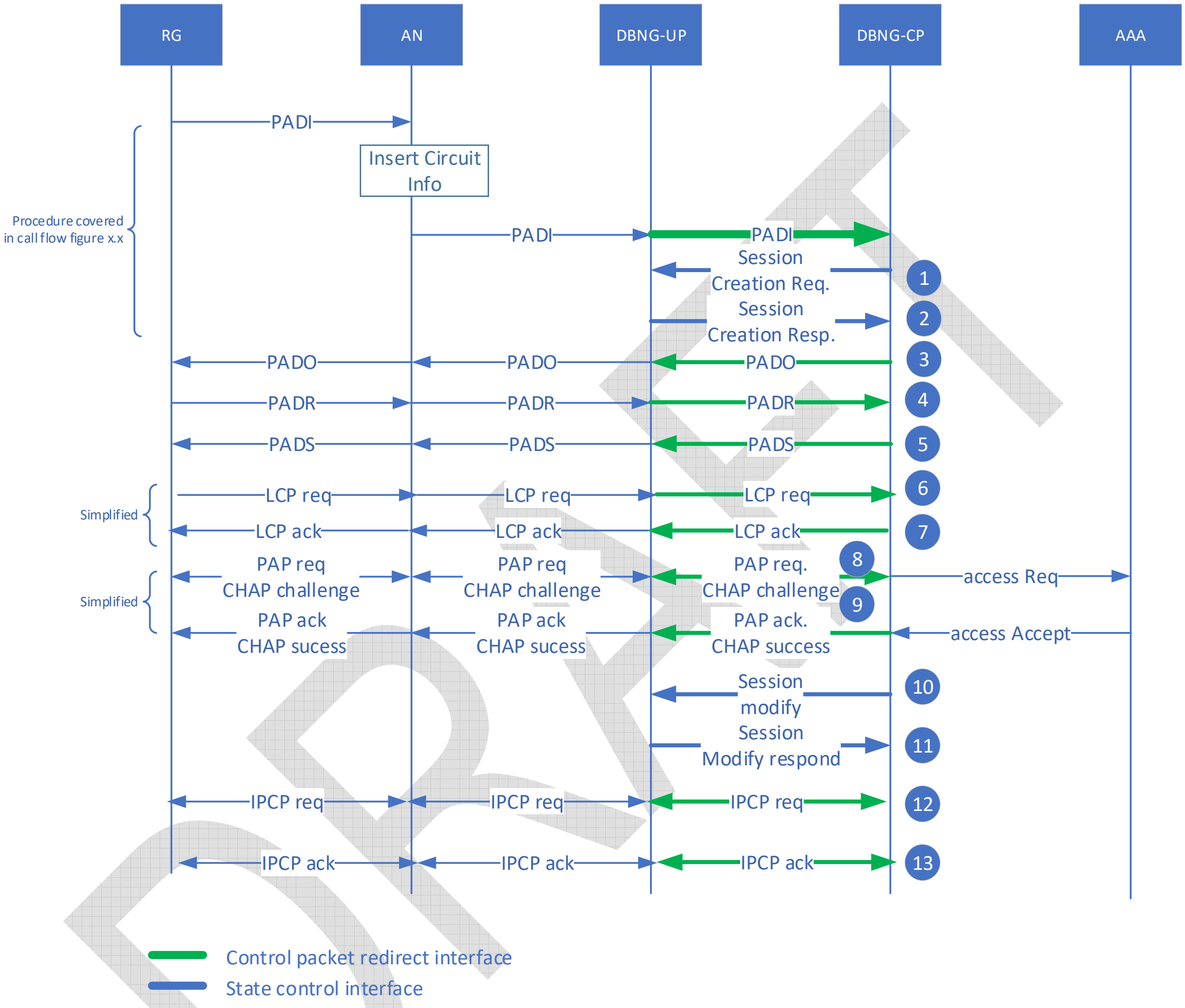


Figure 18: PPPoE call flow

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

1. *Upon learning 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 subscribers PPP control packets.
3. The DBNG-CP sends the PADO back to the RG through the DBNG UP utilizing the control packet redirect interface.
4. The PADR is sent from the RG through the DBNG UP utilizing the control packet redirect interface.
5. The DBNG-CP sends the PADS back to the RG through the DBNG UP utilizing the control packet redirect interface.
6. The LCP config request is sent from the RG through the DBNG UP utilizing the control packet redirect interface.

7. The DBNG-CP sends the LCP config ack back to the RG through the DBNG UP utilizing the control packet redirect interface. The LCP config 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 control packet redirect interface. The PAP password is sent as a 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 control packet redirect interface. The RG responds back to the challenge to the DBNG-CP. The challenge is sent to the AAA server.
9. The AAA successfully authenticates the RG and reply to the RG with PAP/CHAP success.
10. Address could be assigned to the RG either through the AAA reply or through a local address server. 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.
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 subscribers IP data packets.
8. **Both DBNG and RG sends NCP config req for parameter negotiation, utilizing a dedicated session control packet redirect tunnel. The RG is assigned an IPv4 address. As noted, if a session has not yet been established, the session must be established at this step.
12. The NCP config ack is sent from 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 would be sent immediately

4.4.7 PPPoEv6 Call Flow

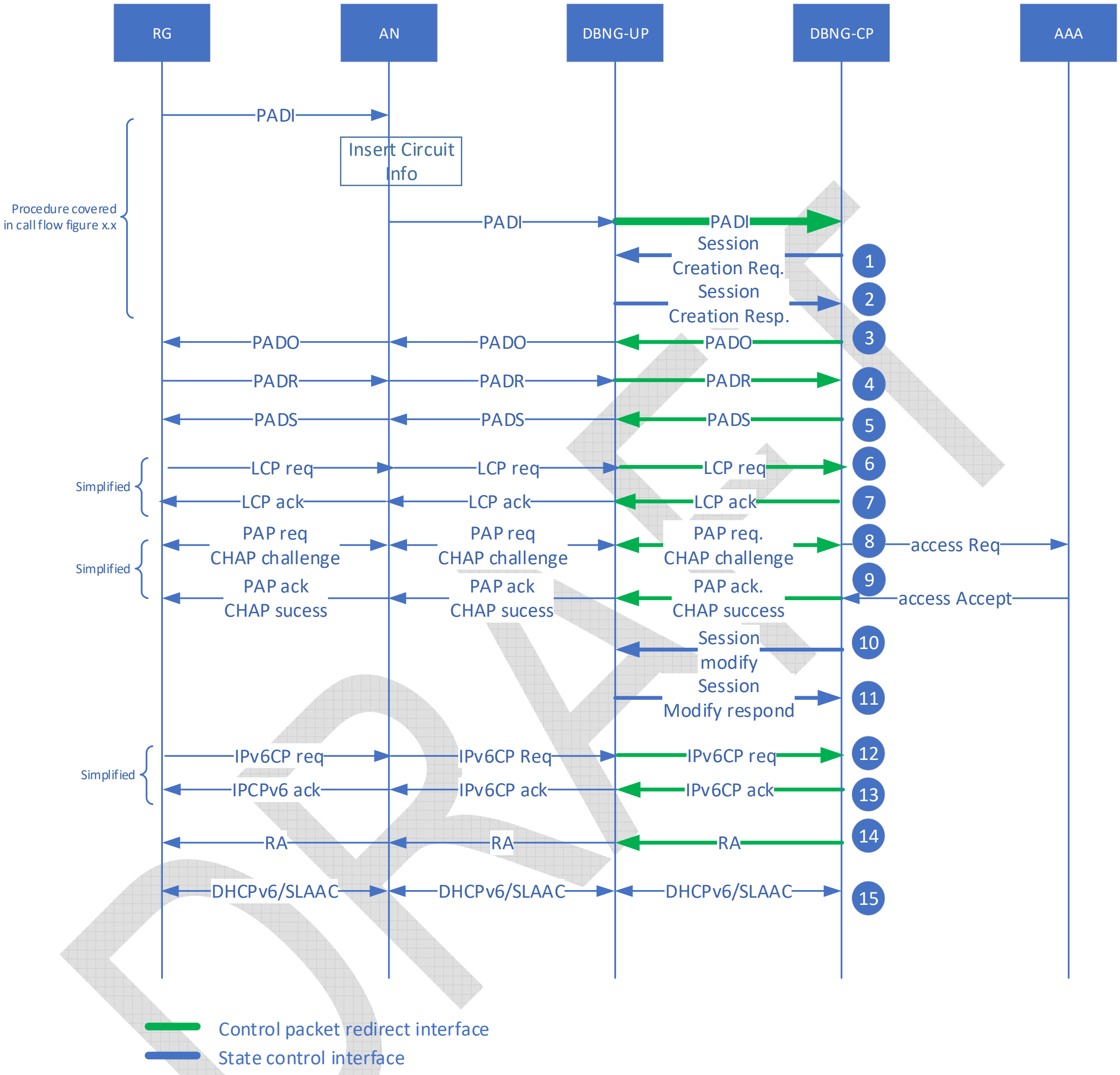


Figure 19: PPPoEv6 call flow

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

1. *Upon learning 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 subscribers 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 a the control packet redirect interface.
4. The PADR is sent from the RG through the DBNG UP utilizing the control packet redirect interface.

5. The DBNG-CP sends the PADS back to the RG through the DBNG UP utilizing the control packet redirect interface.
6. The LCP config request is sent from the RG through the DBNG UP utilizing the control packet redirect interface.
7. The DBNG-CP sends the LCP config ack back to the RG through the DBNG UP utilizing the control packet redirect interface. The LCP config 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 control packet redirect interface. The PAP password is sent as a 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 control packet redirect interface. The RG responds back to the challenge to the DBNG-CP. The challenge is sent to the AAA server.
9. The AAA successfully authenticates the RG and reply to the RG with PAP/CHAP success.
10. At this point, the DBNG-CP would know 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 rule 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.
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 subscribers IP data packets.
12. The NCP config request is sent from the RG through the DBNG UP utilizing the control packet redirect interface.
13. The DBNG-CP sends the NCP config ack to the RG through the DBNG UP utilizing the control packet redirect interface.
14. The DBNG-CP sends an RA to the RG informing the LLA.
15. **The DBNG-CP responds to the RG DHCPv6 or SLAAC request. As noted, if a session has not yet been established, the session must be established at this step.

*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 would be sent immediately

4.4.8 LAC Call Flow

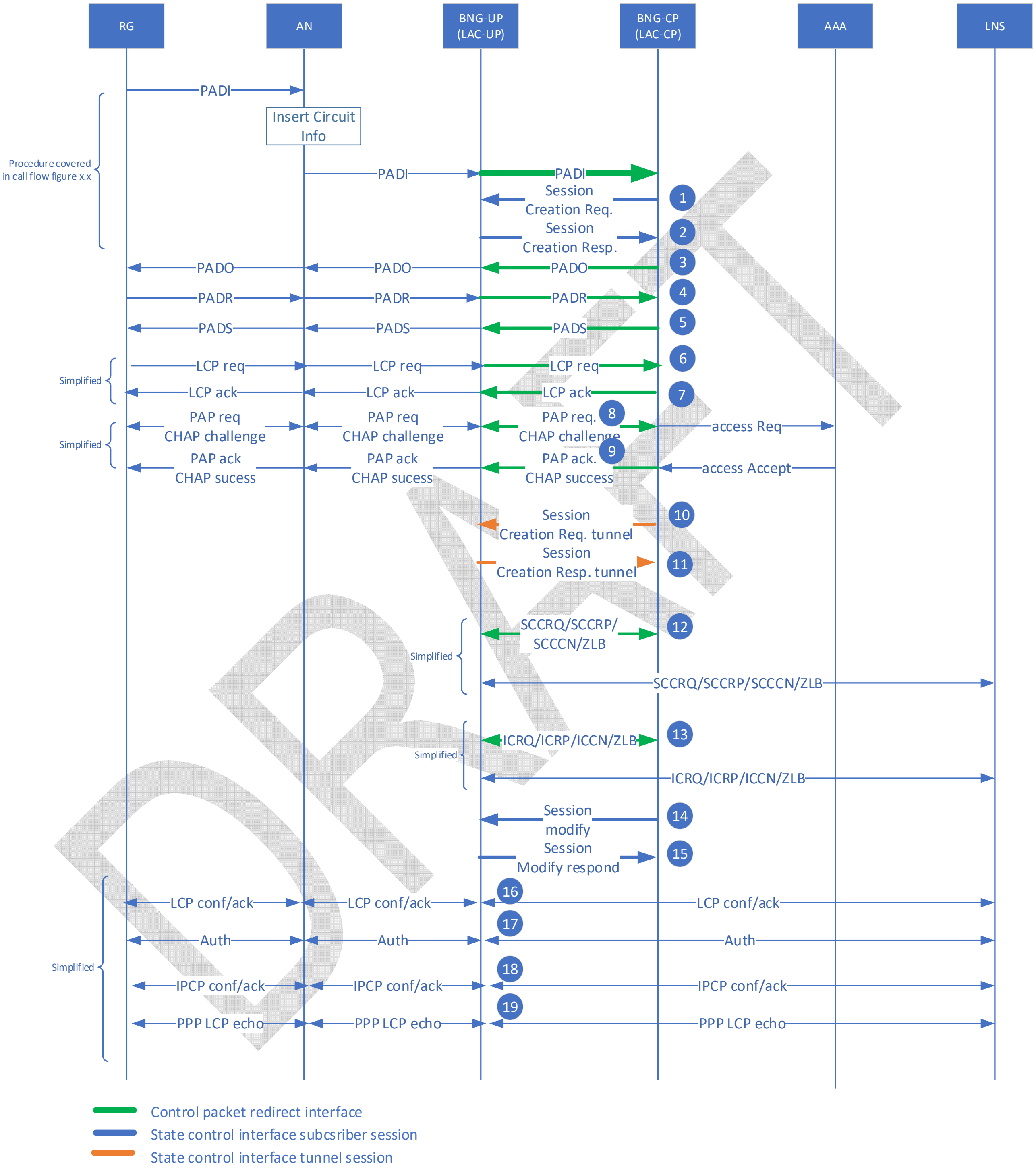


Figure 20: LAC call flow

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

1. *Upon learning 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 subscribers PPP control packets.
3. the DBNG-CP sends the PADO back to the RG through the DBNG UP utilizing the control packet redirect interface.
4. The PADR is sent from the RG through the DBNG UP utilizing the control packet redirect interface.
5. The DBNG-CP sends the PADS back to the RG through the DBNG UP utilizing the control packet redirect interface.
6. The LCP config request is sent from the RG through the DBNG UP utilizing the control packet redirect interface.
7. The DBNG-CP sends the LCP config ack back to the RG through the DBNG UP utilizing the control packet redirect interface. The LCP config 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 control packet redirect interface. The PAP password is sent as a 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 control packet redirect interface. The RG responds back to the challenge to the DBNG-CP. The challenge is sent to the AAA server.
9. The AAA successfully authenticates the RG and reply to the RG with PAP/CHAP success and that this is a L2TP session
10. DBNG-CP sends a session establishment message to the DBNG-UP. The DBNG-CP programs the DNBG-UP control packet redirect rules to 1) decapsulate and send the L2TP control message towards the LNS. 2) redirect L2TP control message back to the DBNG-CP. This session establishment is only 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 sends 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 control packet redirect 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 control packet redirect interface
14. **The DBNG-CP sends a session modify request if there is a previous session established to allow for data packet forwarding to the LNS (and control packet if not done already). If not, previous session were established, this is a session 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 subscribers PPP control and data packets.
16. If the LNS cached LCP config and there is no negotiation disagreement, this step can be skipped. If LNS has not cached LCP config or the session require renegotiation, then LCP negotiation takes place.
17. If the LNS cached authentication information and there is no disagreement on authentication, this step can be skipped. If LCP has not cached authentication information or authentication failed, then a re-auth takes place.
18. IPCP takes place between the RG and the LNS through the DBNG-UP
19. PPP LCP echo hello 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 would be sent immediately

4.4.9 LNS Call Flow – PPPoEv4

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

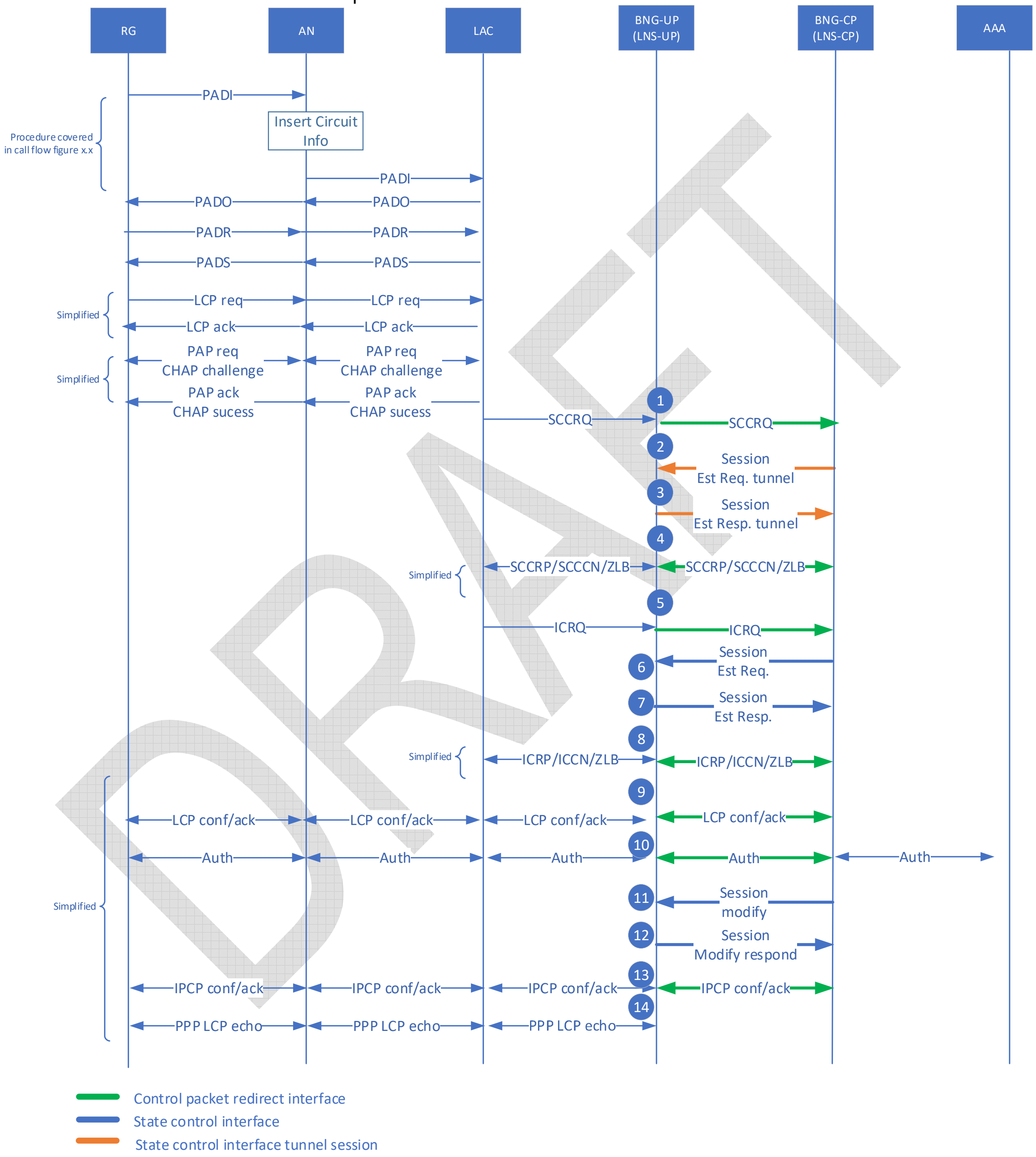


Figure 21: LNS PPPoEv4 call flow

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 control packet redirect 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 control packet redirect interface
5. The DBNG-CP receives the ICRQ message (include AVP defined in RFC 5515)
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 exchange ICRP, ICCN, and ZLB with the LAC by utilizing the control packet redirect interface
9. If the LNS cached LCP config and there is no negotiation disagreement, this step can be skipped. If LCP has not cached LCP config or the session require renegotiation, then LCP negotiation takes place.
10. If the LNS cached authentication information and there is no disagreement on authentication, this step can be skipped. If LCP has not cached authentication information or authentication failed, then a re-auth takes place.
11. **After authentication, the DBNG-CP knows the IP address and/or prefix for the subscriber either though the local address server or from AAA returned VSAs. 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 sessions, this requires a session establishment request to update the data plane.
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 subscribers PPP control and data packets.
13. IPCP takes place between the RG and the LNS through the DBNG-UP
14. PPP LCP echo hello 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 would be sent immediately

4.4.10 LNS Call-Flow (Dual Stack)

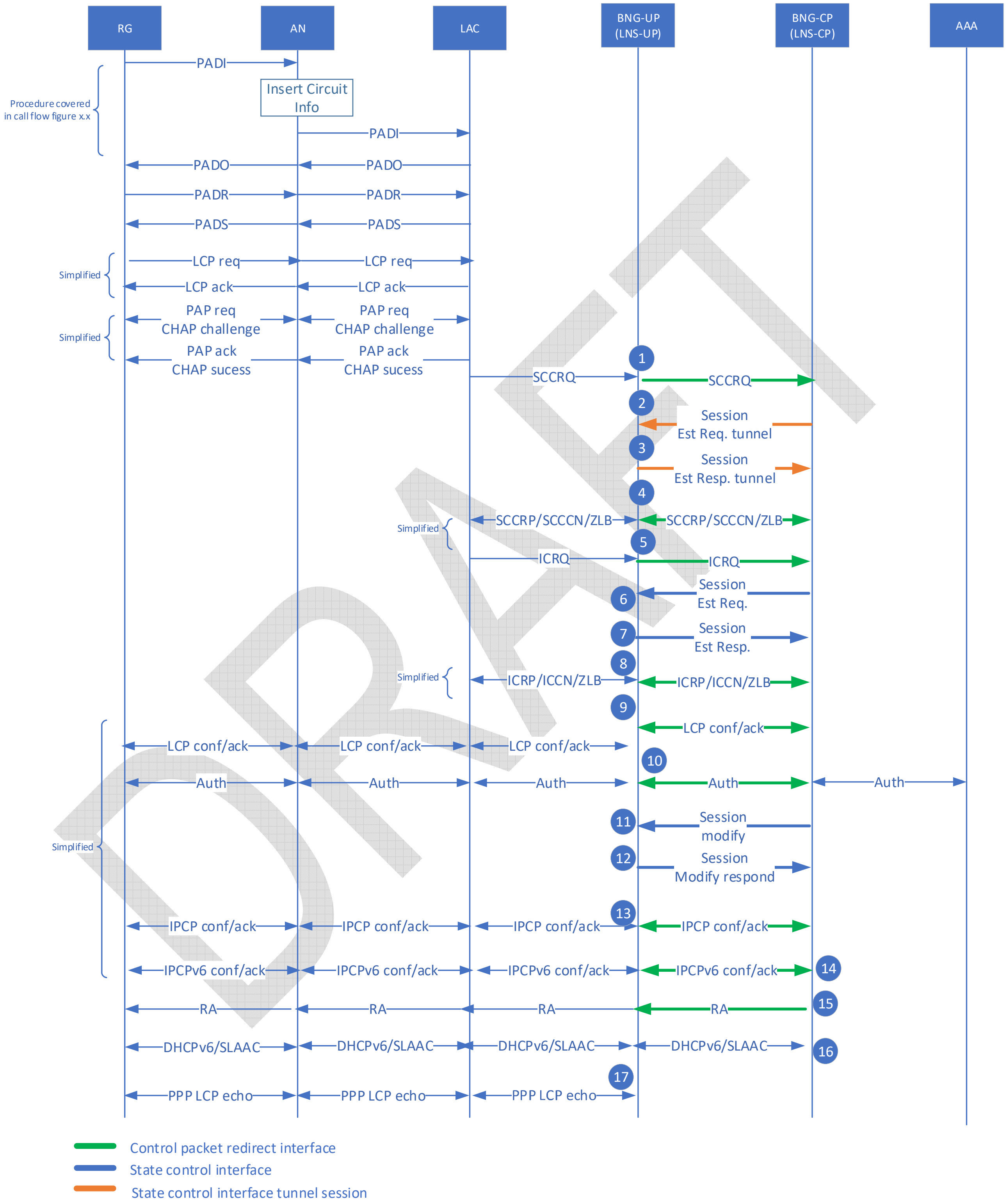


Figure 22: LNS Dual Stack call flow

Procedure 1 to 13 would follow the same LNS procedure outlined in section 4.4.9

14. The IPCPv6 config request is sent from the RG through the DBNG UP utilizing the control packet redirect interface.
15. The DBNG-CP sends the IPCPv6 config ack to the RG through the DBNG UP utilizing the control packet redirect interface.
16. The DBNG-CP sends an RA to the RG informing the LLA.

**The DBNG-CP responds to the RG DHCPv6 or SLAAC request. As noted, if a session has not yet been established, the session must be established at this

4.4.11 TWAG Call flows

The call flow for TWAG follows TR-291 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 EPC access is provided to the UE. The DBNG terminates an S2a interface with the 3GPP PGW;

In this call flow the TWAG/DBNG 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 message (such as DHCP, RS, and DHCPv6) to the DBNG-CP, see section XX. The procedure related to interaction to external system stays the same as in TR-291. This procedure requires the GTP c and GTP u to utilize different IP address endpoints.

NOTE: 3GPP S2a signalling already supports that the 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).

4.4.11.1S2a initial attach based on layer 2 trigger: IPv4 based on DHCPv4

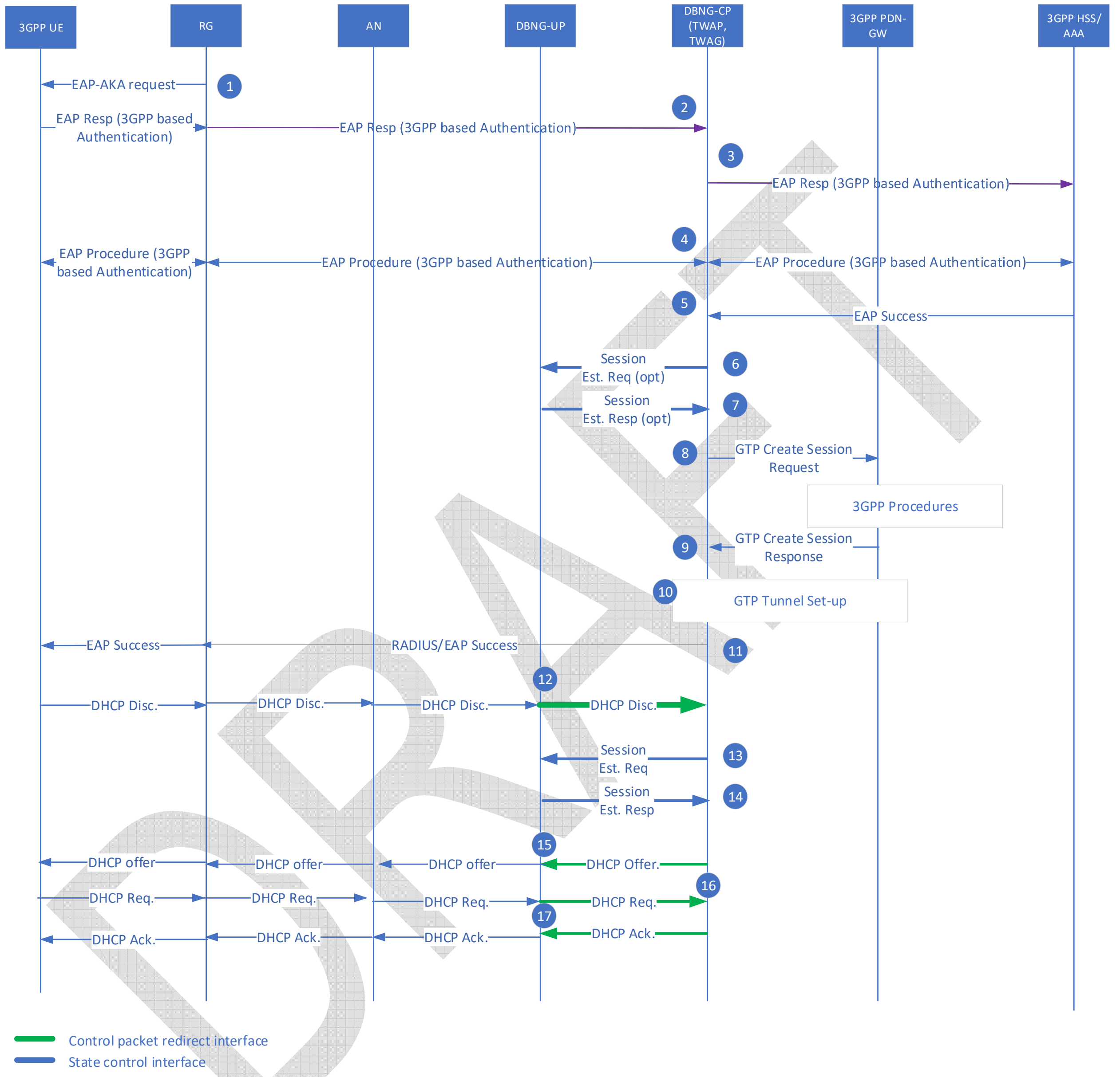


Figure 23: S2a initial attached based on layer 2 trigger: DHCPv4

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 [22]). 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 DBNG 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 NAI.

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 TS 23.402 [XX] clause 16.2 and 33.402 [22].
4. The BNG-CP acting as a TWAP relays back and forth EAP signaling between the 3GPP AAA server and the RG.
5. Once it has decided to grant access to the 3GPP UE, 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 (i.e. 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.
7. [Optional] The DBNG-UP responds with a DNBG-UP Control session establishment response supplying the requested TEID.
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 TS 23.402 [XX] 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 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 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 control packet redirect 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 encap, 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 BNG-UP sends a response back to the BNG-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 control packet redirect interface.
16. The 3GPP UE sends a DHCP request message and is redirected to the DBNG-CP through the DBNG-UP via the control packet redirect interface.
17. The DBNG-CP sends a DHCP ack through the control packet redirect interface.

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

4.4.11.2S2a initial attach based on layer 2 trigger: IPv6 prefix based on SLAAC

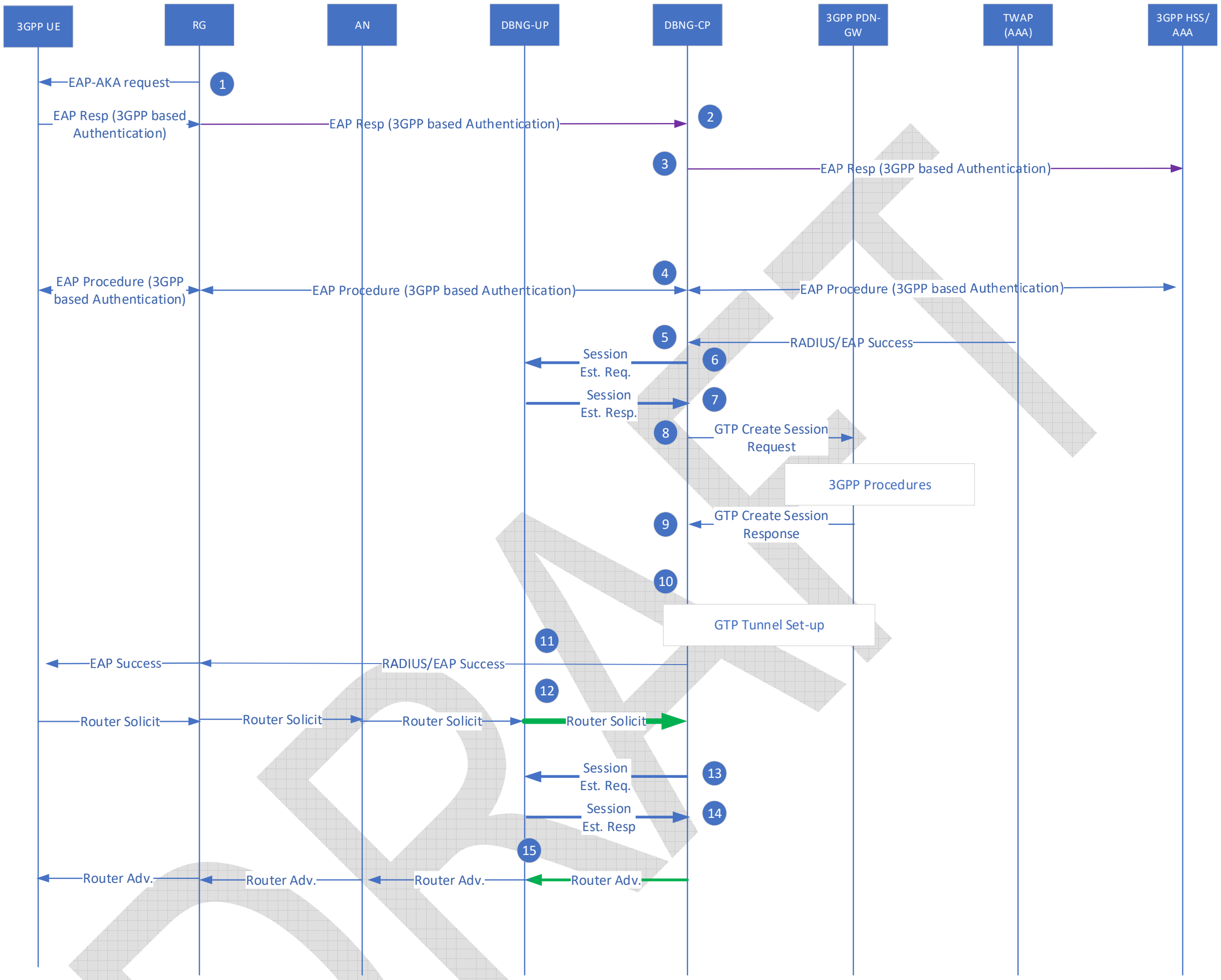


Figure 24: S2a initial attached based on layer 2 trigger: SLAAC

Procedure 1 to 11 would follow the same DHCPv4 procedure outlined in section 4.4.11.1

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 encap, 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 BNG-UP sends a response back to the BNG-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 control packet redirect interface.

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

4.4.11.3S2a initial attach based on layer 3 trigger: IPv4 based on DHCP

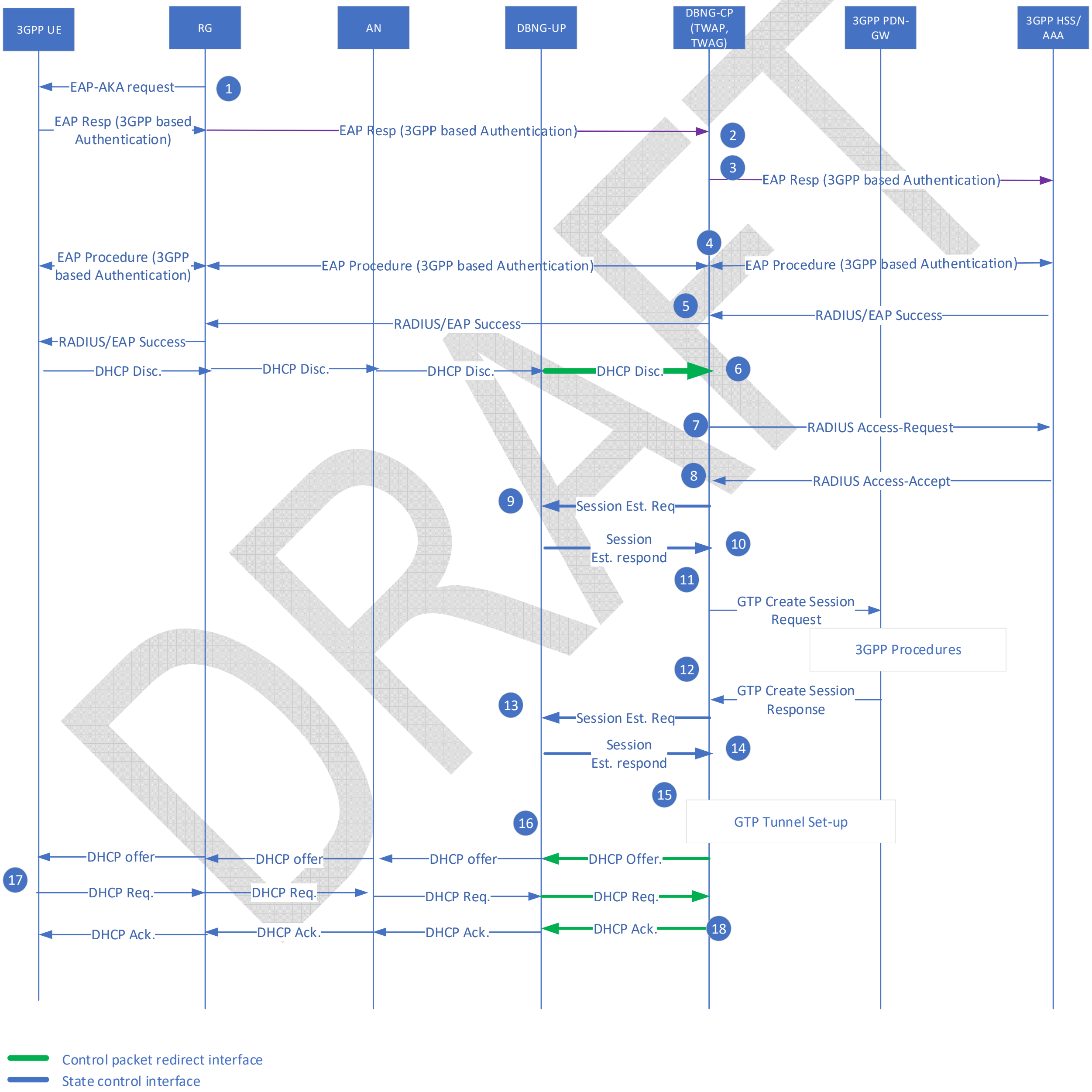


Figure 25: S2a initial attached based on layer 3 trigger: DHCPv4

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 [22]). 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 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 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 TS 23.402 [XX] clause 16.2 and 33.402 [22].
4. The BNG-CP acting as a TWAP relays back and forth EAP signaling between the 3GPP AAA server and the RG.
5. Once it has decided to grant access, 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 TS 23.402 [XX] 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 encap, 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 BNG-UP sends a response back to the BNG-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 control packet redirect interface.
17. The 3GPP UE sends a DHCP request message and is redirected to the DBNG-CP through the DBNG-UP via the control packet redirect interface.
18. The DBNG-CP sends a DHCP ack through the control packet redirect interface

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

4.4.12 Hybrid Access Gateway Call Flow

The call flow correction to L3 Network-based Tunneling in both TR-348 and TR-378

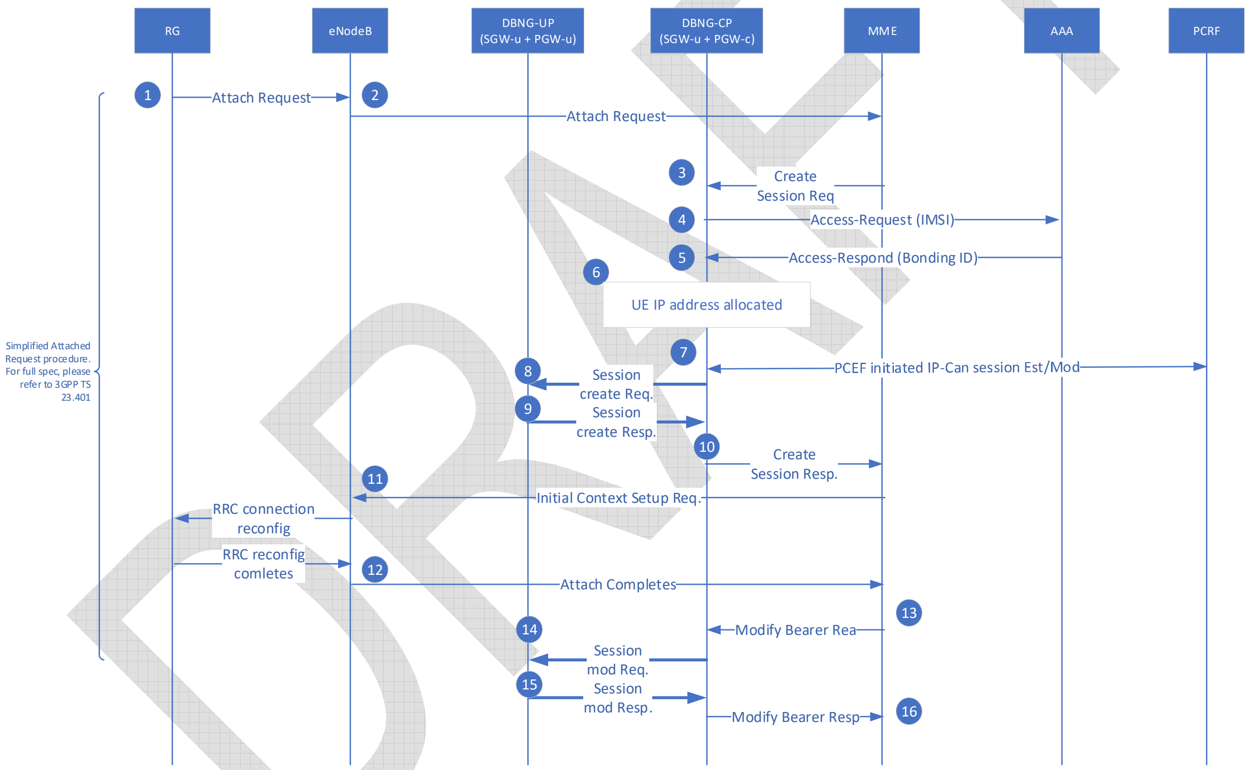


Figure 26: Hybrid Access Gateway L3 network-based Tunneling call flow

Above LTE UE attach procedure is simplified, for full attachment procedure, refer to TS 23.401. The HAG is a BBF defined element where PGW, SGW, and 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 BNG to be integrated into the HAG. The HAG in the call flow procedure is split between the DBNG-CP and DBNG-UP.

The RG can start with either the wireless or wireline connection. To bond the two connection, is 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 contacts 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:

- 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 TS 23.401 [xx]
2. The eNodeB forwards the Attach Request to the MME. This takes place as defined in step 2 of TS 23.401 [xx] Figure 5.3.2.1. The MME may carry out security features and retrieve subscription data as defined in step 3 to 11 of TS 23.401 [xx] Figure 5.3.2.1.
3. MME identifies the BNG (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 TS 23.401. The MME sends a session request to the BNG-CP (acting as both the SGW and PGW from MME view point). This takes place as defined in steps 12 to 13 of TS 23.401 [xx] Figure 5.3.2.1.
4. The BNG-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 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. And sends a create session response back to the MME. This takes place as defined in steps 15 to 16 of TS 23.401 [xx] Figure 5.3.2.1;
11. The MME sends the NAS attach accept back to the RG via the eNodeB: the NAS attach accept is sent within a S1-AP Initial Context Setup Request as defined in steps 17 of TS 23.401 [xx] Figure 5.3.2.1.
12. The eNodeB forwards the Attach complete message to the MME.
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, 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 BNG-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

4.4.13 Lawful Intercept Callflow

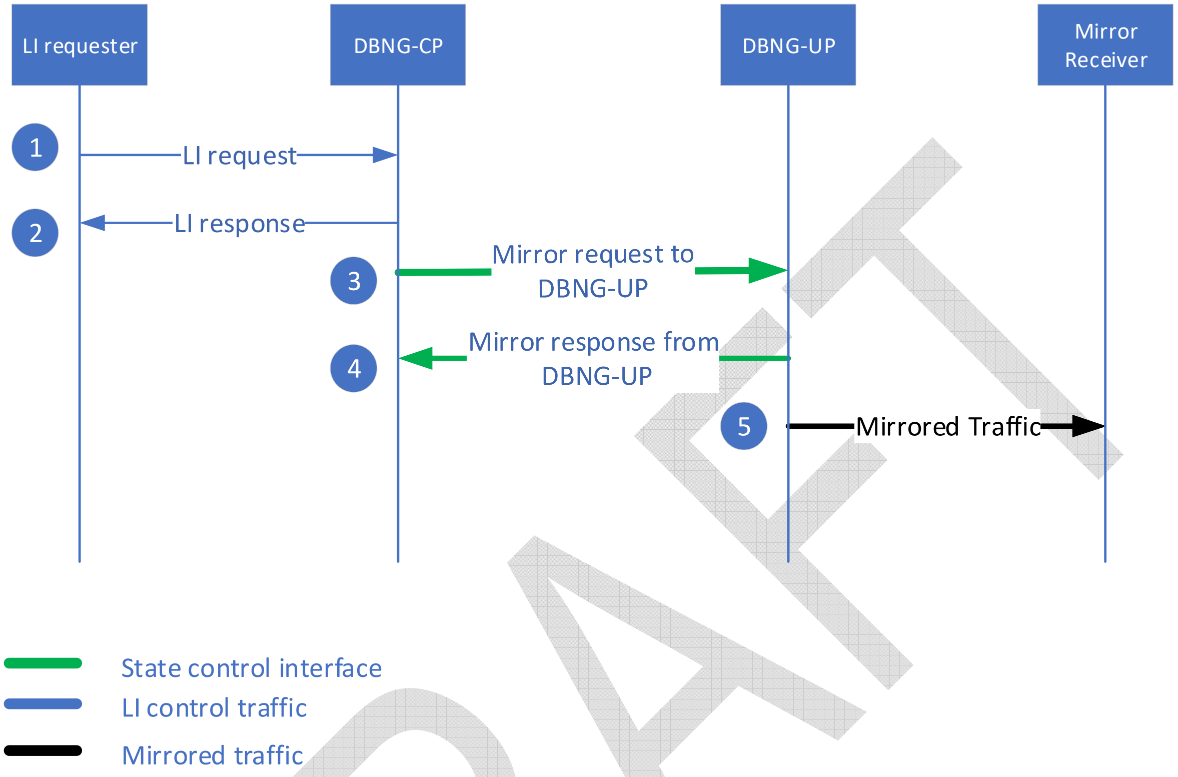


Figure 27: Lawful intercept Request

1. The LI requester 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 receiving the request 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 DBNG-CP
5. DBNG-UP, sends mirrored traffic to the mirror receiver

UPs other than that identified as serving the specified subscriber will not be affected by the LI request.

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 configuration must also be moved accordingly.

4.5 High level Information models

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 the text terms ‘CUPS protocol’ and ‘protocol’ are used interchangeably.

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

To fulfill BNG functionality, instances of DBNG-CP, and DBNG-UP form associations. It is possible that instances that belong to the same association support different subsets of functions identified as the version of the protocol.
[R-7] The protocol MUST be extensible, e.g., allow introduction of the new information elements., in a backward compatible manner.

[R-8] To deliver a high quality of experience to a subscriber, all DBNG components must be designed with resiliency of the overall system as the target.
[R-9] DBNG-CP and DBNG-UP 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.
[R-15] The SCi protocol MUST provide means to report be for the DBNG-UP to report per subscriber session statistics to DBNG-CP(s).
[R-16] The SCi protocol MUST be able to support a DBNG-CP to:

- add subscriber frame/network/host routes on a DBNG-UP and notify the DBNG-UP to advertise the routes.
- update subscriber frame/network/host routes on a DBNG-UP and notify the DBNG-UP to advertise the routes.

- delete subscriber frame/network/host routes on a DBNG-UP and notify the DBNG-UP to advertise the routes

[R-17] The SCi protocol MUST ensure that DBNG supports all access types documented on the fourth column of Table 2.

- add subscriber session states on DBNG-UP(s).
- update subscriber session states on DBNG-UP(s).
- delete subscriber session states on DBNG-UP(s).

[R-18] The SCi protocol MUST be able to support session status synchronization between a DBNG-CP and a DBNG-UP.

[R-19] 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 BNG MUST supports a variety of access types: fixed wirelines, 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 action. (perform **action)**

The match and action rules would provide platform independent abstraction to derive data-path state and processing by the DBNG-UP. The following are examples on how the DBNG-CP using a CUPS protocol to instruct the DBNG-UP to install traffic detection and forwarding rules on the DBNG-UP.

Access Types	**Upstream (access to network)**		**Downstream (network to access)**	
	Match	**Action**	**Match**	**Action**
PPPoE single stack	Port Ether header Session ID IPv4	Remove eth+pppoe Traffic mgmt. Forward to network	IPv4	Encap eth+pppoe Traffic mgmt. Forward to access
PPPoE Dual Stack	Port Ether header Session ID IPv4 IPv6 NA/PD IPv6 SLAAC	Remove eth+pppoe Traffic mgmt. Forward to network	IPv4 IPv6 NA/PD IPv6 SLAAC	Encap eth+pppoe Traffic mgmt. Forward to access
IPoE single stack	Port Ether header IPv4	Remove eth Traffic mgmt. Forward to network	IPv4	Encap eth Traffic mgmt. Forward to access
IPoe Dual Stack	Port Ether header IPv4 IPv6 NA/PD IPv6 SLAAC	Remove eth encap Traffic mgmt. Forward to network	IPv4 IPv6 NA/PD IPv6 SLAAC	Encap eth Traffic mgmt. Forward to access
Public Wifi	Port GRE tunnel	Remove GRE/eth Traffic mgmt.	IP	Encap eth/GRE Traffic mgmt..

	Ether header IP	Forward to network		Forward to access
TWAG	Port Ether header IP	Remove eth Encap GTP Traffic mgmt. Forward to network	GTP	Remove GTP Encap ethernet Traffic mgmt. Forward to access
Hybrid (combined)	Port Ether header IP	Remove eth Traffic mgmt. Forward to network	IP	Encap eth Traffic mgmt. Forward to access
	GTP	Remove GTP Traffic mgmt. Forward to network		Encap GTP Traffic mgmt. Forward to s1u

To support data forwarding for different types of access, as shown in the table above, 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:

- Flexibility to cover all different access types for current BNG deployments
- Flexibility to cover the A10 transport protocol as specified on Table 3 used for current BNG deployments.
- Extensibility to handle future types of access and transport protocol
  - Do not require versioning to cover future types of access and transport

[R-20] 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 they are signaled is up to the protocol, for example, expressing the relationship between the set of rules and actions is protocol specific.

[R-21] The CUPS protocol MUST be able to support A10 transport protocols defined in the scope necessary for user plane encapsulation such as: l2tp and gtp.

[R-22] The CUPS protocol MUST be able to perform credit control for usage monitoring and reporting. **(Editor's note: accepted in principle: contribution solicited for more detail)**

[R-23] The CUPS protocol MUST be able to specify QoS information per subscriber session. **(Editor's note: accepted in principle: contribution solicited for more detail)**

[R-24] The CUPS protocol MUST gracefully handle scaling in and out of DBNG-CP and DBNG-UP resources

A BNG that is also acting as a PE (as per TR-178) may have multiple virtual networks to which a subscriber may be connected.

[R-25] The SCi MUST support the identification of virtual network to which the subscriber should be connected.

As per section 4, it is an option for routing protocols to be deployed on the DBNG-CP. In the case that all routing protocols are deployed on the DBNG-CP, the DBNG-CP will have the full information to install the required forwarding entries via the SCi. Note that this implies additional actions for traffic from the subscriber towards the virtual network and additional match criteria for traffic from the virtual networks.

[R-26] The SCi MUST support the communication of match and action rules to support Virtual Networks in the case that the routing protocol is deployed on the DBNG-CP.

It is also valid for the IGP to be deployed on the user plane (such that the DBNG-UP can be responsible for reacting to local topology changes) but BGP or other service level control plane is deployed on the DBNG-CP. In this case, the DBNG-CP does not have full information to program the DBNG-UP, and the DBNG-UP does not have VPN level information. The DBNG-CP must therefore request a recursive lookup via the SCi (for example: the DBNG-CP may signal service label and next hop IP to the DBNG-UP, and the DBNG-UP will use this to correctly install the forwarding entry)

[R-27] The SCi MUST support the communication of an action rule with a recursive lookup.

5.2 Control packet redirect interface requirements

[R-28] Subscriber control messages to and from RGs MUST be tunneled between DBNG-CP and DBNG-UP through the control packet redirect interface.
[R-29] 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-30] The DBNG-UP MUST pass access interface information (eg. vpn, port or virtual-port on which the control traffic is received) together with the tunneled subscriber control packet to the DBNG-CP where applicable. eg. control packets: DHCP PPP, RA, data-trigger
[R-31] The DBNG-CP MUST pass access interface information (e.g., vpn, port or virtual-port on which the control traffic is received) together with the tunneled control packet to the DBNG-UP where applicable.
[R-32] 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-33] The DBNG-CP MUST be able to send control packets to the A10 interface through the DBNG-UP
[R-34] 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 type of services provided by the DBNG. E.g. some subscribers connect to the internet using PPPoE, IPTV services through DHCP, and only enterprise customers are using data-trigger service.
[R-35] 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

In all circumstances, redirected control packets should be rate limited to protect the DBNG-CP. The DBNG should be able to treat subscriber individually. E.g. rate limiting malicious users from the rest of the subscriber rate limit data-trigger subscriber redirected packets and prioritize control messages for authenticated subscriber vs. yet to be authenticated subscriber. Unnecessary control packets must be filtered out at the DBNG-UP before reaching the control packet redirect interface.
[R-36] The CUPS protocol MUST allow the DBNG-CP to signal the DBNG-UP the priority of specific control messages (proposal) per match criteria. e.g. match criteria could be a granular as per subscriber or as general as per DBNG-UP node.
[R-37] The DBNG-UP MUST be able to perform rate limit on the control packets per subscriber
Notes: where the control packets include the data-trigger packets.

5.3 Management interface requirements

One of the main functions of the CUPS management interface is a 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. Some example of increasingly popular encoding used in today's network are: Extensible Markup Language (XML 1.0) and Protocol Buffer (protobuf ver3) binary encoding.

Editor's note for reference: protobuf (ver3) and XML reference. How YANG is encoded into XML and protobuf.

Extensible Markup Language (XML) was designed to store and transport data. XML was designed to be self-descriptive and is human-readable. Protocol Buffers (commonly referred to as protobuf) are encoded into binary format. The main advantage is that it is significantly smaller than XML. Therefore, it is much faster to parse and encode for state retrieval.

[R-38] The management interface MUST support transactional config from DBNG-CP to DBNG-UPs based on YANG data model

[R-39] The management interface MUST support operational state retrieval based on YANG data model

5.4 Disaggregated BNG control plane requirements

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

[R-40] DBNG-CP MUST support IPv4/IPv6 address pool management;

[R-41] DBNG-CP MUST support IPv4/IPv6 address prefix and prefix length allocation

[R-42] DBNG-CP MUST support resource and state management of DBNG-UP;

[R-43] DBNG-CP MUST support association and disassociation with DBNG-UP;

Editor's note: R-42 and R-43 are amended from the minutes on Sept 3 Q3 2019 meeting. In addition Control Procedure must be anchored to a particular agreed call flow.

[R-44] 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-45] DBNG-CP MUST be able to support dynamic address prefix allocation on behalf of DBNG-UP upon subscriber access control procedure.

5.5 Disaggregated BNG user plane requirements

DBNG-U is responsible for routing control and subscriber data forwarding, and terminates user's 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 which process the light-traffic services.

[R-46] DBNG-UP MUST support network management interfaces to the operator's EMS.

[R-47] The DBNG-UP MUST support V-interface encapsulations

5.6 Disaggregated BNG functional requirements

"Editor's Note: The status (i.e., MUST, SHOULD, MAY) of these requirements is intended to be a starting point for discussion and initial agreement. Contributions are encouraged to discuss, justify and refine more stringent status (i.e., MUST, SHOULD, MAY) specification."

[R-48] The protocol MUST support cold standby for a redundant DBNG-CPs.
[R-49] The protocol MUST support cold standby for a redundant DBNG-UPs.
[R-50] The protocol SHOULD support warm standby for a redundant DBNG-CPs.
[R-51] The protocol SHOULD support warm standby for a redundant DBNG-UPs.
[R-52] The protocol MAY support hot standby for a redundant DBNG-CPs.
[R-53] The protocol MAY support hot standby for a redundant DBNG-UPs.

6 PFCP CUPS protocol

PFCP is the selected CUPS protocol for the DBNG state control interface 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 “interface between the control plane and user plane node”. PFCP addresses the technical and functional requirements listed in this document.

PFCP contains two main message types: node messages and session messages. Node messages are mainly used to form association between DBNG-CP and DBNG-UP. Session message are mainly used to program the subscriber forwarding state. Both node and session message 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 Table 8.1.2-1. The following section describe IE extensions required to support various BNG use cases.

6.1 PFCP messages

6.1.1 PFCP node messages

PFCP node message consists of:

- 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: program subscriber forwarding state, typically used when a subscriber is logs onto the DBNG.
- Session modification: update subscriber forwarding state, typically used to update subscriber attributes when can be triggered by a RADIUS CoA
- Session deletion: removing a subscriber forwarding state, typically used when a subscriber terminates the broadband session or logs off the network.
- Report session: report information about the session, allows the DBNG-UP to report subscriber PFCP session information to the DBNG-CP.

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): specify the matching criteria for packets
- Forward action Rule (FAR): specify the action (e.g. forward/drop/mirror) to be taken based on the matching PDI.
- QoS Enforcement Rule (QER): specify the QoS treatment based on the matching PDI.
- Usage Reporting Rule (URR) : specify 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 BNG use cases, this document separates PDRs two categories.

- PDRs to match on subscriber control packets
  - Typically require a minimum of two PDRs 1) to redirect control packets from BNG access to the DBNG-CP through the CPRi and 2) to redirect control packets from DBNG-CP back to the BNG access through the CPRi. Control packets can include: DHCP, PPP discovery, and router solicits
- PDRs to match on subscriber data packet
  - Again, typically require a minimum of two PDRs 1) to forward traffic upstream by matching on data packets arriving from the BNG access and forwarding the packets to the network interface 2) to forward traffic downstream by matching on IP packets from the network interface and forward 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 and to the DBNG-CP, the following grouped IE 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 rule 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 redirected control packet. The control messages are encapsulated for tunneling.
- For more information on:
  - o Traffic endpoint see section 6.5.5.5
  - o Filter see section 6.2.3

A typical template is constructed below as a reference for control packet redirection from the DBNG-UP to the DBNG-CP through the CPRi.

Direction	PDR	FAR

Control packet from DBNG-UP 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 encap 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:
  - o Traffic endpoint see section 6.5.5.5

From the attributes above, a typical template is constructed below for control packet redirection from the DBNG-UP to the DBNG-CP through the control packet redirect interface.

Direction	PDR	FAR
Control packet from DBNG-CP to DBNG-UP	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 utilize a list of IEs PDR, FAR, QER, and URR 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 rule 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.
- QER ID – optional IE to specify the QoS rule for the subscriber upstream data traffic
- URR ID – optional IE to specify the Accounting rule for the subscriber upstream data traffic
- For more information on:
    - Traffic endpoint see section 6.5.5.5
    - BBF Outer Header removal see section 6.6.4

Below is a typical template for upstream data packet forwarding from the subscriber through the DBNG-UP and then to the network core.

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

***Bolded text indicates BBF PFCP extension**

For the downstream direction, IP packets routes 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.
- QER ID – an optional IE to specify the QoS rule for the subscriber downstream data traffic
- URR ID – an optional IE to specify the Accounting rule for the subscriber downstream data traffic
- For more information on:
    - Traffic endpoint see section 6.5.5.5

- BBF Outer Header creation see section 6.6.3

Below is a typical template for upstream data packet forwarding from the subscriber through the DBNG-UP and then to the network core.

Direction	PDR	FAR

Downstream	PDR ID
	PDI:
	  Source Interface
	  Traffic-Endpoint
	FAR ID
	QER ID
	URR 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 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 TS 29.244. 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 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 CPRi 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 CPRi a new extension is required:

- BBF UP Function Features: A BBF IE extension for capability flag. In this case, additional flag 'CPRI' is required. Please see new extension in section 6.5.1

6.3.1.1 PFCP control packet redirection rule

Control packet redirection PFCP rules follows the general description highlighted in section 0. Filters rule would be required to match control packet including: DHCPv4 and PPPoE. A new extension is required for 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 NSH header 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 is split between control packet forwarding and data traffic forwarding. Control packets, DHCP, DHCPv6, and router solicit packets should be redirected through the CPRi to DBNG-CP for address assignment. And subscriber IPoE data traffic are forwarded through the network interface.

6.3.2.1 PFCP Control Pack redirection rule

Control packet redirection PFCP rules follows the general description highlighted in section 6.3.2.1. 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

6.3.2.2 PFCP Data Packet Forwarding rule

Data packet forwarding PFCP rules follows the general description highlighted in section 6.3.3.2. Below are further extensions are required to support IPoE use case for data forwarding:

- BBF Outer Header Removal: BBF IE extension to remove the Ethernet header from data packets before forwarding to the network interface. Details of the extension are in section 6.6.4
- BBF Outer Header Creation: BBF IE extension to construct the Ethernet header for packet forwarding to the subscriber. Details of the extension are in section 6.6.3
- 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

6.3.3 Use case: PPPoE

For PPPoE, the forwarding is 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 CPRi while PPPoE data traffic should be routed through the network interface.

6.3.3.1 PFCP Control Pack redirection rule

PFCP Control packet redirection PFCP rules follows the general description highlighted in section 6.3.2.1. 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:

- 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
- Ethernet packet filter IE extension required: to specify PPP attributes such as the PPP protocol type. Details of the extension are in section 6.5.5.2
- BBF PFCP-SMreq-flags: to trigger LCP keepalive checks from the DBNG-CP

6.3.3.2 PFCP Data Packet Forwarding rule

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

- BBF Outer Header Removal: a BBF IE extension to remove the PPPoE header from data packets before forwarding to the network interface. Details of the extension are in section 6.6.4
- BBF Outer Header Creation: a BBF IE extension to construct the PPPoE header for packet forwarding to the subscriber. Details of the extension are in section 6.6.3
- 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
- Ethernet packet filter IE extension required: to specify PPP attributes such as the PPP . Details of the extension are in section 6.5.5.2
- L2 connectivity IE: An IE to specify the LCP echo hello properties. Note, upon failure, PFCP session report from the DBNG-UP it sent to the DBNG-CP informing the inactivity.
- MTU: used to enforced 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, authentication will inform the BNG that the subscriber requires a 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 tunnel to the LNS. Therefore, the PFCP sessions are as follows:

1. 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. A modification to subscriber PFCP session 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 CP and UP. The PFCP rules to redirect L2TP tunnel setup control messages follow the general description highlighted in section 6.2.1instead 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 CP. Further extensions are required on Traffic Endpoint to support L2TP tunnel signaling:

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

6.3.4.2 PFCP update for L2TP session

The PFCP rule in section 6.3.3.1 will be updated to continue to redirect PPPoE discovery control packets to the local LAC CP. While previous PPP control packets redirected to the LAC CP would be updated to be forwarded to the LNS instead, specified in section. Both PPP control and data packet forwarding PFCP rules to the LNS follows 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 Removal: BBF IE extension 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
- BBF Outer Header Creation: BBF IE extension to construct the Ethernet downstream and creating the L2TP header upstream. Details of the extension are in section 6.6.3
- 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
- Ethernet packet filter IE extension required: to specify PPP attributes such as the ppp protocol. Details of the extension are in section 6.5.5.3
- L2TP type: Identify to only match on L2TP data messages.

6.3.5 Use Case: L2TP LNS

After UP and CP association, a default PFCP rule is install to redirect new L2TP control message for tunnel setup from UP to 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 are used to redirect L2TP control packets from the UP to 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 UP to 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
- L2TP type: Identify to only match on L2TP control messages.

6.3.5.2 PFCP Control Pack 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 follows the general description highlighted in section 6.2.1. L2TP data packet containing PPP control message must be redirected to the CP for processing. Further extensions are required on Traffic Endpoint and Ethernet Filter to support L2TP use case:

- 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
- Ethernet packet filter IE extension required: to redirect PPP control messages within the L2TP data packet only. Details of the extension are in section 6.5.5.3
- L2TP type: Identify to only 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 6.3.6.3. Further extensions are required to support LNS use case for data forwarding:

- BBF Outer Header Removal: BBF IE extension to remove the both l2tp and ppp header in the upstream direction. Details of the extension are in section 6.6.4

- BBF Outer Header Creation: BBF IE extension to construct both L2TP and PPP header downstream. Details of the extension are in section 6.6.3
- 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
- L2TP type: Identify to only match on L2TP data messages.
- L2 connectivity IE: An IE to specify the LCP echo hello properties. Note, upon failure, PFCP session report from the UP it sent to the CP informing the inactivity.
- MTU: used to enforced the MRU specified by the CPE

6.3.6 Use Case: TWAG

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

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

Both options are covered in section 6.3.6.1. Afterwards, the PFCP session will update the 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 encap

6.3.6.1 DBNG-UP TEID assignment (optional)

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

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

6.3.6.2 PFCP Control Pack redirection rule

For upstream: From step 8 of the layer 2 trigger initial attached call flow and step 12 of the layer 3 trigger initial attached call flow, the PDN GW would have assigned the BNG-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 CPRi following the general description highlighted in section 6.3.6.2. 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

6.3.6.3 PFCP Data Packet Forwarding rule

Data packet forwarding PFCP rules follows the general description highlighted in section 6.3.6.3. Further extensions are required to support TWAG use case for data forwarding:

- BBF Outer Header Removal: BBF IE extension 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

6.4 BBF PFCP Information Element Summary

A PFCP message may contain several IEs. In order to have forward compatible type definitions for the PFCP IEs, all of them shall be TLV (Type, Length, Value) coded. BBF PFCP IE type values are specified in the Table 5.

Table 5: BBF extended Information Element Types and applicability

IE Type value (Decimal)	Information Element	Section Ref.	CP and UP Assoc.	Default CPR.	PPPoE	IPoE	LAC tunnel	LAC sub session	LNS tunnel	LNS sub 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	BBF UE IP Address	6.6.5	No	Opt	Yes	Yes	No	No	No	Yes	Yes
32773	PPPoE Session ID	6.6.6	No	No	Yes	No	No	Yes	No	No	No
32774	PPP protocol	6.6.7	No	Opt	Yes	No	No	Yes	No	Yes	No
32775	Verification Timers	6.6.8	No	No	Yes	No	No	No	No	Yes	No
32776	PPP LCP Magic Number	6.6.9	No	No	Yes	No	No	No	No	Yes	No
32777	MTU	6.6.10	No	No	Yes	No	No	No	No	Yes	No
32778	L2TP tunnel endpoint	6.6.11	No	Opt	No	No	Yes	Yes	Yes	Yes	No
32779	L2TP session ID	6.6.12	No	No	No	No	No	Yes	No	Yes	No
32780	L2TP type	6.6.13	No	Opt	No	No	Yes	Yes	Yes	Yes	No
32781	PPP LCP connectivity	6.5.7	No	No	Yes	No	No	No	No	Yes	No
32782	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 BNG use cases.

6.5.1 PFCP Association Setup Request

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

Table 6: BBF extended Information Element(s) in a PFCP Association Setup Request

Information elements	P	Condition / Comment	IE Type
BBF UP Function Features	C	This IE shall 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 shall indicate the features the BBF DBNG-UP function supports.	**BBF UP Function Features**

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 CPRi functional support.

Table 7: BBF extended Information Element(s) in a PFCP Association Setup Response

Information elements	P	Condition / Comment	IE-Type
BBF UP Function Features	O	This IE shall 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 shall indicate the features the BBF DBNG-UP function supports.	**BBF UP Function Features**

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 CPRi functional support.

Table 8: BBF extended Information Element(s) in a PFCP Association Update Request

Information elements	P	Condition / Comment	IE Type
BBF UP Function Features	C	This IE shall 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 shall indicate the features the BBF DBNG-UP function supports.	**BBF UP Function Features**

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 CP of CPRi functional support.

Table 9: BBF extended Information Element(s) in a PFCP Association Update Response

Information elements	P	Condition / Comment	IE-Type
BBF UP Function Features	O	This IE shall 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 shall indicate the features the BBF DBNG-UP function supports.	**BBF UP Function Features**

6.5.5 PFCP Session Establishment Request

Table 10: BBF extended Information Element(s) in an PFCP Session Establishment Request

Information elements	P	Condition / Comment	IE Type
PPP LCP connectivity	C	This IE shall be present if periodic LCP echo hello is required.	**L2 connectivity**

6.5.5.1 Create PDR

The Create PDR grouped IE

Table 11: 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 elements	**P**	**Condition / Comment**	**IE Type**
BBF Outer Header Removal	C	This IE shall be present if the DBNG-UP function is required to remove header(s) from the packets matching this PDR.	**BBF Outer Header Removal**

6.5.5.2 PDI

Table 12: 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 elements	**P**	**Condition / Comment**	**IE Type**
L2TP type	C	This IE shall identify the L2TP type control or data	L2TP type

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. The IE is used to match on sub flow of a traffic endpoint.

Table 13: 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 elements	**P**	**Condition / Comment**	**IE Type**
PPP Protocol	O	If present, this IE shall identify the PPP protocol to match for the incoming packet. (see section 6.6.7 for IE details)	PPP Protocol

6.5.5.4 Forwarding Parameters

Table 14: 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 shall be present if the DBNG-UP function is required to add outer header(s) to the outgoing packet.	BBF Outer Header Creation
MTU	C	This IE shall be present to enforce an MTU on outgoing packets. In the case of PPPoE, this may be based on negotiated MRU value	MTU

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 RS 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.

Editor's note: <presence flag should be worked in later>

Table 15: 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		If present, this IE identify the MAC address of the traffic endpoint. (see 3GPP TS 29.244 for IE details)	MAC address
C-TAG		If present, this IE identify the customer VLAN tag of the traffic endpoint (see 3GPP TS 29.244 for IE details)	C-TAG
S-TAG		If present, this IE identify the service VLAN tag of the traffic endpoint (see 3GPP TS 29.244 for IE details)	S-TAG
BBF Extended IEs below			
Logical Port		If present, this IE provides 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
PPPoE Session ID		If present, this IE identify the PPPoE session ID of the subscriber. (see section 6.6.5 for IE details)	PPPoE Session ID
L2TP tunnel		This IE shall be present if a L2TP tunnel is required. (see section 6.5.8 for IE details)	L2TP tunnel

6.5.6 PFCP Session Modification Request

Table 16: BBF extended Information Element(s) in a PFCP Session Modification Request

Information elements	P	Condition / Comment	IE Type
PPP LCP connectivity	C	This IE shall be present if periodic LCP echo hello is required.	**L2 connectivity**

6.5.6.1 Update PDR

The Update PDR grouped IE.

Table 17: 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 elements	**P**	**Condition / Comment**	**IE Type**
BBF Outer Header Removal	C	This IE shall be present if the DBNG-UP function is required to remove header(s) from the packets matching this PDR. This IE shall be present if it needs to be changed.	**BBF Outer Header Removal**

6.5.6.2 Update Forwarding Parameters

Table 18: 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 elements	**P**	**Condition / Comment**	**IE Type**
BBF Outer Header Creation	C	This IE shall be present if the DBNG-UP function is required to add outer header(s) to the outgoing packet. This IE shall only be provided if it is changed.	BBF Outer Header Creation
MTU	C	This IE shall be present to enforce an MTU on outgoing packets. In the case of PPPoE, this may be based on negotiated MRU value	MTU

6.5.6.3 Update Traffic Endpoint IE

Table 19: 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		If present, this IE identify the MAC address of the traffic endpoint and needs to be changed. (see 3GPP TS 29.244 for IE details)	MAC address
C-TAG		If present, this IE identify the customer VLAN tag of the traffic endpoint and needs to be changed (see 3GPP TS 29.244 for IE details)	C-TAG
S-TAG		If present, this IE identify the service VLAN tag of the traffic endpoint and needs to be changed (see 3GPP TS 29.244 for IE details)	S-TAG
BBF Extended IEs below			
Logical Port		If present, this IE provides 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
PPPoE Session ID		If present, this IE identify the PPPoE session ID of the subscriber and needs to be changed. (see section 6.6.5 for IE details)	PPPoE Session ID
L2TP tunnel		This IE shall be present if a L2TP tunnel is required and needs to be changed. (see section 6.5.8 for IE details)	L2TP tunnel

6.5.7 L2 Connectivity

The table below is a new BBF specified grouped IE used to specify l2 connectivity check parameters.

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

Octet 1 and 2	L2 Connectivity IE Type = NN (decimal)		
Octets 3 and 4	Length = n		
Octest 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	**O**	**This IE indicates the frequency and number of retries for verification messages.** **If this IE is not present, no periodic verification is started.**	**Verification Timers**
PPP LCP Magic Number	**C**	**If present this IE indicates which magic number to use when generating keepalives and which magic number to verify incoming keepalives against.**	**PPP LCP Magic Number**

Table 20: L2 Connectivity

6.5.8 L2TP Tunnel

Octet 1 and 2	Update Forwarding Parameters IE Type = 11 (decimal)		
Octets 3 and 4	Length = n		
Information elements	**P**	**Condition / Comment**	**IE Type**
L2TP tunnel endpoint	C	A BBF specific extended IE The CP function shall set the CHOOSE (CH) bit to 1 if the UP function supports the allocation of L2TP tunnel IP address and the CP function requests the UP function to assign the L2TP tunnel IP to the Traffic Endpoint. If present, this IE identify the L2TP tunnel ID and IP information. (see section 6.6.11 for IE details)	L2TP tunnel endpoint
L2TP Session ID	O	If present, this IE identify the L2TP session ID. (see section 6.6.12 for IE details)	L2TP session ID

Table 21: L2TP Tunnel

6.6 BBF PFCP IE extensions

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

Figure 28 depicts the format of a vendor-specific Information Element, which content is not specified and the IE Type value shall 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 28: Vendor-Specific Information Element Format

6.6.1 BBF UP Function Features

The BBF UP Function Features IE indicates the features supported by the DBNG-UP function. It is coded as depicted in Figure 8.2.25-1.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = NN decimal)							
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 29: 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. Spare bits must be set to zero by senders and shall be ignored by the receiver.

The following table specifies the features defined on the DBNG-UP.

Table 22: BBF UP Function Features

Feature Octet / Bit	Feature	Description
7/1	CPRi	Informs the DBNG-CP that the UP supports CPRi
7/2	LNS	Informs the DBNG-CP that the DBNG-UP supports LNS

6.6.2 Logical Port

The Logical Port IE shall be encoded as:

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = NN decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID (3561?)							
7 to n+4	logical-port-id							

Figure 30: Logical Port

Octets “7 to n+4” encode an logical-port-id, which is an opaque value to indicate the logical port on which ethernet traffic is received. This should not contain S-VLAN or C-VLAN values, which are signaled more explicitly in PFCP.

6.6.3 BBF Outer Header Creation

The BBF Outer Header Creation indicates a header is to be added to the packet before forwarding. The BBF Outer Header also contain parameters to construct the header. This IE can be used in combination with the Outer Header Creation IE. If both are present, both header 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 = NN decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID (3561?)							
7 to 8	Outer Header Creation Description							
m to m+1	Tunnel ID							
p to p+1	Session ID							
q to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 31: BBF Outer Header Creation

The BBF Outer Header Creation Description field, when present, shall be encoded as specified in **Error! Reference source not found.**. It takes the form of a bitmask where each bit indicates the outer header to be created in the outgoing packet. Spare bits shall be ignored by the receiver.

Tunnel ID: indicates the L2TP Tunnel ID

Session ID: indicates the L2TP Session ID

Table 23: 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**

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

- CPR-NSH: an NSH header 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 encap the PPP packet with a L2TP header before forwarding to LNS. For LNS, this is used in combination with PPP to encap the IP packet with both PPP and L2TP before forwarding to the LAC.
- PPP – creates the PPP data packet header.

*Editor's Note: for meta data, there need to explicit data to be included in the meta is to be further discussed.

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. This header looks as follows:

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Ver|O|U|    TTL    |   Length  |U|U|U|U|MD Type| Next Protocol |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Service Path Identifier              | Service Index |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Metadata Class       |      Type     |U|    Length   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                   Variable-Length Metadata                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   ~                                                               ~
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Metadata Class       |      Type     |U|    Length   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                   Variable-Length Metadata                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 32: NSH header information

Where OAM is 0, TTL is 1, MD Type is 2 and Next Protocol is 0x3 (ethernet). Service Path Identifier is initially not used and always 0, service index is 255. Version and (NSH) length are per RFC.

A DBNG specific Metadata class will be allocated, with following types:

- Logical port (0, length=N): an opaque byte string identifying an access context on a DBNG-UP (e.g. port, lag, ethernet tunnel, …)
- MAC (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 is encoded as shown:

<table>
<tr><th></th><th colspan="8">Bits</th></tr>
<tr><th>Octets</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td>1 to 2</td><td colspan="8">Type = NN decimal)</td></tr>
<tr><td>3 to 4</td><td colspan="8">Length = n</td></tr>
<tr><td>5 to 6</td><td colspan="8">Enterprise ID (3561?)</td></tr>
<tr><td>7 to 8</td><td colspan="8">Outer Header Removal Description</td></tr>
<tr><td>9 to (n+4)</td><td colspan="8">These octet(s) is/are present only if explicitly specified</td></tr>
</table>

Figure 33: BBF Outer Header Removal

The Outer Header Removal Description field shall be an 8-bit integer and indicates which headers need to be removed from an incoming packet. The values are as defined as follows:

Table 24: 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: removal the ethernet header including S-Tags and C-Tags.
- PPPoE / Ethernet: removal of the PPP header and ethernet header including S-Tags and C-Tags.
- PPP / PPPoE/ Ethernet: removal of the PPP header, PPPoE header, and ethernet header including S-Tags and C-Tags.
- L2TP: removes only the L2TP header
- PPP/L2TP: removes PPP and L2TP header together.

6.6.5 BBF UE IP Address (editor's note: awaiting 3GPP confirmation)

The BBF UE IP Address IE type shall be encoded as shown in Figure 8.2.62-1. It contains a source or destination IP address. The below IE is intended to be same as the 3GPP IE UE IP Address which is currently under approval process to allow IANA and multiple IPv6 prefix/address assignment.

(Editor's note: This IE can only send 1 IPv4 and 1 iPv6 address, there it will need to be repeated within an IE to indicate the multiple IP address(es) assigned to the subscriber. For example, BBF UE IP address is repeated 2 times inside Create Traffic Endpoint IE to express 1 IPv4 address and 1 IPv6 address. It is typical for a wireline subscriber to be assigned more than one UE IP address.)

<table>
<tr><th></th><th colspan="8">Bits</th></tr>
<tr><th>Octets</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td>1 to 2</td><td colspan="8">Type = NN</td></tr>
<tr><td>3 to 4</td><td colspan="8">Length = n</td></tr>
<tr><td>5 to 6</td><td colspan="8">Enterprise ID</td></tr>
<tr><td>7</td><td colspan="2">Spare</td><td>IP6PL</td><td>CH</td><td>IPv6D</td><td>S/D</td><td>V4</td><td>V6</td></tr>
<tr><td>m to (m+3)</td><td colspan="8">IPv4 address</td></tr>
<tr><td>p to (p+15)</td><td colspan="8">IPv6 address</td></tr>
<tr><td>r</td><td colspan="8">IPv6 Prefix Delegation Bits</td></tr>
<tr><td>s</td><td colspan="8">IPv6 Prefix Length</td></tr>
<tr><td>k to (n+4)</td><td colspan="8">These octet(s) is/are present only if explicitly specified</td></tr>
</table>

Figure 34: BBF UE IP Address

The following flags are coded within Octet 5:

- Bit 1 – V6: If this bit is set to "1" and the CH bit is not set, then the IPv6 address field shall be present in the UE IP Address, otherwise the IPv6 address field shall not be present.
- Bit 2 – V4: If this bit is set to "1" and the CH bit is not set, then the IPv4 address field shall be present in the UE IP Address, otherwise the IPv4 address field shall not be present.
- Bit 3 – S/D: This bit is only applicable to the UE IP Address IE in the PDI IE. It shall be set to "0" and ignored by the receiver in IEs other than PDI IE. In the PDI IE, if this bit is set to "0", this indicates a Source IP address; if this bit is set to "1", this indicates a Destination IP address.
- Bit 4 – IPv6D: This bit is only applicable to the UE IP address IE in the PDI IE and when V6 bit is set to "1". If this bit is set to "1", then the IPv6 Prefix Delegation Bits field shall be present, otherwise the UP function shall consider IPv6 prefix is default /64.
- Bit 5 – CH (CHOOSE): If this bit is set to "1", then the IPv4 address and IPv6 address fields shall not be present and the UP function shall assign an IP4 or an IPv6 address if the V4 or V6 bit is set respectively. This bit shall only be set by the CP function.
- Bit 6 – IP6PL (IPv6 Prefix Length): this bit is only applicable when the V6 bit is set to "1" and the "IPv6D" bit is set to "0", for an IPv6 prefix other than default /64. If this bit is set to "1", then the IPv6 Prefix Length field shall be present.
- Bit 7 to 8 Spare, for future use and set to 0.

Octets "m to (m+3)" or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.
Octet r, if present, shall contain the number of bits allocated for IPv6 prefix delegation (relative to the default /64 IPv6 prefix), e.g. if /60 IPv6 prefix is used, the value shall be set to "4". When using UE IP address IE in a PDI to match packets, the UP function shall only use the IPv6 prefix part and ignore the interface identifier part.
The IPv6 Prefix Length in octet s, when present, shall be encoded as a 8 bits binary integer, e.g. if /72 prefix is used, the value shall be set to to (decimal) 72. The prefix length value "128" indicates an individual /128 IPv6 address.

6.6.6 PPPoE Session ID

The PPPoE Session ID IE shall be encoded as:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = NN decimal)							
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 35: PPPoE Session ID

Octets “7 to 8” encode a PPPoE Session ID as specified in RFC 2516.

6.6.7 PPP Protocol

The PPP Protocol IE shall be encoded as:

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = NN decimal)							
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 36: PPP Protocol

Following flags are encoded in octet 7:

Exactly one shall be set:

- 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.

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

6.6.8 Verification Timers

The Verification Timers IE shall be encoded as:

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = NN decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID (3561?)							
7 to 10	Interval							
P to (p+3)	count							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 37: Verification Timers

Octets 7 to 8: specify an unsigned 16 bit interval in 10 milli-seconds that indicates how frequent the verification procedure is started.
Octet 9: specifies an unsigned 8 bit integer on how many unanswered keepalive messages should be sent before connection is considered down.

6.6.9 PPP LCP Magic Number

The PPPoE LCP Magic Number IE shall be encoded as:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = NN decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID (3561?)							
7 to 10	Tx Magic Number							
P to (p+3)	Rx Magic Number							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 38: PPP LCP Magic Number

Octets “7 to 10” encode a PPP LCP Magic Number as defined in RFC 1661. This is the magic number used when transmitting LCP keepalive messages.
Octets “p to p+13” are only present if length >=10 and encode a PPP LCP Magic Number as defined in RFC 1661. When present, received LCP keepalive messages need to verified against this magic number. When not present (length < 10), magic numbers are not verified.

6.6.10 MTU

This IE shall be encoded as:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = NN decimal)							
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 39: MTU

The MTU shall be encoded as an unsigned 16-bit integer value. Packets exceeding the MTU must either be fragmented (IPv4 without DF bit) or answered with an ICMP/ICMPv6 Packet Too Big error code (IPv4 with DF bit, IPv6). MTU is applied on IP level, before any outer header or ethernet encapsulation. A UPF may apply a lower MTU if the associated forwarding construct requires so.

6.6.11 L2TP Tunnel Endpoint

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = NN decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID (3561?)							
7						CH	V6	V4
8 to 9	Tunnel ID							
p to p+3	IPv4 Address							
q to q+15	IPv6 Address							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 40: L2TP Tunnel Endpoint

-v4, v6, and CH are mutually exclusive. IPv4 means an IPv4 address is included, IPv6 means an IPv6 address is included and CH means no IP is included and the UP should reflect the chosen IP in the response. (CH clarificaition)

Tunnel ID – specify the L2TP tunnel ID to match
IPv4 address – specify the L2TP IPv4 local terminating address
IPv6 address – specify the L2TP IPv6 local terminating address

6.6.12 L2TP Session ID

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

Figure 41: L2TP Session ID

Where:
L2TP session ID – specify the L2TP session ID to match

6.6.13 L2TP type

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = NN decimal)							
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							

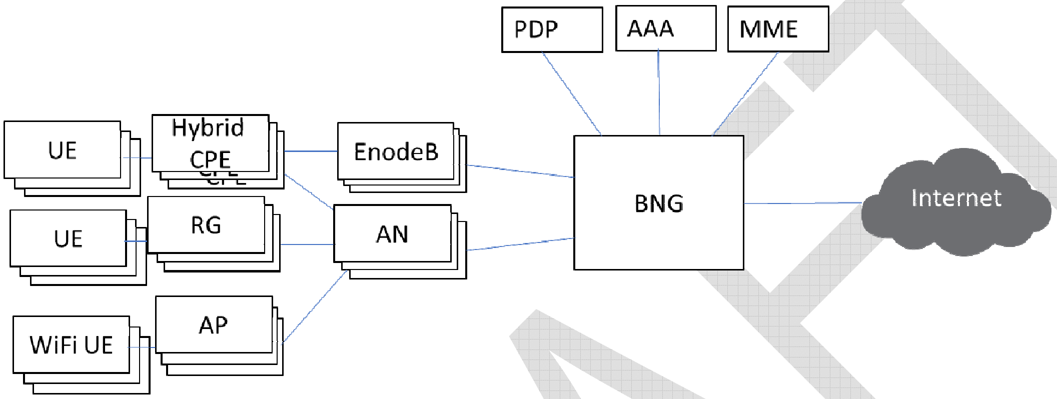
Figure 42: L2TP type

Where:
T identify the l2tp type, 1 means l2tp control and 0 means l2tp data (RFC 2661)

Annex A: Use Cases

A.1 Multi-access BNG CUPS use case

Since TR-101, the BNG have evolved beyond basic broadband wireline access. The BNG has enable broadband services to be served over multiple access types which includes: fixed line users, hybrid access, and even public wifi. The figure below, depicts a multiple server BNG serving multiple access. Each “box” below represents a single physical network element. Redundancy mechanism within a single physical network element is out of scope of this use case.

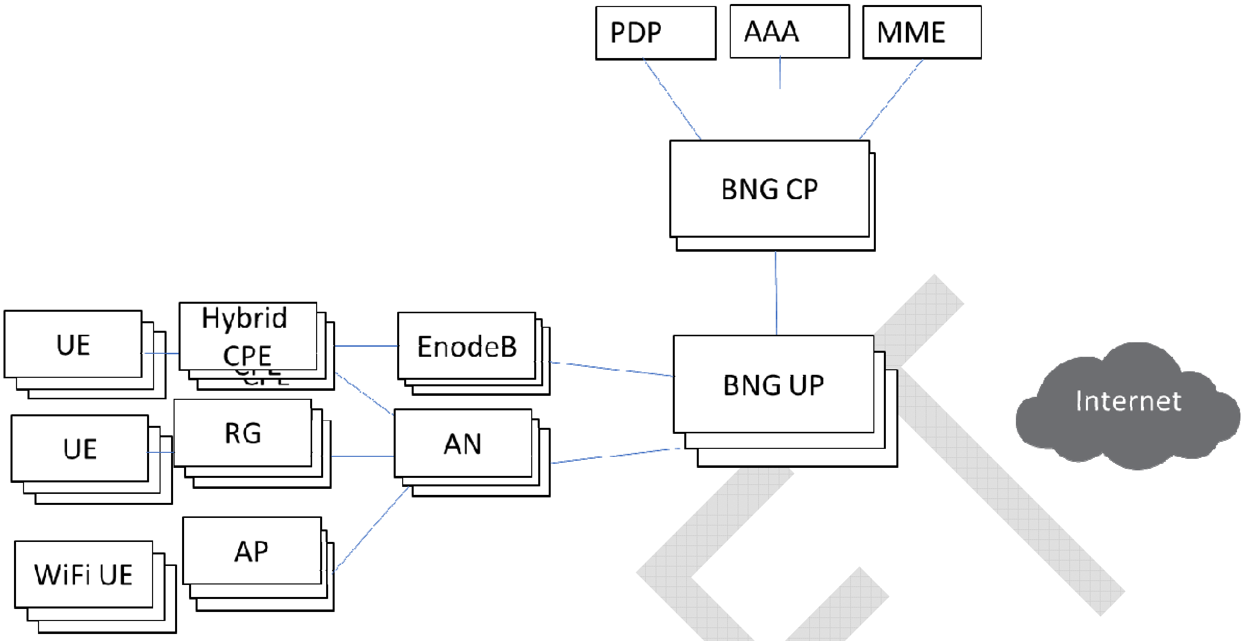


As subscribers scale and bandwidth scale increased, traditionally, this required introducing a new BNG into the network. The new BNG is a separate entity and require separate commissioning.

BNG control and user plane separation addresses:

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

BNG CUPS simplifies in scaling up both subscriber and bandwidth. The CUPS architecture must allow the service provider to either 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 provide a single point of management for all User Plane instances. The BNG CUPS architecture must continue to offer the same number of functions as today’s BNGs deployed in production networks.



A.2 Wireline-Access disaggregated BNG use case

From perspective of wireline access services, it consists of residential subscriber access service and enterprise access service. Residential subscriber access services include HSI, IPTV, VoIP, ITMS (TR-069), and enterprise subscriber access service is usually leased line service. Subscriber dials up through the access network, and BNG User Plane redirects the access control packets to BNG Control Plane which authenticates the subscriber and creates subscriber forwarding entries upon which BNG User Plane forwards the subscriber data traffic. Usually after the completion of the subscriber access procedure, BNG needs to do network address translation for the subscriber, both native IP and MPLS VPN could be the underlying technologies for BNG network-side data traffic forwarding.
The typical wireline access service scenarios include multicasting, CGN, L2TP, LI (Lawful interception) with access types of PPPoE, L2/L3 IPoE, dual-stack IPoE, L2-line, L3-line, L2TP, L2VPN（VLL/VPLS）,etc. Address management will require special consideration when the BNG control plane and use plane function are separated.

A.3 Subscriber frame/network/host route advertisement use case

Normally, the DBNG-CP could allocate one or more blocks of IP addresses to the DBNG-UP. Each address block contains a series of IP addresses. Those IP addresses will be allocated to subscribers who will dial-up to the DBNG-UP.

In order to make sure that other nodes within the network learn how to reach those IP addresses, the DBNG-CP needs to install one or more routes on the DBNG-UP and notify the DBNG-UP to advertise the routes to the network.

A.4 Data Synchronization between DBNG-CP and DBNG-UP use case

Under some circumstances, it is necessary to synchronize state between the DBNG-CP and DBNG-UP. For example: State Control Channel restarts, a DBNG-UP switches to a backup DBNG-CP due to master DBNG-CP failed, etc.

Synchronization includes two directions. One direction is from DBNG-UP to DBNG-CP. The other direction is from DBNG-CP to DBNG-UP.

A.5 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 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.6 Wholesale Retail model with L2TP use case

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-U to the DBNG-C via the general control packet redirect 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). 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, NDRA, 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.

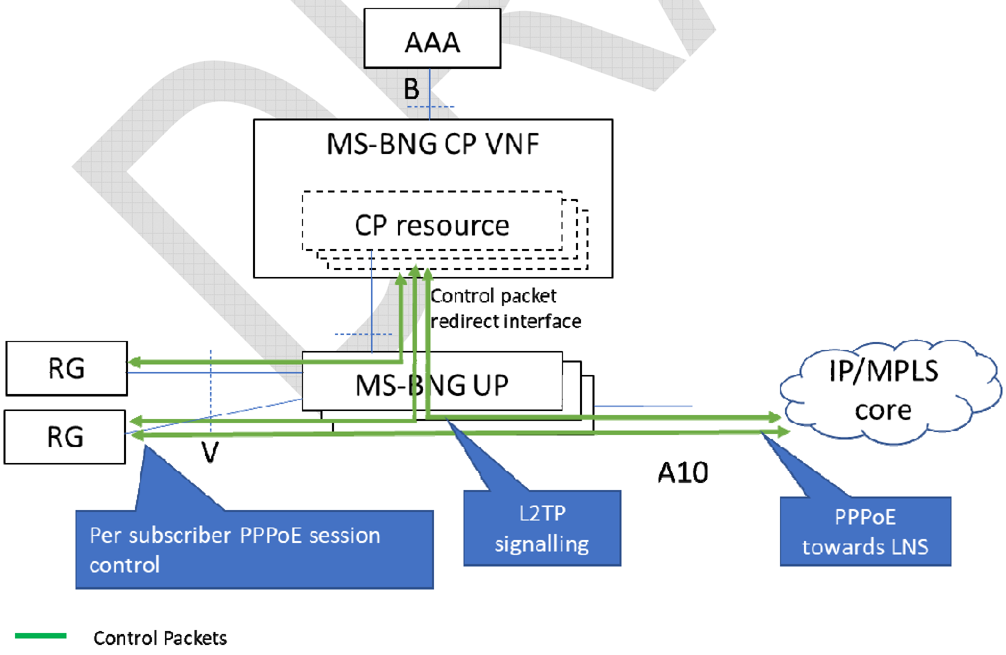


Figure 43: L2TP deployment model