Abstract

This document defines an architecture for Broadband Network Gateway (BNG) devices with control plane (CP) and user plane (UP) separation. A BNG-CP is a user control management component while a BNG-UP takes responsibility as the network edge and user policy implementation component. Both BNG-CP and BNG-UP are core components for fixed broadband services and are deployed separately at different network layers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Distribution of this document is unlimited. Comments should be sent to the authors or the RGTWG working group mailing list: rtgwg@ietf.org.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html. The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.
Table of Contents

1. Introduction............................................3
   1.1 Motivation.............................................3

2. Terminology.............................................4

3. CU Separated BNG Architecture.........................5
   3.1 Internal Interfaces Between the CP and UP..........7

4. Usage of the CU Separation BNG........................8

5. Security Considerations...............................10

6. IANA Considerations....................................10

Normative References.......................................11
Informative References.....................................11

Authors’ Addresses..........................................12
1. Introduction

A Broadband Network Gateway (BNG) device is defined as an Ethernet-centric IP edge router, and the aggregation point for user traffic. It performs Ethernet aggregation and packet forwarding via IP/MPLS, and supports user management, access protocols termination, QoS, policy management, etc.

This document describes an architecture for BNG devices with control plane (CP) and user plane (UP) separation. A BNG-CP is a user control management component while a BNG-UP takes responsibility as the network edge and user policy implementation components. Both BNG-CP and BNG-UP are core components for fixed broadband services and are deployed separately at different network layers in the network.

1.1 Motivation

The rapid development of new services, such as 4K TV, IoT, etc., and increasing numbers of home broadband service users present some new challenges for BNGs such as:

Low resource utilization: The traditional BNG acts as both a gateway for user access authentication and accounting and an IP network’s Layer 3 edge. The mutually affecting nature of the tightly coupled control plane and forwarding plane makes it difficult to achieve the maximum performance of either plane.

Complex management and maintenance: Due to the large numbers of traditional BNGs, configuring each device in a network is very tedious when deploying global service policies. As the network expands and new services are introduced, this deployment mode will cease to be feasible as it is unable to manage services effectively and rectify faults rapidly.

Slow service provisioning: The coupling of control plane and forwarding plane, in addition to a distributed network control mechanism, means that any new technology has to rely heavily on the existing network devices.

To address these challenges for fixed networks, the framework for a cloud-based BNG with CU separation conception is defined in [TR-384]. The main idea of Control-Plane and User-Plane separation is to extract and centralize the user management functions of multiple BNG devices, forming a unified and centralized control plane (CP). And the traditional router’s Control Plane and Forwarding Plane are both preserved on BNG devices in the form of a user plane (UP). Note that the CU separation concept has also been introduced in the 3GPP 5G architecture [3GPP.23.501].
2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following acronyms are used as specified below:


BNG: Broadband Network Gateway. A broadband remote access server (BRAS (Broadband Access Server), B-RAS or BBRAS) that routes traffic to and from broadband remote access devices such as digital subscriber line access multiplexers (DSLAM) on an Internet service provider’s (ISP) network. BRAS can also be referred to as a Broadband Network Gateway (BNG).

CP: Control Plane. The CP is a user control management component which manages the UP’s resources such as the user entry and user’s QoS policy.

DHCP: Dynamic Host Configuration Protocol.

EMS: Element Management System.

IPoE: IP over Ethernet.

MANO: Management and Orchestration.

NFV: Network Function Virtualization.

NFVI: NFV Infrastructure.

PPPoE: Point-to-Point Protocol over Ethernet.

UP: User Plane. UP is a network edge and user policy implementation component. The traditional router’s Control Plane and forwarding plane are both preserved on BNG devices in the form of a user plane.
3. CU Separated BNG Architecture

The functions in a traditional BNG can be divided into two parts: one is the user access management function, the other is the router function. In a cloud-based BNG, we find that tearing these two functions apart can make a difference. The user management function can be centralized and deployed as a concentrated module or device, called the BNG-CP (Control Plane). The other functions, such as the router function and forwarding engine, can be deployed in the form of the BNG User Plane. Thus, the Cloud-based BNG architecture is made up of control plane and user plane.

The following figure describes the architecture of CU separated BNG:

```
+------------------------------------------------------------------+
|        Neighboring policy and resource management systems        |
|                                                                  |
|   +-------------+   +-----------+   +---------+   +----------+   |
|   |AAA    Server|   |DHCP Server|   |   EMS   |   |   MANO   |   |
|   +-------------+   +-----------+   +---------+   +----------+   |
+------------------------------------------------------------------+
+------------------------------------------------------------------+
|                       CU-separated BNG system                      |
| +--------------------------------------------------------------+ |
| |   +----------+  +----------+ +------++------++-----------+   | |
| |   | Address  |  |Subscriber| | AAA  ||PPPoE/||    UP     |   | |
| |   |management|  |management| |      ||IPoE  ||management |   | |
| |   +----------+  +----------+ +------++------++-----------+   | |
| |                              CP                              | |
| +--------------------------------------------------------------+ |
|                                                                  |
|                                                                  |
| +---------------------------+      +--------------------------+  |
| |  +------------------+     |      |  +------------------+    |  |
| |  | Routing control  |     |      |  | Routing control  |    |  |
| |  +------------------+     | ...  |  +------------------+    |  |
| |  |Forwarding engine |     |      |  |Forwarding engine |    |  |
| |  +------------------+  UP |      |  +------------------+  UP|  |
| +---------------------------+      +--------------------------+  |
+------------------------------------------------------------------+
```

Figure 1. Architecture of CU Separated BNG

As in Figure 1, the BNG Control Plane could be virtualized and centralized, which provides significant benefits such as centralized session management, flexible address allocation, high scalability for subscriber management capacity, and cost-efficient redundancy, etc.
The functional components inside the BNG Service Control Plane can be implemented as Virtual Network Functions (VNFs) and hosted in a Network Function Virtualization Infrastructure (NFVI).

The User Plane Management module in the BNG control plane centrally manages the distributed BNG User Planes (e.g. load balancing), as well as the setup, deletion, and maintenance of channels between Control Planes and User Planes. Other modules in the BNG control plane, such as address management, AAA, etc., are responsible for the connection with outside subsystems in order to fulfill those services. Note that the User Plane SHOULD support both physical and virtual network functions. For example, BNG user plane L3 forwarding related network functions can be disaggregated and distributed across the physical infrastructure. And the other control plane and management plane functions in the CU Separation BNG can be moved into the NFVI for virtualization [TR-384].

The details of CU separated BNG’s function components are as following:

The Control Plane should support:

(1) Address management: unified address pool management.

(2) AAA: This component performs Authentication, Authorization and Accounting, together with RADIUS/DIAMETER. The BNG communicates with the AAA server to check whether the subscriber who sent an Access-Request has network access authority. Once the subscriber goes online, this component together with the Service Control component implement accounting, data capacity limitation, and QoS enforcement policies.

(3) Subscriber management: user entry management and forwarding policy management.

(4) PPPoE/IPoE: process user dialup packets via PPPoE/IPoE.

(5) UP management: management of UP interface status, and the setup, deletion, and maintenance of channels between CP and UP.

The User Plane should support:

(1) Control plane functions including routing, multicast, and MPLS.

(2) Forwarding plane functions including traffic forwarding, QoS and traffic statistics collection.
3.1 Internal Interfaces Between the CP and UP

To support the communication between the Control Plane and User Plane, several interfaces are involved. Figure 2 illustrates the internal interfaces of CU Separated BNG.

![Diagram of internal interfaces]

**Figure 2. Internal Interfaces Between the CP and UP of the BNG**

**Service Interface:** The CP and UP use this interface to establish tunnels with each other and transmit PPPoE and IPoE packets over those tunnels. VXLAN is commonly used for such tunnels as discussed in [hu-nvo3-vxlan-gpe-extension-for-vbng].

**Control Interface:** The CP uses this interface to deliver service entries, and the UP uses this interface to report service events to the CP. The requirements of this interface are introduced in [cuspdt-rtgw-cusp-requirements], and the carrying protocol is presented in [cuspdt-rtgw-cu-separation-bng-protocol] which specifies the Simple Control and User Plane Separation protocol (S-CUSP). The information model of this interface is presented in [cuspdt-rtgw-cu-separation-infor-model].

**Management Interface:** The CP uses this interface to deliver configurations to the UP. This interface uses NETCONF [cuspdt-rtgw-cu-separation-yang-model].
4. Usage of the CU Separation BNG

In the CU separated BNG scenario, there are several processes when a home user accesses the Internet:

(1) User dialup packets via PPPoE or IPoE from the BNG-UP are sent to the BNG-CP through the BNG-UP’s Service Interface.

(2) BNG-CP processes the dialup packet. Confirming the user’s authorization with the outside neighboring systems in the management network, the BNG-CP makes the decision to permit or deny the user access.

(3) After that, the BNG-CP tells the UP to do perform authorized forwarding actions with appropriate QoS policies.

(4) If the user is certificated and permitted, the UP forwards the traffic into the Internet with appropriate QoS policies such as limited bandwidth, etc. Otherwise, the user is denied to access the Internet.

In actual deployments, a CU separated BNG device is composed of a CP and one or more UPs. The CP is usually centrally deployed and takes responsibility as a user control management component managing UP’s resources such as the user entry and forwarding policy. The UPs are distributed and act as a network edge and user policy implementation component.

In order to fulfill a service, neighboring policy and resource management systems are deployed outside the BNG. In the neighboring systems, different service systems such as RADIUS/DIAMETER server, DHCP server and EMS are included. If a BNG-CP is virtualized as a NFV, the NFVI management system MANO is also included here. A BNG-CP has connections with the outside neighboring systems to transmit management traffic.

The deployment scenario is shown in the following figure:
Figure 3. Deployment Example
5. Security Considerations

The Service, Control, and Management Interfaces between the CP and UP might be across the general Internet or other hostile environment. Thus, appropriate protections MUST be implemented to provide integrity, authenticity, and secrecy of traffic over those interfaces. For example, the implementation of IPSEC, DTLS, or TLS as appropriate. However, such security protocols need not always be used and lesser security precautions might be appropriate because, in some cases, the communication between the CP and UP might be in a more benign environment.

6. IANA Considerations

This document requires no IANA actions.
Normative References


Informative References


Authors’ Addresses

Shujun Hu
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: hushujun@chinamobile.com

Fengwei Qin
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: qinfengwei@chinamobile.com

Zhengqiang Li
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: lizhenqiang@chinamobile.com

Tee Mong Chua
Singapore Telecommunications Limited
31 Exeter Road, #05-04 Comcentre Podium Block
Singapore City  239732
Singapore

Email: teemong@singtel.com

Victor Lopez
Telefonica
Spain

Email: victor.lopezalvarez@telefonica.com
Copyright, Disclaimer, and Additional IPR Provisions

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Control Plane and User Plane Separated BNG Deployment Model
draft-cuspdt-rtgwg-cu-separation-bng-deployment-02

Abstract

This document describes the deployment model for a Broadband Network Gateway (BNG) device with Control Plane (CP) and User Plane (UP) separation. It is intended to give guidance for the deployment of CP and UP separated BNG devices in an operators' network.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Distribution of this document is unlimited. Comments should be sent to the authors or the BESS working group mailing list: bess@ietf.org.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html. The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Table of Contents

1. Introduction and Overview...............................3
2. Concept and Terminology.................................5
1. Introduction and Overview

A Broadband Network Gateway (BNG) is an Ethernet-centric IP edge router and acts as the aggregation point for the user traffic with some additional functions such as address management and cooperating with AAA (Radius/Diameter) systems and subscriber management. Because of the rapid development of new services, such as 4K, IoT, etc. and the increasing numbers of distributed home broadband service users, high resource utilization, high-efficiency management, and fast service provisioning are required. This calls for a new BNG architecture with CP and UP separation, which is also called Cloud BNG, as proposed in [BBF-CloudCO] [TR-384].

The CP and UP separation architecture of the BNG is composed of a Control Plane and a User Plane, with the concentrated CP responsible for control and management of the UP’s resources and subscribers’ information, and with the distributed UP taking charge of policy implementation and traffic forwarding. The obvious advantages of this new architecture are listed below.

Resource Utilization Improvement: A centralized Control Plane provides unified management capability for network resources and users information. The CP has an overview of all the resources and can distribute resources as specific users require, thus resources can be totally controlled and balanced.

Management with High Efficiency: A centralized CP provides a unified management interface to the outside systems such as EMS, DHCP Server, AAA Server, etc. In this situation, management can be easier for the centralized CP as it’s the only device interfacing with the outside systems.

Dynamic and Flexible: The CP can be virtualized as a VNF with MANO management in an NFVI, while the UP can be a virtual machine or physical device as needed. A software-oriented CP can be designed with flexibility. The CP can handle all the situations dynamically over a wide range from few users accessing to large numbers of users accessing.

Fast TTM: The CP and UP can be deployed separately with the CP deployed centrally and the UP deployed in distribution closer to users. Thus, according to different situations such as session overload or extremely high throughput, the CP and UP can be extended separately. This can help shorten the time to market (TTM).

As noted, the new BNG architecture has CP and UP separation. The CP and UP are deployed with separation due to practical requirements. This document gives the CU separation BNG deployment model for actual
deployments.
2. Concept and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1 Terminology

BNG: Broadband Network Gateway. A broadband remote access server (BRAS, B-RAS or BBRAS) routes traffic to and from broadband remote access devices such as digital subscriber line access multiplexers (DSLAM) on an Internet service provider’s (ISP) network. BRAS can also be referred to as a Broadband Network Gateway (BNG).

CP: Control Plane. The CP is a user control management component which manages UP’s resources such as the user entry and user’s QoS policy.

CUPS: Control/User Plane Separation

UP: User Plane. The UP is a network edge and user policy implementation component. The traditional router’s Control Plane and forwarding plane are both preserved on BNG devices in the form of a user plane.

TTM: Time to Market. It is the length of time it takes from a product or a service being conceived until it is available for sale.

MANO: Management and Orchestration. Functions are collectively provided by NFVO, VNFM and VIM.

VNF: Virtual Network Function. Implementation of a Network Function that can be deployed on a Network Function Virtualization Infrastructure (NFVI).

PNF: Physical Network Function

DHCP: Dynamic Host Configuration Protocol

PPPoE: Point-to-Point Protocol over Ethernet

IPoE: Internet Protocol over Ethernet
3. BNG with CP and UP Separation Deployment Model

3.1 CP and UP of BNG Deployment Within One District

Take a one district example as in Figure 1. Here BNG-CP and BNG-UP are separated as deployed. Since the CP is computationally intensive, a virtualized CP acting as a VNF can meet the requirements of flexibility and fast calculation. The UP is traffic intensive, which can be virtualized or stay physical depending on traffic. The virtualized UP with low expense and high flexibility can be suitable for light traffic. In high traffic, special hardware is needed with high traffic forwarding performance.

In order to fulfill the function of a BNG, the BNG-CP needs to communicate with outside systems such as a AAA (Radius/Diameter) server and many others in the management network. In addition, the...
BNG-CP has three interfaces with the BNG-UP separated by their traffic categories: Service Interface, Control Interface, and Management Interface.

![Diagram of BNG-CP and BNG-UP interfaces]

Figure 2. Internal Interfaces Between the BNG CP and UP

The functions of the three interfaces are as follows:

Service Interface: The CP and UP use this interface to establish VXLAN tunnels with each other and transmit PPPoE and IPoE packets over the VXLAN tunnels for authentication.

Control Interface: The CP uses this interface to deliver service entries to the UP, and the UP uses this interface to report service events to the CP.

Management Interface: The CP uses this interface to deliver basic configurations to the UP. This interface uses NETCONF.

Several related drafts exist describing these interfaces in detail. The VXLAN-GPE extension draft for C/U separated BNG is related to the Service Interface [huang-nov3-vxlan-gpe-extension-for-vbng]. The draft YANG data model for CU separated BNG focuses on Management Interface, seeing in [cuspdt-rtgw-cu-separation-yang-model]. Another two drafts [cuspdt-rtgw-cusp-requirements] and [cuspdt-rtgw-cu-separation-infor-model] are related to the control interface giving an information model abstraction and suitable protocol.

3.2. CP and UP of BNG Deployment in Multiple Districts
If subscribers are distributed in several districts, the CP can be deployed centrally with the UP deployed in different districts close to subscribers as shown in Figure 3. Thus the deployment model can be a bit complex.

Take three districts A, B, and C for example. Here three UPs are placed with one shared CP. The CP is usually deployed in a Core Data Center such as in a provincial datacenter with UPs in edge Data 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 provinces for control and management, while edge data centers are in cities or towns for easy service access.

In this scenario, a centralized CP interfaces to the subsystems outside and communicate with all these UPs for control and management.
Under the CP’s control, the corresponding traffic is forwarded by UP to the Internet.
4. The Process of BNG with CUPS in Home Service

Take a user Bob accessing to the Internet using Home Broadband Service as an example. The process includes the service traffic from user to the internet and signaling traffic between BNG-UP and BNG-CP. Below is the whole process.

(1) User Bob dials up with packets of PPPoE or IPoE from BNG-UP which will be sent to the BNG-CP with the user’s information. This is signaling traffic.

(2) The BNG-CP processes the dialup packets. Confirming with the outside neighboring systems in the management network, the BNG-CP makes the decision to permit or deny of the dial access through certification. In this step, the BNG-CP manages resources and generates tables with information such as User Info, IP Info, QoS Info, etc. This is signaling traffic.

(3) The BNG-CP sends tables to the corresponding UP or to one UP it chooses from the corresponding UPs. This is signaling traffic.

(4) The BNG-UP receives the tables, matches rules and performs corresponding actions.

(5) If Bob is certificated and permitted, the UP forwards their traffic into the Internet with related policies such as limited bandwidth, etc. Otherwise, Bob is denied to access the Internet. This is service traffic.

From Step 2 to Step 4, the information model defined in [cuspdt-rtgwg-cu-separation-infor-model] can be used.
5. High Availability Considerations

As the BNG-CP takes responsibility for control and management, such as communicating with outside systems, generating flow tables, and managing the UP’s resources, high availability of this key component should be considered. Some redundancy should be adopted for reliability, such as N+N or N+K active standby BNG-CPs. N+N standby means 1:1 backup for each BNG-CP, which enables easy rapid switch of any number of BNG-CP to their backup but is expensive because it requires a large number of backup CPs. N+K means a smaller number of backup CPs, for example N2:1 backup where N2<N which is less expensive but does not handle more than 1 failure in the N2 subset of N BNG-CPs.
6. Security Considerations

TBD.

7. IANA Considerations

This document requires no IANA actions.
Normative References


Informative References


Authors’ Addresses

Rong Gu
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: gurong_cmcc@outlook.com

Sujun Hu
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: shujun_hu@outlook.com

Michael Wang
Huawei Technologies
101 Software Avenue, Yuhua District
Nanjing, Jiangsu  210012
China

Email: wangzitao@huawei.com

Donald Eastlake, 3rd
Huawei Technologies
1424 Pro Shop Court
Davenport, FL  33896
USA

Phone: +1-508-333-2270
Email: d3e3e3@gmail.com

Fangwei Hu
ZTE Corporation
No.889 Bibo Rd
Shanghai  201203
China

Phone: +86 21 68896273
Email: hu.fangwei@zte.com.cn
Copyright, Disclaimer, and Additional IPR Provisions

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Abstract

This document specifies the Simple Control Plane (CP) and User Plane (UP) Separation Broadband Network Gateway (BNG) control channel Protocol (S-CUSP) for communications between a CP and a UP. S-CUSP is designed to be flexible and extensible so as to easily allow for the addition of further messages and data items, should requirements be expressed in the future.
# Table of Contents

1. Introduction .............................................5  
2. Terminology .............................................6  
   2.1 Acronyms ...............................................6  
3. Protocol Overview .......................................8  
   3.1 S-CUSP Configuration ...................................8  
   3.2 S-CUSP Session Establishment ...........................9  
   3.3 Overview of S-CUSP Procedures .........................9  
   3.4 Network Resource Report ..............................11  
   3.5 BNG Access Procedures ................................11  
   3.5.1 IPoE Access .........................................12  
   3.5.2 PPPoE Access ........................................13  
   3.5.3 L2TP LAC Access .....................................14  
   3.5.4 L2TP LNS Access .....................................14  
   3.5.5 L2TP LTS Access .....................................16  
   3.6 Setting the User’s QoS Information .................16  
   3.7 CP and UP Synchronization .............................17  
   3.8 CGN Address Allocation ...............................18  
4. S-CUSP Message Formats ................................19  
   4.1 Common Message Header .................................19  
   4.1.1 Control Messages ....................................20  
   4.1.2 Table Messages ......................................20  
   4.1.3 Resource Reporting Message ........................20  
   4.1.4 Event Reporting Message .............................20  
   4.1.5 Vendor Message ......................................21  
   4.1.6 Resource Allocation Messages ......................21  
   4.2 Common Message TLV Format ............................21  
   4.3 Basic Data Fields .....................................22  
   4.4 Sub-TLV Format and Specific Sub-TLVs ............23  
   4.4.1 VRF-Name ............................................23  
   4.4.2 Ingress-QoS-Profile ................................23  
   4.4.3 Egress-QoS-Profile ................................24  
   4.4.4 User-ACL-Policy ....................................24  
   4.4.5 Multicast-Profile-v4 ...............................24  
   4.4.6 Multicast-Profile-v6 ................................24  
   4.4.7 Ingress-CAR .........................................24  
   4.4.8 Egress-CAR ..........................................25  
   4.4.9 NAT-Instance ........................................25  
   4.4.10 Pool-Name ..........................................25  
   4.4.11 If-Desc ............................................26  
5. Basic TLVs .............................................27  
   5.1 Interface Information TLV ............................27  
   5.2 Basic User Information TLVs ........................29  
   5.2.1 Basic User Information TLV .......................29  
   5.2.2 User PPP Information TLV .........................31  
   5.3 User IPv4 Information TLV ...........................32
Table of Contents (continued)

5.4 User IPv6 Information.................................33
5.5 User QoS Policy Information TLV.......................34
5.6 Routing Table TLVs....................................35
5.6.1 IPv4 Routing Information TLV.......................35
5.6.2 IPv6 Routing Information TLV.......................36
5.7 Static User Information TLVs..........................37
5.7.1 Static IPv4 User Information TLV....................38
5.7.2 Static IPv6 User Information TLV....................39
5.8 L2TP User Information TLVs............................40
5.8.1 L2TP-LAC User Information TLV.....................40
5.8.2 L2TP-LNS User Information TLV.....................40
5.8.3 L2TP-LAC Tunnel TLV...............................41
5.8.4 L2TP-LNS Tunnel TLV...............................42
5.9 NAT User Information TLV.............................42
5.10 Vendor Defined TLV...................................43

6. Control TLVs...........................................45
6.1 Hello TLV............................................45
6.2 Error Information TLV................................46

7. Resource Reporting TLVs................................47
7.1 Interface Resource Information TLV.....................47
7.2 UP Board Status Report Information TLV..............47

8. Event TLVs.............................................49
8.1 User Traffic Statistics Report TLV....................49
8.2 User Detection Result Report TLV......................50
8.3 User Basic Table Operation Result TLV..............51

9. Resource Allocation TLVs...............................52
9.1 Request Address Allocation TLV........................52
9.2 Address Assignment Response TLV......................52
9.3 Address Renewal Request TLV..........................53
9.4 Address Renewal Response TLV........................54
9.5 Address Release Request TLV..........................54
9.6 Address Release Response TLV........................55

10. Implementation Status.................................56
10.1 Implementations....................................56
10.1.1 Huawei Technologies................................56
10.1.2 ZTE..............................................57
10.1.3 H3C..............................................57
10.2 Hackathon...........................................57
10.3 EANTC Testing.......................................58

11. Security Considerations...............................59

12. IANA Considerations...................................60
12.1 Service Name and Port Number.........................60
Table of Contents (continued)

12.2 S-CUSP Parameters........................................60
12.2.1 Message Types........................................60
12.2.2 TLV Types.............................................61
12.2.3 TLV Operation Codes.................................62
12.2.4 Sub-TLV Types.........................................62
12.2.5 ERRID Codes...........................................63

Contributors.....................................................65

Normative References..........................................66
Informative References.........................................66

Authors’ Addresses............................................68
1. Introduction

A fixed network Broadband Network Gateway (BNG) is an Ethernet-centric IP edge router, and the aggregation point for user traffic. To provide centralized session management, flexible address allocation, high scalability for subscriber management capacity, and cost-efficient redundancy, the Control/User (CU) separated BNG framework is described in [TR-384]. The CU separated Service Control Plane (CP), which is responsible for user access authentication and setting forwarding entries in User Planes (UPs), can be virtualized and centralized. The routing control and forwarding plane, i.e. the BNG user plane (local), can be distributed across the infrastructure. Other structures can also be supported such as both CP and UP being virtual or both being physical.

This document specifies the simple CU Separation BNG control channel Protocol (S-CUSP) for communications between a BNG Control Plane (CP) and a set of User Planes (UPs). S-CUSP is designed to be flexible and extensible so as to easily allow for additional messages and data items, should further requirements be expressed in the future.
2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1 Acronyms

ACK: Acknowledgement message.

BNG: Broadband Network Gateway. A broadband remote access server (BRAS (BRoadband Access Server), B-RAS or BBRAS) routes traffic to and from broadband remote access devices such as digital subscriber line access multiplexers (DSLAM) on an Internet Service Provider’s (ISP) network. BRAS can also be referred to as a Broadband Network Gateway (BNG).

BRAS: BRoadband Access Server (BNG).

CAR: Committed Access Rate.

CBS: Committed Burst Size.

CGN: Carrier Grade NAT.

Ci: Control Interface.

CIR: Committed Information Rate.

CP: Control Plane. CP is a user control management component which supports the management of the UP’s resources such as the user entry and forwarding policy.

CU: Control-plane / User-plane.


DEI: Drop Eligibility Indicator. A bit in a VLAN tag after the priority and before the VLAN ID. (This bit was formerly the CFI (Canonical Format Indicator).)

IPoE: IP over Ethernet.

L2TP: Layer 2 Tunneling Protocol [RFC2661].

LAC: L2TP Access Concentrator
LNS: L2TP Network Server
Mi: Management Interface.
MSS: Maximum Segment Size.
MRU: Maximum Receive Unit.
NAT: Network Address Translation [RFC3022].
ND: Neighbor Discovery.
PBS: Peak Burst Size.
PD: Prefix Delegation.
PIR: Peak Information Rate.
PPP: Point to Point Protocol [RFC1661].
PPPoE: PPP over Ethernet.
Si: Service Interface.
TLV: Type, Length, Value. See Section 4.2.
UP: User Plane. UP is a network edge and user policy implementation component. The traditional router’s Control Plane and Forwarding Plane are both preserved on BNG devices in the form of a user plane.
URPF: Unicast Reverse Path Forwarding.
user: Equivalent to "customer".
VRF: Virtual Routing and Forwarding.
3. Protocol Overview

This section shows example message exchanges.

3.1 S-CUSP Configuration

To support Control Plane and User Plane separation, as defined in [SCUSP-architecture], three interfaces are defined. These are referred to as the Control Interface (Ci), Service Interface (Si) and Management Interface (Mi).

NETCONF [RFC6241] is the protocol used on the Management Interface between a CP and UP. It is used to configure the parameters of the Control Interface, Service Interface and the Access interfaces. The parameters are defined in [SCUSP-YANG].

Once the parameters are configured, a UP can start to establish S-CUSP session(s) with the specified CP(s) through the S-CUSP Session Establishment as defined Section 3.2 of this document.
3.2 S-CUSP Session Establishment

The S-CUSP session establishment consists of two successive steps:

1) Establishment of a TCP [RFC793] connection (3-way handshake) between the CP and the UP using port tbd1.

2) Establishment of a S-CUSP session over the TCP connection.

Once the TCP connection is established, the CP and the UP initialize the S-CUSP session during which the version negotiation is performed. The version information is carried within Hello messages (see Section 6.2). If the S-CUSP session establishment phase fails because the CP or UP disagree on the version parameters or one of the CP or UP does not answer after the expiration of the establishment timer. When the S-CUSP session establishment fails, the TCP connection is promptly closed.

3.3 Overview of S-CUSP Procedures

The five sequences below give a high level view of the S-CUSP message sequences. These sequences are covered in more detail below as indicated.

1. UP reports the Statistic INFO
   ------to CP via S-CUSP---------->

   UP reports the Event INFO
   ------to CP via S-CUSP---------->

   UP reports Resource INFO
1. See Sections 3.4 and 4.1.3 for more details on Resource reporting. See Section 4.1.4 for more details on Event reporting. Traffic statistics are also reported using the Event message.

2. UP relays User Dial-up Request
   ----to CP via Si---------------------
   CP sends User Dial-up Response
   <----to UPs via Si-------------------

2. This interaction is via the Service Interface and corresponds to the initial interaction in the message sequence charged in the sub-sections of Section 3.5.

3. CP sends User INFO
   <-----to UP via S-CUSP---------------
   CP sends User Policy INFO
   <-----to UP via S-CUSP---------------
   CP sends Route INFO
   <-----to UP via S-CUSP---------------
   CP sends Tunnel INFO
   <-----to UP via S-CUSP---------------

3. See Section 4.1.2 for more detail on CP messages updating UP tables.

4. CGN Address Allocation via S-CUSP
   ------------------------------------

4. See Sections 3.8 and 4.1.8 for more detail on CGN Address Allocation.

5. Data Synchronization via S-CUSP
   --------------------------------
5. See Sections 3.7 and 4.1.1 for more detail on CP and UP Synchronization.

3.4 Network Resource Report

Once an S-CUSP session is established between a CP and an UP. The UP will begin to report the status/attributes of its slots, interfaces, and sub-interfaces.

<table>
<thead>
<tr>
<th>UP</th>
<th>CP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Slot attributes report</td>
</tr>
<tr>
<td></td>
<td>via S-CUSP</td>
</tr>
<tr>
<td></td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td>Port attributes report</td>
</tr>
<tr>
<td></td>
<td>via S-CUSP</td>
</tr>
<tr>
<td></td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td>Sub-interface attributes report</td>
</tr>
<tr>
<td></td>
<td>via S-CUSP</td>
</tr>
<tr>
<td></td>
<td>-----------------------</td>
</tr>
</tbody>
</table>

Details of the Resource Report Messages can be found in Sections 4.2.3 and 7.

3.5 BNG Access Procedures

The subsection below give an overview of various "dial up" interactions over the Service Interface followed by the setting of various information in the UP by the CP using S-CUSP over the Control Interface.
3.5.1 IPoE Access

<table>
<thead>
<tr>
<th>UP</th>
<th>CP</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Negotiation Messages</td>
<td></td>
</tr>
<tr>
<td>&lt;------------------via Si-----------------&gt;</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_BASEC_INFO</td>
<td></td>
</tr>
<tr>
<td>&lt;---to UPs via S-CUSP-------------------</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_POLICY_INFO</td>
<td></td>
</tr>
<tr>
<td>&lt;---to UP via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_IPV4/6_INFO</td>
<td></td>
</tr>
<tr>
<td>&lt;---to UPs via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>CP sends ROUTE4/6 INFO</td>
<td></td>
</tr>
<tr>
<td>&lt;---to UPs via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>UP reports USER_DETECT_RESULT_INFO</td>
<td></td>
</tr>
<tr>
<td>----to CP via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>UP reports USER_TRAFFIC_INFO</td>
<td></td>
</tr>
<tr>
<td>----to CP via S-CUSP---------------------</td>
<td></td>
</tr>
</tbody>
</table>
3.5.2 PPPoE Access

<table>
<thead>
<tr>
<th></th>
<th>UP</th>
<th>CP</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPPoE Negotiation Messages</td>
<td>&lt;----------via Si------------------------&gt;</td>
<td></td>
</tr>
<tr>
<td>LCP Negotiation Messages</td>
<td>&lt;----------via Si------------------------&gt;</td>
<td></td>
</tr>
<tr>
<td>User Authentication Messages</td>
<td>&lt;----------via Si------------------------&gt;</td>
<td></td>
</tr>
<tr>
<td>IPCP Negotiation Messages</td>
<td>&lt;----------via Si------------------------&gt;</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_BASEC_INFO</td>
<td>----to UP via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_POLICY_INFO</td>
<td>----to UP via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_IPV4/6_INFO</td>
<td>----to UP via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>CP sends ROUTEV4/6_INFO</td>
<td>----to UP via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_PPP_INFO</td>
<td>----to UP via S-CUSP---------------------</td>
<td></td>
</tr>
<tr>
<td>UP reports USER_DETECT_RESULT_INFO</td>
<td>----to CP via S-CUSP--------------------&gt;</td>
<td></td>
</tr>
<tr>
<td>UP reports USER_TRAFFIC_INFO</td>
<td>----to CP via S-CUSP--------------------&gt;</td>
<td></td>
</tr>
</tbody>
</table>
### 3.5.3 L2TP LAC Access

<table>
<thead>
<tr>
<th>UP</th>
<th>CP</th>
<th>LNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPPoE Negotiation Messages</td>
<td>LCP Negotiation Messages</td>
<td>User Authentication Messages</td>
</tr>
<tr>
<td>-----------via Si-------------</td>
<td>-----------via Si-------------</td>
<td>-----------via Si-------------</td>
</tr>
<tr>
<td>/\</td>
<td>forward</td>
<td>/\</td>
</tr>
<tr>
<td>|</td>
<td>|</td>
<td></td>
</tr>
<tr>
<td>| forward</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
<tr>
<td>|</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LAC Tunnel Negotiation Messages
-----------------------------------------via Si-----------------------------------------

LAC Session Negotiation Messages
-----------------------------------------via Si-----------------------------------------

/\ | forward | /\ |
| \|                  |
| \|                  |
| \|                  |
| \|                  |
| \|                  |
| \|                  |
| \|                  |
| \|                  |
| \|                  |
| \|                  |

CP sends USER_BASIC_INFO
-------------------to UP via S-CUSP-------------------

CP sends LAC_TUNNEL_INFO
-------------------to UP via S-CUSP-------------------

CP sends LAC_USER_INFO
-------------------to UP via S-CUSP-------------------

UP reports USER_TRAFFIC_INFO
-------------------to CP via S-CUSP-------------------

### 3.5.4 L2TP LNS Access

Hu, et al
<table>
<thead>
<tr>
<th>UP</th>
<th>CP</th>
<th>LAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNS Tunnel Negotiation Messages</td>
<td>---------------------via Si---------------------</td>
<td></td>
</tr>
<tr>
<td>/\ forward</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\</td>
<td>_________________________LNS Tunnel Negotiation _____________</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LNS Session Negotiation Messages</td>
<td>---------------------via Si---------------------</td>
</tr>
<tr>
<td>/\ forward</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\</td>
<td>_________________________LNS Session Negotiation _____________</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LCP Negotiation Messages</td>
<td>---------------------via Si---------------------</td>
</tr>
<tr>
<td></td>
<td>User Authentication Messages</td>
<td>---------------------via Si---------------------</td>
</tr>
<tr>
<td></td>
<td>IPCP Negotiation Messages</td>
<td>---------------------via Si---------------------</td>
</tr>
<tr>
<td></td>
<td>CP sends LNS_TUNNEL_INFO</td>
<td>----to UP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>CP sends USER_BASEC_INFO</td>
<td>----to UP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>CP sends USER_IPV4/6_INFO</td>
<td>----to UP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>CP sends ROUTEV4/6 INFO</td>
<td>----to UP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>CP sends USER_PPP_INFO</td>
<td>----to UP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>CP sends LNS_USER_INFO</td>
<td>----to UP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>CP sends USER_POLICY_INFO</td>
<td>----to UP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>UP reports USER_DETECT_RESULT_INFO</td>
<td>----to CP via S-CUSP--------------------------</td>
</tr>
<tr>
<td></td>
<td>UP reports USER_TRAFFIC_INFO</td>
<td>----to CP via S-CUSP--------------------------</td>
</tr>
</tbody>
</table>
3.5.5 L2TP LTS Access

<table>
<thead>
<tr>
<th>UP</th>
<th>CP</th>
<th>LAC/LNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAC/LTS Tunnel Negotiation Messages</td>
<td>&lt;--------via Si--------&gt;</td>
<td>-- forward</td>
</tr>
<tr>
<td></td>
<td>\</td>
<td>-- LAC/LTS Tunnel Negotiation ----&gt;</td>
</tr>
<tr>
<td>LAC/LTS Session Negotiation Messages</td>
<td>&lt;--------via Si--------&gt;</td>
<td>-- forward</td>
</tr>
<tr>
<td></td>
<td>\</td>
<td>-- LAC/LTS Session Negotiation ----&gt;</td>
</tr>
<tr>
<td>CP sends LAC_TUNNEL_INFO</td>
<td>&lt;----to UP via S-CUSP----&gt;</td>
<td></td>
</tr>
<tr>
<td>CP sends LNS_TUNNEL_INFO</td>
<td>&lt;----to UP via S-CUSP----&gt;</td>
<td></td>
</tr>
<tr>
<td>CP sends USER_BASEC_INFO</td>
<td>&lt;----to UP via S-CUSP----&gt;</td>
<td></td>
</tr>
<tr>
<td>CP sends LAC_USER_INFO</td>
<td>&lt;----to UP via S-CUSP----&gt;</td>
<td></td>
</tr>
<tr>
<td>CP sends LNS_USER_INFO</td>
<td>&lt;----to UP via S-CUSP----&gt;</td>
<td></td>
</tr>
</tbody>
</table>

3.6 Setting the User’s QoS Information
Once an S-CUSP session has been established, if a user’s Quality of Service (QoS) needs to be set dynamically, the CP initiate a NETCONF session to configure the requested User’s QoS template. Then the user dials up via the Si, the CP sends the USER_BASIC_INFO message, USER_IPV4_INFO message, and USER_ROUTEV4_INFO messages to the UP, the UPs report the user detection results and user’s traffic status.

Once the above process has been accomplished, the CP sends the USER_QOS_AUTH_INFO message to the UPs; this message contains a variety of objects that specify the set of constrains and attributes for the user’s required QoS. (The format of these QoS attributes should be parallel to the QoS configuration templates.)

### 3.7 CP and UP Synchronization

Under some circumstances it is necessary to synchrnoize state between the CP and UP, for example if a CP fails and the UP is switched to a different CP. There may be multiple Resource INFO messages between the Synchronization Begin and Synchronization End.
3.8 CGN Address Allocation

UP sends Address Allocation Req.
<-----to CP via S-CUSP

CP sends Address Allocation Res.
<-----to UP via S-CUSP

See Section 4.1.6
4. S-CUSP Message Formats

This section specifies the format of the common S-CUSP message header, the format of the TLVs that appear in S-CUSP messages, the format of the sub-TLVs that appear within the values of some TLVs, and the format of some basic data fields.

An S-CUSP message consists of a common header followed by a variable-length body consisting entirely of TLVs. Receiving an S-CUSP message with a missing mandatory TLV MUST trigger an Error message (see Section 5.6). Conversely, if a TLV is optional, the TLV may or may not be present.

Network byte order is used for all multi-byte fields.

4.1 Common Message Header

Common header:

\[
\begin{array}{cccccc}
  & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 \\
\hline
\text{Ver} & | & \text{Resv} & | & \text{Message-Type} & | & \text{Message-Length} & | & \text{Transaction-ID} & | & \text{Reserved} & | & \text{Reserved} & |
\end{array}
\]

S-CUSP Message Common Header

Ver (4 bits): The major version of the protocol. This document specifies version 1. Different major versions of the protocol may have significantly different message structure and format except that the Ver field will always be in the same place at the beginning of each message. A successful S-CUSP session depends on the CP and UP both using the same major version of the protocol.

Resv (4 bits): Reserved. MUST be sent as zero and ignored on receipt.

Message-Type (8 bits): The set of message types specified in this document is listed in Section 12.2.1.

Message-Length (16 bits): Total length of the CUSP message including the common header, expressed in number of bytes as an unsigned integer.
Transaction ID (16 bits): This field is used to identify requests. It is echoed back in any corresponding ACK / response / Error message.

4.1.1 Control Messages

Control messages are listed below.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Notes and TLVs that can be carried</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hello</td>
<td>Capability negotiation.</td>
</tr>
<tr>
<td>2</td>
<td>Keepalive</td>
<td>Keepalive.</td>
</tr>
<tr>
<td>3</td>
<td>Synch_Request</td>
<td>Synchronization request.</td>
</tr>
<tr>
<td>4</td>
<td>Sync_Begin</td>
<td>Synchronization starts.</td>
</tr>
<tr>
<td>5</td>
<td>Sync_Data</td>
<td>Synchronization data: TLVs specified in Section 5.</td>
</tr>
<tr>
<td>6</td>
<td>Sync_End</td>
<td>End synchronization.</td>
</tr>
</tbody>
</table>

4.1.2 Table Messages

Table messages are listed below.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Notes and TLVs that can be carried</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Update_Request</td>
<td>TLVs specified in Section 5.</td>
</tr>
<tr>
<td>8</td>
<td>Update_Response</td>
<td>TLVs specified in Section 5.</td>
</tr>
</tbody>
</table>

4.1.3 Resource Reporting Message

The Resource Reporting message is as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Notes and TLVs that can be carried</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Report</td>
<td>Interface-Info, Board-Info.</td>
</tr>
</tbody>
</table>

4.1.4 Event Reporting Message

The Event Reporting message is as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Notes and TLVs that can be carried</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Event</td>
<td>Traffic-Info, Detect-Info.</td>
</tr>
</tbody>
</table>
4.1.5 Vendor Message

The Vendor message is as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Notes and TLVs that can be carried</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Vendor</td>
<td>Vendor-Defined, any other TLV(s) as implemented by the vendor.</td>
</tr>
</tbody>
</table>

4.1.6 Resource Allocation Messages

The Resource Allocation messages are listed below.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Notes and TLVs that can be carried</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Addr_Allocation_Req</td>
<td>Addr-Alloc-Req</td>
</tr>
<tr>
<td>201</td>
<td>Addr_Allocation_Ack</td>
<td>Addr-Alloc-Resp</td>
</tr>
<tr>
<td>202</td>
<td>Addr_Renew_Req</td>
<td>Addr-Renew-Req</td>
</tr>
<tr>
<td>203</td>
<td>Addr_Renew_Ack</td>
<td>Addr-Renew-Resp</td>
</tr>
<tr>
<td>204</td>
<td>Addr_Release_Req</td>
<td>Addr-Release-Req</td>
</tr>
<tr>
<td>205</td>
<td>Addr_Release_Ack</td>
<td>Addr-Release-Resp</td>
</tr>
</tbody>
</table>

4.2 Common Message TLV Format

CUSP messages consist of the common header specified in Section 4.1 followed by TLVs formatted as specified in this section.

```
+-----------------------------------------------+-
| Oper  |      TLV-Type     |       TLV-Length               |
+-----------------------------------------------+-
|                        Value                    |
+-----------------------------------------------+-
```

Oper (4 bits): For Message-Types that indicate an operation on a data set, the Oper field is interpreted as Update, Delete, or Reserved as specified in Section 12.2.3. For all other Message-Types, the Oper field MUST be sent as zero and ignored on receipt.

TLV-Type (12 bits): The Type of a TLV, that is the meaning and format of the Value part, are determined by the TLV-Type of the TLV. See Section 12.2.2.
TLV-Length (2 bytes): The length of the Value portion of the TLV in bytes as an unsigned integer.

Value (variable length): This is the value portion of the TLV whose size is given by TLV-Length.

4.3 Basic Data Fields

This section specifies the binary format of several standard basic data fields that are used within other data structures in this specification.

STRING
0 to 255 octets. Will be encoded as a sub-TLV (see Section 4.4) to provide the length.

MAC-Addr
6 octets. Ethernet MAC Address.

IPv4 Address
8 octets. 4 octets of the IPv4 address value followed by a 4 octet address mask in the format XXX.XXX.XXX.XXX.

IPv6 Address
20 octets. 16 octets of IPv6 address followed by a 4 octet integer n in the range of 0 to 128 which gives the address mask as the one’s complement of 2**(128-n) - 1.

VLAN ID
2 octets. As follows:

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | PRI |D|      VLAN-ID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```


D: Drop Eligibility Indicator (DEI). Default value 0.

VLAN-ID: Unsigned integer in the range 1-4094.
4.4 Sub-TLV Format and Specific Sub-TLVs

In some cases, the Value portion of a TLV, as specified above, can contain one or more Sub-TLVs formatted as follows:

```
+--------------------------------------------------+
|          Type          |          Length          |
+--------------------------------------------------+
| +-------------------+-------------------------------+   ...
|       Value        |
+-------------------+-------------------------------+   ...
```

Type (2 bytes): The Type of a Sub-TLV, that is the meaning and format of the Value part, are determined by the Type of the TLV. Sub-TLV Types numbers have the same meaning regardless of the TLV Type of the TLV within which the Sub-TLV occurs. See Section 12.2.4.

Length (2 bytes): The length of the Value portion of the TLV in bytes as an unsigned integer.

Value (variable length): This is the value portion of the TLV whose size is given by Length.

The sub-TLVs currently specified are specified in the following subsections.

4.4.1 VRF-Name

The name of the VRF (Virtual Routing and Forwarding instance) that the BNG user accesses. Optional.

Sub-TLV Type: 1, VRF Name
Length: 1-255 octets.
Value: STRING.

4.4.2 Ingress-QoS-Profile

Indicates the upstream QoS Profile Name. Optional.

Sub-TLV Type: 2, Ingress QoS Profile Name
Length: 1-255 octets.
Value: STRING.
4.4.3 Egress-QoS-Profile

Indicates the downstream QoS Profile Name. Optional.

Sub-TLV Type: 3, Egress QoS Profile Name
Length: 1-255 octets.
Value: STRING.

4.4.4 User-ACL-Policy

Indicates the name of the ACL policy group to which the user belongs. Optional.

Sub-TLV Type: 4, User ACL Policy Name
Length: 1-255 octets.
Value: STRING.

4.4.5 Multicast-Profile-v4

Name of the IPv4 multicast program list a user can order. Optional.

Sub-TLV Type: 5, Multicast Profile of IPv4.
Length: 1-255 octets.
Value: STRING.

4.4.6 Multicast-Profile-v6

Name of the IPv6 multicast program list a user can order. Optional.

Sub-TLV Type: 6, Multicast Profile of IPv6.
Length: 1-255 octets.
Value: STRING.

4.4.7 Ingress-CAR

Indicates the authorized upstream Committed Access Rate (CAR) parameters. Optional.

Sub-TLV Type: 7, Ingress CAR.
Length: 16 Octets.
Value: The following four fields in the order given:

Hu, et al
### 4.4.8 Egress-CAR

Indicates the authorized downstream Committed Access Rate (CAR) parameters. Optional.

Sub-TLV Type: 8, Egress CAR.  
Length: 16 Octets.  
Value: The following four fields in the order given:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIR</td>
<td>4 bytes</td>
<td>Guaranteed rate in bits/second.</td>
</tr>
<tr>
<td>PIR</td>
<td>4 bytes</td>
<td>Burst rate in bits/second.</td>
</tr>
<tr>
<td>CBS</td>
<td>4 bytes</td>
<td>The token bucket in bytes.</td>
</tr>
<tr>
<td>PBS</td>
<td>4 bytes</td>
<td>Burst token bucket in bytes.</td>
</tr>
</tbody>
</table>

### 4.4.9 NAT-Instance

Name of the Network Address Translation (NAT) Instance to which the user belongs. Optional.

Sub-TLV Type: 9, NAT Instance Name.  
Length: 1-255 octets.  
Value: STRING.

### 4.4.10 Pool-Name

Indicates the name of the address pool to which the public network segment belongs. Optional.

Sub-TLV Type: 10, IP Address Pool Name.  
Length: 1-255 octets.  
Value: STRING.
4.4.11 If-Desc

Description of an interface. Mandatory.

Sub-TLV Type: 11, Interface Description
Length: 12
Value: Several fields structured as follows:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If-Type</td>
<td>Chassis</td>
<td>Slot</td>
<td>Port Information</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>

If-Type: Interface Type:
0 = Reserved, 1 = FE, 2 = GE, 3 = 10GE, 4 = 100GE, 5: Eth-Trunk, 6: Tunnel, 7: VE

Chassis: Subrack Number
Slot: Slot
Port Information:
If-Type = Physical, the Port Information consists of a 1-byte Physical Slot number followed by a 1-byte Physical port number.
If-Type = virtual port, the Port Information consists of a 2-byte logical number of the virtual interface.
Sub-Port: Sub-port Number
5. Basic TLVs

This section describes basic TLVs.

5.1 Interface Information TLV

The Interface Information TLV can be used by a CP to control the access mode, authentication methods, and other related functions of an interface.

The format of the Interface Information TLV value part is as below:

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          If-Index                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Access-Mode  |  Auth-Method4 |  Auth-Method6 |    Reserved   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Flags                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        sub-TLVs (optional)                                      
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 5.1: Interface Information TLV
```

Function: Service information about the user access interface on the BNG.

TLV Type: 1

TLV Length: variable

TLV fields:

- **If-Index**: 4 bytes in length, a unique identifier of an interface of a BNG.
- **Access-Mode**: 1 byte in length, indicates the access mode of the interface; this document defines following values:
  - 0: Layer 2 subscriber;
  - 1: Layer 3 subscriber;
  - 2: Layer 2 leased line;
  - 3: Layer 3 leased line;
  - 4-255: Reserved.

- **Auth-Method4**: 1 byte in length, for IPv4 scenario, indicates the authentication on this interface; this field is defined as a bitmap, this document defines following values (other bits are reserved and MUST be sent as zero and ignored on receipt):
  - 0x1: PPPoE authentication;
0x2: DOT1X authentication;
0x4: Web authentication;
0x8: Web fast authentication;
0x10: Binding authentication.

Auth-Method6: 1 byte in length, for IPv6 scenario, indicates the
authentication on this interface; this field is defined as a bitmap, this document defines following values
(other bits are reserved and MUST be sent as zero and ignored on receipt):
0x1: PPPoE authentication;
0x2: DOT1X authentication;
0x4: Web authentication;
0x8: Web fast authentication;
0x10: Binding authentication;

The flags field is defined as below:

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----------------------------------------------+
| MBZ |Y|X|P|I|N|A|S|F|
+-----------------------------------------------+
```

Figure 5.2: Interface Flags

Where:

F (IPv4 Trigger) bit: Indicates whether IPv4 packets can trigger a
subscriber go to online.
1: enabled, 0: disabled.

S (IPv6 Trigger) bit: Indicates whether IPv6 packets can trigger a
subscriber go to online.
1: enabled, 0: disabled.

A (ARP Trigger) bit: Indicates whether ARP packets can trigger a
subscriber go to online.
1: enabled, 0: disabled.

N (ND Trigger) bit: Indicates whether ND packets can trigger a
subscriber go to online.
1: enabled, 0: disabled.

I (IPoE-Flow-Check): Used for UP detection. IPoE 1: Enable traffic
detection. 0: Disable traffic detection.

P (PPP-Flow-Check) bit: Used for UP detection. PPP 1: Enable traffic
detection. 0: Disable traffic detection.
X (ARP-Proxy) bit: 1: The interface is enabled with ARP proxy and can process ARP requests across different Port+VLANS.
0: The ARP proxy is not enabled on the interface, and only the ARP requests of the same Port+VLAN are processed.

Y (ND-Proxy) bit: 1: The interface is enabled with ND proxy and can process ND requests across different Port+VLANS.
0: The ND proxy is not enabled on the interface, and only the ND requests of the same Port+VLAN are processed.

MBZ: Reserved bits that MUST be sent as zero and ignored on receipt.

5.2 Basic User Information TLVs

The Basic User Information TLVs are defined for a CP to carry the basic information about a user to an UP.

5.2.1 Basic User Information TLV

The format of the Basic User Information TLV value part is as below:

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          User ID                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          User MAC                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    User MAC          |   Oper ID     |    Reserved   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Access Type   |Sub-access Type|  Account Type | Address Family|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               C-VID           |          P-VID                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Detect Times    |          Detect Interval      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            If-Index                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
˜                            sub-TLVs (optional)                ˜
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5.3: Basic User Information TLV
Function: Basic information about a BNG user.
TLV Type: 2
TLV Length: variable in length;

TLV Fields: 

<table>
<thead>
<tr>
<th>Name</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID.</td>
</tr>
<tr>
<td>User-Mac</td>
<td>MAC-Addr</td>
<td>User MAC Address.</td>
</tr>
<tr>
<td>Oper-ID</td>
<td>1 byte</td>
<td>Indicates the ID of an operation performed by a user. This field is carried in the response from the UP.</td>
</tr>
<tr>
<td>Session-ID</td>
<td>4 bytes</td>
<td>Session ID of a PPPoE user. Zero for non-PPPoE user.</td>
</tr>
<tr>
<td>Access-Type</td>
<td>1 byte</td>
<td>See Section 5.2.1.1.</td>
</tr>
<tr>
<td>Sub-Access-Type</td>
<td>1 byte</td>
<td>Indicates whether PPP termination or PPP relay is used. 0: N/A 1: PPP2 on the LAC side: Termination, PPP on the LNS side</td>
</tr>
<tr>
<td>Account-Type</td>
<td>1 byte</td>
<td>IPv4/IPv6 charging: 0 separate charging: Collects statistics on IPv4 and IPv6 traffic of terminals independently. 1: Statistics and charging Collects statistics on IPv4 and IPv6 traffic of terminals.</td>
</tr>
<tr>
<td>User-IP-Type</td>
<td>1 byte</td>
<td>1:IPv4 stack and 2:IPv6 stack 3: dual stack</td>
</tr>
<tr>
<td>C-VID</td>
<td>VLAN-ID</td>
<td>Indicates the inner VLAN ID. The value 0 indicates that the VLAN ID is invalid. The default value of PRI is 7, the value of DEI is 0, and the value of VID is 1˜4094. The PRI value can also be obtained by parsing terminal packets.</td>
</tr>
<tr>
<td>P-VID</td>
<td>VLAN-ID</td>
<td>Outer VLAN ID. The value 0 indicates that the VLAN ID is invalid. The format is the same as that the C-VID.</td>
</tr>
<tr>
<td>Detect-Times</td>
<td>2 bytes</td>
<td>Number of detection timeout times. The value 0 indicates that no detection is performed.</td>
</tr>
<tr>
<td>Detect-Interval</td>
<td>2 bytes</td>
<td>Detection interval in seconds.</td>
</tr>
<tr>
<td>If-Index</td>
<td>4 bytes</td>
<td>Interface index.</td>
</tr>
</tbody>
</table>

The Reserved field MUST be sent as zero and ignored on receipt.
5.2.1.1 Access Types Table

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PPP access (PPP)</td>
</tr>
<tr>
<td>2</td>
<td>PPP over Ethernet over ATM access (PPPoEoA)</td>
</tr>
<tr>
<td>3</td>
<td>PPP over ATM access (PPPoA)</td>
</tr>
<tr>
<td>4</td>
<td>PPP over Ethernet access (PPPoE)</td>
</tr>
<tr>
<td>5</td>
<td>PPPoE over VLAN access (PPPoEoVLAN)</td>
</tr>
<tr>
<td>6</td>
<td>PPP over LNS access (PPPoLNS)</td>
</tr>
<tr>
<td>7</td>
<td>IP over Ethernet DHCP access (IPoE_DHCP)</td>
</tr>
<tr>
<td>8</td>
<td>IP over Ethernet EAP authentication access (IPoE_EAP)</td>
</tr>
<tr>
<td>9</td>
<td>IP over Ethernet Layer 3 access (IPoE_L3)</td>
</tr>
<tr>
<td>10</td>
<td>IP over Ethernet Layer 2 Static access (IPoE_L2_STATIC)</td>
</tr>
<tr>
<td>11</td>
<td>Layer 2 Leased Line access (L2_LeasedLine)</td>
</tr>
<tr>
<td>12</td>
<td>Layer 2 VPN Leased Line access (L2VPN_LeasedLine)</td>
</tr>
<tr>
<td>13</td>
<td>Layer 3 Leased Line access (L3_LeasedLine)</td>
</tr>
<tr>
<td>14</td>
<td>Layer 2 Leased line Sub-User access</td>
</tr>
<tr>
<td>15</td>
<td>L2TP LAC tunnel access (L2TP_LAC)</td>
</tr>
<tr>
<td>16</td>
<td>L2TP LNS tunnel access (L2TP_LNS)</td>
</tr>
</tbody>
</table>

5.2.2 User PPP Information TLV

The User PPP Information TLV is defined to carry PPP information of a User, from a CP to an UP.

The format of the TLV value part is as below:

```
<table>
<thead>
<tr>
<th>User ID</th>
<th>MSS</th>
<th>MRU</th>
<th>Magic Number</th>
<th>Peer Magic Number</th>
</tr>
</thead>
</table>
```

Function: PPP [RFC1661] information for a BNG user.
TLV Type: 3
TLV Length: 20 bytes in length
TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID.</td>
</tr>
<tr>
<td>MSS-Value</td>
<td>2 bytes</td>
<td>Indicates the MSS value.</td>
</tr>
<tr>
<td>MSS-Enable</td>
<td>1 bit</td>
<td>Indicates whether the MSS is enabled. 0: The function is disabled. 1: Enable</td>
</tr>
<tr>
<td>MRU</td>
<td>2 bytes</td>
<td>PPPoE local MRU.</td>
</tr>
<tr>
<td>Magic-Number</td>
<td>4 bytes</td>
<td>Local magic number in PPP negotiation packets.</td>
</tr>
<tr>
<td>Peer-Magic-Number</td>
<td>4 bytes</td>
<td>Remote peer magic number.</td>
</tr>
</tbody>
</table>

The Reserved fields MUST be sent as zero and ignored on receipt.

5.3 User IPv4 Information TLV

The User IPv4 Information TLV is defined to carry IPv4 related information for a BNG user.

The format of the TLV value part is as below:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          User ID                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          User IPv4 Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Gateway IPv4 Address                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          MTU                  |   Reserved            |U|E|W|P|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
˜                            sub-TLVs                           ˜
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5.5: User IPv4 Information TLV

Function: IPv4 information for a BNG user.
TLV Type: 4
TLV Length: variable

TLV fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID.</td>
</tr>
<tr>
<td>User-IPv4</td>
<td>IPv4</td>
<td>User IPv4 address.</td>
</tr>
<tr>
<td>Gateway-IPv4</td>
<td>IPv4</td>
<td>User gateway.</td>
</tr>
</tbody>
</table>
| Portal Force | 1 bit    | (P) Push advertisement switch, 0: off, 1:
Web-Force 1 bit (W) IP4 Web push flag. 0: off, 1: on.
Echo-Enable 1 bit (E) Compatible with PPP/ARP and the UP returns ARP Req or PPP Echo. 0: off, 1: on.
IPv4-URPF 1 bit (U) Unicast Reverse Path Forwarding (URPF) flag of a user. 0: off, 1: on.
MTU 2 bytes MTU value. The default value is 1500.
VRF-Name Sub-TLV VRF name.

The Reserved field MUST be sent as zero and ignored on receipt.

5.4 User IPv6 Information

The User IPv6 Information TLV is defined to carry IPv6 related information of a BNG user.

The format of the TLV value part is as below:

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          User ID                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
˜                          User PD-Address                      ˜
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
˜                          Gateway ND-Address                   ˜
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          User IANA Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          IPv6 Interface ID                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          IPv6 Interface ID (cont.)            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          MTU                  |   Reserved            |U|E|W|P|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
˜                          sub-TLVs (VRF Name sub-TLV)          ˜
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5.6: User IPv6 Information TLV

Function: IPv6 information for a BNG user.
TLV Type: 5
TLV Length: variable
TLV fields:
Name          Type     Description
-------------- ------ ----------------------
User-ID        4 bytes  User ID.
PD-Address     IPv6     Prefix Delegation (PD) address.
ND-Address     IPv6     Neighbor Discovery (ND) address.
IANA-Address   IPv6     IANA address.
Interface-ID   8 bytes  IPv6 interface ID.
Portal Force   1 bit    (P) Push advertisement switch, 0: off, 1: on.
Web-Force      1 bit    (W) IP6 Web push flag. 0: off, 1: on.
Echo-Enable    1 bit    (E) Compatible with PPP/ARP and the UP returns ARP Req or PPP Echo. 0: off, 1: on.
IPv6-URPF      1 bit    (U) User Reverse Path Forwarding (URPF) flag of a user. 0: off, 1: on.
MTU            2 bytes  MTU value. The default value is 1500.
VRF-Name       Sub-TLV  VRF name.

The Reserved field MUST be sent as zero and ignored on receipt.

5.5 User QoS Policy Information TLV

The format of the TLV value part is as follows:

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          User ID                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   I-Priority  |   E-Priority  |   Reserved                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                                             -
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 5.7: User QoS Policy Information TLV

Function: BNG user authorization information.

TLV Type: 6

TLV length: variable in length

TLV Fields:
Name          Type     Description
-------------- ------ ----------------------
User-ID        4 bytes  User ID.
Ingress-Priority 1 byte Indicates the upstream priority. The value is 0~7.
Egress-Priority 1 byte Indicates the downstream priority. The value is 0~7.
Ingress-CAR Sub-TLV Upstream CAR.
Egress-CAR Sub-TLV Downstream CAR.
Ingress-QoS-Profile Sub-TLV Indicates the name of the QoS-Profile profile in the upstream direction.
Egress-QoS-Profile Sub-TLV Indicates the name of the QoS-Profile profile in the downstream direction.
User-ACL-Policy Sub-TLV All ACL user policies, including v4ACLIN, v4ACLOUT, v6ACLIN, v6ACLOUT, v4WEBACL, v6WEBACL, v4SpecialACL, and v6SpecialACL.
Multicast-Profile4 Sub-TLV IPv4 multicast policy name.
Multicast-Profile6 Sub-TLV IPv6 multicast policy name.
NAT-Instance Sub-TLV Indicates the instance ID of a NAT user.

The Reserved field MUST be sent as zero and ignored on receipt.

5.6 Routing Table TLVs

5.6.1 IPv4 Routing Information TLV

The format of the TLV value part is as below:

```
 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
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
|                          User ID                              |
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
|                          Dest-Address                         |
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
|                          Next-Hop                             |
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
|                          Out-If-Index                         |
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
|                          Cost                                  |
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
|                          Tag                                  |
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
|        Route Type             |          Reserved           |A|
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
˜                          sub-TLVs                             ˜
+-----------------------------------+-----------------------------------+-----------------------------------+-----------------------------------+
```

Figure 5.8: IPv4 Routing Information TLV

Function: IPv4 routing information.
TLV Type: 7
TLV Length: Variable length
# TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID. This field is filled with all Fs when a non-user route is delivered to the UP.</td>
</tr>
<tr>
<td>Dest-Address</td>
<td>IPv4</td>
<td>Destination address.</td>
</tr>
<tr>
<td>Next-Hop</td>
<td>IPv4</td>
<td>Next hop address.</td>
</tr>
<tr>
<td>Out-If-Index</td>
<td>4 bytes</td>
<td>Indicates the interface index.</td>
</tr>
<tr>
<td>Cost</td>
<td>4 bytes</td>
<td>Cost value of the route.</td>
</tr>
<tr>
<td>Tag</td>
<td>4 bytes</td>
<td>Route tag value.</td>
</tr>
<tr>
<td>Route-Type</td>
<td>2 bytes</td>
<td>Route type. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST_RT = 0 user host route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FRAME_RT = 1 Radius authorization FrameRoute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NET_RT = 2, network segment route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GATEWAY_RT = 3, gateway route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RADIUS_IP_RT = 4, Radius authorized IP route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LNS_USER_RT = 5 L2TP LNS side user route</td>
</tr>
<tr>
<td>Advertise-Flag</td>
<td>1 bit</td>
<td>Indicates the route advertisement flag. 0: Not advertised, 1: advertised.</td>
</tr>
<tr>
<td>VRF-Name</td>
<td>Sub-TLV</td>
<td>VRF name.</td>
</tr>
</tbody>
</table>

The Reserved field MUST be sent as zero and ignored on receipt.

## 5.6.2 IPv6 Routing Information TLV

The format of the TLV value part is as follows:

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+
|                       User ID                       |                        IPv6 Dest-Address                     |                        IPv6 Next-Hop                     |
+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+
|                        Out-If-Index                      |                        Cost                          |                        Tag                          |
+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+
|                        Route Type                        |                  Reserved|                        VRF-Name sub-TLVs |                        -                     |
+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+-----------------------------------------------+
```

Hu, et al [Page 36]
Figure 5.9: IPv6 Routing Information TLV

Function: IPv4 routing information.
TLV Type: 8
TLV Length: Variable

<table>
<thead>
<tr>
<th>TLV Fields:</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID. This field is filled with all Fs when a non-user route is delivered to the UP.</td>
</tr>
<tr>
<td>Dest-Address</td>
<td>IPv6</td>
<td>Destination address.</td>
</tr>
<tr>
<td>Next-Hop</td>
<td>IPv6</td>
<td>Next hop address.</td>
</tr>
<tr>
<td>Out-If-Index</td>
<td>4 bytes</td>
<td>Indicates the interface index.</td>
</tr>
<tr>
<td>Cost</td>
<td>4 bytes</td>
<td>Cost value of the route.</td>
</tr>
<tr>
<td>Tag</td>
<td>4 bytes</td>
<td>Route tag value.</td>
</tr>
<tr>
<td>Route-Type</td>
<td>2 bytes</td>
<td>Route type. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST_RT = 0 user host route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FRAME_RT = 1 Radius authorization FrameRoute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NET_RT = 2, network segment route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GATEWAY_RT = 3, gateway route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RADIUS_IP_RT = 4, Radius authorized IP route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LNS_USER_RT = 5 L2TP LNS side user route</td>
</tr>
<tr>
<td>Advertise-Flag</td>
<td>1 bit</td>
<td>Indicates the route advertisement flag. 0: Not advertised, 1: advertised.</td>
</tr>
<tr>
<td>VRF-Name</td>
<td>Sub-TLV</td>
<td>VRF name.</td>
</tr>
</tbody>
</table>

The Reserved field MUST be sent as zero and ignored on receipt.

5.7 Static User Information TLVs
5.7.1 Static IPv4 User Information TLV

Figure 5.10: Static IPv4 User Information TLV

Function: User information which is used proactively to detect and go on line.

TLV Type: 9

TLV Length: variable

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If-Index</td>
<td>4 bytes</td>
<td>Indicates the interface index.</td>
</tr>
<tr>
<td>C-VID</td>
<td>VLAN-ID</td>
<td>Indicates the inner VLAN ID. The value 0 indicates that the VLAN ID is invalid. The valid value is 1−4094.</td>
</tr>
<tr>
<td>P-VID</td>
<td>VLAN-ID</td>
<td>Outer VLAN ID. The value 0 indicates that the VLAN ID is invalid. The format is the same as that the C-VID. The valid value is 1−4094. For a single-layer VLAN, set this parameter to PeVid.</td>
</tr>
<tr>
<td>User Address</td>
<td>IPv4-Addr</td>
<td>Terminal IP address.</td>
</tr>
<tr>
<td>Gateway Address</td>
<td>IPv4-Addr</td>
<td>Gateway IP Address.</td>
</tr>
<tr>
<td>User-MAC</td>
<td>MAC-Addr</td>
<td>MAC address of the terminal.</td>
</tr>
<tr>
<td>VRF-Name</td>
<td>Sub-TLV VRF Name.</td>
<td></td>
</tr>
</tbody>
</table>

The Reserved field MUST be sent as zero and ignored on receipt.
5.7.2 Static IPv6 User Information TLV

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.8 L2TP User Information TLVs

5.8.1 L2TP-LAC User Information TLV

Function: Information about the L2TP-LAC for a BNG user.
TLV Type: 11
TLV Length: 12

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>The User identifier.</td>
</tr>
<tr>
<td>Local-Tunnel-ID</td>
<td>2 bytes</td>
<td>The local ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Local-Session-ID</td>
<td>2 bytes</td>
<td>The local session ID with the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Tunnel-ID</td>
<td>2 bytes</td>
<td>The remote ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Session-ID</td>
<td>2 bytes</td>
<td>The remote session ID with the L2TP tunnel.</td>
</tr>
</tbody>
</table>

5.8.2 L2TP-LNS User Information TLV

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>The User identifier.</td>
</tr>
<tr>
<td>Local-Tunnel-ID</td>
<td>2 bytes</td>
<td>The local ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Local-Session-ID</td>
<td>2 bytes</td>
<td>The local session ID with the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Tunnel-ID</td>
<td>2 bytes</td>
<td>The remote ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Session-ID</td>
<td>2 bytes</td>
<td>The remote session ID with the L2TP tunnel.</td>
</tr>
</tbody>
</table>
Function: Information about the L2TP tunnel for a BNG user.
TLV Type: 12
TLV Length: 12

TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>The User identifier.</td>
</tr>
<tr>
<td>Local-Tunnel-ID</td>
<td>2 bytes</td>
<td>The local ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Local-Session-ID</td>
<td>2 bytes</td>
<td>The local session ID with the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Tunnel-ID</td>
<td>2 bytes</td>
<td>The remote ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Session-ID</td>
<td>2 bytes</td>
<td>The remote session ID with the L2TP tunnel.</td>
</tr>
</tbody>
</table>

5.8.3 L2TP-LAC Tunnel TLV

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Local Tunnel ID         |       Remote Tunnel ID        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Source Port         |        Destination Port       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Tunnel Source Address               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Tunnel Destination Address           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       sub-TLVs (VRF Name sub-TLV)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5.14: L2TP-LAC Tunnel TLV

Function: Information about the L2TP tunnel for a BNG user.
TLV Type: 13
TLV Length: variable

TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local-Tunnel-ID</td>
<td>2 bytes</td>
<td>The local ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Tunnel-ID</td>
<td>2 bytes</td>
<td>The remote ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Source-Port</td>
<td>2 bytes</td>
<td>Indicates the source UDP port number of an L2TP user.</td>
</tr>
<tr>
<td>Dest-Port</td>
<td>2 bytes</td>
<td>Indicates the destination UDP port number of an L2TP user.</td>
</tr>
<tr>
<td>Source-IP</td>
<td>IPv4/v6</td>
<td>The source IP address of the tunnel.</td>
</tr>
<tr>
<td>Dest-IP</td>
<td>IPv4/v6</td>
<td>The destination IP address of the tunnel.</td>
</tr>
<tr>
<td>Tunnel-VRF-Name</td>
<td>Sub-TLV</td>
<td>L2TP user tunnel VRG name.</td>
</tr>
</tbody>
</table>

Hu, et al
5.8.4 L2TP-LNS Tunnel TLV

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Tunnel ID</td>
</tr>
<tr>
<td>Remote Tunnel ID</td>
</tr>
<tr>
<td>Source Port</td>
</tr>
<tr>
<td>Destination Port</td>
</tr>
<tr>
<td>Tunnel Source Address</td>
</tr>
<tr>
<td>Tunnel Destination Address</td>
</tr>
<tr>
<td>sub-TLVs (VRF Name sub-TLV)</td>
</tr>
</tbody>
</table>

Figure 5.15: L2TP-LNS Tunnel TLV

Function: Information about the L2TP tunnel for a BNG user.
TLV Type: 14
TLV Length: variable

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local-Tunnel-ID</td>
<td>2 bytes</td>
<td>The local ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Remote-Tunnel-ID</td>
<td>2 bytes</td>
<td>The remote ID of the L2TP tunnel.</td>
</tr>
<tr>
<td>Source-Port</td>
<td>2 bytes</td>
<td>Indicates the source UDP port number of an L2TP user.</td>
</tr>
<tr>
<td>Dest-Port</td>
<td>2 bytes</td>
<td>Indicates the destination UDP port number of an L2TP user.</td>
</tr>
<tr>
<td>Source-IP</td>
<td>IPv4/v6</td>
<td>The source IP address of the tunnel.</td>
</tr>
<tr>
<td>Dest-IP</td>
<td>IPv4/v6</td>
<td>The destination IP address of the tunnel.</td>
</tr>
<tr>
<td>Tunnel-VRF-Name Sub-TLV</td>
<td></td>
<td>L2TP user tunnel VRG name.</td>
</tr>
</tbody>
</table>

5.9 NAT User Information TLV

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
</tr>
<tr>
<td>NAT Port Start</td>
</tr>
<tr>
<td>NAT Port End</td>
</tr>
<tr>
<td>NAT Address</td>
</tr>
</tbody>
</table>

Figure 5.16: NAT User Information TLV
Function: NAT [RFC3022] public network information for a BNG user.
TLV Type: 15
TLV Length: 12

TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID.</td>
</tr>
<tr>
<td>NAT-Port-Start</td>
<td>2 bytes</td>
<td>NAT start port number.</td>
</tr>
<tr>
<td>NAT-Port-End</td>
<td>2 bytes</td>
<td>NAT end port number.</td>
</tr>
<tr>
<td>NAT-Sub-IP</td>
<td>4 bytes</td>
<td>NAT public network address.</td>
</tr>
</tbody>
</table>

5.10 Vendor Defined TLV

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Vendor ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Sub-Type            |       Sub-Type-Version        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          sub-TLVs (optional)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5.17: Vendor Defined TLV

Function: Used to indicate vendor, sub-type, and version for a Vendor Defined message.
TLV Type: 1024
TLV Length: variable

TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor-ID</td>
<td>4 bytes</td>
<td>Vendor ID, which is defined in the RADIUS [RFC2865].</td>
</tr>
<tr>
<td>Sub-Type</td>
<td>2 bytes</td>
<td>Used by the Vendor to distinguish multiple different vendor messages.</td>
</tr>
<tr>
<td>Sub-Type-Version</td>
<td>2 bytes</td>
<td>Used by the Vendor to distinguish different versions of a Vendor Defined message sub-type.</td>
</tr>
</tbody>
</table>

Since Vendor code will be handling the TLV after the Vendor ID field is recognized, the remainder of the TLV value can be organized however the vendor wants. But it desirable for a vendor to be able to define multiple different vendor messages and to keep track of different versions of its vendor defined messages. Thus, it is RECOMMENDED that the vendor assign a Sub-Type value for each vendor.
message that it defines different from other Sub-Type values that vendor has used. Also, when modifying a vendor defined messages in a way potentially incompatible with a previous definition, the vendor SHOULD increase the value it is using in the Sub-Type-Version field.
6. Control TLVs

6.1 Hello TLV

Figure 6.1: Hello TLV

Function: Hello Message.
TLV Type: 100
TLV Length: 12

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VerSupported</td>
<td>32 bits</td>
<td>This is a bit map of the Sub-Versions of the S-CUSP protocol that the sender supports. This document specifies Sub-Version zero of Major Version 1, that is, Version 1.0. The VerSupported field MUST be non-zero. Bit 0 indicates support of Sub-Version zero, bit 1 indicates support of Sub-Version one, etc.</td>
</tr>
<tr>
<td>Vendor-ID</td>
<td>4 bytes</td>
<td>Vendor ID, which is defined in RADIUS [RFC2865].</td>
</tr>
<tr>
<td>Capabilities</td>
<td>32 bits</td>
<td>Flags that indicate the support of particular capabilities by the sender of the Hello.</td>
</tr>
</tbody>
</table>

After the exchange of Hello messages, the CP and UP each perform a logical AND of the Sub-Version supported and of the Capabilities bits fields.

If the result of the AND of the Sub-Versions supported is zero, then no session can be established and the connection is torn down. If the result of the AND of the Sub-Versions supported is non-zero, then the session uses the highest Sub-Version supported by both the CP and UP.

For example, if one side supports Sub-Versions 1, 3, 4, and 5 (VerSupported = 0x5C000000) and the other side supports 2, 3, and 4 (VerSupported = 0x38000000) then 3 and 4 are the Sub-Versions in
common and 4 is the highest Sub-Version supported by both sides. So Sub-Version 4 is used for the session that has been negotiated.

The result of the logical AND of the Capabilities bits will show what additional capabilities both sides support. If this result is zero, there are no such capabilities so none can be used during the session. If this result is non-zero, it shows the additional capabilities that can be used during the session.

6.2 Error Information TLV

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9</th>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>+------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Message Type</td>
</tr>
<tr>
<td>+------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Status Code</td>
</tr>
<tr>
<td>+------------------------------------</td>
<td>----------------------------------------</td>
</tr>
</tbody>
</table>

Figure 6.2: Error TLV

Function:   Error response.
TLV Type:   101
TLV Length: 8

<table>
<thead>
<tr>
<th>TLV Fields:</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Message-Type</td>
<td>4 bytes</td>
</tr>
<tr>
<td>Name</td>
<td>Status-Code</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>
7. Resource Reporting TLVs

7.1 Interface Resource Information TLV

Function: BNG interface resource information.
TLV Type: 200
TLV Length: variable

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If-Index</td>
<td>4 bytes</td>
<td>Indicates the interface index.</td>
</tr>
<tr>
<td>MAC-Address</td>
<td>MAC-Addr</td>
<td>Interface MAC address.</td>
</tr>
<tr>
<td>Phy-State</td>
<td>1 byte</td>
<td>Physical status of the interface. 0: down, 1: Up</td>
</tr>
<tr>
<td>MTU</td>
<td>4 bytes</td>
<td>Interface MTU value.</td>
</tr>
</tbody>
</table>

The Reserved field MUST be sent as zero and ignored on receipt.

7.2 UP Board Status Report Information TLV

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-Slot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board-Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 7.1: Interface Resource TLV

Figure 7.2: Interface Resource TLV
Function: Board information reported by the UP, including the board type and in-position status
TLV Type: 201
TLV Length: 8

TLV Fields:
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>1 byte</td>
<td>Subrack number.</td>
</tr>
<tr>
<td>Slot</td>
<td>1 byte</td>
<td>Slot number.</td>
</tr>
<tr>
<td>Sub-Slot</td>
<td>1 byte</td>
<td>Sub-slot number.</td>
</tr>
<tr>
<td>Board-Type</td>
<td>1 byte</td>
<td>1: CGN service card, 2: Interface board.</td>
</tr>
<tr>
<td>State</td>
<td>1 byte</td>
<td>Board status 0: Normal, 1: Abnormal.</td>
</tr>
</tbody>
</table>

The reserved field must be sent as zero and ignored on receipt.
8. Event TLVs

8.1 User Traffic Statistics Report TLV

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                User-ID                                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Statistics Type                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Packets (upper part)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Packets (lower part)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Bytes (upper part)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Bytes (lower part)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Loss Packets (upper part)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Loss Packets (lower part)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Loss Bytes (upper part)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Ingress Loss Bytes (lower part)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Packets (upper part)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Packets (lower part)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Bytes (upper part)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Bytes (lower part)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Loss Packets (upper part)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Loss Packets (lower part)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Loss Bytes (upper part)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Egress Loss Bytes (lower part)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 8.1: User Traffic Statistics Report TLV

Hu, et al                                            [Page 49]
Function: User traffic statistics report.
TLV Type: 300
TLV Length: 72

TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID.</td>
</tr>
<tr>
<td>Statistics-Type</td>
<td>4 bytes</td>
<td>Traffic type. The options are as follows: 0: IPv4 traffic, 1: IPv6 traffic, 2: Dual stack traffic.</td>
</tr>
<tr>
<td>Ingress-Packets</td>
<td>8 bytes</td>
<td>Upstream traffic: number of packets (UNIT64).</td>
</tr>
<tr>
<td>Ingress-Bytes</td>
<td>8 bytes</td>
<td>Upstream traffic: byte count (UINT64).</td>
</tr>
<tr>
<td>Ingress-Loss-Packets</td>
<td>8 bytes</td>
<td>Upstream packet loss: number of data packets (UNIT64).</td>
</tr>
<tr>
<td>Ingress-Loss-Bytes</td>
<td>8 bytes</td>
<td>Upstream packet loss: byte count (UINT64).</td>
</tr>
<tr>
<td>Egress-Packets</td>
<td>8 bytes</td>
<td>Downstream traffic: number of packets (UNIT64).</td>
</tr>
<tr>
<td>Egress-Bytes</td>
<td>8 bytes</td>
<td>Downstream traffic: byte count (UINT64).</td>
</tr>
<tr>
<td>Egress-Loss-Packets</td>
<td>8 bytes</td>
<td>Downstream packet loss: number of data packets (UNIT64).</td>
</tr>
<tr>
<td>Egress-Loss-Bytes</td>
<td>8 bytes</td>
<td>Downstream packet loss: byte count (UINT64).</td>
</tr>
</tbody>
</table>

8.2 User Detection Result Report TLV

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td>User-ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect Type</td>
<td>Detect Result</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>+--------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8.2: User Detection Result Report TLV

Function: Report BNG user detection.
TLV Type: 301
TLV Length: 8

TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID.</td>
</tr>
<tr>
<td>Detect-Type</td>
<td>1 byte</td>
<td>0: IPv4 detection, 1: IPv6 detection, 2: PPP detection.</td>
</tr>
</tbody>
</table>

Hu, et al [Page 50]
Detect-Result  1 bytes  0: indicates that the detection is
successful, 1: Detection failure. The UP
needs report only when the detection fails.

The Reserved field MUST be sent as zero and ignored on receipt.

8.3 User Basic Table Operation Result TLV

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Oper-ID</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Error Code</td>
</tr>
</tbody>
</table>

Figure 8.3: User Detection Result Report TLV

Function: Report the operation result of a table update.
TLV Type: 302
TLV Length: 12

TLV Fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td>4 bytes</td>
<td>User ID.</td>
</tr>
<tr>
<td>Oper-ID</td>
<td>1 byte</td>
<td>When a user connection number, dual stack, or Modify operation is performed, the response message carries the ConnectID carried in the following table. The CP verifies the corresponding operation.</td>
</tr>
<tr>
<td>Oper-Code</td>
<td>1 byte</td>
<td>Operation code. 1: update, 2: delete.</td>
</tr>
<tr>
<td>Oper-Result</td>
<td>1 byte</td>
<td>Operation Result. 0: Success, Others: Failure</td>
</tr>
<tr>
<td>Error-Code</td>
<td>4 bytes</td>
<td>Operation failure cause code. For details, see Section 12.2.5.</td>
</tr>
</tbody>
</table>

The Reserved field MUST be sent as zero and ignored on receipt.
9. Resource Allocation TLVs

9.1 Request Address Allocation TLV

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| sub-TLV |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Figure 9.1: Request Address Allocation TLV**

Function: Request address allocation.
TLV Type: 400
TLV Length: variable

**TLV Fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool-Name</td>
<td>Sub-TLV</td>
<td>Address pool name.</td>
</tr>
</tbody>
</table>

9.2 Address Assignment Response TLV

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Lease Time                                                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| IPv4 Addr and Mask                                                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| IPv4 Addr and Mask continued                                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Result Code | Reserved | sub-TLVs                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Figure 9.2: Address Assignment Response TLV**

Function: The CGN sends a response to the address assignment request.
TLV Type: 401
TLV Length: variable
9.3 Address Renewal Request TLV

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>++++++++++++++++ ++++++++++++++++ ++++++++++++++++ ++++++++++++++++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv4 Address and Mask</td>
<td></td>
<td></td>
</tr>
<tr>
<td>++++++++++++++++ ++++++++++++++++ ++++++++++++++++ ++++++++++++++++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv4 Address and Mask continued</td>
<td></td>
<td></td>
</tr>
<tr>
<td>++++++++++++++++ ++++++++++++++++ ++++++++++++++++ ++++++++++++++++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sub-TLVs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>++++++++++++++++ ++++++++++++++++ ++++++++++++++++ ++++++++++++++++</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 9.3: Request Address Renewal TLV

Function: Request address renewal.

TLV Type: 402
TLV Length: variable

TLV fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-IP</td>
<td>IPv4-Addr</td>
<td>Start address and mask of the address segment.</td>
</tr>
<tr>
<td>Pool-Name</td>
<td>Sub-TLV</td>
<td>Address segment address pool name.</td>
</tr>
</tbody>
</table>
### 9.4 Address Renewal Response TLV

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-IP</td>
<td>IPv4-Addr</td>
<td>Start address and mask of the address segment.</td>
</tr>
<tr>
<td>Result-Code</td>
<td>1 bytes</td>
<td>Processing Result, 0: Success, 1: Failure</td>
</tr>
<tr>
<td>Pool-Name</td>
<td>Sub-TLV</td>
<td>Address segment address pool name.</td>
</tr>
</tbody>
</table>

#### Figure 9.4: Address Renewal Response TLV

**Function:** Request address renewal.

**TLV Type:** 403

**TLV Length:** variable

### 9.5 Address Release Request TLV

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result-Code</td>
<td>1 bytes</td>
<td>Processing Result, 0: Success, 1: Failure</td>
</tr>
<tr>
<td>Pool-Name</td>
<td>Sub-TLV</td>
<td>Address segment address pool name.</td>
</tr>
</tbody>
</table>

#### Figure 9.5: Request Address Renewal TLV

**Function:** The CGN request the release of IP addresses.

**TLV Type:** 404

**TLV Length:** variable
TLV fields:
Name            Type     Description
--------------  ------   ----------------------
Client-IP       IPv4-Addr Start address and mask of the address segment.
Pool-Name       Sub-TLV  Address segment address pool name.

9.6 Address Release Response TLV

Function:   Request address renewal.
TLV Type:   405
TLV Length: variable

TLV fields:
Name            Type     Description
--------------  ------   ----------------------
Client-IP       IPv4-Addr Start address and mask of the address segment.
Result-Code     4 bytes  Processing Result, 0: Success, 1: Failure
Pool-Name       Sub-TLV  Address segment address pool name.
10. Implementation Status

This section is NOT intended to appear in any resulting RFC.

This section discusses the status of implementations that have provided information and the testing of this protocol at the time of posting of this Internet-Draft, and is based on the proposal in [RFC7942] ("Improving Awareness of Running Code: The Implementation Status Section"). The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation or test results here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their testing or features. Readers are advised to note that other implementations may exist.

According to [RFC7942], "this will allow reviewers ... to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature."

10.1 Implementations

Information on three S-CUSP implementations appears below.

10.1.1 Huawei Technologies

Name: Cloud-based BNG.

Maturity: Production.

Coverage: According to S-CUSP protocol.

Contact information:
    Zhouyi Yu: yuzhouyi@huawei.com

Date: 2018-11-01
10.1.2 ZTE

Name: ZXR10 V6000 vBRAS

Maturity: Production

Coverage: According to S-CUSP protocol.

Contact information:
Yong Chen: 10056167@zte.com.cn
Huaibin Wang: 10008729@zte.com.cn

Date: 2018-12-01

10.1.3 H3C

Name: CUSP protocol for BRAS Control Plane and User Plane Separation

Maturity: Research

Coverage: According to S-CUSP protocol

Contact information: mengdan@h3c.com; liuhanlei@h3c.com

Date: 2019-1-30

10.2 Hackathon

Successful use of the protocol at the IETF-102 Hackathon, Montreal, Quebec, in 2018.

Hackathon Project: Control Plane and User Plane Separation BNG control channel Protocol (CUSP)

Champions: Zhenqiang Li, Michael Wang

10.3 EANTC Testing

EANTC (European Advanced Networking Test Center (www.eantc.de)) tested the Huawei implementation. Their summary was as follows: "EANTC tested advanced aspects of the Cloud-based Broadband Network Gateway (vBNG) with a focus on performance, scalability and high availability with up to 20 Million emulated subscribers. The solution performed very well across all test scenarios."

11. Security Considerations

The S-CUSP messages do not provide security. Thus, if these messages are exchanged in an environment where security is a concern, that security must be provided by another protocol such as TLS 1.3 [RFC8446].
12. IANA Considerations

IANA is requested to perform the actions below in this section.

12.1 Service Name and Port Number

IANA is requested to assign a service name and port for BNG S-CUSP as follows:

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port</th>
<th>Transport</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>s-cusp</td>
<td>tbd1</td>
<td>tcp</td>
<td>Control-plane and User-plane Separation Protocol</td>
<td>[this document]</td>
</tr>
</tbody>
</table>

12.2 S-CUSP Parameters

IANA is requested to create an "S-CUSP Parameters" web page and include thereon the registries set up in the Sub-Sections below.

12.2.1 Message Types

IANA is requested to create an S-CUSP Message Types registry on the S-CUSP Parameters Web Page as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>- Reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Hello</td>
<td>[this document]</td>
</tr>
<tr>
<td>2</td>
<td>Keepalive</td>
<td>[this document]</td>
</tr>
<tr>
<td>3</td>
<td>Sync_Request</td>
<td>[this document]</td>
</tr>
<tr>
<td>4</td>
<td>Sync_Begin</td>
<td>[this document]</td>
</tr>
<tr>
<td>5</td>
<td>Sync_Data</td>
<td>[this document]</td>
</tr>
<tr>
<td>6</td>
<td>Sync_End</td>
<td>[this document]</td>
</tr>
<tr>
<td>7</td>
<td>Update_Request</td>
<td>[this document]</td>
</tr>
<tr>
<td>8</td>
<td>Update_Response</td>
<td>[this document]</td>
</tr>
<tr>
<td>9</td>
<td>Report</td>
<td>[this document]</td>
</tr>
<tr>
<td>10</td>
<td>Event</td>
<td>[this document]</td>
</tr>
<tr>
<td>11</td>
<td>Vendor</td>
<td>[this document]</td>
</tr>
</tbody>
</table>
12.2.2 TLV Types

IANA is requested to create an S-CUSP TLV Types registry on the S-CUSP Parameters Web Page as follows:

Registry Name: S-CUSP TLV Types
Registration Procedure: Expert Review
Reference: [this document]

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Usage Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access-IfSrv</td>
<td>Service information about the user access interface on the BNG.</td>
</tr>
<tr>
<td>2</td>
<td>User-Basic</td>
<td>Basic information about a BNG user.</td>
</tr>
<tr>
<td>3</td>
<td>User-PPP</td>
<td>PPP information about a BNG user.</td>
</tr>
<tr>
<td>4</td>
<td>User-IPv4</td>
<td>IPv4 address of a BNG user.</td>
</tr>
<tr>
<td>5</td>
<td>User-IPv6</td>
<td>IPv6 address of a BNG user.</td>
</tr>
<tr>
<td>6</td>
<td>User-Auth</td>
<td>QoS authorization information of a BNG user.</td>
</tr>
<tr>
<td>7</td>
<td>RouteV4-Info</td>
<td>BNG IPv4 routing information.</td>
</tr>
<tr>
<td>8</td>
<td>RouteV6-Info</td>
<td>BNG IPv6 routing information.</td>
</tr>
<tr>
<td>9</td>
<td>Static-IPv4-User</td>
<td>Static user information on a BNG. Used to proactively detect and go online.</td>
</tr>
<tr>
<td>10</td>
<td>Static-IPv6-User</td>
<td>Static user information on a BNG. Used to proactively detect and go online.</td>
</tr>
<tr>
<td>11</td>
<td>User-L2TP-LAC</td>
<td>L2TP LAC user information.</td>
</tr>
<tr>
<td>12</td>
<td>User-L2TP-LNS</td>
<td>L2TP LNS user information.</td>
</tr>
<tr>
<td>13</td>
<td>User-L2TP-LAC-Tnl</td>
<td>L2TP LAC tunnel information.</td>
</tr>
<tr>
<td>14</td>
<td>User-L2TP-LNS-Tnl</td>
<td>L2TP LNS tunnel information.</td>
</tr>
<tr>
<td>15</td>
<td>User-NAT</td>
<td>Public network segment information for a NAT user.</td>
</tr>
<tr>
<td>16-99</td>
<td>unassigned</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>Hello-Info</td>
<td>The CP and UP advertise versions to each other</td>
</tr>
<tr>
<td>101</td>
<td>Error-Info</td>
<td>The Ack of the control message carries the processing result, success, or error.</td>
</tr>
<tr>
<td>102-199</td>
<td>unassigned</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>Interface-Info</td>
<td>Interfaces reported by the UP including</td>
</tr>
</tbody>
</table>
physical interfaces, sub-interfaces, trunk interfaces, and tunnel interfaces.

201  Board-Info  Board information reported by the UP including the board type and in-position status.

202-299 unassigned -

300  Traffic-Info  User traffic statistics.
301  Detect-Info  User detection information.
302  User-TBL-Result  Processing result of user forwarding table delivery.

303-299 unassigned -

400  Addr-Alloc-Req  Request address allocation.
401  Addr-Alloc-Ack  Address allocation response.
402  Addr-Renew-Req  Request for address lease renewal.
403  Addr-Renew-Ack  Response to a request for extending an IP address lease.
404  Addr-Release-Req  Request to release the address.
405  Addr-Release-Ack  Ack of a message releasing an IP address.

406-1023 unassigned -

1024  Vendor-Defined  As implemented by vendor.

1025-65535 unassigned -

12.2.3 TLV Operation Codes

IANA is requested to create an S-CUSP TLV Operation Codes registry on the S-CUSP Parameters Web Page as follows:

Registry Name: S-CUSP TLV Operation Codes
Registration Procedure: Expert Review
Reference: [this document]

<table>
<thead>
<tr>
<th>Code</th>
<th>Operation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>- reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Update</td>
<td>[this document]</td>
</tr>
<tr>
<td>2</td>
<td>Delete</td>
<td>[this document]</td>
</tr>
<tr>
<td>3-15</td>
<td>- unassigned</td>
<td></td>
</tr>
</tbody>
</table>

12.2.4 Sub-TLV Types

IANA is requested to create an S-CUSP Sub-TLV Types registry on the S-CUSP Parameters Web Page as follows:

Registry Name: S-CUSP Sub-TLV Types
Registration Procedure: Expert Review
Reference: [this document]
## 12.2.5 ERRID Codes

IANA is requested to create an S-CUSP ERRID Codes registry on the S-CUSP Parameters Web Page as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Name</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
<td>Success</td>
</tr>
<tr>
<td>1</td>
<td>Fail</td>
<td>Failure. The reason is not classified.</td>
</tr>
<tr>
<td>2</td>
<td>TLV-Unknown</td>
<td>The TVL type cannot be identified.</td>
</tr>
<tr>
<td>3</td>
<td>TLV-Length</td>
<td>The TLV length is abnormal.</td>
</tr>
<tr>
<td>4</td>
<td>TLV-Value</td>
<td>The TLV value is abnormal.</td>
</tr>
<tr>
<td>5-999</td>
<td>- unassigned</td>
<td>Unassigned basic error codes.</td>
</tr>
<tr>
<td>1000</td>
<td>- reserved</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The subsequent service processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>corresponding to the UP are suspended.</td>
</tr>
<tr>
<td>1002-1999</td>
<td>- unassigned</td>
<td>Unassigned version negotiation error codes.</td>
</tr>
<tr>
<td>2000</td>
<td>- reserved</td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td>Synch-NoReady</td>
<td>The data to be smoothed is not ready.</td>
</tr>
<tr>
<td>2002</td>
<td>Synch-Unsupport</td>
<td>The request for smooth data is not supported.</td>
</tr>
<tr>
<td>2003-2999</td>
<td>- unassigned</td>
<td>Unassigned data synchronization error codes.</td>
</tr>
<tr>
<td>3000</td>
<td>- reserved</td>
<td></td>
</tr>
<tr>
<td>3001</td>
<td>Pool-Mismatch</td>
<td>The corresponding address pool cannot be found.</td>
</tr>
</tbody>
</table>

Hu, et al [Page 63]
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3002</td>
<td>Pool-Full The address pool is fully allocated and no address segment is available.</td>
</tr>
<tr>
<td>3003</td>
<td>Subnet-Mismatch The address pool subnet cannot be found.</td>
</tr>
<tr>
<td>3004</td>
<td>Subnet-Conflict Subnets in the address pool have been classified into other clients.</td>
</tr>
<tr>
<td>3005-3999</td>
<td>unassigned Unassigned address allocation error codes, used in NAT address allocation.</td>
</tr>
<tr>
<td>4000</td>
<td>reserved</td>
</tr>
<tr>
<td>4001</td>
<td>Update-Fail-No-Res The forwarding table fails to be delivered because the forwarding resources are insufficient.</td>
</tr>
<tr>
<td>4002</td>
<td>QoS-Update-Success The QoS policy takes effect.</td>
</tr>
<tr>
<td>4003</td>
<td>QoS-Update-Sq-Fail Failed to process the queue in the QoS policy.</td>
</tr>
<tr>
<td>4004</td>
<td>QoS-Update-CAR-Fail Processing of the CAR in the QoS policy fails.</td>
</tr>
<tr>
<td>4005</td>
<td>Statistic-Fail-No-Res Statistics processing failed due to insufficient statistics resources.</td>
</tr>
<tr>
<td>4006-4999</td>
<td>unassigned forwarding table delivery error codes.</td>
</tr>
<tr>
<td>5000-4294967295</td>
<td>reserved</td>
</tr>
</tbody>
</table>
Contributors

Zitao Wang
Huawei Technologies
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Email: wangzitao@huawei.com
Normative References


Informative References


Authors’ Addresses

Shujun Hu
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: hushujun@chinamobile.com

Donald Eastlake, 3rd
Huawei Technologies
1424 Pro Shop Court
Davenport, FL  33896
USA

Phone: +1-508-333-2270
Email: d3e3e3@gmail.com

Mach Chen
Huawei Technologies
Huawei Bldg., No. 156 BeiQing Road
Beijing 100095 China

Email: mach.chen@huawei.com

Fengwei Qin
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: qinfengwei@chinamobile.com

Zhenqiang Li
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: lizhenqiang@chinamobile.com
Copyright, Disclaimer, and Additional IPR Provisions

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Requirements for Control Plane and User Plane Separated BNG Protocol

draft-cuspdt-rtgwg-cusp-requirements-03

Abstract

This document introduces the Control Plane and User Plane separated BNG (Broadband Network Gateway) architecture and defines a set of associated terminology. It also specifies a set of protocol requirements for communication between the BNG-CP and the BNG-UPs in the Control Plane and User Plane Separated BNG.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 25, 2019.
1. Introduction

A Broadband Network Gateway (BNG) is an Ethernet-centric IP edge router and the aggregation point for user traffic. To provide centralized session management, flexible address allocation, high scalability for subscriber management capacity, and cost-efficient redundancy, the CU separated BNG is introduced [TR-384]. The CU separated Service Control Plane could be virtualized and centralized;
it is responsible for user access authentication and sending forwarding entries to user planes. The routing control and forwarding plane, i.e. BNG user plane (local), could be distributed across the infrastructure.

This document introduces the Control Plane and User Plane separated BNG architecture and modeling. This document also defines the protocol requirements for Control Plane and User Plane Separated BNG (CUSP).

2. Concept and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1. Terminology

BNG: Broadband Network Gateway. A broadband remote access server (BRAS, B-RAS or BBRAS) that routes traffic to and from broadband remote access devices such as digital subscriber line access multiplexers (DSLAM) on an Internet service provider’s (ISP) network. BRAS can also be referred to as a Broadband Network Gateway (BNG).

CP: Control Plane. The CP is a user control management component which manages UP’s resources such as the user entry and user’s QoS policy.


UP: User Plane. UP is a network edge and user policy implementation component. The traditional router’s Control Plane and forwarding plane are both preserved on BNG devices in the form of a user plane.

3. CU Separated BNG Model

Figure 1 shows the architecture of CU separated BNG
Briefly, a CU separated BNG is made up of a Control Plane (CP) and a set of User Planes (UPs) [TR-384], [I-D.cuspdt-rtgw-cu-separation-bng-deployment]. The Control Plane is a user control management component which manages UP’s resources such as the user entry and user’s Quality of Service (QoS) policy, for example, the access bandwidth and priority management. This Control Plane could be virtualized and centralized. The functional modules inside the BNG Service Control Plane can be implemented as Virtual Network Functions (VNFs) and hosted in a Network Function Virtualization Infrastructure (NFVI). The User Plane Management module in the BNG control plane centrally manages the distributed BNG user planes (e.g. load balancing), as well as the setup, deletion, update, and maintenance of channels between control planes and user planes [TR-384], [I-D.cuspdt-rtgw-cu-separation-bng-deployment]. The User Plane (UP) is a network edge and user policy implementation component. It can support the forwarding plane functions on traditional BNG devices,
such as traffic forwarding, QoS, and traffic statistics collection, and it can also support the control plane functions on traditional BNG devices, such as routing, multicast, etc [TR-384], [I-D.cuspdt-rtgwg-cu-separation-bng-deployment].

3.1. Internal interfaces between the CP and UP

To support communication between the Control Plane and User Plane, several interfaces are involved. Figure 2 illustrates the three internal interfaces of CU Separated BNG.

```
+----------------------------------+
|                                  |
|               BNG-CP             |
|                                  |
|              |  2.Control  |  3.Management| |
| 1.Service    |   Interface |   Interface  | |
| Interface    |              |              | |
|              |  2.Control  |  3.Management| |
|              |   Interface |   Interface  | |
|              |              |              | |
|              |  1.Service   |              | |
|              |   Interface  |              | |
|              |              |              | |
|              |              |              | |
|              |              |              | |
+----------------------------------+
```

Figure 2. Interfaces between the BNG-CP and the BNG-UP

Service interface: The CP and UP use this interface to establish VXLAN tunnels with each other and transmit PPPoE and IPoE packets over the VXLAN tunnels.

Control interface: The CP uses this interface to deliver service entries, and the UP uses this interface to report service events to the CP.

Management interface: The CP uses this interface to deliver configurations to the UP. This interface uses NETCONF.

The CUSP (Control plane and User plane Separated BNG protocol) defines the control interface, and specifies the communication between the centralized control plane and user planes. This protocol should be designed to support establishing and maintaining a conversation between CP and UPs, and transporting the tables that are specified in [draft-cuspdt-rtgwg-cu-separation-infor-model].
4. The usage of CU separation BNG protocol

As shown in Figure 3, when users access the BNG network, the control plane solicits user information (such as user’s ID, user’s MAC, user’s access methods, for example via PPPoE/IPoE), associates users with available bandwidth which is reported by User planes, and, based on the service’s requirement, generates a set of tables, which may include user’s information, UP’s IP segment, and QoS, etc. Then the control plane can transmit these tables to the User planes. User
planes receive these tables, parse them, and then perform corresponding actions.

5. Control Plane and User Plane Separation Protocol Requirements

This section specifies the requirements for the CU separation protocol.

5.1. Transmit information tables

The Control Plane and User Plane Separation Protocol MUST allow the CP to send tables to each User Plane device.

a) The current BNG service requires that the UP should support at least 2000 users being accessed every second. And every user requires at least 2000 bytes. To achieve high performance, the CU Separation protocol SHOULD be lightweight.

b) CU separation protocol should support data encoded as either XML or binary. It allows user information data to be read, saved, and manipulated with tools specific to XML or binary.

c) In order to provide centralized session management, high scalability for subscriber management capacity, and cost-efficient redundancy, batching ability should be provided. The CU Separation protocol should be able to group an ordered set of commands to a UP device. Each such group of commands SHOULD be sent to the UP in as few messages as practical. Furthermore, the protocol MUST support the ability to specify if a command group MUST have all-or-nothing semantics.

d) The CU Separation protocol SHOULD be able to support at least hundreds of UP devices and tens of thousands of ports. For example, the protocol field sizes corresponding to UP or port numbers SHALL be large enough to support the minimum required numbers. This requirement does not relate to the performance of the system as the number of UPs or ports in the system grows.

5.2. Message Priority

The CU Separation protocol MUST provide a means to express the protocol message priorities.

5.3. Reliability

Heartbeat is a periodic signal generated by hardware or software to test for some aspects of normal operation or to synchronize other parts of network system.
In the CU separation BNG, a heartbeat is sent between CP and UPs at a regular interval on the order of seconds. If the CP/UP does not receive a heartbeat for a time—usually a few heartbeat intervals—the CP/UP that should have sent the heartbeat is assumed to have failed.

The CU separation protocol should support some kind of heartbeat monitoring mechanism. And this mechanism should have ability to distinguish whether the interruption is an actual failure. For example, in some scenarios (i.e. CP/UP update, etc), the connection between the UP and CP need to be interrupted. In this case, the interruption should not be reported.

5.4. Support for Secure Communication

As mentioned above, CP may send some information tables to the UP which may be critical to the network function (e.g, User Information, IPv4/IPv6 information) and may reflect the business information (e.g, QoS, service level agreements, etc). Therefore, supporting the integrity of all CU Separation protocol messages and protecting against man-in-the-middle attacks MUST be supported.

The CP Separation protocol should support security in a variety of scenarios. For example, the connections between the CP and UPs could be dedicated lines, VPNs within one domain, or could cross several domains, that is, cross third party networks. Thus it is likely that more than one security mechanism SHOULD be supported. TLS and IPsec are good candidates for such mechanisms.

5.5. Version negotiation

The CU separated BNG may consist of different vendors’ devices implementing different versions of protocol. Therefore, the CU separation protocol MUST provide some mechanisms to perform the version negotiation.

Version negotiation is the process that the CU separated BNG’s Control-Plane uses to evaluate the protocol versions supported by both the control-plane and the user-plane devices. Then a suitable protocol version is selected for communication in CUSP. The process is a "negotiation" because it requires identifying the most recent protocol version that is supported by both the control-plane and the user-plane devices or determining that they have no version in common.
5.6. Capability Exchange

The UP Capability Report displays the device's profile, service capability, and other assigned capabilities within the CU separated BNG. The CU separation protocol should provide some mechanism to exchange the UP device's capabilities.

5.7. CP primary/backup capability

A backup CP for failure recovery is required for the CU separated BNG network. And the CUSP should provide some mechanism to implement the backup CP:

a) In some scenarios, there may be two CP devices both declaring the primary CP. Thus the CUSP should support or associate with some mechanisms to determine which CP is the primary device.

b) In the scenario of the primary CP down, the CUSP should support switching between primary and backup CP.

5.8. Event Notification

The CUSP protocol SHOULD be able to asynchronously notify the CP of events on the UP such as failures and changes in available resources and capabilities. Some scenarios that may initiate event notifications are listed below.

a) Sending response message: As mentioned above, the control plane solicits users' information, associates them with available bandwidth, and generates a set of tables based on the service's requirement. Then the control plane transmits these tables to the corresponding User plane. The UP should respond with an event notification to inform the CP that the tables are received.

b) User trace: The user trace mechanism can support the Control Plane tracing and monitoring the network status for users (for example the real-time bandwidth, etc), to help debug the user’s application. Therefore, the UPs SHOULD be able to notify the CP with the User trace message.

c) Sending statistics parameters: In CU separation BNG, the User-plane will report the traffic statistics parameters to the Control-plane, such as the ingress packets, ingress bytes, egress packets, egress bytes, etc. These parameters can help measure the BNG network performance. Available network resources can be allocated basing on the statistics parameters by the BNG-CP. Therefore, the UPs SHOULD be able to notify the CP with statistics parameters.
d) Report the result of User Detect: "User Detect" message will be sent periodically to detect user dial-up and disconnect. The UPs SHOULD be able to notify the CP with the result of User Detect.

5.9. Query Statistics

The CUSP protocol MUST provide a means for the CP to be able to query statistics (performance monitoring) from the UP.

6. Security Considerations

As this is an Informational requirements document, detailed technical Security Considerations are not included. However, Section 5.4 covers general security requirements and Section 5.7 covers backup requirements relevant to some denial of service scenarios.

7. IANA Considerations

This document requires no IANA actions.

8. References

8.1. Normative References

[I-D.cuspdt-rtgwg-cu-separation-bng-deployment]

[I-D.cuspdt-rtgwg-cu-separation-infor-model]


8.2. Informative References


Authors’ Addresses

Shujun Hu
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: shujun_hu@outlook.com

Victor Lopez
Telefonica
Sur 3 building, 3rd floor, Ronda de la Comunicacion s/n
Madrid  28050
Spain

Email: victor.lopezalvarez@telefonica.com

Fengwei Qin
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: qinfengwei@chinamobile.com

Zhenqiang Li
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing, Beijing  100053
China

Email: lizhenqiang@chinamobile.com
Tee Mong Chua
Singapore Telecommunications Limited
31 Exeter Road, #05-04 Comcentre Podium Block
Singapore City 239732
Singapore

Email: teemong@singtel.com

Donald Eastlake, 3rd
Huawei
1424 Pro Shop Court
Davenport, FL 33896
USA

Email: d3e3e3@gmail.com

Michael Wang
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Email: wangzitao@huawei.com

Jun Song
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Email: song.jun@huawei.com
Network based Bonding solution for Hybrid Access
draft-muley-network-based-bonding-hybrid-access-03

Abstract

In order to address increasing bandwidth demands, operators are considering bundling of multiple heterogeneous access networks (Hybrid access) for residential and enterprise customers. This document describes a solution for Hybrid access and covers the use case scenarios.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
Table of Contents

1. Introduction...................................................3
2. Terminology....................................................3
3. Reference Architecture........................................4
4. Network Based Bonding Solution Overview ......................5
   4.1. Separate BNG and PGW.....................................5
   4.2. Integrated BNG and SGW/PGW.............................6
5. HAG Function...................................................7
   5.1. Address Assignment.......................................7
       5.1.1. Separate BNG and PGW.............................7
       5.1.2. Integrated BNG and SGW/PGW......................8
   5.2. Setup and Tunnel Management............................9
   5.3. Traffic distribution policies..........................10
   5.4. Path Management.......................................11
   5.5. Backward compatibility..............................12
6. Applicability in Mobile networks............................12
7. Inter-working with MP-TCP...................................14
8. Security Considerations.......................................14
9. IANA considerations..........................................15
10. References..................................................15
   10.1. Normative References................................15
   10.2. Informative References.................................15
11. Acknowledgments............................................16

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with
respect to this document. Code Components extracted from this
document must include Simplified BSD License text as described in
Section 4.e of the Trust Legal Provisions and are provided without
warranty as described in the Simplified BSD License.

Internet-Drafts are draft documents valid for a maximum of six
months and may be updated, replaced, or obsoleted by other documents
at any time. It is inappropriate to use Internet-Drafts as
reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 30, 2019.
1. Introduction

To address the increasing demand of bandwidth by residential and enterprise customers, operators are looking for alternatives that can avoid rebuilding of the existing fixed access networks.

In Hybrid Access network, a Customer Premise Equipment (CPE) is connected to heterogeneous access networks (e.g. DSL, LTE etc) simultaneously. Traffic is distributed in flexible manner over these heterogeneous links thus increasing the bandwidth capacity of a residential or an enterprise customer.

This document describes a solution to implement the network based bonding Hybrid Access architecture. The solution is generic enough that it is applicable to fixed as well mobile nodes with multiple Access technologies.

2. Terminology

All mobility related terms are to be interpreted as defined in [RFC5213] and [RFC5844]. Additionally, this document uses the following terms:

- **IFOM**: IP flow mobility
- **NB-IFOM**: Network based IFOM
- **ePDG**: Evolved Packet Data Gateway (defined in 3GPP [24.302])
- **RR**: Routing Rule
- **HAG**: Hybrid Access Gateway
- **PcRF**: Policy and Charging Rules Function
- **NBF**: Network based Bonding Function
- **MCP**: Multi-path conversion point (defined in [NAMPTCP])
3. Reference Architecture

A CPE with HAG Figure 1 shows the network based bonding hybrid access architecture. In this architecture, HAG with network bonding function is deployed at the remote side of the CPE. The HAG receives the downstream traffic from internet and can apply the policies to distribute downstream traffic towards the CPE over available paths.

An in-band control protocol between the CPE and the HAG MAY be used to negotiate the traffic distribution policies for uplink traffic.

However, there SHOULD be flexibility to download the traffic distribution policies OUT-of-band.

Traffic distribution policies on CPE and HAG can have independent packet-based behavior.

Operators can have flexibility to distribute flows over multiple paths or associate affinity of flow to a particular access type. Traffic policies can also be applied taking into account the access networks link status such as latency, state etc.

Operator can also apply policy to fill one access link first before utilizing other (MAX-FILL). Affinity to one access MAY be due to cost or application characteristics. In this case the distribution of traffic is adjusted dynamically based on the load.
Behavior to adjust on moving around flows or packet is a matter of local policy.

4. Network Based Bonding Solution Overview

4.1. Separate BNG and PGW

\[\text{DSL Access} \quad \text{PMIPv6/GTP Tunnel} \]

\[\text{Non-3GPP access} \]

\[\text{3GPP Access}\]

\[\text{S1-AP} \quad \text{S11}\]

\[\text{S1-u} \quad \text{S5-u}\]

\[\text{S1-u} \quad \text{S5-c}\]

\[\text{SGW} \quad \text{MME} \quad \text{eNB}\]

\[\text{S1-AP} \quad \text{S11} \quad \text{S5-c}\]

\[\text{DSL Access} \quad \text{PMIPv6/GTP Tunnel} \]

Figure 2 Hybrid access service in Fixed mobile convergence
In Figure 2, CPE (either home or enterprise) is connected to internet via fixed access network using DSL as well as wireless access network using 4G cellular network.

The fixed access network BNG is connected to the PGW using 3GPP s2b reference point [TS23401]. The 4G cellular network is connected to the same PGW using S5 reference point (GPRS Tunneling Protocol (GTP) or Proxy Mobile IPV6 (PMIPv6) [RFC5213]) as specified by the 3GPP system architecture [TS23401].

The 3GPP as well non-3GPP access is bonded in CPE and the HAG which consist of NBF and PGW function. The bonding at HAG is achieved by allocating the same "IP address" when LTE access is setup on s5 and fixed (DSL) access over s2b.

The packet distribution policies applied to the bonded session on the HAG and CPE. Policies applied on HAG helps steering downlink traffic on specific access type or distribute percentage of traffic across both access types on per flow basis or per packet basis. Similarly policies applied CPE helps steering uplink traffic on specific access type or distribute percentage of traffic on per flow basis or per packet basis.

4.2. Integrated BNG and SGW/PGW
In Figure 3, CPE is connected to internet through HAG by fixed and wireless access. HAG consist of BNG, SGW/PGW and NBF function.

HAG performs address assignment for all access types and acts as IP anchor point for IP services.

5. HAG Function

5.1. Address Assignment

```
======       ::::::::       ======
CPE         LTE/DSL        HAG
```

5.1.1. Separate BNG and PGW

Following are steps for address allocation when BNG and PGW are separate. HAG in this case performs the NBF and PGW function.

[...CPE obtains LTE WAN IF address "A" during Pdp from HAG...]

(...CPE performs LTE attach for IMSI "X" APN "Y"...)

(...HAG allocates address "A" from APN.............)

[...CPE obtains DSL WAN IF address "A" during PPPoE from HAG...]
(...CPE begins the PPPoE setup with BNG....................)
(...BNG authenticates the CPE ..............................)
(...BNG receives all the 3GPP attributes from AAA server...)
(...BNG signals on s2b to HAG for address allocation.......)
(...HAG receives the s2b attach for APN "Y" with same IMSI.)
(...HAG finds session for IMSI "X" in APN "Y" RAT=LTE......)
(...HAG bonds the LTE session with s2b session............)
(...HAG returns address "A" in S2b response to BNG.........)
(...BNG stitches the PPPoE session with s2b session .......)
(...BNG returns the address "A" in PPPoE/DHCP to CPE.......)

HAG performs Address assignment for all access type which acts as anchor point for IP services.

APN "Y" on HAG is configured with property of "bonding" so that it can accept request from another access type for the same IMSI within same APN for same Pdp type. This helps in bonding the session with another access type session instead of treating it as handover.

BNG performs authentication of CPE. As part of authentication, it also receives the 3GPP attributes like IMSI, APN and HAG information from AAA server. It uses (3GPP) S2b reference point in [TS23402], specified by the 3GPP system architecture to get IP address from HAG and stitches the fixed access (PPPoE/IPoE) session with the s2b session both in control plane and data-plane.

The CPE remains unchanged as it uses standard method of IP address management for IPv4 and IPv6, on LTE link as well as DSL link.

5.1.2. Integrated BNG and SGW/PGW

Following are the steps for address allocation when BNG, SGW and PGW function is integrated along with the HAG function

[...CPE obtains LTE WAN IF address "A" during Pdp from PGW/HAG...]
(...CPE performs LTE attach for IMSI "X" APN "Y"...)  
(...HAG allocates address "A" from APN.............)

[...CPE obtains DSL WAN IF address "A" during PPPoE from BNG/HAG..]  
(...CPE begins the PPPoE setup with on BNG................)

(...BNG authenticates the CPE ............................)

(...BNG receives all the 3GPP attributes from AAA server...)  
(...BNG/HAG finds session for IMSI "X" in APN "Y" RAT=LTE..)

(...BNG bonds the PPPoE session with LTE session.........)

(...BNG returns the address "A" in PPPoE/DHCP to CPE.......

Address assignment is done in the HAG for all access type which acts as anchor point for IP services.

APN "Y" on HAG is configured with property of "bonding" so that it can accept request from another access type for the same IMSI within same APN for same Pdp type. This helps in bonding the session with another access type.

BNG performs authentication of CPE. As part of authentication, it also receives the 3GPP attributes like IMSI, APN and PGW information from AAA server. BNG detects that the PGW is local and hence internally bonds the fixed (PPPoE/IPoE) session with the LTE session with the same IMSI and APN. As part of bonding it uses the same IP allocated for the LTE session and sends back in PPPoE response or waits for DHCP to request for the address in the DHCP response. Traffic distribution policies are applied to the bonded LTE and fixed (PPPoE/IPoE) session to distribute the traffic.

The CPE remains unchanged as it uses standard method of IP address management for IPv4 and IPv6, on LTE link as well as DSL link.

5.2. Setup and Tunnel Management

There is no extra tunnel apart from the link tunnels representing each access used in this solution.
Any link can be setup first. The link that sets up access tunnel first gets the IP address from HAG. The link which comes later is bonded in HAG with the control plane to the existing access tunnel and the same IP address is returned to the later tunnel setup.

BNG stitches the fixed (PPPoE/IPoE) tunnel to the s2b tunnel setup towards the HAG. As part of it, it maps the setup and tear down event of the fixed (PPPoE/IPoE) tunnel to the s2b tunnel and vice versa.

5.3. Traffic distribution policies

As mentioned in earlier section, traffic distribution policies for upstream traffic is applied at CPE where as the downstream policies are applied at HAG. Given that single IP is allocated to all access type in this solution, it greatly helps to do flow mobility within the accesses.

Traffic distribution can be done on per flow basis, per MP-TCP sub-flow basis or on per packet. Flow based traffic distribution avoids out-of-order packets resulting out of differential latencies on each access tunnel and doesn't require buffering resources at the CPE or HAG to re-order the packets.

Policies applied in CPE can be downloaded out-of-band using ANDSF mechanism. Some CPEs are capable of sending initial uplink traffic on access type using random hashing but are able to move the flow to the access type chosen by network for the downlink traffic of that flow. Such CPEs need zero to minimal traffic policy configuration.

Traffic distribution policies applied at HAG for downlink traffic distribution can help in distributing flows or packets using hashing.

Traffic policies MUST have the flexibility to configure the amount of percentage of traffic to be steered over a given access type. This allows addressing the use case where operator MAY want to send a particular type of traffic over a specific access type (Video over DSL). In this case a video rule with affinity of DSL access can be set to steer 100 percent of traffic over DSL link whereas traffic matching any-any rule can be set to steer 50% over DSL and 50 % over LTE.

Traffic policies MUST allow asymmetric affinity association of access type for upstream and downstream traffic which allows splitting of a flow in upstream and downstream direction. Applying
such polices operators can use LTE for uplink where as fixed (DSL) for downlink. Studies of such configuration have shown application performance improvement over use same access for an application.

For the use case where a desired access link bandwidth is filled first (MAX-FILL) and use of second link is for the bandwidth overflow, one can use flow based or packet based approach for traffic distribution. The desirability of preferred access can be due to cheap access path or link characteristics for the given application.

To fulfill this requirement, two rate Three color marker (trTCM) can be used. Each access link uses token buckets to meter the packets as per configuration both at CPE and the HAG. Colored based policy is applied at CPE and HAG to steer packets to an access based on color. For ex. Green packets are steered to DSL if that is the preferred access, whereas yellow packets are steered over LTE access.

If flow based distribution is used, then on reaching certain thresholds there MUST be flexibility to move the flows from preferred access (say DSL) to another (LTE) by changing the percentage distribution. However, moving of FAT flows MAY result in under utilization of preferred access link. Similarly once the threshold drops, the traffic can be move back to preferred access by reverting the percentage distribution.

To avoid FAT flow distribution issues, packet based traffic distribution can be used to fully utilize the preferred access. Packets sent over different access for the same flow can reach out-of-order at the receiving end, due to differential transport latencies. Hence receiving end needs buffering and re-ordering capabilities to deliver flow packets correctly to an application.

5.4. Path Management

This solution relies of existing mechanism of Path management for wireless (LTE) and fixed (PPPoE/IPoE) tunnels.

In case of failure of any access tunnel the traffic MUST be switched to the alternate available access tunnel based on the traffic distribution policies.
5.5. Backward compatibility

This solution does not introduce any new protocol extensions. In this solution the CPE uses ANDSF routing rules to do the traffic distribution downloaded off-band in the CPE.

The policies at the HAG are either local configured or downloaded from PCRF. The existing service (ex. IPTV traffic MUST remain on DSL access) remains untouched by configuring appropriate traffic distribution policies. The exact configuration of those policies is outside the scope of this document.

6. Applicability in Mobile networks

A mobile node (MN) (also called User Equipment UE) connected to a 3GPP access network specified by the 3GPP system architecture [TS23401] is connected over the S5 reference point (Proxy Mobile IPV6 (PMIPv6) [RFC5213] or GPRS Tunneling Protocol (GTP)) to the PGW where the mobile node’s session is anchored.

The (3GPP) S2b reference point in [TS23402], specified by the 3GPP system architecture defines a mechanism for allowing the mobile node (MN) attached to an "untrusted" non-3GPP IP access network to securely connect to a 3GPP network and access IP services. In this scenario, the mobile node establishes an IPSec ESP tunnel [RFC4303] to the security gateway called evolved packet data gateway (ePDG) and which in turn establishes a GPRS Tunneling Protocol (GTP) [TS23402] or Proxy Mobile IPV6 (PMIPv6) [RFC5213] tunnel to the packet data gateway (PGW) [TS23402] where the mobile node’s session is anchored.

The figure below shows the hybrid access figure where the mobile node is connected to 3GPP and non-3GPP access simultaneously getting access to IP services via a PGW.
Figure 4 Hybrid access service in Mobile network

In the hybrid access architecture, an User equipment (UE) is connected to multiple access technology at the same time. It MAY connect to same network or different IP network based on the operator service. A mobile node with Third Generation Partnership Project (3GPP) access technology such as LTE, UMTS and non-3GPP access such as WIFI having simultaneous network connections is a use case of hybrid access in mobile networks.

As shown in Figure 4, the LTE access is bonded with the WIFI access and the same IP address is allocated on s2b as well as
s5 3gpp reference point. As discussed above, traffic distribution policies can be applied to steer traffic over specific access type or distribute over both access type to increase the bandwidth for the mobile node.

In some mobile networks, WIFI is preferred access since it’s cheap, in that case policies described in MAX-FILL can be applied.

In some mobile networks, mobile nodes are configured to prefer WIFI access as local break out policy. However it’s been observed that if mobile node has LTE access as well WIFI access available and if the mobile node connects to WIFI access over the s2b reference point to the same PGW, the PGW treats it as 3GPP to non-3GPP access handover and disconnecting the LTE access. But since mobile node is configured to be always connected over LTE access, mobile node reconnects over LTE and the PGW treats it as non-3GPP to 3GPP access handover disconnecting the WIFI access. This results in ping-pong effect. Since both accesses are simultaneously connected, in this solution, it helps in addressing the ping-pong issue as well.

7. Inter-working with MP-TCP

When used flow based hashing, it is possible that a FAT flow may cause to over congest the access link. To address FAT flow issues operator can deploy a MCP with the NBF. Operator in that case can apply policy to ensure the FAT flow traffic is split among small multi-path flows which can be seamlessly moved between the access types based on traffic distribution policies.

Inter-working helps operators in using MP-TCP for selective traffic thus ensuring effective utilization of buffering resources both at CPE as well as at MCP.

8. Security Considerations

The security considerations applicable while deploying the access types independently remains same while deploying network based bonding hybrid access architecture. This specification does not introduce any new security vulnerabilities.
9. IANA considerations

10. References

10.1. Normative References


[24.008] 3GPP, "Technical specification Group Core Network and Terminals: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3"

[24.301] 3GPP, "Technical specification Group Core Network and Terminals: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3"


10.2. Informative References


[TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", .

11. Acknowledgments

The authors are thankful for the detailed review and valuable feedback provided by Guiu Fabregas and Laurent Thiebaut.
Authors’ Addresses

Praveen Muley
Nokia
805. E. Middle Field Rd.
Mountain View, CA, 94043

Email: praveen.muley@nokia.com

Wim Henderickx
Nokia
Copernicuslaan 50
Antwerp 2018
Belgium

Email: wim.henderickx@nokia.com

Geng Liang
China Mobile
32 Xuanwumen West Street,
Xicheng District, Beijing, 100053,
China

Email: gengliang@chinamobile.com

Hans Liu
D-Link Corporation
289, Sinhu 3rd Road,
Neihu District, Taipei City, 11494,
Taiwan, R.O.C.

Email: hans_liu@dlink.com.tw

Loris Cardullo
Vodafone
Italy

Email: Loris.Cardullo@vodafone.com

Jonathan Newton
Vodafone
United Kingdom

Email: Jonathan.Newton@vodafone.com
Architecture for Control and User Plane Separation on BNG
draft-wadhwa-rtgwg-bng-cups-03.txt

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on September 11, 2019.
Abstract

This document discusses separation of subscriber-management control plane and data-plane for BNG. Traditionally, the BNG provides aggregation of fixed access nodes (such as DSLAM and OLTs) over Ethernet and provides subscriber management and traffic management functions for residential subscribers. The BNG has however evolved to become a multi-access edge device that also provides termination of subscribers over fixed-wireless and hybrid access. Therefore, this document proposes interfaces between control and user-plane of a BNG that can support multi-access BNG.

Table of Contents

1. Introduction...................................................3
   1.1. Requirements Language.....................................3
2. CUPS for BNG...................................................3
   2.1. Convergence...............................................5
3. Interfaces for CUPS............................................6
   3.1. In-band Signaling Channel.................................7
3.2. State Control Interface...................................8
   3.2.1. Session level state management.......................8
   3.2.2. Session level event notifications...................14
   3.2.3. Node level management...............................15
1. Introduction

This document describes requirements and architecture for separation of subscriber management control plane and user plane for the BNG. In rest of the document the control plane is referred to as CP, user plane as UP, and the separation is referred to as CUPS (control and user plane separation). The draft describes the functional decomposition between CP and UP, and applicability of CUPS to a BNG that can support multiple access technologies such as fixed (DSL or Fiber), fixed-wireless (LTE, 5G) and hybrid access i.e. simultaneous fixed and wireless access described in BBF [WT378]. The subsequent sections of the draft also define the interfaces required between CP and UP and briefly discusses a candidate base protocol for these interfaces.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. CUPS for BNG

In a CUPS architecture, signaling to setup subscriber sessions CP terminates signaling to setup subscriber sessions, and interfaces with the UP to create forwarding state for these sessions on the UP.

For fixed access subscribers, the CP terminates the signaling protocols (e.g. DHCP, PPPoE, SLAAC) from the customer premise, performs authorization/authentication with AAA Server, participates in address assignment, and then interfaces with the UP to create state related to forwarding and SLA management for the subscriber sessions on the UP. A subscriber session is a single IP connection, such as an IPoE or PPPoE session. The session can be single-stack (IPv4 or IPv6 only), or dual-stack (both IPv4 and IPv6). A CPE can
have multiple sessions, if multiple IP connections are required (e.g. on per service, or one per device behind the CPE).

The CP also processes solicited or unsolicited event notifications from the UP e.g. periodic accounting updates, usage reports, or session inactivity notifications. The interface between CP and UP that is used by the CP to manage session related forwarding state on the UP is being referred to as "state control interface". Asynchronous event notifications from UP to CP are also part of this interface.

In typical fixed access deployments, signaling (e.g. DHCPv4/v6, PPPoE, ICMPv6 RS/RA) to setup the subscriber sessions is in-band, and hence the UP receives the signaling messages from the customer premise. The UP should transparently forward (unmodified) in-band control messages as received from the customer premise to the CP and return messages from CP to the customer premise. Therefore, an in-band signaling channel is required between UP and CP. With a typical "CUPS BNG" deployment, the CP and UP are connected over a network, and the in-band signaling channel must be over a tunnel.

The UP performs forwarding and traffic management for the subscriber sessions. The infrastructure routing and signaling is done on the local control plane of the UP for fast convergence on network topology changes. In rest of the document the term "UP" is used generically for both functions performed by the local control plane on the UP and the data-plane.

A typical deployment architecture for CUPS includes a centralized CP running as a VNF interacting with multiple BNG UP instances that may be more distributed than the CP and could run as VNF or PNF. In this model, the CP and UP association is 1:N. This composite system containing CP VNF and one or more UP instances is referred to as a "CUPS BNG" in rest of the document. For operational ease, the CP MUST provide a single point for control and management for the entire "CUPS BNG". It MUST expose a single interface on behalf of the "CUPS BNG" to external systems such as AAA servers, OSS/BSS, Policy and charging servers. The CP VNF MUST support scale-out in order to cope with growth in number of subscriber sessions and/or increase in number of UP instances in the "CUPS BNG". Figure 1 below shows the functional components and interfaces for a "CUPS BNG".
2.1. Convergence

A single BNG can support subscribers over fixed, "fixed-wireless" or hybrid access. When a residential gateway has fixed-wireless access (LTE or 5G), then the BNG participates in 3GPP signaling with an MME.
or AMF (i.e. support 3GPP S11 and N11 interfaces) to setup connections from (NG)RAN. With Hybrid access the customer premise initiates both fixed and wireless connections. The BNG in this case aggregates subscribers over Ethernet from fixed access nodes (DSLAMs and OLTs), but simultaneously terminates connections from (NG)RAN by participating in signaling with MME or AMF (S11/N11 interface). These deployment models are drivers for fixed-mobile convergence. It is important to ensure that the interfaces between CP and UP for CUPS can support not only fixed L2 access, but also the converged access scenario shown in Figure 2. One key requirement on the CP in these cases is the need to participate in 3GPP signaling (which is out-of-band) to setup the data-path. The data-path is a GTP-u (GPRS Tunneling protocol - User Plane) tunnel from the RAN (i.e. S1-u interface for LTE) as described in 3GPP [TS29281], and it terminates on the UP. It carries data traffic but also subscriber signaling messages (e.g. DHCPv4, DHCPv6, SLAAC) from the customer premise. The UP therefore still requires an in-band signaling channel to transport these protocol messages to the CP.

3. Interfaces for CUPS

A "CUPS BNG" MUST support the following interfaces between CP and UP, as shown in the figure in section 2.
3.1. In-band Signaling Channel

Section 2 describes the need for a signaling channel between CP and UP to transport in-band control messages between CP and the customer premise. Following are some key requirements for this interface.

- The UP MUST pass the access circuit identifier over which the signaling messages are received as meta-data to the CP. This includes port, VLAN tags, tunnel endpoint IPs, any tunnel identifiers such as GTP TEID, MPLS labels, L2TP tunnel-id etc. The UP MUST also pass the L2 or L3 transport service that the access circuit is associated with. In case the control message PDU is carried in an Ethernet frame, then the UP SHOULD pass the received Ethernet frame to the CP. Both access circuit identifier and information in the Ethernet header are required by the CP to construct successful response packet (control message) back towards the customer premise. The access circuit identifier MUST be reflected from CP to UP, so UP can identify the access circuit over which it needs to send the CP’s response packet. In the control message sent from UP to CP, the UP MUST also include the local MAC address associated with access circuit. This is because certain control messages from the customer premise are destined to a broadcast MAC (e.g. DHCP DISCOVER) or multicast (e.g. ICMPv6 RS), so CP cannot infer the local MAC from these messages. Certain messages also require the local MAC address to be inserted in the message (e.g. Link-Layer address in ICMPv6 RA messages)

- The CP MUST be able to control the UP to forward only specific control messages to the CP.

- The CP MUST be able to control the UP to block certain control messages received on a particular access circuit.

- The CP MUST be able to control the UP to limit the rate of control messages (of specified type) to be sent by the UP.

- The CP MUST be able to prioritize reception of certain control messages over others in a granular manner (e.g. prioritize DHCP RENEWS over DISCOVERS or prioritize PPP Keepalive over other messages).

- The in-band signaling channel MUST support both fixed and converged access as described in section 2.1. The tunnel used for transporting these messages should therefore support both Ethernet and IP payloads.
3.2. State Control Interface

The CP and UP can exchange state at two levels using the "state control interface". One is at the node level and includes node-level information such as supported features, software releases, available resources, and operational state (e.g. active, failed, or overloaded). The other is at the subscriber session level. Subscriber session is described in section 2. The session level state includes basic forwarding and traffic management rules per session, that need to be provided by the CP to the UP in order to control per session forwarding and traffic management on the UP. It also includes state that triggers routing related actions on the UP. The session level state can include asynchronous event notifications from UP to CP, such as notifications to report per session usage (periodically or based on thresholds), notification to report session inactivity, and session liveness.

The interactions between CP and UP over "state control interface" can be categorized as:

- Session level state management
- Session level event notifications
- Node level management
- Node level event notifications

Following sub-sections provide more details on these interactions. The interactions between CP and UP over "state control interface" are modeled via abstract request/response messages between CP and UP. These messages will need to be defined as part of the protocol specification for this interface.

The protocol selected to implement this interface MUST support both fixed access and converged access (described in section 2.1) on BNG.

3.2.1. Session level state management

Once the CP has successfully authorized and/or authenticated the subscriber session, and completed address assignment, it uses the "state control interface" to install forwarding and related state for the session on the forwarding path of the UP. This is abstracted as a "session create request" call from CP to UP, as shown in the figure below. The UP MUST ack or NACK via a response back to CP.
Since BNG can support different access types (e.g. fixed L2 access, or tunneled L3 in case of fixed-wireless, or a combination in case of hybrid access), it is important that the forwarding state information for the subscriber sessions, sent from CP to UP, can be specified as flexible packet matching rules and set of actions related to forwarding and traffic management. The UP should be able to use these match rules and actions to derive various lookup tables and processing in the forwarding path to forward traffic to and from the CPE.

The basic forwarding state in upstream direction (i.e. access to network) and downstream direction (i.e. network to access) fundamentally consists of session identification and one or more actions. Following shows a logical representation of a directive from CP to UP to install basic forwarding state on the UP for fixed L2 access (i.e. access from DSLAM or OLTs over Ethernet).

### Direction Upstream - Access to Network:
- **Subscriber-identification**: Port/VLAN-tag(s) + subscriber-MAC
- **Action**: remove encapsulation, IP FIB lookup, forward to network.

### Direction Downstream - Network to Access:
- **Subscriber-identification**: IP address
- **Action**: lookup IP DA, build encapsulation using Port/VLAN-tag(s) + subscriber-MAC, forward to access.

Optionally, the IP address assigned to the CPE can also be provided for subscriber-identification (e.g. for anti-spoofing) in the upstream direction.

In case of PPPoE sessions, the subscriber-identification for upstream direction and encapsulation for downstream direction also includes the PPPoE session-id.

Based on the directive from CP to UP (as shown in the example above), the UP can then populate appropriate tables in the forwarding path, e.g. subscriber lookup tables, IP-FIB, and ARP or IPv6 Neighbor discovery table. It can also program the packet processing in both upstream and downstream direction based on the specified actions.

In case of "fixed-wireless" access, the access circuit is a GTP-u tunnel. In this case there is no physical interface (or port), and hence the CP MUST provide a tunnel definition to the UP to use as access circuit in upstream direction, and encapsulation in downstream direction. The tunnel definition will include the tunnel endpoint IP, and TEID that is established via out-of-band signaling.
between the CP and the customer premise. It can also include the routing context for transporting the tunnel.

In addition to setting up the forwarding state as directed by the CP, the UP also needs to announce in routing the aggregate prefixes from which the CP assigns IPv4 and IPv6 addresses (or prefixes) to the CPEs. The CP SHOULD provide these aggregate prefixes to the UP as part session state. In case the aggregate prefixes are not provided, the UP MUST announce individual CPE addresses in routing, or it MAY try to aggregate in case addresses for multiple CPEs are from a contiguous address space.

The CPE can have a routed subnet behind it (aka framed-route). CP can learn the framed-routes during authentication/authorization. The CP should provide the framed-route to the UP as part of session state. The UP MUST install this route in the forwarding path and associate it with the forwarding state of the corresponding subscriber session. It should also announce this in routing towards the Network.

The CP MUST also provide to the UP the address assigned as IP gateway address to the CPEs in DHCP. The UP MUST locally configure this address appropriately, such that it can respond to ARP requests for this address from the CPEs.

The session state on the UP is always controlled by the CP i.e. the UP just follows the directive from the CP to install, modify and delete the session state. In addition to the basic forwarding state, the 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
- NAT
- Application aware policies

BNG deployments use hierarchical QoS (H-QoS) models which follows from a combination of link-layer over-subscription, multi-service networks and multiple layers of aggregation. For example, a common hierarchy exists of at least a QoS layer per access-node, and per
CPE. The CP MUST provide SLA management information to the UP per CPE. This includes applicable QoS parameters (e.g. rates, queues, markings) and the QoS hierarchy to which the CPE belongs. The CP may choose to signal this via a QoS policy that is locally pre-configured on the UP.
Session Creation Sequence

DHCP Discover

DHCP Discover

In-band signaling channel

Access Request

DHCP Offer

In-band signaling channel

Access Accept

DHCP Request

In-band signaling channel

Session Creation Req

Session Creation Resp.

DHCP ACK

In-band signaling channel

DHCP Ack

Session Creation Sequence
CP can trigger update of session state on the UP, triggered by re-authentication or COA from AAA or policy-server, as shown in the figure below.

```
+-----+       +-----+       +-----+
| UP  |       | CP  |       | AAA |
+-----+       +-----+       +-----+
                      | Server |
                      +--------+
                         +-----+
                         | UP  |
                         +-----+
```

Session Modification

CP can trigger the deletion of session state based on signaling messages (as shown in the figure below), administrative action or disconnect-message initiated from the AAA server.
3.2.2. Session level event notifications

UP can asynchronously generate Session level event notifications to the CP. An example of asynchronous notification is periodic usage reporting from UP to the CP, so that the CP can report the usage to a AAA server via interim accounting-updates. The CP can set the periodicity of this notification on the UP based on interim accounting interval configured by the operator on the CP.
Async Event Notification
(periodic usage)

Async Event Response

Acct Update Req

Acct Update Resp

Async Event Notification for periodic usage

Following are some other examples requiring asynchronous notifications from UP to CP.

- Threshold based usage reporting
- Inactivity timeout
- Subscriber unreachability detection

The protocol for "state control interface" MUST support asynchronous notifications from UP to CP.

3.2.3. Node level management

There needs to exist a concept of association between CP and UP. When the CP or UP comes online it should setup an association with configured or discovered peers via a message exchange. In association setup, the nodes should be able to exchange supported capabilities, version of software, load/overload information, and resource information. Also, any node-wide parameters can be exchanged during association setup.
No session state related messages should be accepted from the peer by either CP or UP unless an association exists.

Either node should be able to update the association to report changed feature capabilities, overload condition, resource exhaustion or any other node-wide parameters.

The UP should be able to request a graceful association release from the CP. In this case the CP should delete all sessions from that UP and process the final stats report for each session and send it in accounting-stop to the AAA server. During this process the CP MUST not create new sessions on the UP. Once all sessions are successfully deleted, the CP should release the association.

There needs to be a periodic node-level heartbeat exchange between CP and UP to detect if the peer is reachable and active. If peer is determined to be down based on heartbeat messages, then all the data-plane session state associated with the peer should be deleted.

```
+----+                    +----+
|UP  |                    |CP  |
+----+                    +----+
               Association Setup Req
                        --------------------->
               Association Setup Resp
                        <----------------------
               Periodic Heartbeats
                        <---------------------->
+----+                    +----+
|UP  |                    |CP  |
+----+                    +----+
```

Node Association Setup and Maintenance

3.2.4. Node level event notifications

There needs to be support for asynchronous node level event notifications from UP to CP. Example includes switchover.
notification in case ports or UP failures when UP node level warm-standby redundancy is enabled. Based on this notification, the CP can create session state for all the sessions associated with the failure domain on the new primary UP.

3.3. Management Interface

The CP MUST provide a single point for local management of "CUPS BNG" system to the operator. This requires a management interface between CP and each of its associated UPs for pushing configuration to the UP and retrieving operational state from the UP. The interface MUST minimally include BNG specific configuration and state.

The Management interface SHOULD support transactional configuration from CP to UPs and SHOULD support state retrieval, both based on a well-defined data schema. The management interface SHOULD support unsolicited signaling of state changes (events) from UP to CP i.e. MUST provide telemetry for events. Either gNMI or NETCONF can be considered as acceptable candidates for model driven management interface.

4. Resiliency

"CUPS BNG" system MUST be protected against failure of CP VNF and MUST be able to recover the session state without operator intervention and reliance on CPEs. This can be achieved by providing redundancy for processing resources within CP VNF and maintaining redundant instance of session state.

Protection against UP failures based on 1:1 UP (hot-redundancy) and N:M (warm-redundancy) SHOULD be supported. For 1:1 hot-redundancy the CP needs to create data-plane state for sessions on both UPs that form a redundant pair, using the "state control interface". The CP needs to ensure the data-plane state for a session stays synchronized between the two nodes. A given session’s data-plane should only be active on one UP in the pair, which serves as active UP for the session. However, sessions that share the redundant UP pair can be distributed between the two UPs for active forwarding.

N:M warm-redundancy (N > M) can be supported via creation of data-plane state on the designated backup chassis after the failure has been detected. This would result in longer failover times than 1:1 hot-redundancy.
Redundant network connectivity between CP and UPs MUST be supported. In the "CUPS BNG" architecture, it is important to configure redundant connectivity that doesn’t share fate.

5. Protocol Selection for CUPS Interfaces

It is important that the selected protocol for "state control interface" between CP and UP works not just for fixed access but also works for converged access on BNG. 3GPP has defined PFCP (Packet Forwarding Control Protocol) in [TS29244] as the interface between CP and UP for LTE gateways. This protocol is suited for large scale state management between CP and UP. Following are some of the key attributes of this protocol:

- It supports management of forwarding and QoS enforcement state on the UP from CP. It also supports usage reporting from UP to CP.
- It is over UDP transport and doesn’t suffer from any HOL blocking.
- It provides reliable operation based on request/response with message sequencing and retransmissions.
- It provides an overload control procedure where overload on UP can be handled gracefully.
- The protocol is extensible and allows addition of new IEs.

For fixed access BNG, the protocol requires simple extensions in form of additional IEs. The required extensions are mainly due to fact that typically a fixed access BNG requires tighter control over L2 behavior and manages access and subscriber using L2 identifiers (such as VLANs and MAC addresses), whereas mobile access works in terms of L3, either routed or tunneled.

The details of the protocol as applicable to the BNG and the required extensions will be defined in a separate draft.

[TS29244] also describes an in-band signaling channel based on GTP-u tunnel between CP and UP. GTP-u (GPRS Tunneling protocol - User Plane) is defined in 3GPP [TS29281] and defines a tunneling protocol which carries IP payloads. The protocol runs over a UDP/IP stack and uses UDP port number 2152. Data within a tunnel can be multiplexed based on Tunnel Endpoint Identifiers (TEIDs). The protocol supports optional sequence numbers. The protocol supports extension headers to allow development of new features. GTP-u tunnels are signaled between CP and UP, and it is possible
to associate filters to block certain control packets from being forwarded from UP to CP. The payload type carried by GTP-u can be extended to Ethernet (via payload type in extension header). The tunnel encapsulation can also be extended similarly to carry any required meta-data.

6. Address Pool Management

The CP MUST support management of IPv4 and IPv6 address pools, where each pool can contain one or more subnets. The pool management MUST support pool selection based on one or more of the following criteria:

- UP
- Access port on the UP,
- Redundancy domain on the UP (e.g. set of access ports that share fate with respect to switchovers due to failures, when UP node level redundancy is enabled).
- Service (e.g. HSI, VoIP, IPTV etc.).
- Location (e.g. based on circuit-id/remote-id or part of circuit-id/remote-id in DHCP and PPPoE).

Pool management on CP SHOULD NOT statically link subnets to UPs but SHOULD dynamically allocate subnets to UP based on load i.e. on-demand, and signal allocated subnets using the "state control interface" as described in section 3.2.1. This allows for better IP resource utilization and less subnet fragmentation.

7. Security Considerations

For security between CP and UP, Network Domain Security (NDS) as defined in [TS33210] can be considered. As per NDS, the network can be split into security domains. Communication within a single security domain is considered secure, and protocols can operate without any additional security. When communication has to cross security domains, then IPSEC can be used.

8. IANA Considerations

None.
9. References

9.1. Normative References


9.2. Informative References


Authors’ Addresses

Sanjay Wadhwa
Nokia
777 East Middlefield Road
Mountain View
USA

Email: Sanjay.wadhwa@nokia.com
Requirements for Protocol between Control and User Plane on BNG
draft-wadhwa-rtgwg-bng-cups-protocol-requirements-02.txt

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on September 11, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
Traditionally, the BNG provides aggregation of fixed access nodes (such as DSLAM and OLTs) over Ethernet and provides subscriber management and traffic management functions for residential subscribers. The BNG has however evolved to become a multi-access edge device that also provides termination of subscribers over fixed-wireless and hybrid access. An overall architecture and interfaces required between separated control and user-plane for a multi-access BNG are described in draft-wadhwa-rtgwg-bng-cups-01.txt. This document describes requirements for protocol between subscriber-management control-plane and user-plane for BNG to achieve separation.

Contents
1. Introduction...................................................3
   1.1. Requirements Language..................................3
2. Requirements for "CUPS protocol"...............................3
   2.1. State Control Interface Requirements..................5
   2.2. Extensibility...........................................8
   2.3. Scalability and Performance...........................9
   2.4. Transport Protocol....................................10
   2.5. In-band Control Channel Requirements................10
   2.6. Resiliency............................................12
   2.7. Security.............................................13
3. "CUPS protocol" candidate..................................13
4. Security Considerations.....................................14
5. Management Interface Requirements..........................14
1. Introduction

This document describes a set of requirements for protocol between subscriber-management control and user plane for BNG, that need to be met, in order to achieve separation. In rest of the document the control plane is referred to as CP, user plane as UP, and the separation is referred to as CUPS (control and user plane separation). The protocol between control and user-plane to achieve separation is referred to as "CUPS protocol". These requirements should form the basis for "CUPS protocol" selection. The functional decomposition between CP and UP, and applicability of CUPS to a BNG that can support multiple access technologies such as fixed (DSL or Fiber), fixed-wireless (LTE,5G) and hybrid access are described in [CUPS].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Requirements for "CUPS protocol"

[CUPS] defines overall operation and architecture for control and user-plane separation on BNG. It also defines key functional interfaces between CP and UP, as shown in Fig 1, to realize the separation. "CUPS protocol" MUST provide support for information exchange to realize the "state control interface" and "in-band signaling channel" as defined in [CUPS].
2.1. State Control Interface Requirements

. "CUPS protocol" MUST support convergence on BNG, where the CPEs terminating connections on the BNG can have fixed-access (e.g. xDSL/PON/Ethernet), fixed-wireless access (LTE/5G) or hybrid-access (i.e. combined fixed and wireless access).

. "CUPS protocol" MUST support messages and information exchange for node level management. There needs to exist a concept of association between CP and UP. When the CP or UP comes online it should setup an association with the configured or discovered peers via a message exchange. In association setup, the nodes should be able to exchange supported capabilities, version of software, load/overload information, and resource information. Also, any node-wide parameters can be exchanged during association setup.

. "CUPS protocol" MUST allow either node to update the association to report changed feature capabilities, overload condition, resource exhaustion or any other node-wide parameters.

. "CUPS protocol" MUST provide support for UP to request a graceful association release from the CP.

. "CUPS protocol" MUST support periodic node-level heartbeat exchange between CP and UP to detect if the peer is reachable and active.

. "CUPS protocol" MUST support exchange of messages and information elements (IEs) between CP and UP for session level state management on the UP.

A subscriber session is a single IP connection, such as an IPoE or PPPoE session. A CPE can have multiple sessions, if multiple IP connections are required (e.g. one per service, or one per device behind the CPE). The session level state on the UP, managed from the CP includes:

- Data-plane state for forwarding data traffic from subscriber sessions in upstream direction (access to network), and downstream direction (network to access).

- Forwarding state related to in-band control plane messages (such as messages for DHCP, PPPoE, SLAAC) that are forwarded
from CPE to CP via the UP (in upstream direction), and from CP to CPE via the UP (in downstream direction).

In addition to the basic forwarding state, the "CUPS protocol" MUST support messages and information elements (IEs) for CP to associate, update and disassociate other data-plane related state with the session e.g. state related to:
- Filtering
- SLA management
- Statistics collection
- Credit control (usage monitoring and reporting)
- Traffic mirroring for legal intercept
- NAT
- Application (L4-L7) aware policies

Depending on the type of access and the network between access-nodes and the BNG, the subscriber traffic from the CPEs can be encapsulated and transported over an L2 connection or over an L3 tunnel. Common scenarios for fixed access include Ethernet (q-in-q, 1q), L2oGRE, L2TPv3, VxLAN, and MPLS PW. For fixed-wireless the access is over a GTP tunnel (as defined in [CUPS]). The tunnel transport for L3 tunneled subscriber traffic can IPv4 or IPv6. The subscriber traffic itself can be IPv4, IPv6 or PPPoE. In case of PPPoE, the BNG can terminate PPPoE or tunnel it over L2TP to another gateway. The data-plane on the BNG decapsulates the upstream (access->network) traffic and routes it towards the network in appropriate routing-context, and optionally perform NAT before routing. It determines the subscriber for downstream (network->access) IP traffic, encapsulates it appropriately before forwarding towards the access. In addition, it does traffic-management and SLA management, maintains traffic statistics and optionally monitors and reports usage. The "CUPS protocol" MUST be able to carry state from CP to UP for IPv4, IPv6 and PPPoE sessions, for various flavors of transport connections mentioned above.

Given the variety of access types on the CPE and type of transport networks between access-nodes and BNG (as outlined above), the "CUPS protocol" MUST specify forwarding state information for the subscriber sessions, for both data and in-band control, as flexible packet matching rules and set of actions related to forwarding and traffic management, rather than just fixed-format lookup tables understood by particular UP implementation. Using the flexible match rules and actions conveyed in the "CUPS protocol" IEs, the UP should unambiguously be able to derive
various lookup tables and processing in the forwarding path to forward traffic to and from the CPE. The basic forwarding state in upstream direction (i.e. access to network) and downstream direction (i.e. network to access) fundamentally consists of session identification and one or more actions. Following shows a logical representation of a directive from CP to UP to install basic forwarding state on the UP for fixed L2 access (i.e. access from DSLAM or OLTS over Ethernet).

- **Direction Upstream - Access to Network:**
  - Subscriber-session identification: Port/VLAN-tag(s) + subscriber-MAC + Session IP address + PPPoE Session-ID
  - Action: remove encapsulation (i.e. Ethernet and PPPoE/PPP headers), apply policer, do IP FIB lookup, forward to network.

- **Direction Downstream - Network to Access:**
  - Subscriber-session identification: IP address
  - Action: apply subscriber-shaper, build encapsulation using (PPPoE session-id and Port/VLAN-tag(s)+ subscriber-MAC), forward to access.

Examples of actions and processing related to forwarding and traffic management include encapsulation/decapsulation, table lookups, drop, forward, mirror, count, redirect, police, classify, queue, shape etc.

In addition to packet-matching rules and actions to setup datapath on the UP, the "CUPS protocol" MUST allow CP to specify subscriber routing and IP interface related information. This includes the following:

- Aggregate IPv4 subnets and IPv6 prefixes that are used for assigning addresses or prefixes (e.g. IPv6 delegated-prefix) to subscribers on a UP. These are announced in routing by the UP to draw downstream traffic.
- UE’s IP address and subnet mask.
- Default gateway IP address within the subscriber subnets. This is used to draw upstream traffic from the CPEs and the UP is required to respond to ICMP requests for this address from the CPEs.
- Subnets for network behind a CPE (also known as framed-routes).
The "CUPS protocol" MUST provide support for CP to specify session level HQOS related information to the UP. A common QoS hierarchy on BNG consists of at least a QoS layer per access-node, and per CPE. "CUPS protocol" MUST provide support for CP to specify QoS parameters (e.g. rates, queues, markings) and the QoS hierarchy to which the CPE belongs, to the UP. The CP may choose to signal this via a QoS policy that is locally pre-configured on the UP. "CUPS protocol" MUST provide support for CP to specify HQOS-policy that the session is associated with.

"CUPS protocol" MUST support asynchronous session level event notifications from UP to CP. Session level asynchronous notifications include:

- Periodic usage-reports
- Threshold based usage-reports
- Inactivity timeout
- Subscriber unreachability detection

"CUPS protocol" MUST support asynchronous node level event notifications from UP to CP. Example includes switchover notification in case ports or UP failures when node level redundancy is enabled.

2.2. Extensibility

"CUPS protocol" MUST support exchange of software version and feature capabilities when a node level association is setup between a CP and UP.

"CUPS protocol" MUST encode information in messages as TLVs.

"CUPS protocol" MUST allow extension to defined Information Elements (IEs) i.e. it MUST allow adding new information to existing IEs while maintaining backwards compatibility.

"CUPS protocol" MUST allow addition of new IEs exchanged in protocol messages.

"CUPS protocol" MUST support vendor specific IEs (modelled as TLVs) by carving out TLV space for vendor specific extensions.
"CUPS protocol" processing on UP MUST support graceful handling when an unknown TLV is received. The UP MUST ignore unknown TLV and continue with normal message processing. This ensures the CP MAY send non-mandatory TLVs to the UP. However, CP MUST only send mandatory TLVs if it knows the UP will accept it (based on local configuration or based on capability exchange during association setup). A TLV is considered mandatory if session state cannot be installed or updated without it.

2.3. Scalability and Performance

A single CP VNF can control multiple UP nodes. Each UP can support its maximum scale of subscriber sessions as allowed by its data-plane. External control plane running as a VNF can horizontally scale-out as needed with the growth in CUPS system-wide subscriber scale. In typical deployments CP may be centralized whereas the UPs may be distributed, with multiple L2 or L3 hops between CP and UPs. There are scenarios where a large number of sessions may be getting created or deleted close in time via "CUPS protocol". It is important that latency to bring subscribers online is minimized. The transport protocol chosen for "CUPS protocol" MUST NOT suffer from head-of-line (HOL) blocking where transport of messages related to one subscriber can be adversely impacted by messages being exchanged for other subscribers.

"CUPS protocol" MUST limit chattiness by minimizing number of messages required to create fully functional subscriber on the UP with complete forwarding, traffic management, HQOS, and routing state. Ideally, a single request/response message exchange between CP and UP should be able to create subscriber with all the required state in the data-plane. The "CUPS protocol" message that creates the subscriber session MUST therefore be able to signal IEs for all the required subscriber state.

To further reduce latency the protocol MUST be binary encoded.

"CUPS protocol" MUST allow dynamic scale-out for control plane VNF with the growth in subscriber scale of the CUPS system, as more UPs are added to the CUPS system or more ports are enabled on a UP in a CUPS system.
The "CUPS Protocol" MUST allow mechanism to provide balancing of processing load amongst compute resources of control-plane VNF that supports dynamic scale-out.

"CUPS protocol" SHOULD support signaling of overload state and optionally overload mitigation parameters from UP to CP, when UP determines the incoming signaling from CP is exceeding (or about to exceed) its nominal processing capacity. Overload mitigation can include a temporary message throttling on CP towards UP. Mitigation parameters can include message rate and validity time for the specified rate.

2.4. Transport Protocol

As mentioned in section 2.3, the transport protocol used for "CUPS protocol" MUST NOT suffer from HOL blocking. Therefore, TCP is not an option for the transport protocol.

Ideally, the transport protocol SHOULD preserve message boundary with datagram semantics and should be available or easily implementable on any simple forwarding devices. Therefore, UDP is the preferred option.

"CUPS protocol" MUST therefore support reliability and ordering for exchanged messages. The reliability and ordering can be based on request/response with message sequencing and re-transmissions.

2.5. In-band Control Channel Requirements

"CUPS protocol" MUST support setting up of control channel between UP and CP for transporting in-band control messages (e.g. DHCPv4/v6 and PPPoE) received on the UP (from CPEs) to the CP, and for return messages sent from CP to the UP (destined to CPEs).

There can be a L3 network between CP and UPs. Therefore, L3 tunneling is required between CP and UP to carry messages for in-band control plane protocols. "CUPS protocol" MUST support exchange of tunnel identifiers between CP and UP.
Because L2 access setup is in-band, control plane messages will arrive on the UP before any per-session state is learned. Therefore, "CUPS protocol" MUST support messages and information exchange to install forwarding state related to in-band control plane messages that do not match any existing subscriber session. These messages should be forwarded to the CP over a common default control channel.

The in-band control channel setup by "CUPS protocol" MUST have support for UP to pass access-circuit identifier over which the signaling messages are received from the CPEs. Based on type of access, access-circuit identifier can include port/VLAN tags or tunnel identifiers which includes tunnel endpoint IPs and de-multiplexers such as GTP TEID, MPLS labels, L2TP tunnel-id etc. "CUPS protocol" MUST support setting up logically separate control channels for in-band control messages per access-circuit.

In case of fixed-access CPEs with Ethernet based network between access-nodes and BNG, the control messages are received in Ethernet frames. The Ethernet frame carrying the control messages received on UP MUST be carried over the control channel to the CP, as outlined in [CUPS]. In case of fixed-wireless access, control messages (e.g. DHCPv4 and DHCPv6) are received on the UP over GTP-u tunnel from the RAN. The GTP-u tunnel directly carries IP payload. Therefore, control channel setup via "CUPS protocol" MUST support transporting both Ethernet and IP payloads.

"CUPS protocol" MUST provide support for CP to specify the control protocols that should be forwarded by the UP over in-band control channel to the CP.

The "CUPS protocol" SHOULD have support for CP to specify rate-limits for specific control protocols and optionally specific messages within a control protocol, that the UP should enforce.

The "CUPS protocol" SHOULD provide support for CP to direct the UP to drop certain control messages received on a particular access-circuit.
The "CUPS protocol" SHOULD provide support for CP to prioritize reception of certain control messages over others.

2.6. Resiliency

- "CUPS protocol" MUST allow support for both 1:1 (hot standby) and N:M (warm standby) UP node level redundancy.

- "CUPS protocol" MUST provide support for CP to specify the "redundancy domain" that a subscriber session is associated with during session level state creation on the UP. The "redundancy domain" is set of resources that share fate with respect to switchover on failure, e.g. a set of VLANs on a port, or a set of ports on a UP, or entire UP. "CUPS protocol" MUST also provide support for CP to provide relevant parameters to UP about the "redundancy domains". The UPs can then locally preform failure detection and switchover for the redundancy domains.

- The "CUPS protocol" MUST provide support for UP to notify the CP about switchover event. This notification must be on the granularity of "redundancy domain" on a UP.

- For warm standby redundancy, "CUPS protocol" MUST provide support for CP to create session level state on the backup UP node(s) for all subscribers associated with the impacted "redundancy domain".

- "CUPS protocol" MUST support in-service software upgrade (ISSU) on UPs. The protocol MUST provide support for UP to notify CP when it is completed ISSU to the new software release.
2.7. Security

"CUPS protocol" MUST be compatible with proven security mechanisms such as IPSEC or DTLS to satisfy following security requirements:

. Data-integrity and confidentiality MUST be ensured for the information exchanged via "CUPS protocol".
. Protection against man-in-the-middle attacks MUST be provided.
. Anti-replay protection MUST be provided.

3. "CUPS protocol" candidate

3GPP has defined PFCP (Packet Forwarding Control Protocol) in [TS29244] as the interface between CP and UP for LTE gateways. This protocol is suited for large scale state management between CP and UP and can be extended for BNG providing converged access. The protocol provides a good base for satisfying the requirements outlined in this draft for BNG "CUPS protocol". Following are some of the key attributes of this protocol/

. It supports management of forwarding and QoS enforcement state on the UP from CP.
. It also supports usage reporting from UP to CP.
. It is over UDP transport and doesn’t suffer from any HOL blocking.
. It provides reliable operation based on request/response with message sequencing and retransmissions.
. It provides support for graceful handling of overload on UP.
. The protocol is extensible and allows addition of new IEs.
. For fixed access BNG, the protocol requires simple extensions in the form of additional IEs. The required extensions are mainly due to fact that typically a fixed access BNG requires tighter control over L2 behavior and manages access and subscriber using L2 identifiers (such as VLANs and MAC
addresses), whereas mobile access works in terms of L3, either routed or tunneled.

[T529244] also describes an in-band signaling channel based on GTP-u tunnel between CP and UP. GTP-u (GPRS Tunneling protocol User Plane) is defined in 3GPP [T529281] and defines a tunneling protocol which carries IP payloads. The protocol runs over a UDP/IP stack and uses UDP port number 2152. Data within a tunnel can be multiplexed based on Tunnel Endpoint Identifiers (TEIDs). The protocol supports optional sequence numbers. The protocol supports extension headers to allow development of new features. GTP-u tunnels are signaled between CP and UP, and it is possible to associate filters to forward or block certain control packets from UP to CP. The payload type carried by GTP-u can be extended to Ethernet (via payload type in extension header). The tunnel encapsulation can also be extended by introducing an additional NSH (network services header) to carry any required meta-data.

4. Security Considerations

For security between CP and UP, Network Domain Security (NDS) as defined in [T533210] can be considered. As per NDS, the network can be split into security domains. Communication within a single security domain is considered secure, and protocols can operate without any additional security. When communication has to cross security domains, then IPSEC can be used.

5. Management Interface Requirements

. The CP MUST provide a single point for management of "CUPS BNG" system to the operator.

. Management interface for the CUPS system MUST provide support for both configuration of UPs, and state retrieval. The interface MUST minimally support BNG specific configuration and state.

. Management interface SHOULD support transactional configuration from CP to UPs, based on a well-defined data schema. Transactional configuration may be achieved by editing a candidate configuration on the UP which is subsequently activated (commit) or by providing the whole transaction in a
single command. In case UP data-stores are used, it MUST be possible for the CP to lock a data-store for exclusive access.

The management interface SHOULD support transaction confirmation, where an unconfirmed transaction gets reverted automatically after a timeout even if the transaction succeeded. This is to avoid configuration errors where a valid configuration breaks communication between UP and CP, requiring on-site intervention.

The management interface SHOULD support state retrieval based on a well-defined data schema. This includes retrieval for any state that is not signaled via the state control interface.

The management interface SHOULD support unsolicited signaling of state changes (events) from UP to CP i.e. SHOULD provide telemetry for events. Even while state changes are sent unsolicited, the CP SHOULD be able to subscribe to a specific subset of state it is interested in.

The management interface MUST provide security through an existing mechanism such as (D)TLS or IPSEC to guarantee confidentiality and authenticity and protect against replay and man in the middle attacks.

6. IANA Considerations

None.

7. References

7.1. Normative References


7.2. Informative References


Authors' Addresses

Sanjay Wadhwa
Nokia
777 East Middlefield Road
Mountain View
USA

Email: Sanjay.wadhwa@nokia.com
Subrat Pani  
Juniper Networks  
10 Technology Park Dr.  
Westford, MA  
USA  

Email: spani@juniper.net