Requirements for BNG Control-plane And User-plane Separation
draft-cups-rtgwg-cu-separation-requirement-00

Abstract

This document aims to abstract requirement of an extensible and flexible Control Plane (CP) and User Plane (UP) Separated BNG Architecture.

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 September 9, 2019.

Copyright Notice

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 (https://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.
Table of Contents

1. Introduction ...................................................... 2
2. Specification of Requirements ................................. 2
3. CU Seperation Basic Model ................................. 3
4. Protocol Independent Relay (PIR) ......................... 3
5. Generic-Service Flow Protocol (GSF) .................... 4
6. Management Interface ................................. 8
7. Resiliency .......................................................... 9
8. Security Considerations ..................................... 10
9. IANA Considerations ......................................... 10
10. Normative References ........................................ 10
Author’s Address ................................................. 11

1. Introduction

The architecture aims to decouple CP and UP.

CP focus on protocol signaling processing, service info management, and communication with external servers (e.g. Radius, DHCP servers).

Up focus on packet forwarding based on forwarding instructions from CP.

CUPS architecture brings significant benefits below:

- Simplified management: UP is simplified focus on forwarding behavior. Interactions with service platforms are decoupled to CP.
- Higher Resiliency: CPUS architecture allows CP inter-site resiliency and UP multi-homing active-active resiliency.
- Fast service provisioning: with a highly abstracted service based interface between CP and UP, CUPS architecture allows fast innovation on CP with minimum changes on UP.
- Higher IP address utilization: As IP address management centralized into CP, CP can have the intelligence to optimize the best subnet allocated to UP.

2. Specification of Requirements

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.
3. CU Separation Basic Model

To support communication between the Control Plane and User Plane, several interfaces are involved. Figure 1 illustrates the three communication interfaces between CP and UP BNG.

```
+----------------------------------+
|                                  |
|               BNG-CP              |
|                                  |
|              +-- 1.PIR           |
|              |                 2.GSF |
|              |            3.Magment |
|              +--                  |
+----------------------------------+

Figure 1: Interfaces between the BNG-CP and the BNG-UP
```

4. Protocol Independent Relay (PIR)

To achieve a dis-aggregated system, a protocol independent Relay channel is required. PIP allows BNG to relay signaling protocols to the remote CP instead of processing and maintain status locally.

- PIR MUST be protocol independent. It means it has the capability to rely on protocols without extra customization. It can be a Relay channel for any protocols that requires participations of CP, e.g. PPP, DHCP, ICMP (with options).
- PIR MUST be reliable, in case of packet loss, retransmission applies. PIR SHOULD be TCP based.
- PIR MUST provide a secure connectivity between BNG and remote CP. PIR MUST provide authentication mechanism between UP and remote CP. PIR MAY provide encryption between UP and remote CP, e.g. IPSEC.
- PIR MUST provide a keepalive/heartbeat mechanism allowing detecting the availability between UP and remote CP.
- A UP MUST have the capability to identify protocol packets and relay via PIR.
A UP MUST have the capability to relay part of the protocols to remove server. For example relay DHCP to remote CP but IGMP and PIM remain locally.

PIR MAY be applied in any service access point: vlan-sub interface, PW, GRE, L2TP tunnel, etc.

5. Generic-Service Flow Protocol (GSF)

GSF protocol is the interface for CP to deliver service based forwarding entries. Also UP will use this interface to notify whether the forwarding entries successfully delivered.

GSF SHOULD be highly flexible and extendable considering the variety, complexity of BNG services and possibility of the future service. To achieve this, a "generic-service" is abstracted with requirement below:

GSF is designed to be service oriented instead of instruction oriented. GSF defines service module precisely and UP adopts the service to the pipeline itself.

A generic-service MUST have ONE identifier (GSI). The identifier CAN be:

* GSI1: intf + sMAC + sIP (normal way of identifying a subscriber)
* GSI2: sMAC + sIP + dIP + dIP (subscriber traffic toward a particular platform)
* GSI3: dIP with mask (identifying ip pool prefix)
* GSI4: sIP with mask (identifying a NAT ip pool input from subscriber private side to internet public)
* GSI5: dIP with mask (identifying a NAT ip pool input from internet public side to subscriber private)
* GSI6: dIP with mask + dPort with mask (identifying an ACL criteria matching traffic toward specific IP+ port range)
* GSI7: intf + VLAN(s) + PPPOE session ID + sMAC + sIP (identifying an PPPOE session over VLAN(s))
* GSI8: intf + sMAC + sIPV6 prefix (identifying a V6 subscriber)

GSI SHOULD have the capability of using L2+L3+L4 with mask info to identify a GS, GSI MAY use L5-L7 information to identify a GS.
A generic-service MUST have at least one and MAY have more than one forwarding behavior (GSB). The behavior CAN be:

* **NSB1**: Route recursive. Basic FIB search and forward. An example of this GSB is: direct traffic of a subscriber to a MPLS based core network.

* **GSB2**: A specific GSI. The usage of this behavior includes but not limited:
  
  + **Service bounding within UP**: The behavior of GSI2 is GSI1, which means GSI2 is a sub-service of GSI1. This allows UP process per flow based service + per subscriber based service.
  
  + **Service channing within UP**: The behavior of GSI1 is GSI4, which means NAT need to be done after finishing processing subscriber service.

* **GSB3**: Search a forwarding entry in a specific GSI table. One usage of this behavior is to direct traffic from internet to subscriber side. After processing GSI3, the behavior is to search the right user table in GSI1 table to obtain following user/flow based forwarding entries.

* **GSB4**: Policy based routing, this allows UP to recursive traffic into RSVP-TE LSP, SR-TE LSP (color based also).

* **GSB5**: Service channing, this allows UP to redirect (part of) traffic of subscribers towards remote service platforms (e.g. external NAT platform, cleaning center, DPI).

A generic-service MUST have at least one and MAY have more than one service attribute (GSA). The attribute CAN be:

* **Service type**: specify the GS is subscriber, FIB entry for pool, NAT instance, etc. This attribute is mandatory.

* **Subscriber ID**: this attribute is used to group GSs belong to same subscriber, e.g. V4+V6, flow based(GSI2)+subscriber based(GSI1), fixed + wireless (hybrid-access)

* **QoS related attribute, e.g.**:
  
  + forwarding priority(best effort, Assured Forwarding, WRED info, etc.)
  
  + policing/shaping speed (CIR, PIR)
* Credit/Volumne control.
* Subnets for network behind a CPE (framed-routes)
* Service alive validation method (e.g. ARP detect for IPOE)
* Whether able to be subscribed via OAM channel for traffic counters. This is an enable switch for usage-report.
* Inheritance of the attribute: This is used in case of service bounding or channing. This attribute CAN be: independent, inherit, overwrite.

Below diagrams give some examples of using GS to compose BNG service flows:

```
GSA                               GSB
------------------               ------------------
|GSI2                  |GSI3               |
------------------               ------------------
|GSB1                  |GSB3               |
------------------               ------------------
|GSA:                  |GSA:               |
|type=subs             |type=pool          |
|S-ID=1                |                    |
------------------               ------------------
```

```
GSA’                               
------------------               
|GSI1’                  |               |
------------------               ------------------
|GSB1                  |               |
------------------               ------------------
|GSA:                  |               |
|type=subs             |               |
|S-ID=2                |               |
------------------               ------------------
```

Subs GS table                               IP Pool GS table

Figure 2: Basic BNG Service Flow

Figure 2 shows how to use GS to form basic service flow for IPOE subscribers.

Traffic user->network: Search "Subs GS table" based on sMAC and sIP, traffic match GSA entry and get forwarding behavior is normal route
recursive. UP will forward traffic based on FIB entries of dIP of the packet, which are learned from internet core.

Traffic network->user: Search FIB entries based on dIP will match the IP pool GS table, which is a sub-set of FIB table. The forwarding behavior (GSB3) is to search Subs GS table. UP will search Subs GS table and get the match entry, forward traffic to the interface and vlans of the corresponding subscriber.

User->Network:

<table>
<thead>
<tr>
<th>GS1 Table</th>
<th>GS2 Table</th>
<th>GS3 Table</th>
<th>GS4 Table</th>
</tr>
</thead>
</table>

Figure 3: BNG service flow with service channing

GS1 table is services of subscribers table, the format example of service in GS1 is as below:

----------------------
GS1-1
GSI1-1: dIP = 50.0.0.2, dPort = 520
GSB1-1: GSI2-1 and SR-policy with color = gold
GSA1-1: service-type: service of subscriber
subscriber id = any
qos type: ef (inherit)
qos speed: cir = 128k (independent)
----------------------

GS1-2
GSI1-2: match any
GSB1-2: GSI2-1
GSA1-2: service-type: service of subscriber
subscriber id = any
qs speed: no limit (inherit)

GS2 table is subscriber table, the format example is as below:

GS2-1

GSI2-1: intf = 1/0/2, VLAN = 10, sMAC = 00-20-56-C0-00-0B, sIP = 10.123.0.23

GSB2-1: GSI3-1

GSA2-1: service-type: subscriber

subscriber id = 1000
qs type: be
qs speed: CIR = 10M, PIR = 20M (independent)

GS3 table is CGN NAT table, the format example is as below:

GS3-1

GSI3-1: sIP = 130.123.0.0/24

GSB3-1: Route recursive

GSA3-1: service-type: CGN NAT

The service flow above defines a subscriber with 2 services (VoIP and Internet), with subscriber based QOS (CIR = 10M, PIR = 20M) and service based QOS (VoIP, ef, cir = 128k), VoIP services goes into a gold SR-policy and internet traffic does best effort forwarding with CGN NAT translation.

6. Management Interface

For CUPS architecture, the CP MUST provide a single point for management of entire "CUPS" BNG.
Management interface for the CUPS system MUST provide support for both configuration of UPs, and state retrieval.

Management interface is used to report status, statistics, events from UP to CP. And also CP can use interface to query status of UP. This interface uses NETCONF protocol.

Netconf working group has already (or almost) standardized couple of mechanism can be used in CPUS architecture:

[I-D.ietf-netconf-subscribed-notifications] provides the mechanism of notifying any status changes of subscribers, resource utilisation etc..

[I-D.ietf-netconf-yang-push] provides the mechanism of a continuous, customized stream of updates from a YANG datastore.

UP Should have YANG datastores and subscribed by CP below:

- GS status datastore: maintain session status, in case of status change of GS, notification will be sent to CP. For example:
  - Subscriber status changes, due to failure of heartbeat detection, redial of a subscriber, change of stack statue (V4, V6), change of hybrid-access bundling status.
  - NAT session table aged out.
  - Packet loss of particular policer

- GS status datastore: maintain traffic statistics where applicable. For example:
  - Traffic counter of VoIP service.
  - Traffic counter of NAT table.

[RFC5539] provides security mechanism for management interface.

7. Resiliency

- CP MUST provide resiliency mechanism, it MAY be intra-site or inter-site resiliency.

- UP SHOULD NOT synchronise subscriber forwarding entries across each other to achieve resiliency.

- UP SHOULD provide multi-homed connection for BNG access links.
o UP SHOULD provide single-active resiliency

o CPUS SHOULD provide hot and warm resiliency mechanism. Hot resiliency means forwarding entries are pre-installed on both active and backup, where warm not pre-installed, re-installation applies in case of UP failure.

o CUPS MAY provide a mix of hot and warm resiliency. E.g. BNG-A is master, BNG-B is hot backup, BNG-C is warm-backup, in case of a failure of BNG-C, uplift BNG-C to hot-backup.

o UP SHOULD provide active-active resiliency

o UP SHOULD support designated forwarder mechanisms which allows a subscriber based load balancing across UP.

8. Security Considerations

TBD

9. IANA Considerations

TBD

10. Normative References

[I-D.ietf-netconf-subscribed-notifications]

[I-D.ietf-netconf-yang-push]


Author's Address

Tianpeng Yu

EMail: yutianpeng.ietf@gmail.com