service function chain
Internet-Draft
Intended status: Standards Track
Expires: April 9, 2016

C. Xie
China Telecom
W. Meng
C. Wang
ZTE Corporation
B. Khasnabish
ZTE TX, Inc.

October 7, 2015

# service function chain Use Cases in Broadband
# draft-meng-sfc-broadband-usecases-04

## Abstract

This document discusses about service function chain use cases in different scenarios of broadband network. The document provides analysis of different solutions and also describes the suitable scenarios that each solution may be deployed in.

## 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/.

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 9, 2016.

Table of Contents

## 1. Introduction

The object of SFC is trying to unload services from legacy devices in traditional network and deal with such services through corresponding service functions which are topologically independent from physical devices.

As increasingly large number of customers, the possibility of deployment SFC in broadband network seems emergency. And this document aims to illustrate the possibly typical and unified service function chains in Broadband Networks and analyze the possible deployments of diverse service function chains in broadband network.

In figure 1, here outlines the possible SFC deployment architecture in Broadband Networks. This architecture tries to simplify and unify the services in CPEs and unloads the services from CPEs to the SFCs in Access Networks to achieve virtual CPE functions. And as well, extracts the services in BNASs and offloads the services from BNASs to the SFCs in Barrier Networks to accomplish virtual BNAS functions. As a result of that, the Internet Service Provider can manage and maintain the whole Broadband Networks more flexibly.

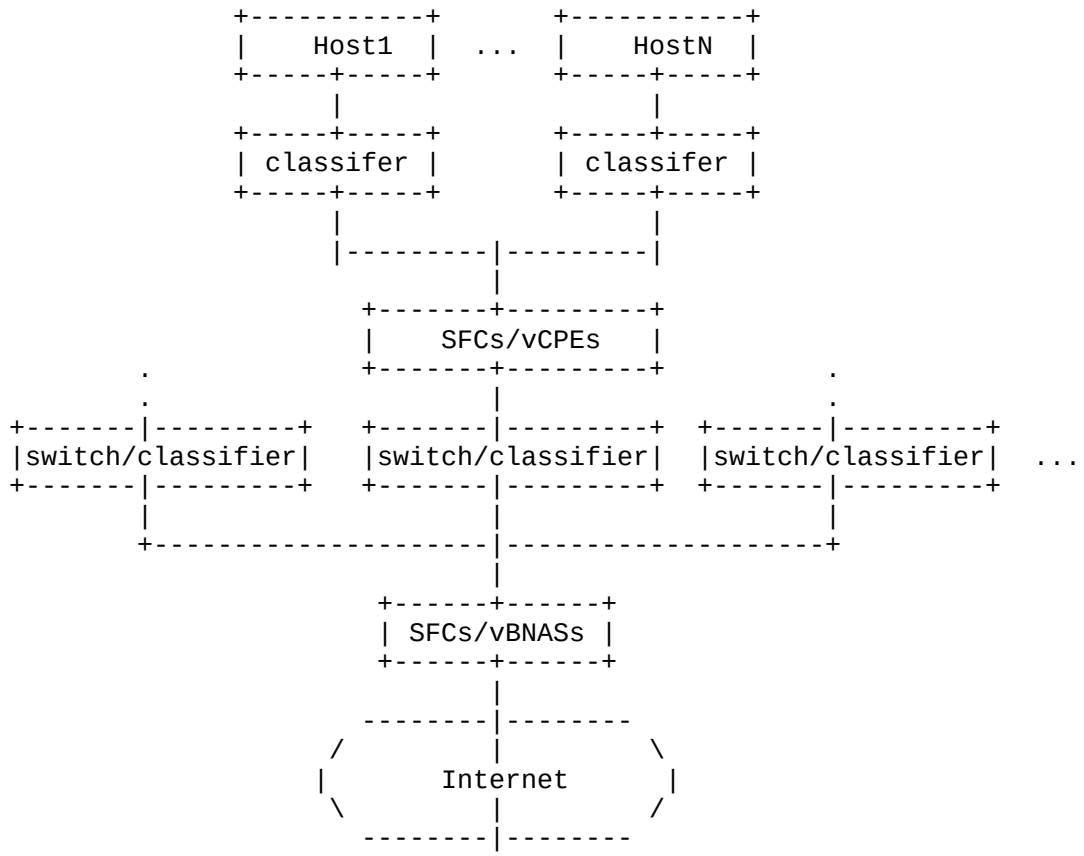


Figure 1: SFC Architecture of Broadband Network

## 2. Convention and Terminology

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 [RFC2119].

The terms about SFC are defined in [I-D.ietf-sfc-problem-statement].

The terms about CGN/DS-Lite/Lightweight 4o6/MAP/NAT64 are defined in [RFC6888]/[RFC6333]/ [I-D.ietf-softwire-lw4over6]/ [I-D.ietf-softwire-map]/ [RFC6146].

## 3. Use cases

The following sections highlight some of the most common broadband network use case scenarios and are in no way exhaustive.

### 3.1. Internet Access from Homes

Figure 2 illustrates an abstract architecture of broadband network, including CPE sitting in home access network, BNAS as broadband access network gateway,CR located in bone network and the Internet.

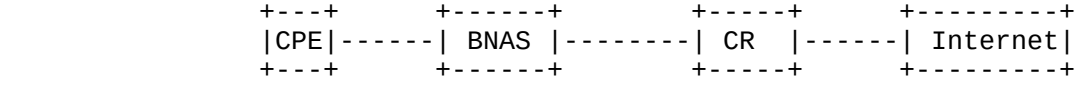


Figure 2: Architecture of Broadband Network

Also, the Broadband Forum(BBF) is developing a study document(SD-326), which aims to study market requirements and usecases for Flexible Service Chaining. Except that, this document tries to develop more typical usecases in Broadband Networks.

#### 3.1.1. Native IPv4 Network or Native IPv6 Network

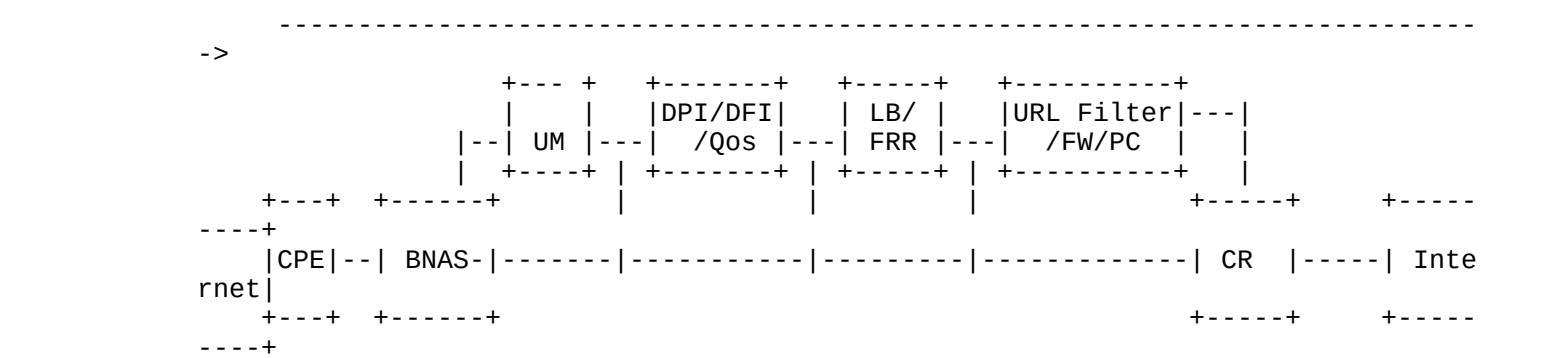


Figure 3: Native IPv4 Network or Native IPv6 Network

Figure 3 shows possible deployment of SFC in native IPv4 network or native IPv6 network. As UM(users management) service, which is the main service of BNAS device in traditional network, consumes large memory and resources, it seems reasonable to decouple UM service from legacy BNAS device and treat it as a service node , which may include DHCP,AAA functions and some other functions related to users management. And what!_s more, only users subscription messages (protocol messages) go through UM service. Once a user is approved by UM service, the following data flow of this user go through the other service function chain which is assigned to this data flow.

'BNAS-' means some functions have been unburdened from traditional BNAS,such as user management,Qos,Load Balance and so forth.

Given that SFC is applied in Broadband network, the main SFs may cover: User Management, DPI, DFI, Qos, Load Balance, Fast Reroute, URL Filter,Firewall,Parental Control and so forth. And the possible order is not as strict as above. The upstream/downstream traffic may go through different permutations and combination of these SNs. For example:

SFC1: UM

This SFC stands for the process of subsribers!_ log-in and log-out. All the broadband subscribers!_ log-in messages and log-out messages need go through this SFC. After approved by this SFC, then the users flow can access the Internet or other services.

SFC2: Qos

This SFC shows some bandwidth restrictions or several priority-based schedules are applied to this approved subscriber. Almost each home subscriber has a corresponding subscribed bandwidth, different services from a home have distinctive priority as well. As a result, this is a basic SFC used in internet access from homes.

SFC3: Qos--LB

This SFC extends SFC2, which utilizes load balance to offload approved subscribers!_ flow from an overload path. This is also a typical scenario in broadband network, especially in metropolitan area network.

SFC4: Qos--LB--URL Filter

Based on SFC3, this SFC gives extra restrictions to the content that the approved subscriber wants to access.

SFC5: Qos--Parental Control

This is similar to SFC4,except there is no Load Balance. Another difference is that SFC5 offers some restrictions to downstream traffic in terms of content. SFC5 allows some legal or appropriate contents to flow to subscribers, while some illegal or inappropriate contents are blocking.

### 3.1.2. IPv4/IPv6 Coexist Network

As showed below in figure 4, the main difference between IPv4/IPv6 native network and IPv4/IPv6 coexist network is whether there exists a NAT funtion. Although in IPv4 native network, there maybe exist NAT44 function as a result of limited IPv4 address, we try to put

this scenario together with other IPv6 transition scenarioes in this section and discuss them in detail.

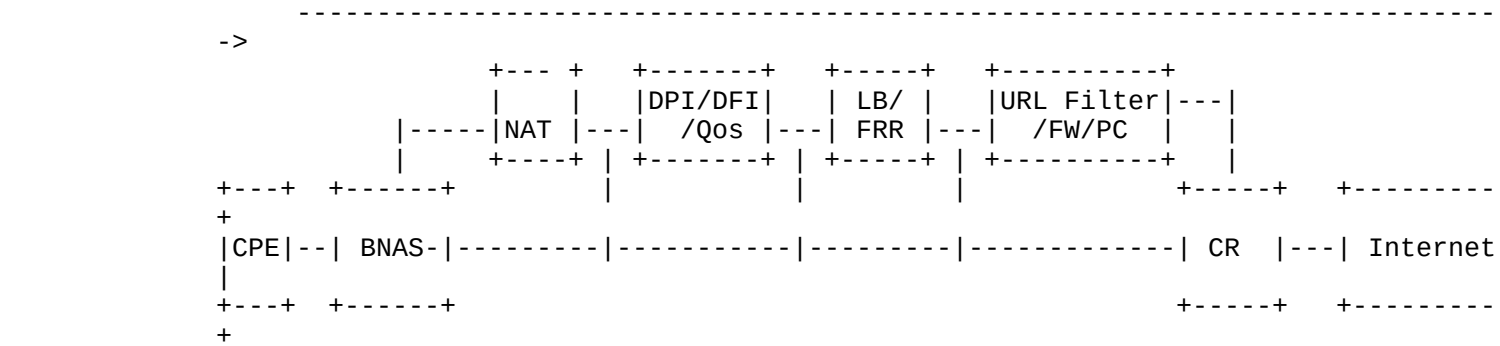


Figure 4: IPv4/IPv6 Coexist Network

Whether NAT stands for NAT44 or NAT64 or NAT46 depends on the the Internet Server Provider. It may be NAT44, which reflects the communication between IPv4 private customer and IPv4 public server. Or it may be NAT64, which means the communication between IPv6 customer and IPv4 Server. And where NAT is deployed is the preferance of the Internet Server Provider as well. It may be besides BNAS,which stands for distributed deployment, or besides CR,which represents central deployment.

Above figure 4 just gives a simple example of a possible deployment position in distributed deployment scenario. Actually, there are some other complicated IPv6 transition scenarioes . And this section tries to give some typical examples in IPv4/IPv6 coexist network, and conclude a feasible SFC architecture in IPv4/IPv6 coexist network. Also, in the following sections, the other SFs emphasized in section 3.1.1 are not highlighted, just try to keep the diagram simple and suitable for the draft’s specification.

#### 3.1.2.1. NAT44

Figure 5 illustrates a simple NAT44 scenario how SF-NAT is deployed and how SF-NAT may work.

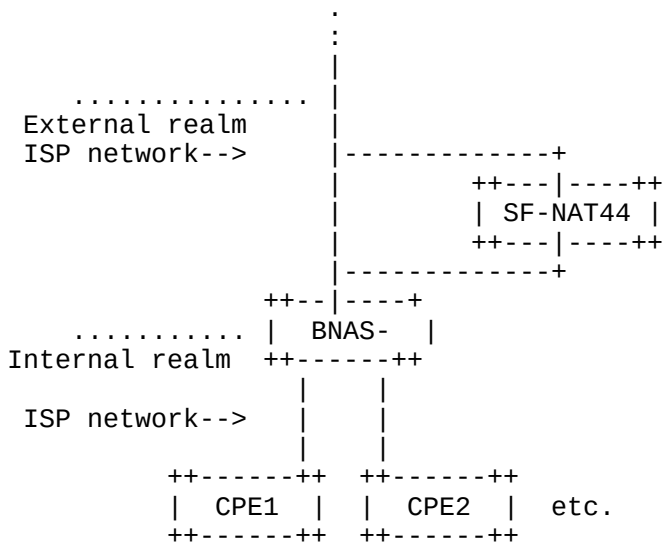


Figure 5: NAT44

In distributed broadband networks, SNs may be deployed beside BNAS. These SNs may contain or logically connect to SF-NAT and other service functions such as UM,QOS,Load Balance,etc.

Here gives an example of possible SFC in IPv4/IPv6 coexist network, which combines NAT function with the service functions in native IPv4/IPv6 network.

SFC6: Qos--NAT--LB--URL Filter

SFC6 combines NAT function with SFC4, and represents the classical scenario in IPv4/IPv6 coexist network. After customers have subscribed, apply subscriber-based Qos policy, then transform IPv4/ IPv6 address into IPv4 address, and do five-tuple load balance for the outbound traffic.

At last, monitor the outbound traffic and decide whether to permit them to the internet or block them.

After the first packet of an outbound flow has been processed by this SFC, this SFC can do SFP optimization to bypass NAT service function to improve the experience of this subscriber. Then, for the following packets of this outbound flow, the SFF connects to NAT service function can forward them according to the forwarding table which is derived from the NAT service function.

As for the inbound flow of this subscriber, there exists an open issue: how the inbound flow is steered to the same NAT service function or the same SFF which connects to the same NAT service function.

#### 3.1.2.2. DS-Lite

Figure 6 describes a scenario of DS-lite, which completes IPv4 communication between IPv4 private customer and IPv4 server across IPv6 network through tunnels. And the main principle of DS-Lite is to encapsulate IPv4 packets in IPv6 Header and forward this IPv4-in-IPv6 packets to CGN device and enforce NAT function in CGN device. Generally, CGN device resides in BNAS device.

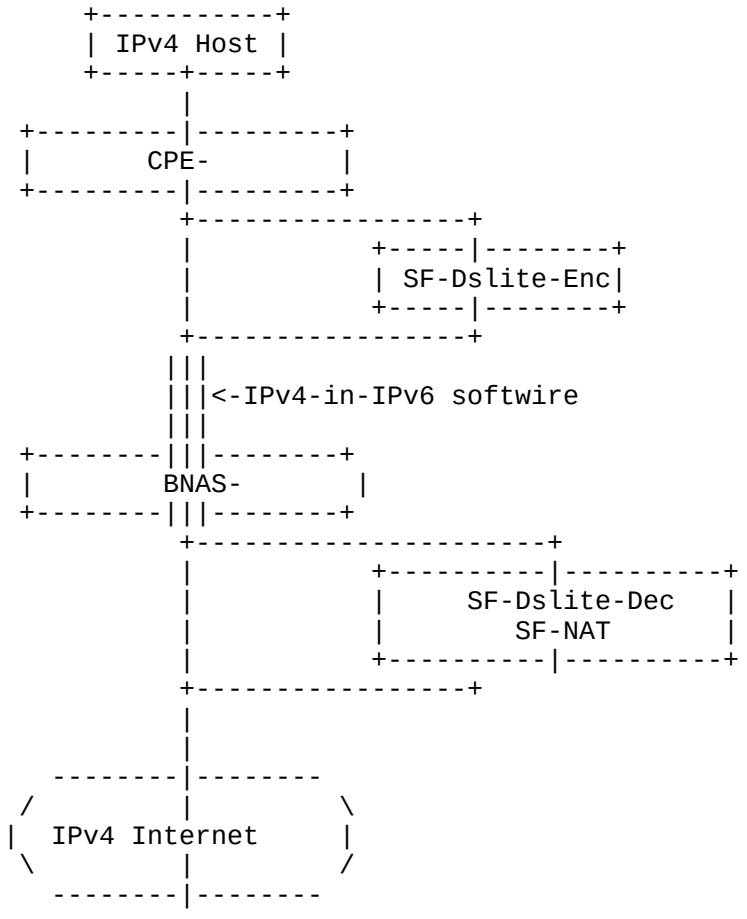


Figure 6: DS-Lite

SFC7: Dslite-Enc---Dslite-Dec---NAT---LB---URL Filter

When the outbound flow are received by the CPE, the CPE sends them to a specific classifier which determines the flow should be forwarded directly or dealed with DS-Lite process. if the flow should be dealed with DS-Lite process, then the classifier sends the datagram within service header encapsulation to Softwire-SN which contains SF-Dslite-Encapsulation instance. In this instance, it fulfils DS-Lite encapsulate and then encapsulates overlay header and forwards this flow to nexthop in the traditional network.

Next, the BNAS- receives the processed flow, the BNAS- sends them to a classifier and finds they are legal flow and need to be dealed with DS-Lite process. then, this flow are forwarded to SF-Dslite-Decapsulation to decapsulate DS-Lite encapsulation. And as well, forwarded to SF-NAT to create and maintain the NAT mapping table for DS-Lite subscriber. SF-Dslite-decapsulation and SF-NAT can reside in one service function or two different service functions. After that, completes the subsequent SFs.

In other words, BNAS-,itself, would decouple DS-lite-related functions to specific service function(s). What!_s more, if SFP optimization function is enabled, BNAS- acts as SFF which connectes to SF-NAT, and derives the NAT/forwarding table from SF-NAT and bypasses SF-NAT to improve the experience of this subscriber.

If deploy SFC7 in this scenario, there also exists a consideration: how to address the relationship between the access side SFC domain and the network side SFC domain. If they are deployed in two different SFC domain, how to cooperate between the SF-Dslite-Encapsulation service function and SF-Dslite-Decapsulation service function. On the other hand, if they are deployed in one big SFC domain, it seems more feasible to carry out this SFC7.

## 3.2. Internet Access from Enterprises

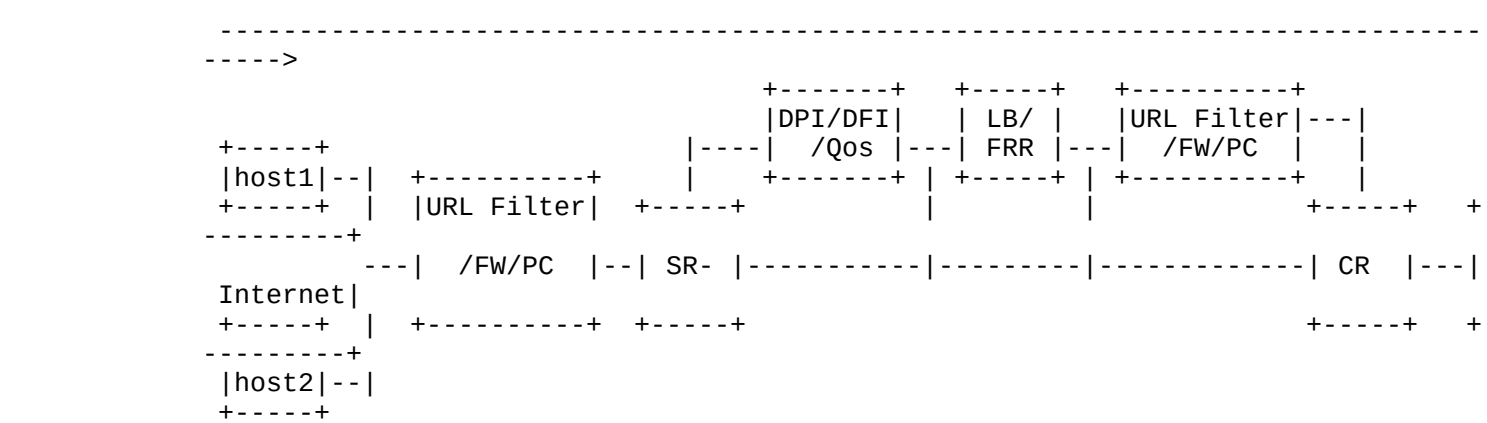


Figure 7: Internet access from enterprises

Internet access from enterprises is another network service. They lease some ports or even some devices from Internet Server Providers. In addition to internal s service functions which are situated in the internal enterprise network, there maybe deploy many external ISP!_s service functions which are sitted on the way to the internet. -.And what!_s more, there maybe deploy IPsec along with VPN users for the sake of the security of enterprise network.

Internal service functions may include: Firewall, NAT function, etc.

As for external service functions deployed by ISP, typical service functions are VPN, like L2VPN,L3VPN,IPsec,IPsec VPN etc. Conventionally, there is a NAT function residing on SR, converting VPN traffic to public traffic to access the internet.

In some cases, service providers need to assign differentiated services to VPN users. In other words, different VPN users may go through differentiated SFC. But, VPN traffic are all encapsulated in outer MPLS header or some other transport headers, how the public network elements classify them to different SFCs? At this time, there maybe need create a mapping between VPN ID/VPN Name and corresponding SFC on the service provider edge device.

Other external service functions involved in Internet access from enterprise network maybe similar to home network, for example, DPI,DFI,Qos,Load Balance, URL Filter,Firewall,Parental Control and so on.

SFC8: URL Filter--FW---NAT---Qos---Load Balance----FW

Here, you may see two FW functions. One is in the inner of enterprise, which represents the URL constrains from the perspective of enterprise. While the other one is sitted in the ISP network, out of the inner enterprise, and stands for the URL restrictions from the standpoint of ISP.

## 3.3. Internet Access from Campuses

TBD

## 3.4. Added-value Service Access

To promote their primary service, ISP try to provide value-added services to add value to the standard service offering. Here maybe focus on some significant value-added services in broadband network such as IPTV,VOIP,etc.

### 3.4.1. Destination Address Accounting(DAA)

Figure 8 illustrates a possible deployment of DAA funtion in broadband network.

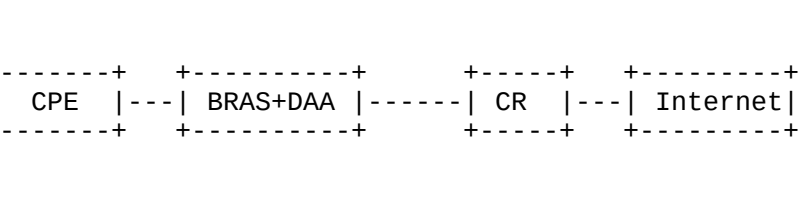


Figure 8: DAA Deployment in broadband network

In this diagram, DAA assists BRAS to accomplish finer-granularity outbound filter or/and inbound filter based on destination IP address. But,in central deployment scenario of DS-Lite, there is a IPv4-in-IPv6 tunnel from CPE to CR. As a result of that, BRAS cannot identify the true IPv4 destination address in this IPv4-in-IPv6 packets. And then, BRAS cannot enforce DAA function to manage the subscriber more flexibly.

SFC9: DAA----Dslite-Enc----Dslite-Dec----NAT

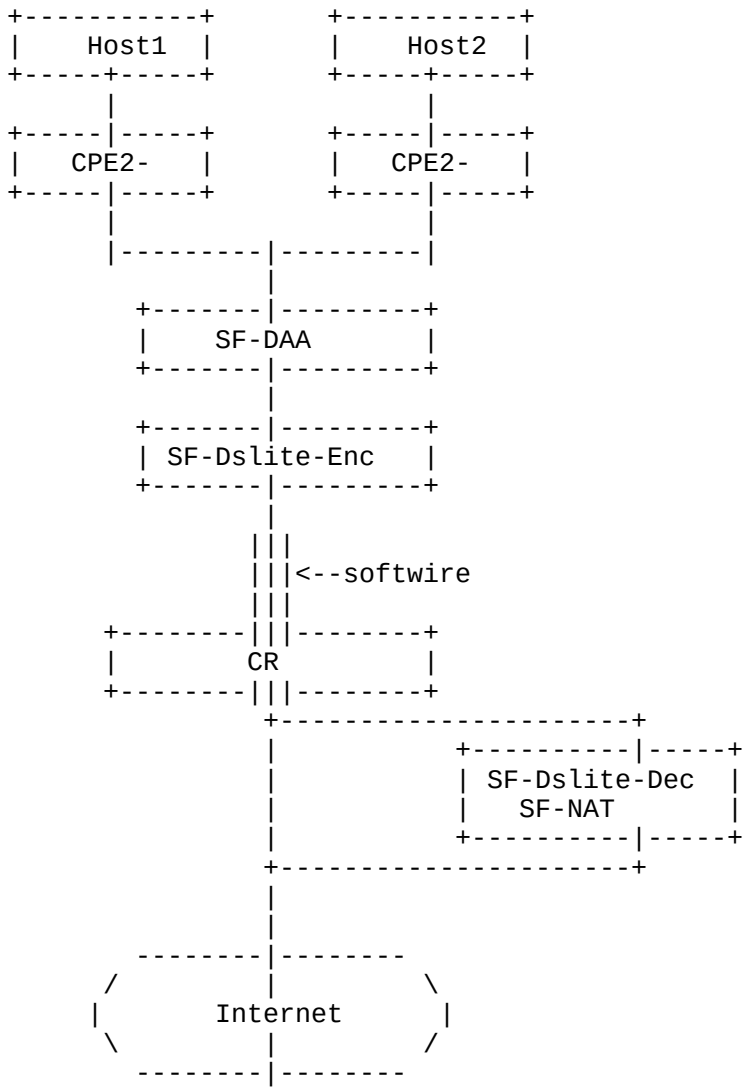


Figure 9: DAA + Softwire Deployment in broadband network

### 3.4.2. IPTV

Figure 10 illustrates a possible deployment of IPTV network via SFC.

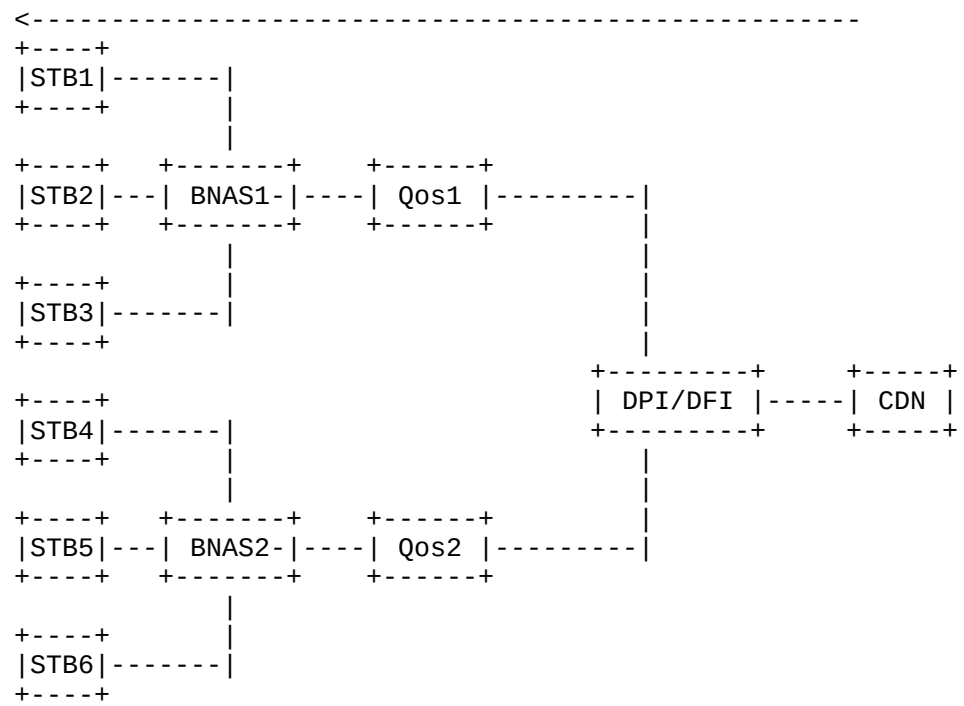


Figure 10: IPTV network via SFC

IPTV is a IP multicast service, in which multi-subscribers should receive the same traffic from the multicast source like Content Distribution Network. Supposed there are six IPTV subscribers, from STB1 to STB6, they are located in different districts and they all need to receive traffic from Program 1. A possible SFC abstract here is :

SFC10: DPI--Qos1

|---Qos2

In SFC10, as for the inbound traffic, there are two different outputs, Qos1 and Qos2. Firstly, traffic from multicast source go through DPI, which used for detecting whether the multicast traffic are legal or unmalicious. After that, legal traffic propagate to different Qos, and next, each goes through different BNAS- to different STB subscirbers separately.

### 3.4.3. VoIP/MoIP

TBD

# 4. Considerations

## 4.1. Service Function Chain Symmetry

A complete end-to-end access in broadband network should consist of a set of service function instances in a specific order. Such as:

## 4.2. Deploying consideration

### 4.2.1. Standalone mode

In broadband networks, service function components are hanging next to routers such as CPEs/BNASs/CRs. All traffics would be received and steered by routers. Routers send the traffic to classifier in which traffic that matches classification criteria is forwarded along a given SFP to realize the specifications of an SFC.

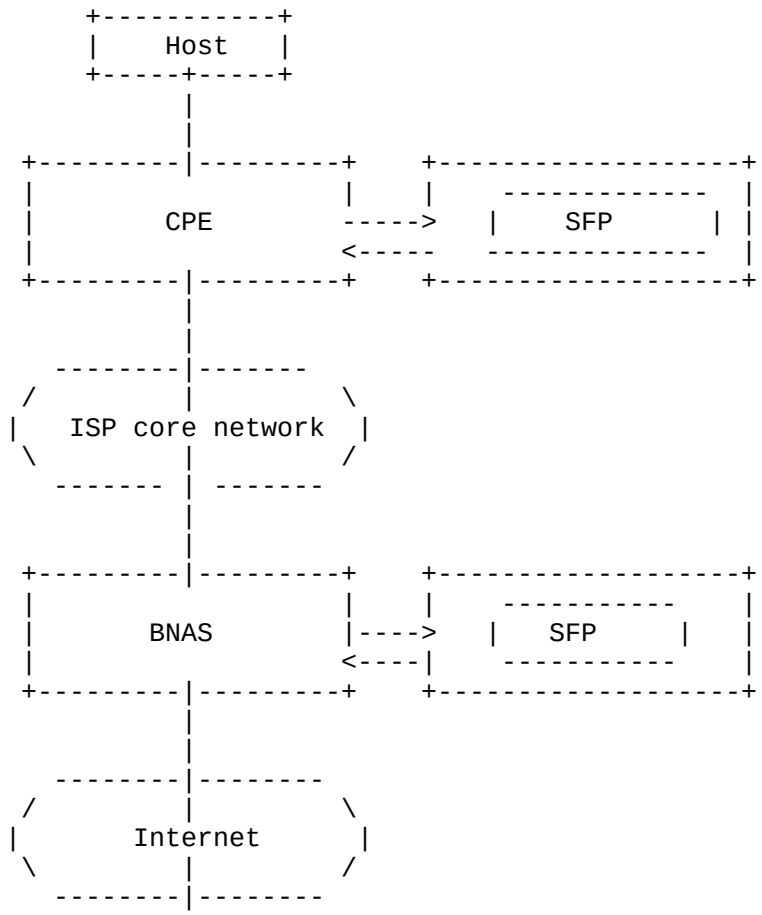


Figure 11: Standalone mode

Take DS-Lite CGN for example.

Outbound traffic:

In the example shown in Figure X, a datagram received by the CPE from the host at address 10.0.0.1, using TCP DST port 10000, will be translated to a datagram with IPv4 SRC address 192.0.2.1 and TCP SRC port 5000 in the Internet.

When the datagram 1 is received by the CPE, the CPE sent it to a specific classifier which determines the datagram should be forwarded directly or dealed with DS-Lite process. Then the classifier sends the datagram within service header encapsulated to the first element

of SFP. SF-SOFTWIRE encapsulates the datagram in another datagram (datagram 2) and forwards it BACK to CPE over the softwire. The datagram 2 would be sent to the Dual-Stack Lite carrier-grade NAT by CPE.

When the BNAS receives datagram 2, the BNAS sends it to a classifier and find it need to be dealed with DS-Lite process. Then the classifier send the datagram within service header encapsulated to the first element of SFP.

SF-SOFTWIRE decapsulates the datagram 2 to datagram 1 and forwards it SF-NAT, which determines from its NAT table that the datagram received on the softwire with TCP SRC port 10000 should be translated to datagram 3 with IPv4 SRC address 192.0.2.1 and TCP SRC port 5000.

The translated datagram would be also sent back to BNAS for next forwarding.

Inbound traffic:

Figure x shows an inbound message received at the classifer. When the BNAS receives datagram 1, the BNAS sends it to a classifier. Then the classifier sends the datagram within service header encapsulated to the first element of SFP. SF- NAT looks up the IP/ TCP DST information in its translation table. In the example in Figure 3, the NAT changes the TCP DST port to 10000, sets the IP DST address to 10.0.0.1, and it will be sent back to BNAS to forwards the datagram to the softwire. The SF-SOFTWIRE of the CPE decapsulates the IPv4 datagram inbound softwire datagram and forwards it to the host.

#### 4.2.2. Directly connecting mode

There is another mode to deploy service function components. In broadband home networks, service function components are directly connected to the network. They are connected straight to a BNAS or Routers.

Under this scenario, it seems like more costly than standalone mode during transition period.

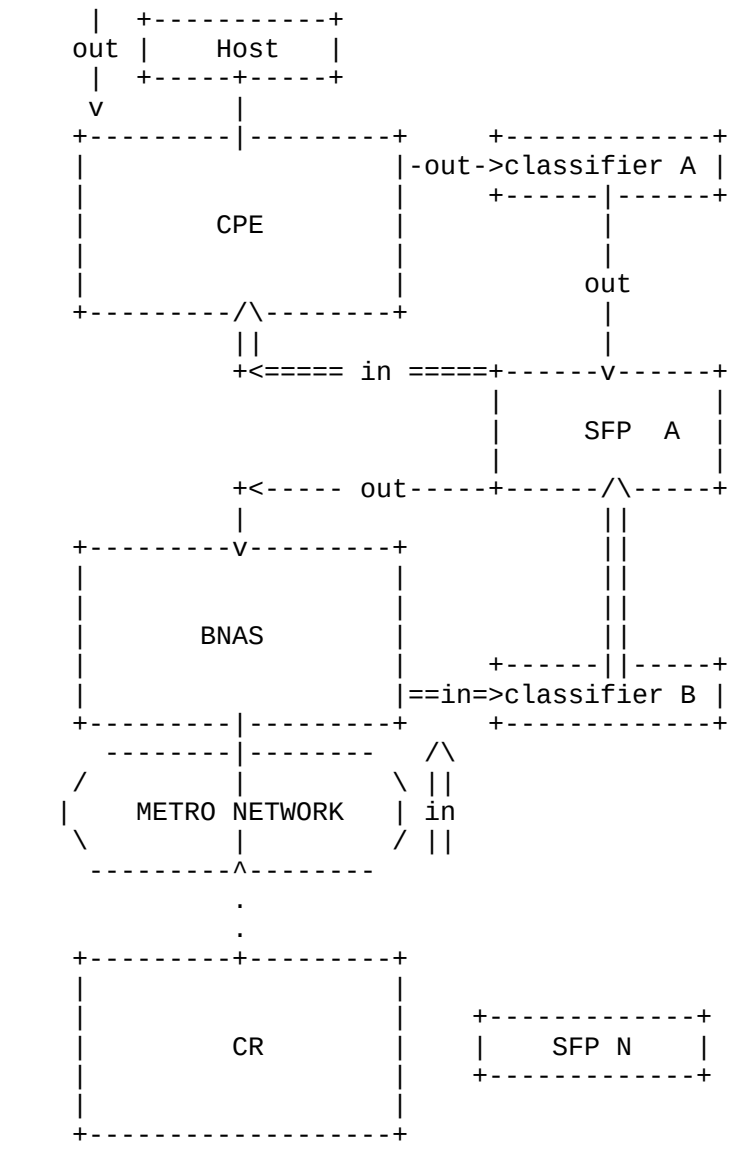


Figure 12: Directly connecting mode

Take NAT44 for example.

Outbound traffic:

For directly connecting mode, the difference in dealing with traffic

is whether the network steer the traffic loopback. That means service function node could send datagrams directly to the next hop.

For example, when the outbound datagram is received by the BNAS and processed by classifer A and SF-NAT which forward the processed datagram straight next to router.

Inbound traffic:

It is quite similar with the process of dealing with outbound traffic. when the inbound datagram is received by the router and processed by classifer B and SF-NAT which forward the processed datagram straight next to NAT BNAS.

### 4.3. Pool consideration

In traditional networks, pools are configured in router one by one. Pool configuration means these IP addresses in each pool MUST be advertised for creating forward routing path to ensures that the message is routed to the correct target, especially to inbound traffic. Thus, pool location is a problem we must face to in SFC framework.

In standalone mode shown in figure 6, pool could be configured in the classifier beside gateway and advertised by the gateway itself. The classifier would assign IP addresses to service functions for creating mapping table. Both-bound traffic should be forward to gateway first and then for NAT treatment in relative service function components.

In Directly connecting mode shown in figure 7, pool could be configured in classifier B and advertised by classifier B for creating inbound routing path.

There is a mechanism to manage the address pools centrally. Pools could be assigned to classifiers by management server which is handled by Operators centrally.

### 4.4. NAT traversal

TBD

### 4.5. Unify home router

TBD

## 5. IANA Considerations

This memo includes no request to IANA.

## 6. Security Considerations

TBD

## 7. Normative References

[I-D.ietf-sfc-problem-statement]
Quinn, P. and T. Nadeau, "Service Function Chaining Problem Statement", draft-ietf-sfc-problem-statement-13 (work in progress), February 2015.

[I-D.ietf-softwire-lw4over6]
Cui, Y., Qiong, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the DS-Lite Architecture", draft-ietf-softwire-lw4over6-13 (work in progress), November 2014.

[I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, "Mapping of Address and Port with Encapsulation (MAP)", draft-ietf-softwire-map-13 (work in progress), March 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <http://www.rfc-editor.org/info/rfc2865>.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, DOI 10.17487/RFC6052, October 2010, <http://www.rfc-editor.org/info/rfc6052>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <http://www.rfc-editor.org/info/rfc6146>.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011, <http://www.rfc-editor.org/info/rfc6333>.

[RFC6519] Maglione, R. and A. Durand, "RADIUS Extensions for Dual-Stack Lite", RFC 6519, DOI 10.17487/RFC6519, February 2012, <http://www.rfc-editor.org/info/rfc6519>.

[RFC6888] Perreault, S., Ed., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, DOI 10.17487/RFC6888, April 2013, <http://www.rfc-editor.org/info/rfc6888>.

Authors' Addresses

Xie Chongfeng
China Telecom
Room 502, No.118, Xizhimennei Street
Beijing
China

Email: xiechf01@gmail.com,xiechf@ctbri.com.cn

Wei Meng
ZTE Corporation
No.50 Software Avenue, Yuhuatai District
Nanjing
China

Email: meng.wei2@zte.com.cn,vally.meng@gmail.com

Cui Wang
ZTE Corporation
No.50 Software Avenue, Yuhuatai District
Nanjing
China

Email: wang.cui1@zte.com.cn

Bhumip Khasnabish
ZTE TX, Inc.
55 Madison Avenue, Suite 160
Morristown, New Jersey 07960
USA

Email: bhumip.khasnabish@ztetx.com