Service Function Chaining
Internet-Draft
Intended status: Informational
Expires: August 17, 2014

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

February 13, 2014

Service Function Chaining Use Cases in Broadband
draft-meng-sfc-broadband-usecases-00

Abstract

This document discusses about service function use cases in different scenarios for each part of broadband network. They are based on the requirements of providing existing broadband services in NAT(v4v6-coexisting or IPv6-only) and firewall and AAA. 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 August 17, 2014.

Table of Contents

1. Introduction

As we known, one of the largest parts of the internet participants is broadband subscriber. Because the global IPv4 addresses is depleting, and most of the internet contents and applications are not ready yet, carrier graded NAT technologies and Large Scale NAT devices (LSN) may be deployed in the broadband network during the initial stage of the IPv6 transition.

This document is aimed to analyze the possible NAT and firewall and AAA service function solutions in every part of the broadband network with considering its features. And it also provides the applicable scenarios for each solution.

The object is trying to unload services from nodes in traditional broadband network and deal with such services through service function chains.

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

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

3. Use cases

3.1. CGN

3.1.1. Simple NAT44

Figure 1 illustrates in a simple NAT44 scenario how SF-NAT deployed.

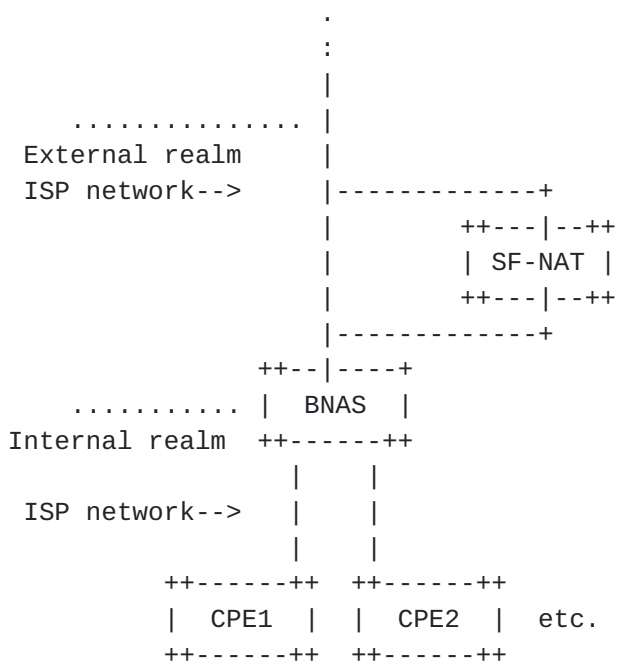

Figure 1: Simple NAT44

In broadband networks, SF-NAT may be deployed beside BNAS. These service nodes may contain SF-NAT and other service functions instances.

3.1.2. DS-Lite

Figure 2 describes a scenario of DS-lite.

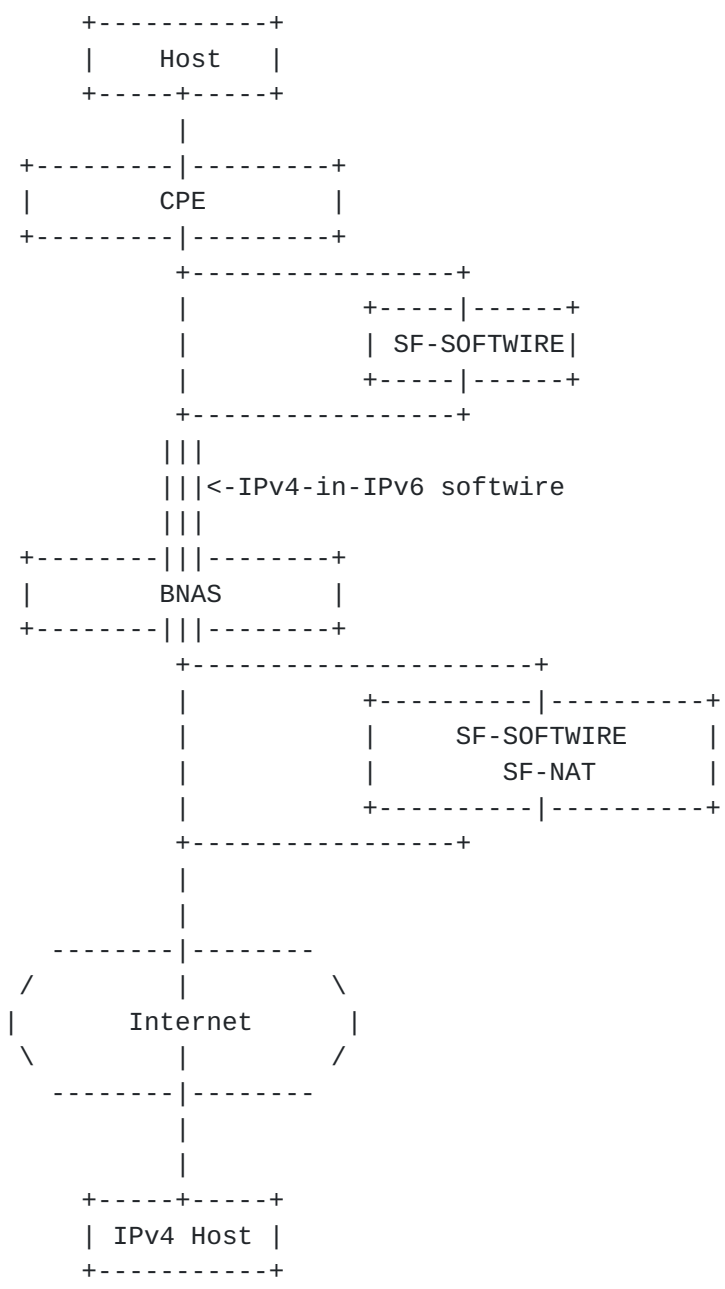

Figure 2: DS-Lite

When the outbound datagram is received by the CPE, the CPE sends 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 which contains SF-SOFTWIRE instance.

Next, the BNAS receives the processed datagram, the BNAS sends it to a classifier and finds it need to be dealed with DS-Lite process.

The SF-NAT creates and maintains the NAT mapping table. That is to say, BNAS, itself, would not be aware of any stateful sessions.

3.1.3. MAP-E/Lightweight 4o6

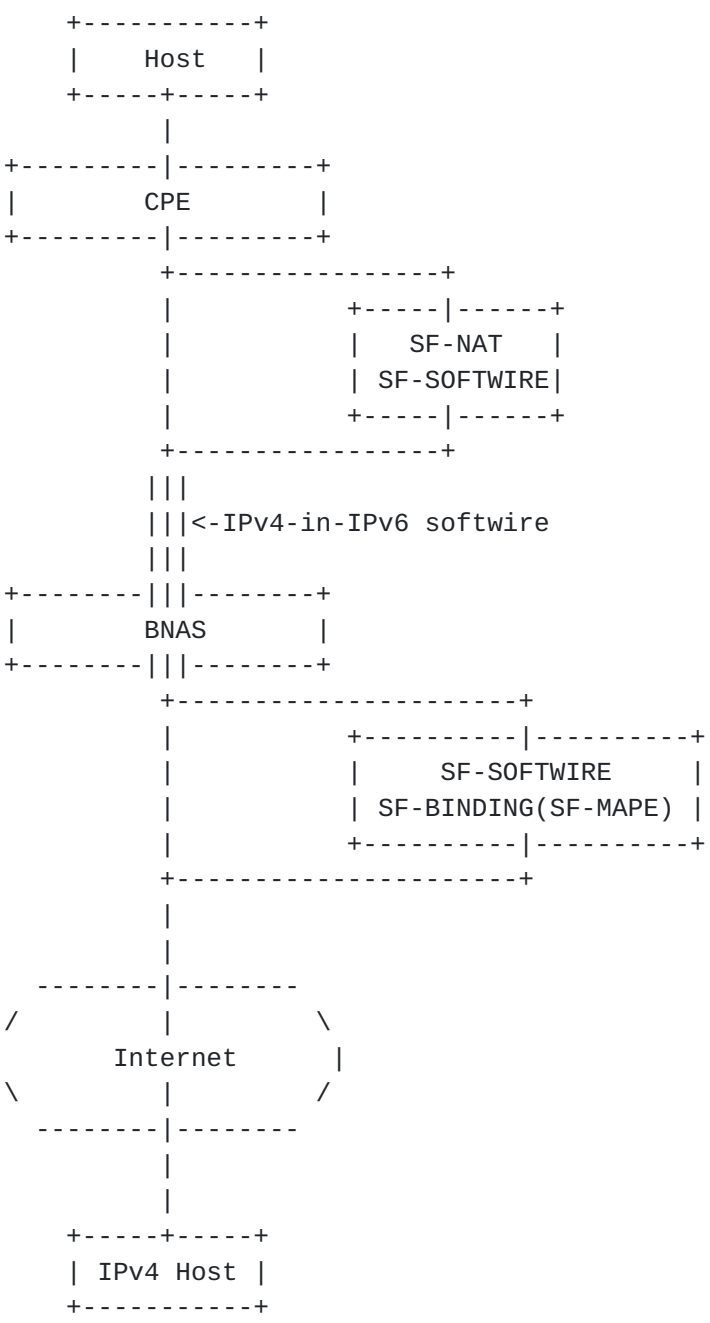

Figure 3: MAP-E/Lightweight 4o6

The main difference between Lightweight 4o6/MAP-E and DS-Lite is where NAT happens, which results in that Lightweight 4o6/MAP-E

realizes NAT on the CPE, and then encapsulates translated IPv4 datagram in IPv6 Header and finally propagates the IPv4-in-IPv6 datagram in IPv6 tunnel to BNAS device.

That is to say, for outbound traffic in lw4o6 SFC scenario, When the datagram 1 is received by the home router, the CPE sends it to a specific classifier named which determines the datagram should be forwarded directly or dealed with lw4o6 process. Then the classifier sends the datagram within service header encapsulated to the first element of this SFP: SF-NAT. SF-NAT translates the IPv4 datagram and forwards translated IPv4 datagram to SF-SOFTWIRE, which encapsulates the datagram with the lwAFTR's IPv6 address as IPv6 encapsulated header and forwards this IPv4-in-IPv6 datagram (datagram 2) to the BNAS device.

When the BNAS device receives such an IPv4-in-IPv6 datagram, the BNAS device sends it to a classifier and finds it need to be dealed with Lightweight 4o6 process. Then the classifier sends the datagram within service header encapsulated to the first element of SFP: SF-BINDING. This SF-BINDING creates a binding table about Lightweight 4o6 and decapsulates this datagram, and then propagates the datagram to internet.

For outbound traffic in MAP-E SFC scenario, When the datagram 1 is received by the CPE, the CPE sends it to a specific classifier named which determines the datagram should be forwarded directly or dealed with MAP-E process. Then the classifier sends the datagram within service header encapsulated to the first element of this SFP: SF-NAT. SF-NAT translates the IPv4 datagram and forwards translated IPv4 datagram to SF-MAPE, which utilizes the MAP-E rules to encapsulate the datagram with the MAP BR's IPv6 address as IPv6 encapsulated header and forwards this IPv4- in-IPv6 datagram (datagram 2) to the BNAS device.

When the BNAS device receives datagram 2, the BNAS device sends it to a classifier and finds it need to be dealed with MAP-E process. Then the classifier sends the datagram within service header encapsulated to the first element of SFP:SF-MAPE. This SF-MAPE utilizes the MAP-E rules to extract the IPv4 datagram, and then propagates the datagram to internet.

3.1.4. NAT64

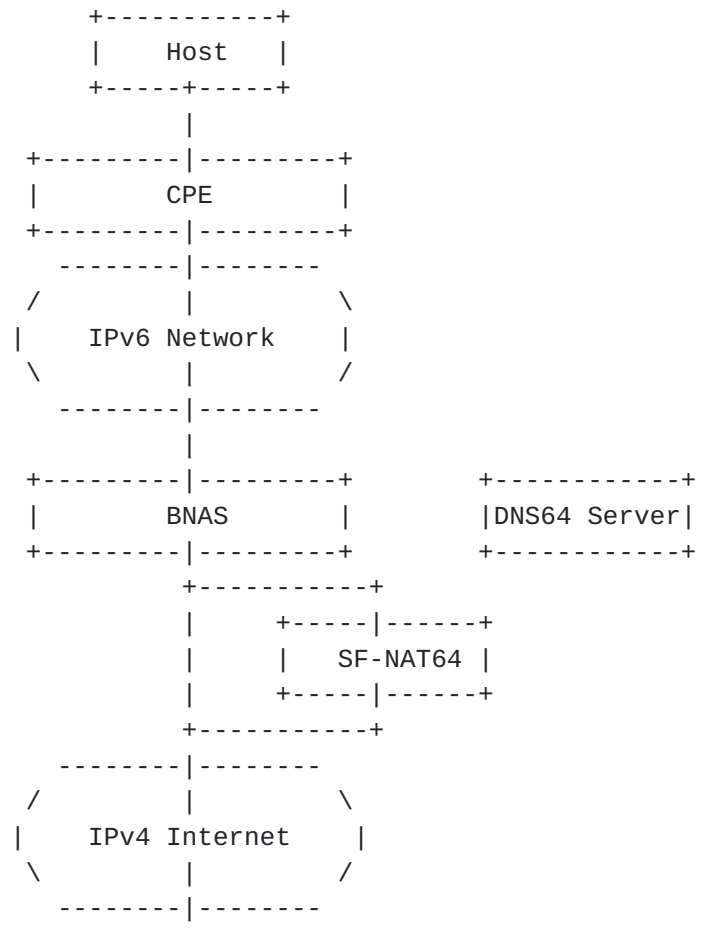

Figure 4: NAT64

NAT64 scenario is similar with the scenario of simple NAT44. The only difference is SF-NAT64 should maintain rules that indicate how to translate a des-IPv6-address to an IPv4 address using a specific prefix64::/n.

3.2. Firewall

TBD

3.3. AAA

Figure 5 illustrates in a scenario how SF-SUBSCRIBER deployed.

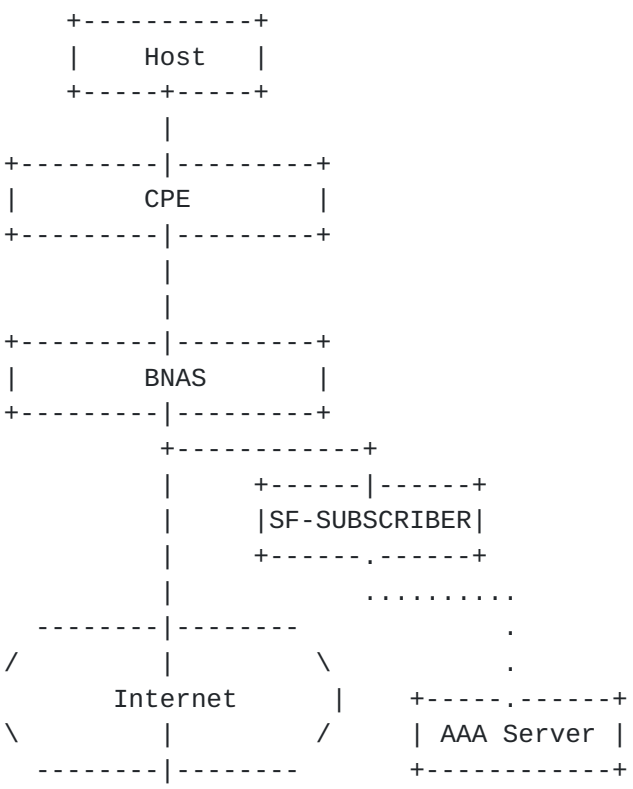

Figure 5: AAA

Under this scenario, BNAS entrusted service node which contains SF-SUBSCRIBER instance with the task of AAA client. A node contains SF-SUBSCRIBER can create a RADIUS session with AAA server. The messages and processes of RADIUS between AAA server and SF-SUBSCRIBER are quite the same with existing process.

The biggest advantage to this consideration is that BNAS is non-subscriber-aware. All subscriber status is maintained in service node which contains SF-SUBSCRIBER instance.

4. Considerations

4.1. Service Function Chains

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

a.1. Outbound : SF-SUBSCRIBER -> SF-NAT

Inbound : SF-NAT -> SF-SUBSCRIBER

a.2. Outbound : SF-SOFTWIRE -> SF-SUBSCRIBER -> SF-SOFTWIRE -> SF-NAT

Inbound : SF-NAT -> SF- SUBSCRIBER -> SF-SOFTWIRE -> SF-SOFTWIRE

a.3. Outbound : SF-SUBSCRIBER -> SF-FIREWALL6 -> SF-NAT64

Inbound : SF-FIREWALL4 -> SF-NAT64 -> SF-SUBSCRIBER

etc.

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.

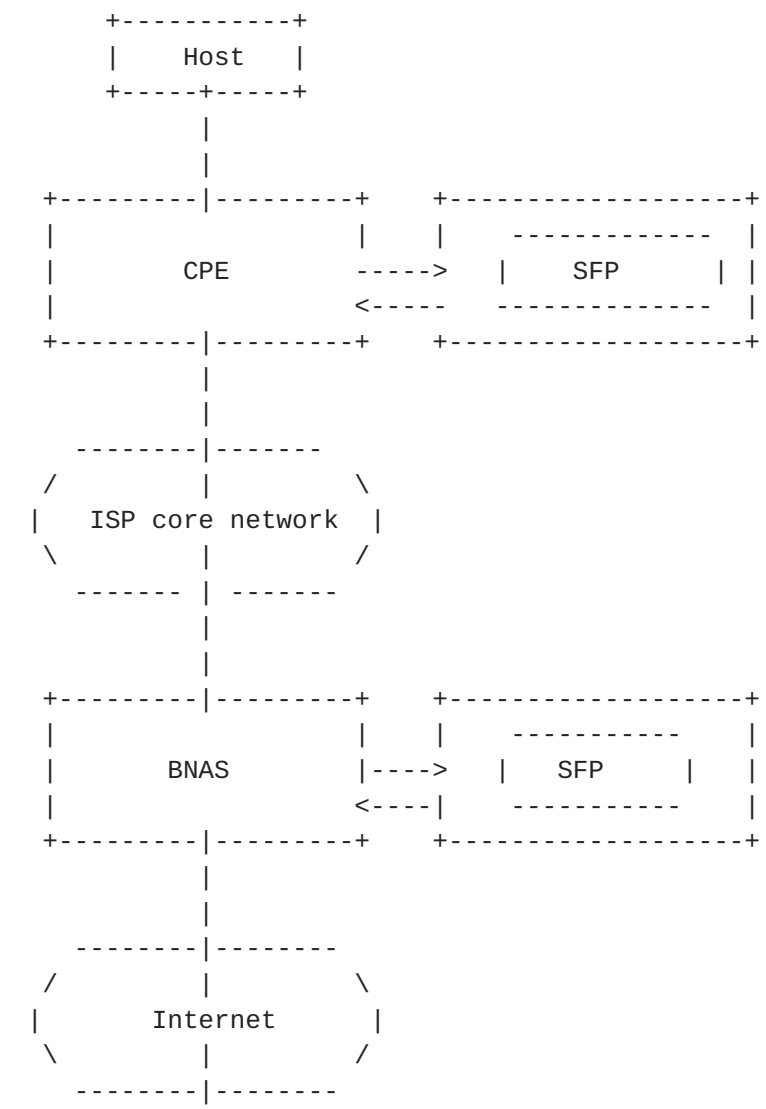

Figure 6: Standalone mode

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.

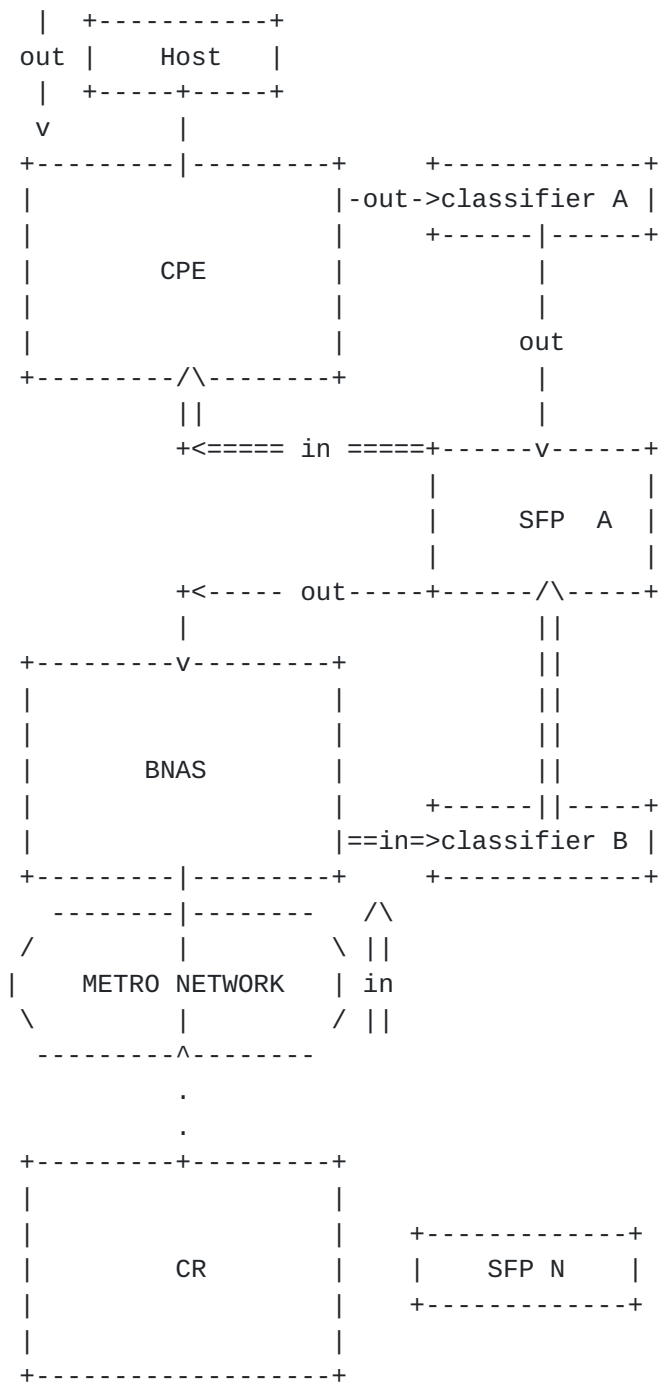

Figure 7: Directly connecting mode

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-00 (work in progress), January 2014.

[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-lw4over6-06 (work in progress), February 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-10 (work in progress), January 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

[RFC6519] Maglione, R. and A. Durand, "RADIUS Extensions for Dual-Stack Lite", RFC 6519, February 2012.

[RFC6888] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, April 2013.

Authors' Addresses

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