Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: October 2, 2012
G. Yang
Y. Li
C. Huang
China Telecom
March 31, 2012

Fundamental Architecture of Services Provider's network Transitioning to IPv6 (FAST6)

draft-yang-v6ops-fast6-00

Abstract

The IANA free pool of IPv4 addresses was depleted, IPv6 migration has become the most imperative task. There are many transition mechanisms designed for different scenarios, however, some problems arosed in the practice. FAST6, specified in this draft, is based on the ideas of native dual stack and address sharing. It can solve the mixed route problem and simplify the planning of private IPv4 address space by using tunnel technology. FAST6 is an economical and stable technology for smooth network transition.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

As mentioned previously, available transition mechanisms have their own drawbacks in practice. Nowadays, most applications do not support IPv6 and the protocol translation technologies, such as NAT64, cannot help in the application level, therefore it is necessary to provide the IPv4 and IPv6 service separately. However, 4over6 technology is a risky method for network migration since any troubles happen in the IPv6 network will influence the IPv4 service, especially in the period when IPv4 flows are dominant in the network. Simultaneously, 4over6 technology does not help to stimulate applications translation of ICPs who are unaware of the well prepared IPv6 network. In the mean time, 6 over 4 technology is not proper for the continuously expanding network. Native dual stack technology can avoid those problems essentially for it can provide dual stack service separately, making IPv4 decoupled from IPv6 and providing network environment for IPv6 service migration. However, native dual stack is not enough and IP address sharing has to be used when the IPv4 addresses were exhausted.

NAT444 seems to be a good solution except some carrier grade problems such as mixed routing (private address routing and public address routing), additional unified arrangement of private IPv4 address spaces among BNGs and so on. All these problems will cause overload maintenance cost. This document specifies the FAST6 technology, which is aimed at balancing the costs and benefits in service provider networks better. FAST6 is based on native dual-stack. By taking the advantages of tunnel technology and native dual-stack technology, FAST6 overcomes carrier grade NAT problems. It stimulates the IPv6 migration and also decouples the IPv4 from IPv6, making network transition smoother and guaranteeing the user experience effectively.

This document will first briefly introduce the overall architecture of FAST6 and then describe the detailed behaviors of FAST6 elements. It will then depict an intuitive example about FAST6 through data flow. At last, we will present the FAST6 implementation in current network and show some of its advantages.

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. Terminologies

The technology described in this document is known as FAST6. The abbreviation "FAST6" will be used throughout this text.

FAST6: Fundamental Architecture of Services Provider's network Transitioning to IPv6

FTN: FAST6 tunnel North

FTS: FAST6 tunnel South.

Resource Pool: One of the element in FTN, including address pool, Tunnel ID-address pool mapping table, port resource pool.

FAST6 NAT: A module use triple-tuple for NAT.

CR: Core Router (CR) in a metropolitan area network is the egress router of the MAN and connecting to the ISP's backbone in upstream and connecting to BRASs for downstream.

BNG: Broadband Network Gateway, BRAS and SR

Dual stack: Defined in RFC 4213

Nat related terminology: Defined in RFC 1417

IP-in-IP tunnel: Defined in RFC 2003

3. FAST6 Architecture

FAST6 consists of two functional modules. One is FTS (FAST6 tunnel south) , the other is FTN(FAST6 tunnel north). FTS is the tunnel endpoint present at the user side. FTN is the tunnel endpoint present at the network side.

```
                      +-----+-----+ +-----+-----+
                      |  IPv4 host| |  IPv6 host|
                      +-----------+ +-----------+
                            |              |
                    --------|--------------|------
                  /         |              |       \
                 |       Internet          |        |
                  \         |              |       /
                    --------|--------------|------
        |-------------------|--------------|--------------|
        |          +-------------------+   |        FAST6 |
        |          |        FTN        |   |              |
        |          +---------|---------+   |              |
        |                   |||            |              |
        |                   ||| IP in IP Tunnel           |
        |          +-------------------+   |              |
        |          |        FTS        |   |              |
        |          +---------|---------+   |              |
        |                    |             |              |
        |____________________|_____________|______________|
                       +-----+-----+       |
                       |  CPE/ host|-------|
                       +-----------+
```

Figure 1: FAST6 architecture

3.1. FTS

As the tunnel endpoint at user side, FTS is responsible for encapsulating private IPv4 packet within a public IPv4 packet to establish an IP-in-IP tunnel, or decapsulating private IPv4 packet from the tunnel.

3.2. FTN

FTN is the tunnel endpoint at network side. It has four functions: encapsulation and decapsulation, address translation, address mapping table maintenance, resource pool maintenance.

From south to north, FTN decapsulates the private IP address packet from the tunnel, marking the public IPv4 address as the tunnel ID and finding the corresponding IP address pool and port resource in the resource pool based on the tunnel ID. Then FTN replaces the private IPv4 address header with the public IPv4 address header and generates an address mapping entry.

From the north to south, FTN searches the address mapping table for the corresponding triple tuple (tunnel ID, private address, port)

according to the received public IPv4 address and port. Then FTN forwards the packet to the corresponding tunnel.

4. FAST6 Tunnel South(FTS)

4.1. Definition

As defined above, FTS is a function module used to establish the IPv4-in-IPv4 tunnel to FTN, encapsulating and decapsulating the packet.

4.2. Encapsulation

FTS uses a public IPv4 address to encapsulate the private IPv4 packet. The packet encapsulation structure is as below.

```
+-----+-----+-----+-----+-----+-----+
|Public IPv4|private IPv4|payload   |
+-----------+-----------+-----------+
```

Figure 2: The encapsulation format

For the encapsulation format and parameters, please refer to RFC2003 and other encapsulation mode will be considered in the future.

4.3. Fragmentation and Reassembly

The encapsulation of IPv4 packet over IPv4 packet will increase 20 extra bytes in IP header,it is necessary for the service provider to manually increase the MTU size for all the links between the FTS element and the FTN elements, by at least 20 bytes to accommodate both the IPv4 encapsulation header and the IPv4 datagram without fragmenting the IPv4 packet.

4.4. Discovery

The number of FTSs (the number of the tunnels) is very limited, so the IPv4-in-IPv4 tunnel establishment between FTN and FTS can be configured manually.

5. FAST6 Tunnel Nouth(FTN)

5.1. Definition

As defined above, FTN has four functions: encapsulation and decapsulation, address translation, address mapping table

maintenance, resource pool maintenance.

```
     +------------------------------------------------------+
     |resource pool                                         |
     |  +-------------------+  +----------+ +-----------+ |
     |  |tunnel ID-address pool|address pool| port resource
     |  |mapping table      |  |          | |           | |
     |  +---------|---------+  +-----|----+ +-|---------+ |
     +------------|------------------ /------/------------+
                  |                  /      /
       +------+  +-----------------+/      / +---------------+
       | encap|  |address traslation------/  | mapping table |
       | decap|  |                 |         |               |
       +----- +  +-----------------+         +---------------+
```

Figure 3: FTN architecture

5.2. Encapsulation

The encapsulation format of FTN is the same as FTS. The fragmentation and reassembly mode are also the same as FTS.

5.3. Resource Pool Maintenance

The resource pool includes the tunnel ID to IP address pool mapping table, address pool and port resource pool. The planning of address pool depends on the specific network deployment. Usually, each tunnel ID has its own IP address pool. In addition, the resource pool has to maintain the available port resource and address for each address pool.

5.4. FAST6 NAT

From south to north, FTN assigns a public address and port after checking the resource table according to the triple tuple (Tunnel ID, private address, port). From north to south, FTN searches the address mapping table after receiving the packet and finds the corresponding tunnel ID, private address and port information, then forwards the packet to corresponding tunnel.

5.5. address mapping table maintenance

From south to north, FTN will generate a network address mapping table. The parameters listed in the entry is in this order,(converted public IPv4 address, converted port, tunnel ID, private IPv4 address, port).

6. FAST6 Data Flow

The following picture describes the procedure of accessing internet from user end through FAST6. Users visit the IPv4 internet resources through IPv4 network and use IPv6 network to access the IPv6 internet resources.

```
                    +-----+-----+ +-----+-----+
                    |  IPv4 host| |  IPv6 host|
                    +-----------+ +-----------+
                          |              |
                  --------|--------------|-----
                /         |              |      \
               |       Internet          |       |
                \         |              |      /
                  --------|--------------|------
         |--------120.0.0.1--|--------------|--------------|
         |          +--------------------+   |        FAST6 |
         |          |        FTN         |   |              |
         |          +---------|---------+   |              |
         |                   |||             |              |
         |         59.43.0.1 ||| IPv4-in-IPv4 Tunnel       |
         |          +--------------------+   |              |
         |          |        FTS         |   |              |
         |          +---------|---------+   |              |
         |                    |              |              |
         |___________10.0.1.1_|_____________|______________|
                     +-----+-----+          |
                     |  CPE/ host|-------|
                     +-----------+
```

Figure 4: FAST6 Data Flow

Customer 1 sends a TCP packet with source address 10.0.1.1 and port 1000 to the ICP server whose address is 198.8.8.8(IP datagram 1). When the packet arrives at the FTS, FTS encapsulates the private IPv4 packet in a public IPv4 header 59.43.0.1 with the destination 59.43.0.2, the other end of tunnel(IP datagram2). When the packet arrives at the FTN, FTN decapsulates it , checks the corresponding IP address pool based on Tunnel ID and chooses 120.0.0.1 and port 2000 to replace the former header(IP datagram 3). Then FTN generates a mapping entry 120.0.0.1,2000,59.43.0.2,10.0.1.1,1000.

From north to south, when FTN receives the packet with the destination address 120.0.0.1/2000, it checks the address mapping table , finds the entry 120.0.0.1,2000,59.43.0.2,10.0.1.1,1000 and forwards the packet to tunnel established by FTS1 according to the last 3 parameters.

Datagram	Header field	Contents
IPv4 datagram 1	IPv4 Dst	198.8.8.8
	IPv4 Src	10.0.1.1
	TCP Dst	80
	TCP Src	1000
---------------	------------	-------------
IPv4 datagram 2	IPv4 Dst outer	59.43.0.2
	IPv4 Src outer	59.43.1.1
	IPv4 Dst	198.8.8.8
	IPv4 Src	10.0.0.1
	TCP Dst	80
	TCP Src	1000
---------------	------------	-------------
IPv4 datagram 3	IPv4 Dst	198.8.8..8
	IPv4 Src	120.0.0.1
	TCP Dst	80
	TCP Src	2000

Figure 5: Datagram Header Contents

7. FAST6 Deployment

This chapter will briefly introduce the FAST6 deployment in real network and some of its advantages. The following picture only depicts IPv4 part of FAST6.The detailed deployment, cutover and network transition will be stated in other document.

```
                                                +-----+-----+
                        |  IPv4 host|
                        +-----------+
                              |
                      --------|------------
                    /         |             \
                   |       Internet          |
                    \         |             /
                      --------|-------------
                              |
                 +---------------------------+
                 |              CR           |
                 +---|---------|---------|---+
                     |         |         |
                  120.0.0.1  120.0.0.2  120.0.1.1
                 +----------------------------+
                 |            FTN             |
                 +----------------------------+
                 ||         ||       \\
                 ||         ||        \\
         59.43.0.1       59.43.0.3    59.43.0.5
        +------//----BNG1--//----+    + \\---BNG2-----+
        |     ||          ||     |    |  \\           |
        | +--//----+  +--//----+ |    | +-\\-----+    |
        | |  FTS   |  |  FTS   | |    | |  FTS   |    |
        | +---|----+  +---|----+ |    | +--|-----+    |
        +-----|-----------|------+    +----|----------+
         10.0.1.1     10.0.1.2         10.0.1.1
        +-----+-----+  +-----+-----+   +-----+-----+
        |  host1    |  | host2     |   |  host3    |
        +-----------+  +-----------+   +-----------+
```

Figure 6: FAST6 Deployment

FAST6 is suitable for layer 2 and layer3 access modes. The FTS component can be installed in BNG equipments tunnel interface. The FTN unit is similar to CGN device and can be embedded in the CR as a card or deployed as an independent device.

FAST6 can eliminate the mixed routing problem by establish a tunnel from BNG to FTN. In the mean time, since it uses the public address as the tunnel ID to separate different BNGs, the private address pool can be overlapped among BNGs, saving the workload for arranging the private IPv4 address pool in the whole network uniformly. Besides, since FTS can be configured in the ingress direction of user interface on BNG, the tunnel can also isolate the mixed route within the device. This feature fits BNG for providing multiple services

which are running behind different address distribution policies (for example, private address for common users and public address for VIP customers.).

The IPv4 address used for tunnel encapsulation is different for different FTS. The address pool can be overlapped for each FTS. FTS can be deployed flexibly in centralized and distributed form in the network depending on private IPv4 traffic flow amount. When the FTN is distributed, FTN and FTS may probably be in the same card in this case, FAST6 is as same as NAT444.

In addition, FAST6 have some the following advantages:

(1) Retaining the current access method and customer behaviors, modifications of CPE are not required.

(2) Providing dual stack services for users, no need for protocol translation and consequently decreasing the influence on applications.

(3) Easier for troubleshooting. IPv4 is decoupled from IPv6, so it will not be influenced by IPv6.

(4) Suitable for the initial period of network transition, and it can be seamlessly compatible with any other technologies used for later stage of transition.

8. Acknowledgements

TBD...

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

This document has no impact on the security properties of specific IPv6 transition tools. When introducing IPv6, it is important to ensure that the necessary security capabilities exist on the network components even when dealing with IPv6 traffic. The security issues should be considered when deploying any transition technology. For instance, firewall and logging system for illegal activity tracing is still a challenge in IPv6 and NAT deployments.

11. References

11.1. Normative References

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

[min_ref] authSurName, authInitials., "Minimal Reference", 2012.

11.2. Informative References

[I-D.arkko-ipv6-transition-guidelines]
Arkko, J. and F. Baker, "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", draft-arkko-ipv6-transition-guidelines-14 (work in progress), December 2010.

[I-D.ietf-behave-lsn-requirements]
Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", draft-ietf-behave-lsn-requirements-05 (work in progress), November 2011.

[I-D.ietf-softwire-dual-stack-lite]
Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", draft-ietf-softwire-dual-stack-lite-10 (work in progress), May 2011.

[I-D.kuarsingh-lsn-deployment]
Kuarsingh, V. and J. Cianfarani, "NAT44/LSN Deployment Options and Experiences", draft-kuarsingh-lsn-deployment-01 (work in progress), January 2011.

[I-D.shirasaki-nat444]
Yamagata, I., Shirasaki, Y., Nakagawa, A., Yamaguchi, J., and H. Ashida, "NAT444", draft-shirasaki-nat444-03 (work in progress), January 2011.

[I-D.shirasaki-nat444-isp-shared-addr]
Shirasaki, Y., Miyakawa, S., Nakagawa, A., Yamaguchi, J., and H. Ashida, "NAT444 addressing models", draft-shirasaki-nat444-isp-shared-addr-05 (work in progress), January 2011.

[I-D.yang-v6ops-fast6-tools-selection]
Yang, G. and C. Huang, "The analysis of tools selection

for broadband ISP", draft-yang-v6ops-fast6-tools-selection-00 (work in progress), May 2011.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC4029] Lind, M., Ksinant, V., Park, S., Baudot, A., and P. Savola, "Scenarios and Analysis for Introducing IPv6 into ISP Networks", RFC 4029, March 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4241] Shirasaki, Y., Miyakawa, S., Yamasaki, T., and A. Takenouchi, "A Model of IPv6/IPv4 Dual Stack Internet Access Service", RFC 4241, December 2005.

[RFC5569] Despres, R., "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", RFC 5569, January 2010.

[RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.

[RFC6036] Carpenter, B. and S. Jiang, "Emerging Service Provider Scenarios for IPv6 Deployment", RFC 6036, 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.

Authors' Addresses

GuoLiang Yang
China Telecom
109, Zhongshan Ave. West,
Guangzhou, Tianhe District 510630
P.R. China

Phone:
Email: iamyanggl@gmail.com

YangChun Li
China Telecom
109, Zhongshan Ave. West,
Guangzhou, Tianhe District 510630
P.R. China

Phone:
Email: liyc_gsta@189.cn

CanCan Huang
China Telecom
109, Zhongshan Ave. West,
Guangzhou, Tianhe District 510630
P.R. China

Phone:
Email: huangcc_gsta@189.cn