Framework of Multi-domain IPv6-only Underlay Network and IPv4 as a Service
draft-xie-v6ops-framework-md-ipv6only-underlay-00

Abstract

For the IPv6 transition, dual-stack deployments require both IPv4 and IPv6 transfer capabilities to be deployed in parallel. IPv6-only is considered as the ultimate stage where only IPv6 transfer capability is used while ensuring global reachability for both IPv6 and IPv4 (usually known as IPv4aaS). This document specifies requirements and propose a framework for deploying IPv6-only as the underlay in multi-domain networks.

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 December 29, 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction

IPv6 capabilities have been widely deployed during the past decade with IPv6 traffic growing faster than IPv4. [I-D.ietf-v6ops-ipv6-deployment] provides an overview of IPv6 transition deployment status and how the transition to IPv6 is progressing among network operators and enterprises.
As per 2022, most IPv6 deployments rely on dual-stack approach [RFC4213]. Dual-stack does have a few disadvantages in the long run, like the duplication of the network resources and states, as well as other limitations for network operation. For this reason, when IPv6 usage increases to a certain limit, it would be better to consider IPv6-only. It is generally supposed that running an IPv6-only network would reduce operational expenditures and optimize operations as compared to a dual-stack environment. In 2016, the IAB announced that it "expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6." [IAB-statement]. In order to provide the connectivity service after IPv4 address depletion, operators need to provide IPv6 services and keep the ability for users to access the global IPv4 Internet. Providing IPv4 service continuity, a.k.a, IPv4 as a Service(IPv4aaS) is a natural consideration for IPv6-only scheme.

Several IPv4 service continuity mechanisms have been designed within IETF during the past twenty years [I-D.ietf-v6ops-transition-comparison]. Different types of IPv4 and IPv6 conversion technologies may be considered, e. g., 464XLAT [RFC6877] uses stateful NAT64 translation, MAP-E [RFC7597] and MAP-T [RFC7599] use stateless NAT64 translation. DS-Lite [RFC6333] adopts AFTR-based 4over6 tunneling technology, etc. This document specifies the requirements for multi-domain IPv6-only underlay networks and proposes a general framework from the perspective of operators. The objective of such a this framework is to help large-scale operators implement the transition to IPv6-only and supporports cross-domain, end-to-end IPv4 service delivery over IPv6-only network. In this document, "IPv6-only network" stands for "IPv6-only underlay network", unless there is a specific statement. This document does not introduce any new IPv6 transition mechanisms.

### 1.1. Requirements Language

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. Terminology

The following terms are defined in this document:

- Multi-domain IPv6-only network: An IPv6-only network which consists of multiple ASes belonging to and operated by the same operator.

- Inter-domain IPv6-only network: An IPv6-only network which consists of multiple ASes belonging to and operated by different operators.

- UE: User Equipment, e.g., mobile phone.

- CPE: Customer Premise Equipment.

- IXP: Internet Exchange Point.

- WKP: Well-Known Prefix.

- NSP: Network-Specific Prefix.

- PE: Provider Edge (Section 5.2 of [RFC4026]).

- IPv4-embedded IPv6 packet: IPv6 packet which is generated from IPv4 packet by algorithmically mapping of the source and destination IPv4 addresses to IPv6 addresses.

- ASBR: A PE which run eBGP routing protocol and peering with the BGP router of external AS.

- Conversion point: A function which provides conversion between IPv4 and IPv6 realms. This is, for example, the XLAT function in [RFC6144]

3. Focus on IPv6-only Networks

The global industry has not given a unified definition of IPv6-only network so far. This document defines such a notion as a IPv6-centric network in which data packets are forwarded upon IPv6 capability, An IPv6-only network may interconnect with external
networks, including IPv4-only networks.

4. Why Considering Multi-domain Factor when Implementing IPv6-only Networks?

Transition to IPv6-only from dual-stack means some or all the IPv4 protocol instances of dual-stack network will be disabled gradually, thereby IPv6 will become the main network-layer protocol.

When IPv4 capabilities are disabled, the first question is how to make remaining IPv4 services running normally and users' experience does not deteriorate. The deployment of IPv6-only should not be based on the premise of the extinction of all IPv4-only services, it is very possible that some portion of the Internet service will consistently be IPv4-based. In other words, IPv6-only network should carry not only native IPv6 services, but also allow to reach IPv4-only services.

[RFC5565] describes the IPv4-over-IPv6 scenario, where the network core is IPv6-only and the interconnected IPv4 networks are called IPv4 client networks. The P Routers (Provider Routers) in the core only support IPv6, but the AFBRs support IPv4 on interfaces facing IPv4 client networks and IPv6 on interfaces facing the core. The routing solution defined in [RFC5565] for this scenario is to run IBGP among AFBRs to exchange IPv4 routing information in the core, and the IPv4 packets are forwarded from one IPv4 client network to the other through a softwire using tunneling technology, such as MPLS, LSP, GRE, L2TPv3, etc.

[RFC6992] describes a routing scenario where IPv4 packets are transported over an IPv6 network, based on [RFC7915] and [RFC6052], along with a separate OSPFv3 routing table for IPv4-embedded IPv6 routes in the IPv6 network.

Generally, the networks of large-scale operators comprise multiple ASes, different ASes may serve different scenarios, such as metro network, backbone network, 4G or 5G mobile core, data center network, and are often managed by different departments or institutions, using different routing and security policies. When introducing the IPv6-only scheme without collaboration between ASes, different ASes
adopt the IPv6 transition approach independently, the result is that multiple IPv6-only islands are connected by IPv4 links between domains. As shown in Figure 1, there will be more IPv4-IPv6 packet conversion gateways with different functions in the network. Under this circumstance, IPv6 packets converted from IPv4 packets need to be transformed back to IPv4 packets at the egress of one AS, and then back to IPv6 in the next domain, and the number of conversion gateways will increase along with the increasing of the number of ASes. Excessive IPv4-IPv6 conversion gateways lead to complexity of network and CAPEX increasing. Therefore, there is an urgent need for multi-domain IPv6-only solutions to eliminate unnecessary conversion functions and improve data forwarding efficiency.
5. Scenarios

This section describes scenarios where IPv4 packets are transported over a multi-domain IPv6-only network. A typical model of multi-domain IPv6 network is depicted in Figure 2. Network 1, belonging to and operated by operator 1, runs IPv6 and is composed of multiple inter-connected ASes, i.e., AS1, AS2 and AS3. In addition, network 1 provides access to multiple types of users, including mobile, home broadband and enterprise customers, denoted by UE1, UE2 and UE3 in Figure 2. Routers that are outside the backbone but directly attached to it are known as "Customer Edge" (CE) routers.

Network 1 is open, it is interworking with the external networks. Operator 2 is one of the neighbor operators of Operator 1, AS4 of operator 2 and AS3 of operator 1 are interconnected through BGP protocol. AS4 is an IPv4-only network, which means that it does not run IPv6 protocol. In addition, cloud services are hosted in data centers and connected across multiple data centers, the edge, and public and private clouds. The cloud data center must be able to communicate across these multiple sites, both on-premises and in the cloud. IPv6-only network needs to provide connections for cloud data center. Network 1 supports two connections modes of cloud data centers, the first one is between cloud data center and individual users, for instance, the user of CPE1 accesses the service hosted in DC1, the second one is the connection between cloud data centers, for instance, communications between VMs hosted in DC1 and DC2 separately.

The edge nodes of the Network 1 are often known as "Provider Edge" (PE) routers. The term "ingress" (or "ingress PE") refers to the...
router at which a packet enters the network, and the term "egress" (or "egress PE") refers to the router at which it leaves the backbone. Interior nodes are often known as "P routers". The P routers in the core only support IPv6, but the PEs support IPv4 on interfaces facing IPv4 client networks and IPv6 on interfaces facing the core. Network 1 provides transportation services for packets that originate outside the network and whose destinations are outside the network. These packets enter the IPv6 network at one of its "edge routers". They are routed through the network to another edge router, after which they leave the network and continue on their way.
Figure 2. Multi-domain IPv6 Underlay Network Model

In order to illustrate the framework of IPv6-only networks, the following scenarios should be considered,

Scenario 1: IPv6 user to IPv4 server, i.e., IPv6-only user accesses IPv4 services hosted in cloud data centers.

Scenario 2: IPv4 user to IPv4 server, i.e., IPv4-only user accesses IPv4 services hosted in cloud data centers.

Scenario 3: IPv6 user to IPv6 server, i.e., IPv6-only user accesses IPv6 services hosted in cloud data centers.

Scenario 4: DC-to-DC, i.e., IPv6-only provide communications between VMs hosted in cloud data centers, despite they are IPv4, IPv6 or IPv4/IPv6 dual-stack.
Scenario 5: Transit for neighbor networks, i.e., IPv6-only network serves as an interconnection between several segregated IPv4-only network, IPv4 packets are transported over the IPv6-only network between IPv4 networks.

Scenario 6: IPv6-Only eBGP Edge peering in Internet Exchange Point (IXP) [I-D.ietf-bess-ipv6-only-pe-design], this serves to eliminate IPv4 provisioning at the Edge of IXP that are facing IPv4 address depletion at large peering points.

Scenario 7: 5G Transport service, SD-WAN, network slicing, etc.

It should be noted that the scenarios above are only a subset of the scenarios that multi-domain IPv6-only network will support in the future.

6. Requirements from Service Traffic

Native-IPv6 traffic can be transported over a multi-domain IPv6-only network following legacy procedures.

In order to support IPv4 service continuity, the following requirements should be met by a multi-domain IPv6-only network.

Requirement 1: beneficial to wider IPv6 adoption

It should largely reduce IPv4 public address consumption and accelerate the deployment of IPv6, rather than prolonging the lifecycle of IPv4 by introducing multiple layers of NAT44.

Requirement 2: IPv4-as-a-Service

IPv6 transition mechanisms should provide IPv4 service delivery and there should be no perceived degradation of customer experience when accessing the remaining IPv4 services.

Requirement 3: Optimized end-to-end

For any given IPv4 traffic flow, there should be no IPv4-IPv6 conversion point in the middle of the IPv6 data path when traversing multi-domain IPv6 network, in other words, IPv4 packet should not appear in the middle of the IPv6 data path, the quantity of the conversion points should not exceed two. In addition, IPv6-only network should support the following two types of IPv6 data path.

-From UE to egress, the packets of IPv4 service can be translated (or
encapsulated) into IPv6 packets within the UE or CPE, and there

should be no IPv4-IPv6 conversion before they reach the egress of the
network.

-From the ingress to egress, since the core of the network is
IPv6-based, so all IPv4 packets which reaches the edge of the network
should be transformed into IPv6 packets by the ingress and forwarded
to the egress of the network.

The end-to-end requirement also be valid for cloud-to-cloud
communications.

Requirement 4: support of double translation and encapsulation

The data-plane has two approaches for traversing the IPv6 provider
network: 4-6-4 translation and 4over6 encapsulation, at least one
mode should be supported by IPv6-only network, the core nodes do not
distinguish between translation-based IPv6 packet and encapsulation-
based IPv6 packet. At the egress, the PE can recover IPv4 packet by
reading the next-header field of the packet. Moreover, translation
mode and encapsulation mode should share the same IPv4-IPv6 address
mapping algorithm. Note that the double translation can reduce to
single translation, while the encapsulation cannot.

Requirement 5: controller independent

In order to forward an IPv4 packet to the right egress point, IPv4
reachability information must be exchanged in advance between the
IPv4 networks over an IPv6-only network. In general, BGP4 is used to
distribute external IPv4 routing information among PEs. It does not
rely on the deployment of any centralized controller. Note that with
this routing solution, the IPv4 and IPv6 header conversion performed
in both directions by the PE is stateless.

Requirement 6: user stateless at the border gateway

Maintaining user status will need great volume of storage and
computation power, so it is generally stored or managed at the edge
of network and close to the user side. It is unsuitable to store
user-related status at the inter-connection point. The border ASBR
that is interworking with external networks should be unaware of the user-related information, it only needs to perform stateless translation or encapsulation/decapsulation.

Requirement 7: high scalability

It should achieve high scalability, simplicity and high availability, especially for large-scale operators. When PE processes IPv4-features at the edge of the network, the quantity of the IPv4-related status should not increase linearly or exponentially along with the quantity of the user or traffic. Considering this, it is better to adopt algorithm-based mapping approach to avoid excessive status storage at the edge. It would also avoid overloading of the IPv6 routing table.

Requirement 8: SRv6 applicable

SRv6 can be supported by inserting SRH in translated IPv6 packet, so the network programming can be realized for IPv4 traffic flow.

Requirement 9: incremental deployment

It should deploy in an incremental fashion and the overall transition process should be stable and operational.

Requirement 10: no security compromise

The technologies proposed must not introduce additional security compromise.

7. Description of the Framework

7.1. Overview

Multi-domain IPv6-only networks should support the forwarding of IPv4 service data, after transforming IPv4 packets into IPv6 ones in the UE/CPE or at the edge of the network. Take the latter case as an example, when IPv4 packets need to traverse IPv6-only network, the ingress PE, i.e., PE1, will convert IPv4 packets into IPv6 packets by translation or encapsulation and send them into IPv6 network. After intra-domain and cross-domain transmission, the IPv6 packet reaches
the egress PE, i.e., PE2, it can be restored to an IPv4 packet. During this process, a specific kind of IPv4-IPv6 prefix mapping struct, namely mapping rule, is adopted to generate corresponding IPv6 source and destination addresses from its IPv4 source and destination address, and vice versa.

- The IPv6 source address is derived by appending the IPv4 source address to the Pref6(ingress PE).

- The IPv6 destination address is derived by appending the IPv4 destination address to the Pref6(egress PE) in the mapping rule.

Since this is prefix-level mapping, there is no need to maintain user-related status at the PE devices. In addition, there is no need to concern oneself with translation tables, as the IPv4 and IPv6 counterparts are algorithmically related.

Furthermore, this multi-domain model can naturally be extended to inter-domain IPv6-only networks operated by different operators.

7.2. ADPT

This section illustrates the framework of multi-domain IPv6 network from the perspective of ADPT in PE devices. ADPT is the entity which accommodates the conversion of IPv4 packets into IPv6 ones for IPv4 service delivery over IPv6-only network. ADPT comprises the following components, as shown in Figure 3.
7.2.1. Rule Management Layer

The routing of IPv4 data in the form of IPv6 packet will follow topology of IPv6 network. With this framework, each PE will be identified by at least one IPv6 mapping prefix, denoted by Pref6(PE), it will also have one or more associated IPv4 prefixes which are extracted from local IPv4 routing table or address pool. The mapping relationship between IPv4 address prefix and IPv6 mapping prefix is called mapping rule. The mapping rule is used to convert the IPv4 destination address of a given IPv4 packet into IPv6 address by stateless mapping when its egress is the given PE. The rule management layer i.e., RM, deals with the management of mapping relationship between IPv4 address prefix and IPv6 address prefix of PEs, as shown in Figure 3. The mapping rule announced by a given PE will have at least the following data structure.

IPv4 address prefix: Pref6(PE)

In each PE, there is a mapping rule database, i.e., MD, to store all the mapping rule records it receives from other PEs. Rule management layer provides management services to mapping rule database through interface I7.

The interface with the ADPT of other PE is I1, which is used for the exchanging of mapping rule with each other.

The interface with routing processing layer is I2, which is used for the transmission of mapping rule through routing processing layer. PE1 can extract the IPv4 address prefixes from its IPv4 BGP routing instance through interface I3, and generate the mapping rules of the
device in combination with its own pref6. When the mapping rules are ready, they will be sent to Routing processing layer through interface I2. Correspondingly, PE1 will receive the mapping rules of other PEs through interface I2 and stores them in the local mapping rule database.

For some IPv4 address prefixes which are not announced explicitly by any egress PEs to the ingress PE, there will be no corresponding mapping rule in the rule database. To solve this problem, the default egress PE is defined in the network, which announces the default IPv6 mapping rule with the default mapping prefix to other PEs. The format of the mapping rule for default IPv4 address is as follows.

0.0.0.0/0: Pref6(PE)

### 7.2.2. Routing Processing Layer

Routing processing layer, i.e., RP, is in charge of the exchanging of mapping rule with other PEs and its related routing information at the routing layer. The exchanging of the mapping rule should precede to the process of IPv4 data transmission, otherwise, the data originated from IPv4 network will be dropped due to the absence of the IPv6 mapping prefix corresponding to its destination address.

When receiving the sending request of mapping rule from rule management layer through interface I2, Routing processing layer will convert the mapping rule into data structure that is suitable for the transmission in the IPv6 routing system and send it to the IPv6 routing engine through interface I4. In opposite direction, when receiving the routing information from IPv6 routing engine through interface I4, Routing processing layer will extract mapping rule from the routing information and send it to the Rule management layer.

To support the transmission of mapping rules at the routing layer, BGP4+ protocol needs to be extended. However, this has been out of the scope of the draft and will be discussed in other drafts. In addition, Routing process layer is responsible for announcing the IPv6 route corresponding to each IPv6 mapping prefix throughout the multi-domain IPv6-only networks.
Data Forwarding Layer

Data forwarding layer i.e., DF, provides data forwarding function to IPv6 packets, including native IPv6 packets and IPv4-embedded IPv6 packets. Multi-domain IPv6-only networks need to support both translation and encapsulation technologies for IPv4 data delivery:

1. Translation

Translation refers to the conversion of IPv4 packets into IPv6 packets or reverse conversion. When receiving IPv4 packet through interface I5 from IPv4 packet forwarding module, the data forwarding layer will look up the mapping rule database through the interface I8, if the mapping rule corresponding to the IPv4 destination address is found, the destination address of IPv6 header required for translation is generated by appending the IPv4 address to the Pref6 in the mapping rule. Otherwise, the default IPv6 mapping prefix is used to create the destination IPv6 address.

2. Encapsulation

Encapsulation means that PE encapsulates IPv4 packets in IPv6 packets without changing the original IPv4 packets, and then transmits them in multi-domain IPv6-only networks. Same to the translation method, the source address and destination address of the IPv6 header required for encapsulation are generated according to the corresponding mapping rule found in the mapping rule database. If the mapping prefix corresponding to the destination IPv4 address is not found, the default IPv6 mapping prefix is used.

For a IPv4-embedded IPv6 packet, the pref6 part of the destination address can identify the egress in the network, so the routing of the IPv6 datagram can be implemented based on the pref6 information of the address.

7.3. Mapping Prefix Allocation

In order to support rule based IPv4-IPv6 address mapping, a specific IPv6 address range will be planned to represent IPv4 address space by
stateless mapping as with [RFC7915]. With this framework, there are two options to allocate IPv6 mapping prefix:

1) WKP: A specific WKP can be allocated from the global IPv6 address prefix, e.g., 64:ff9b:: /96.

Pros: Service providers do not need to allocate IPv6 address prefixes specially used for mapping IPv4 addresses from their own IPv6 address resources.

Cons: After the IPv4 address is converted into IPv6 address with WKP, the IPv4 part of the IPv6 address is used for the routing of the origin of the data packet. In this way, many fine routes with prefix length greater than 96 will be introduced into the global IPv6 network. In most networks, fine routing with long prefix length greater than 96 is not supported.

2) NSP: Operator allocates a specific prefix from their existing IPv6 address resources for IPv4 addresses mapping.

Pros: The specific prefix allocated by operators can be considered as an overall prefix, and each PE can obtain IPv6 mapping prefixes allocated from the overall prefix. Within the multi-domain networks, the length of address prefix can be easily tailored to meet the requirements of IPv6 network for routing length, and the routing of the packets can be based on the information of IPv6 prefix part of IPv6 address. Outside the multi-domain network, because the IPv6 mapping prefix has been included in the original IPv6 address prefix, it will not introduce any new routing items and affect the global IPv6 routing system.

Cons: Not found yet.

As mentioned earlier, each PE will be identified by at least one IPv6 mapping prefix, which is used as the basic routing information to forward IPv4-embedded IPv6 packet to the right egress PE. For a given operator, the selection of the length of IPv6 mapping prefix should be given specific consideration. Firstly, the length of the IPv6 mapping prefix should be smaller than the maximum length of the routing prefix that the IPv6-only network specifies, so the PE can successfully announce to its peers via BGP protocol. Secondly, the length of all the IPv6 mapping prefixes should be the same, to avoid unnecessary processing cost and complexity induced by the length diversity.
8. Procedure

This section gives a brief overview of the procedures of the IPv4 service delivery over IPv6-only network. The end-to-end IPv4 data delivery by IPv6-only network includes the following two cases.

1. IPv4 delivery from ingress PE to egress PE

When an ingress PE receives an IPv4 packet from a client-facing interface destined to a remote IPv4 network, it looks up in its mapping rule database to find the mapping rule which best matches the packet's destination IP address. The IPv6 mapping prefix in the mapping rule will help to find another PE, the egress PE. Since this is a multi-domain IPv6-only network, the ingress and egress may belong to different ASes, as shown in Figure 4, the ingress PE1 is in AS 1 and egress PE3 is in AS 3. The ingress PE must convert the IPv4 destination address into IPv6 destination address using the IPv6 mapping prefix of PE3 and forward it to the egress PE. The egress PE then derives the IPv4 source and destination addresses from the IPv4-embedded IPv6 addresses respectively and restore the original IPv4 packet [RFC6052]. Afterwards, the IPv4 packet will be further forwarded according to the IPv4 routing table maintained on the egress. The IPv6 data-path can be shown as below.

IPv6 Data Path

```
| UE/ | CPE1 | PE1 | AS1 | R1 | R2 | AS3 | AS4 | PE3 | AS5 |
```

Figure 4. IPv6 Data Path from Ingress PE to Egress PE

2. IPv4 delivery from UE/CPE to egress PE

Another case is that IPv4 packets may have been transformed into IPv6 packet in UE/CPE, as done by CLAT of 464XLAT[RFC6877], before they reach the edge of the network.

In this case, when receiving an IPv6 packet from a client facing interface, the ingress PE looks up the packet's destination IPv6 address and forward the packet to the egress PE, i.e., PE3. The egress PE then restore the original IPv4 packet, and forwards it
further by looking up its IPv4 destination address. The IPv6 data-

path can be shown in Figure 5. Different from 464XLAT PLAT which needs to maintain session state to perform the stateful translation between IPv6 and IPv4 addresses, the egress PE in this framework to the external IPv4 network is user stateless.

IPv6 Data Path

Figure 5. IPv6 Data Path from UE/CPE to Egress PE

9. Security Considerations

TBD.

10. IANA Considerations

There are no other special IANA considerations.

11. Acknowledgement

The authors would like to thank Brian E. Carpenter, Bob Harold, Fred Baker, Giuseppe Fioccola and Vasilenko Eduard for their review and comments.

12. References

12.1. Normative References

[I-D.ietf-bess-ipv6-only-pe-design]
Mishra, G., Mishra, M., Tantsura, J., Madhavi, S., Yang, Q., Simpson, A., and S. Chen, "IPv6-Only PE Design for IPv4-NLRI with IPv6-NH", draft-ietf-bess-ipv6-only-pe-
design-02 (work in progress), March 2022.


12.2. Informative References

Internet-Draft  Multi-domain IPv6-only Underlay Framework  June 2022


[I-D.ietf-v6ops-ipv6-deployment]  
draft-ietf-v6ops-ipv6-deployment-06 (work in progress), June 2022.  

[I-D.ietf-v6ops-transition-comparison]  

__________________________________________________________________________  
Internet-Draft  Multi-domain IPv6-only Underlay Framework      June 2022  

[IAB-statement]  
"IAB statement",  

[RFC4213]  
Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213,  
DOI 10.17487/RFC4213, October 2005,  

[RFC6333]  

[RFC6992]  
Cheng, D., Boucadair, M., and A. Retana, "Routing for IPv4-Embedded IPv6 Packets", RFC 6992,  
DOI 10.17487/RFC6992, July 2013,  

[RFC7597]  
DOI 10.17487/RFC7597, July 2015,  

[RFC7599]  
Li, X., Bao, C., Dec, W., Ed., Troan, O., Matsushima, S.,

Authors' Addresses

Chongfeng Xie
China Telecom
Beiqijia Town, Changping District
Beijing, Beijing  102209
China
Email: xiechf@chinatelecom.cn

Chenhao Ma
China Telecom
Beiqijia Town, Changping District
Beijing, Beijing  102209
China
Email: machh@chinatelecom.cn

Xing Li
CERNET Center/Tsinghua University
Shuangqing Road No.30, Haidian District
Beijing, Beijing  100084
China
Email: xing@cernet.edu.cn

Gyan Mishra
Verizon Inc
Email: gyan.s.mishra@verizon.com

Mohamed Boucadair
Orange
France