

Network Working Group
Internet Draft
Intended status: Informational
Expires: December 26, 2009

J. Xu
China Telecom
S. Jiang
Huawei Technologies Co., Ltd
B. Carpenter
University of Auckland
June 30, 2009

A Hybrid ISP Framework for IPv6 Services and IPv6/IPv4 Inter-
communication
draft-xu-v6ops-hybrid-framework-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on December 26, 2009.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft [draft-xu-v6ops-hybrid-framework-00.txt](#)

June 2009

Abstract

Global IPv6 deployment is expected. Many solutions have been specified in order to provide IPv6 connectivity service. In order to provide IPv6 connectivity service to all kinds of host/client devices, ISP networks may need to support as many as possible IPv6 connectivity solutions. This document proposes a hybrid ISP framework that supports the coexistence of various IPv6 connectivity solutions and analyses the configuration requirements raised by this framework. Additionally, the applicability of different configuration mechanisms for performing this configuration is discussed.

Table of Contents

1.	Introduction.....	3
2.	Overview of A Hybrid ISP Framework.....	5
3.	APPs/ICPs Involvement.....	6
4.	Configuration Mechanisms.....	7
4.1.	Manual configuration.....	7
4.2.	DHCPv6.....	7
4.3.	Domain Name Service.....	7
4.4.	Others.....	8
5.	Security Considerations.....	8
6.	IANA Considerations.....	8
7.	References.....	8
7.1.	Normative References.....	8
7.2.	Informative References.....	9
	Author's Addresses.....	11

1. Introduction

Global Internet has grown up rapidly in last 25 years. More and more devices are connected to the global Internet infrastructure. Internet Protocol (version 4 [[RFC0791](#)]) played an essential role during the success of the Internet. IPv4 addresses identify the logical location of every device in the Internet so that data packets can be delivered to the right destination. However, giving the fact that the length of IPv4 addresses is only 32 bits, there are fewer than 4 billion available IPv4 addresses, and the address space is used inefficiently. IPv4 address exhaustion is now confirmed to happen soon. The dynamically-updated IPv4 Address Report [[IPUSAGE](#)] has analyzed this issue. It predicts early 2011 for IANA unallocated address pool exhaustion and middle 2012 for RIR unallocated address pool exhaustion. Individual ISPs will experience address shortage at a date depending on their own situation after the RIRs can make no more allocations.

Although there are a number of mechanisms trying to extend the life time of IPv4, the transition of the Internet to Internet Protocol version 6 [[RFC2460](#)] is the only practical and perennial solution to IPv4 address exhaustion. The Internet industry appears to have reached consensus that global IPv6 deployment is inevitable and has to be done quite quickly. IPv4/IPv6 transition, including inter-communication between IPv4 and IPv6, therefore becomes more critical and complicated for the soon-coming global IPv6 deployment.

On the other hand, many solutions have been specified in order to provide IPv6 connectivity service. The most basic is the deployment of dual stack hosts and routers [[RFC4213](#)] including the support of configured IPv6-over-IPv4 tunnels. However, the dual stack approach cannot be sufficient once IPv4 addresses have run out, because it does not allow IPv6-only hosts to communicate with IPv4-only hosts.

Techniques that extend the dual stack model include 6over4 [[RFC2529](#)], 6to4 [[RFC3056](#)], ISATAP (Intra-Site Automatic Tunnel Addressing

The proposed hybrid ISP framework supports the co-existence of hybrid IPv6 connectivity and IPv6/IPv4 inter-communication solutions. It encourages ISPs to work together with Internet Content Providers (ICPs) to provide IPv6 connectivity and IPv6/IPv4 inter-communication service. ISPs provide as much as possible generic support. ICPs can design and implement their application specific interworking mechanisms utilizing their ISP's generic services.

First, ISPs should deploy required resources for offering IPv6 connectivity and IPv6/IPv4 inter-communication solutions in their operational networks. Depending on each solution, the required devices may be located at different network segments. For example, IPv6/IPv4 inter-communication devices should be placed at the edge between IPv4/IPv6 networks. CGNs may be deployed according to the ISP customer aggregation strategy. Application-specific gateways (ALGs) for IPv6/IPv4 inter-communication may be deployed as services by ICP within ISP network too. Each application may have its customized traversal or interworking mechanisms and servers. As noted above,

this is very straightforward for "relay" applications like mail and HTTP proxy.

All information about deployed services, including IP addresses of servers, needs to be collected and distributed to ISP access devices, such as BRAS. Then, this information, include availability information, can be propagated to the host/client devices through standard protocols, which need to be extended, based on existing Dynamic Host Configure Protocol for IPv6 (DHCPv6) [[RFC3315](#)], IPv6 over PPP [[RFC5072](#)], Network Configuration Protocol (NETCONF) [[RFC4741](#)], Simple Network Management Protocol (SNMP) [[RFC3411](#)] or other protocols. Note that IPv6 autoconfiguration is not powerful enough for this purpose.

Based on the availability information received, applications on the host/client devices can choose the IPv6 connectivity services they can use or prefer.

The operating system (OS) on the host/client devices may filter/drop some IPv6 connectivity services according to its own capability. The OS should provide a standard IPv6 connectivity invoking interface for the upper layer applications.

The hybrid ISP framework provides support for as many as possible different IPv6 connectivity solutions. CPEs and host/client devices may need to be configured or updated to get maximum benefit, but they must all get basic connectivity in a standard way.

In order to realise this hybrid ISP framework, there are two technical gaps that need to be filled: configuration mechanisms in which service information could be pushed to the host/client devices; standard IPv6 connectivity invoking interface on the hosts/client devices. The latter is out of scope of this document. The configuration mechanism is discussed below.

3. APPs/ICPs Involvement

This framework assumes applications or ICPs would ideally be aware of IPv4/IPv6 inter-communication; it requests applications or ICPs to choose among the different inter-communication technologies. This seems to be in conflict with the traditional layered network model.

However, the reality is that applications/ICPs, particularly peer-to-peer applications, have already broken the layered network model so that they can traverse the ubiquitous NAT devices. In the IPv4 networks, the existence of NAT breaks the end-to-end transparency. In order to find NATs and traverse them, applications have to understand

network protocols deeply, invoke or interact with network protocols directly and analyse network behaviours by themselves, since the protocol stack on the end user devices is not aware of NATs. Furthermore, since NAT is not standardized, applications have to handle many different NAT technologies.

The scenarios between IPv4-only hosts and IPv6-only hosts are partly similar to above discussed NAT scenarios. Due to the differences, there can not be pure end-to-end transparency between them. Based on this reality, the better way is to standardize IPv4/IPv6 inter-communication technologies, also mechanisms which propagate relevant information from networks to end hosts. Then, applications could learn inter-communication information from the protocol stack on the hosts instead of detecting by themselves. This learning process may be through a standard API between network layer and application layer on the hosts. This design actually maintains the traditional layered network model.

[4. Configuration Mechanisms](#)

There are a number of configuration mechanisms that could be potentially used to propagate IPv6 connectivity service information to the host/client devices.

[4.1. Manual configuration](#)

Manual configuration has already been used in many IPv6 connectivity solutions. However, this method requires expert knowledge for at least first time configuration. Its scalability is quite poor. Its operational burden would be too large when there are many users. Furthermore, this mechanism is very exposed to human errors.

[4.2. DHCPv6](#)

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [[RFC3315](#)] can assign addresses statefully. Besides, DHCPv6 can also be used to distribute other configuration information. DHCPv6 can be extended to propagate IPv6 connectivity service information. A set of new options needs to be developed and their behaviour must be defined clearly.

[4.3. Domain Name Service](#)

For well-known services, certain DNS records may be defined so that host/client devices can resolve their IP addresses through DNS queries using DNS SRV [[RFC2782](#)]. For example, natpt.isp1.example.net can be used to point all ISP1 customers to available NAT-PT servers.

With a suitable DNS mechanism, client load can be distributed among many available servers.

[4.4. Others](#)

According to different access technologies, certain protocols, such as PPPoE or ICMP [[RFC0792](#)], may be extended to propagate IPv6 connectivity service information to subscribers. Note that router and switch configuration protocols such as NETCONF and SNMP are not considered relevant here.

[5. Security Considerations](#)

The security issues for each solution that provides IPv6 connectivity service are discussed in their own specifications. However, further security analysis will be needed to understand whether there are security issues for configuration mechanisms mentioned in this document.

[6.](#) IANA Considerations

This draft does not request any IANA action.

[7.](#) References

[7.1.](#) Normative References

- [RFC0791] J. Postel, "Internet Protocol", [RFC 791](#), September 1981.
- [RFC0792] J. Postel, "Internet Control Message Protocol", [RFC 792](#), September 1981.
- [RFC2460] S. Deering, et al., "Internet Protocol, Version 6 (IPv6) Specification", [RFC2460](#), December 1998.
- [RFC2529] B. Carpenter, C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", [RFC 2529](#), March 1999.
- [RFC2765] E. Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)", [RFC 2765](#), February 2000.
- [RFC2782] A. Gulbrandsen, P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", [RFC2782](#), February 2000.
- [RFC3053] A. Durand, P. Fasano, I. Guardini, D. Lento, "IPv6 Tunnel Broker", [RFC3053](#), January 2001.

- [RFC3056] B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", [RFC 3056](#), February 2001.
- [RFC3315] R. Droms, et al., "Dynamic Host Configure Protocol for IPv6", [RFC3315](#), July 2003.
- [RFC3411] D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for

Describing Simple Network Management Protocol (SNMP) Management Frameworks", [RFC 3411](#), December 2002.

- [RFC4213] E. Nordmark, R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", [RFC4213](#), October 2005.
- [RFC4741] R. Enns, et al., "NETCONF Configuration Protocol", [RFC 4741](#), December 2006.
- [RFC5072] S.Varada, Ed., D. Haskins, E. Allen, "IP Version 6 over PPP", [RFC 5072](#), September 2007.

7.2. Informative References

- [RFC2663] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", [RFC 2663](#), August 1999.
- [RFC2767] K. Tsuchiya, et al., "Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)", [RFC 2767](#), February 2000.
- [RFC3089] H. Kitamura, "A SOCKS-based IPv6/IPv4 Gateway Mechanism", [RFC3089](#)", April 2001.
- [RFC3142] J. Hagino, "An IPv6-to-IPv4 Transport Relay Translator" [RFC 3142](#), June 2001.
- [RFC3338] S. Lee, et al., "Dual Stack Hosts Using Bump-in-the-API (BIA)", [RFC 3338](#) October 2002.
- [RFC4966] C. Aoun and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", [RFC 4966](#), July 2007.
- [RFC5214] F. Templin, T. Gleeson, and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", [RFC 5214](#), March 2008.
- [IPUSAGE] G. Huston, IPv4 Address Report, March 2009, <http://www.potaroo.net/tools/ipv4/index.html>.

- [6RD] R. Despres, "IPv6 Rapid Deployment on IPv4 infrastructures (6rd)", [draft-despres-6rd](#), working in progress.

- [PortRange] B. Storer, et al., "IPv4 Connectivity Access in the Context of IPv4 Address Exhaustion", [draft-boucadair-port-range](#), work in progress.
- [PRv6] M. Boucadair, et al., "Flexible IPv6 Migration Scenarios in the Context of IPv4 Address Shortage", [draft-boucadair-behave-ipv6-portrange](#), work in progress.
- [DSLite] A. Durand, et al., "Dual-stack lite broadband deployments post IPv4 exhaustion", [draft-ietf-softwire-dual-stack-lite](#), working in progress.
- [ICGN] S. Jiang, et al., "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition" [draft-jiang-v6ops-incremental-cgn](#), working in progress.
- [NAT64] M. Bagnulo, et al., "NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", [draft-bagnulo-behave-nat64](#), work in progress.
- [TURN] G. Camarillo and O.Novo, "Traversal Using Relays around NAT (TURN) Extension for IPv6", [draft-ietf-behave-turn-ipv6](#), working in progress.

Author's Addresses

Jianfeng Xu
China Telecom
No.109, West Zhongshan Street, Tian-He District, Guangzhou 510630
P.R. China
Phone: 86-20-38639112
EMail: xujf@gsta.com

Sheng Jiang
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxu Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82836774
EMail: shengjiang@huawei.com

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand
Email: brian.e.carpenter@gmail.com