

IPvX: IPv4 with 128 bit Address Space
An informationally assured way to expedite AAAA DNS
addresses with IPv4 coexistence
==== DRAFT ==== Version 7 August 23, 2010 ==== DRAFT =====

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026: 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.

Discussion and suggestions for improvement are requested. Distribution of this draft is unlimited. This document will expire before December 2010.

1. Introduction

1.1. Motivation

There are several challenges facing the Internet.

IPv4 addresses are becoming scarce.

There is a great deal of IPv4 infrastructure that is working and would be expensive to replace.

The IPv6 network defense infrastructure is not mature and well-tested.

This paper provides a draft overview of IPvX. IPvX makes use of a simple extension of address space using the available space in the option field of the IPv4 header. It draws on some concepts of RFC 1385, The Extended Internet Protocol[1], for the use of the IPv4 option space and some concepts to maximize forward compatibility with IPvX, and backward compatibility with IPv4.

1.1.1. IPv4 Address Exhaustion

The IPv4 address exhaustion was an concern back in the early 1990's[2,3]. In response to this, work was done to provide

solutions[4-8].

1.1.2. IPv4 Infrastructure and Backward Compatibility

The success of the Internet exceeded the expectations of most network research scientists. The Internet is now being used for various purposes, such as banking, health care, public safety, entertainment and social networking. It has grown far beyond a research interest. There is a significant amount of IPv4 infrastructure, some, of which, cannot be easily replaced. Because of this, any practical solution to these problems should be compatible with today's software and hardware as much as possible.

1.1.3. IPv6 Network Defense Infrastructure

The network defense infrastructure for IPv6 is not mature and well-tested[9]. IPv4 deployment had several growing pains and security issues [10-12]. It is important to avoid security "surprises" that come with a full-out IPv6 deployment. Full IPv6 roll out is not viable for security reasons.

1.2. Goals of IPvX

IPvX is being proposed to do the following:

- (1) Facilitate the transition to AAAA, or 128 bit, DNS records
- (2) Provide for operation and development of 128 bit applications in a mixed and interoperable IPv4 and IPvX.
- (3) Maintain healthy operation of IPv4 while efficacious to individual organizations
- (4) Allow the move to 128 bit addressing while not requiring changes to IPv4 networks.
- (5) Allow secure coexistence of 128 bit IPvX and IPv4 networks.
- (6) Encourage the use of secure DNS systems.
- (7) Provide an easy migration to IPvX leveraging the network security features and operation of IPv4.

1.2.1. Discussion of the Goals of IPvX

This proposal seeks to take advantage of the success of the Internet Protocol Suite, the greatest part, of which, is probably the flexibility of IP itself. There is a reasonable understanding of attack surfaces of the IPv4 protocol that is leveraged in this proposal. The intent of IPvX is to use the features and capabilities of IPv4, maintain current working infrastructures, while moving to the AAAA, or 128 bit, DNS records. The additional address space will

provide the needed for the growth of the Internet. In addition, the IPvX address will use the IPv6 addressing conventions (RFCs), when advantageous.

Like the transition from FM mono to FM stereo and from black and white television to color television, this RFC proposes a mechanism to allow the end-user network to use IPv4 as long as is economically viable or desired and to transition to IPvX when desired, with, at least, the same information assurance than before, without the end-user having to do anything new. The effort of the migration and adaptation is placed where it belongs:

At an organization capable of setting up and maintaining DNSsec service and capable of providing a high performance IPv4/IPvX Network Address Translation (NAT) service for its users within its border network. This activity, henceforth, will be called the IP Super Center (ISC).

Examples of an ISC would be the Internet Service Provider (ISP), large universities, or large organizations with a similar network administration staff.

Using most of the IPv6 address space allows the use of some of a 128 bit addressing schemes without the added challenge of necessitating a dual stack operation for every node and host, which more than doubles the complexity of computer system, network, and security administration. In addition, this RFC strongly suggests using DNSsec as a necessary component, further reducing exposure to malicious DNS attack vectors.

2. Advantages

The advantages of IPvX are similar to those articulated in RFC 1385[1] and are repeated for emphasis. IPvX has the following advantages:

- (1) It allows the Internet to have a 128 bit address space that appears to be the most pressing requirement of today's networks.
- (2) It reduces the amount of modifications to current systems and greatly ease the difficulties in transition. In particular, it does not require the upgraded hosts and subnet routers to run two set of protocols in parallel
- (3) It requires no changes to all assigned IPv4 addresses and subnet structures in local area networks, and
- (4) It requires no modifications to ARP/RARP, ICMP, TCP/UDP checksums in the IPv4 header

- (5) It allows IPv4 hosts to communicate with any hosts in other networks via a simple address translation service, during the transition period.
- (6) It eases the difficulties of transition by not requiring upgrades to networks behind the ISC.
- (7) It provides trivial mechanism for IPv4 to IPvX within a subnet
- (8) It provides appropriate IPv4 and IPvX intercommunication mechanisms.

3. Assumptions

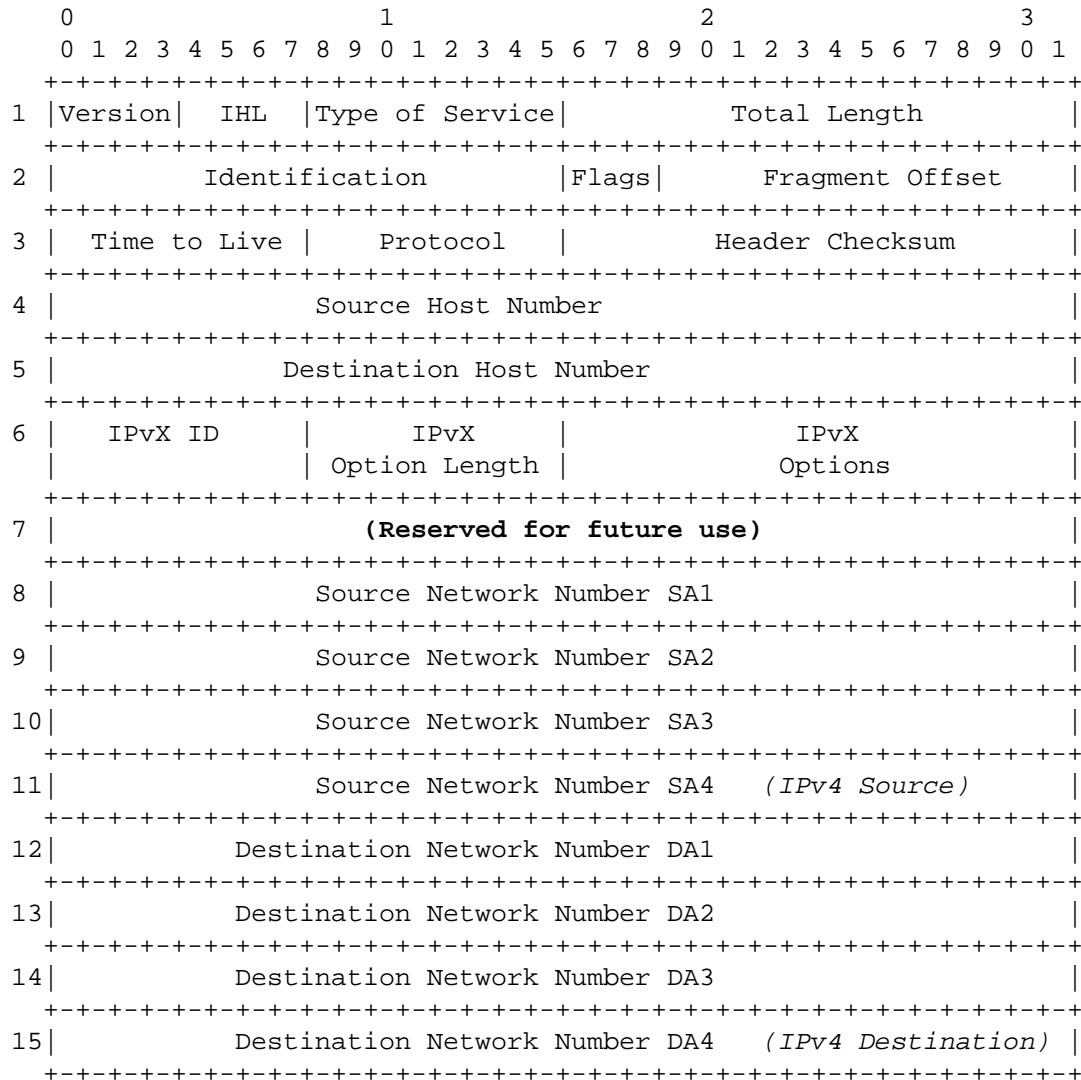
- (1) An IPvX address is a combination of the network portion of a valid IPv6 address with a valid public IPv4 address in the last four octets of the 128 bit address field.
- (2) An organization wants to address of all of its hosts but may not want all external networks to address all of the organization's hosts.
- (3) An organization does wants very few, if any, IPv6 hosts to be able to tunnel through its defensive systems in order to communicate with an IPv4 system.

4. IPvX Components

4.1. IPvX Header: Simple use of IPv4 Option Space

The IPvX Header is in Figure 1 below. The Option Space of the IPv4 header is more than sufficient to hold 128 bit addresses. Careful use of the 128 bit addresses is required. A portion of the Option Space will carry a **SOURCE-EXTENDED** address and a **DESTINATION-EXTENDED** address.

Figure 1: IPvX Header



4.1.1.1. Fields of the IPvX Extension

Field	Bits	Description
Version	4	The Version field is identical to that of IPv4. It is set purely for compatibility with IPv4 hosts.
IHL	4	Internet Header Length is identical to that of IPv4. It is set to the length of IPvX header purely for compatibility with IPv4.

Type of Service	8	The ToS field is identical to that of IPv4.
Total Length	16	The Total Length field is identical to that of IPv4.
Identification	16	The Identification field is identical to that of IPv4.
Flags	3	The Flags field is identical to that of IPv4.
Fragment Offset	13	The Fragment Offset field is identical to that of IPv4.
Time to Live	8	The Time to Live field is identical to that of IPv4.
Protocol	8	The Protocol field is identical to that of IPv4.
Header Checksum	16	The Header Checksum field is identical to that of IPv4. This is used for the IPv4 nodes. However, the IPvX Checksum at the end will be used by IPvX nodes for speed of processing.
Source Host Number	32	The Source Host Number field is used for identifying the source host but is unique only within the source network (the equivalent of the host portion of the source IPv4 address). This address will be used in the local networks behind the ISC to provide interoperability and an economic path toward migration to IPvX.
Destination Host Number	32	The Destination Host Number field is used for identifying the destination host. This is used like the Source Host Number above, except for destination addresses.
IPvX ID	8	The IPvX ID field equals to 0x8A or 1 00 01010 . The IPvX ID value is chosen in such a way that, to IPv4 hosts and IPv4 routers, an IPvX appears to be an IPv4 packet with a new IPv4 option of following parameters from the IPv4 specification: 1 00 01010 has the meaning given below
IPvX Option Length	8	The IPvX Option Length field is 40 , or the maximum, needed for the dual 128 bit addresses with availability for options and Reserved areas.
<i>Reserved for future use</i>	8	This is reserved for future use.
<i>Reserved for future use</i>	32	This is reserved for future use. This could possibly be moved to the end for a rapid checksum operation, however, the pseudoheader checksum will be used as in IPv6.
Source Network Number	128	The first three 32 bit words (8-10) are the source network number. The last 32 bit word (word 11) is the old source IPv4 address while IPv4 address space is not exhausted.
Destination Network Number	128	The first three 32 bit words (12-14) are the destination network number. The last 32 bit word (word 15) is the old destination IPv4

address while IPv4 address space is not exhausted.

		Meaning of 1 00 01010	
1	00	01010	
copy bit set	Class is Control	Option is a new value	

4.1.2. Header Compatibility Features

The IPvX header has the following compatibility features:

- (1) IPvX achieves maximum backward compatibility with IPv4 by making the extended space appear to be an IPv4 option to the IPv4 hosts and routers that can be ignored by them, while being the new 128 bit address for the IPvX nodes, using some of the appropriate IPv6 addressing conventions, for Internet communications.
- (2) When an IPv4 host receives an IPvX packets, the IPvX addresses are safely ignored as it appears to the IPv4 hosts as an new IPv4 option. So an IPvX packet destined to an IPv4 host arrives without a need for subnet routers to be upgraded during the transition period.
- (3) The value in the IPvX ID field allows the IPvX hosts or routers to determine whether a packet is an IPv4 packet or an IPvX packet. Because the IPv4 source and address fields are populated, the IPv4 routers can act on the packet.
- (4) In IPvX, the **Network Numbers** and **Host Numbers** are separate. The IPv4 address field is the **Host Number** and the IPvX address, or the 128 bit address in the IPv4 option field, is the **Network Number**. It is comprised of an assigned IPv6 network address, with the last four octets being the IPv4 address.
- (5) The **Host Number** has meaning within a local network behind and ISC. Outside of the ISC, the **Host Number** is the routed address, to maintain compatibility with IPv4 routers.
- (6) For the reasons expounded in the IPv6 RFC, there will be no checksum in the extended address field.

4.1.3. Host Number Compatibility Features

The **Host Number** concept has the following advantages:

- (1) It maintains full compatibility between IPv4 hosts and IPvX hosts for communications within one network.

Note: The **Network Number** is not needed, initially, for communications within a network. It can be used at a later phase

of implementation (see transition to IPvX below). A host can omit the Extension field if it does not need any other information in the Extension field, when it communicates with another host within the same network [*Possibly even over an IPv4 network*].

- (2) It allows the IPv4 subnet routers to route IPvX packet by treating the **Host Number** as the IPv4 address during the transition period, therefore the **subnet routers are not required to be updated along the ISCs**.
- (3) It allows ARP/RARP to work with both IPvX and IPv4 hosts without any modifications.
- (4) Network Address Translation (NAT), or port translation can occur from the ISC to as far back in the customer network as is judged desirable from a economic and/or security standpoint. During the transition period when the IPv4 addresses are still unique, the network portion of the IPv4 addresses can be directly extracted and mapped to the last 32 bits of the IPvX Network Numbers. At the point there are no more IPv4 machines on the Internet, this will not be an issue.

4.2. IPvX Super Center (ISC)

The IPvX Super Center (**ISC**) is any border area device that does the following:

- (1) Supports IPvX
- (2) Can easily implement DNSsec
- (3) Has the ability to perform NAT/PAT functions between IPv4 addresses and IPvX addresses for all devices behind it.

5. Migration

Changes to a system are as follows:

- (1) An **ISC** must be added if the site wishes to move to 128 bit addresses
- (2) If a site cannot run an **ISC**, it joins an Internet Service Provider with one.
- (3) 128 bit DNS entries must be made for hosts with the **ISC** network prefix prepended for those choosing the IPvX service

No other changes should be necessary in the interim.

6. IPvX Network Operation

Figure 2, below, illustrates the basic operation of IPvX.

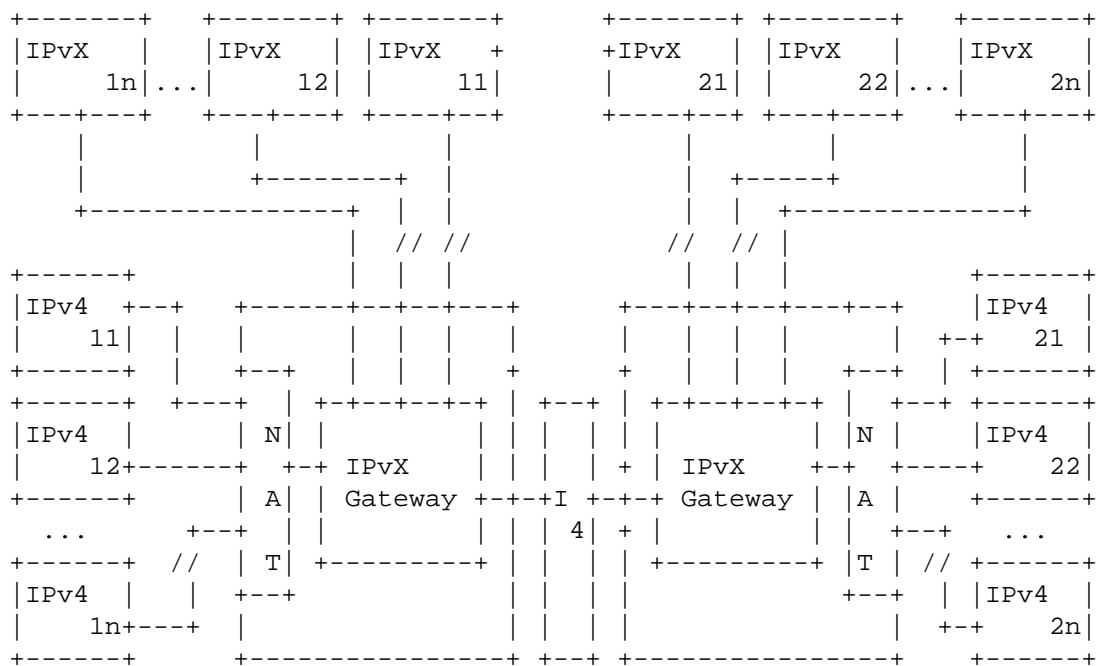


Figure 2 - Overview of IPvX

The node types are given in the *IPvX Network Node Types* section.

6.1. IPvX Network Node Types

For this section and following sections, the following nodes are defined:

H(xy) is an IPv4 node **y** in an IPvX network **x**

F(xy) is an IPvX node **y** in an IPvX network **x**

ISCx is the IP Super Center for network **x**

7. Transition to IPvX

In this section, we outline a plan for transition to IPvX. It is very similar to what was proposed in RFC 1385.

IPvX greatly reduces the complexity of transition.

- (1) There is no need for the updated hosts and subnet routers to run two protocols in parallel in order to achieve interoperability between old and new systems.

- (2) During the transition, IP hosts can still communicate with any machines in the same network without any changes.
- (3) When the IPvX Host Numbers (i.e., the 32-bit IP addresses) are still globally unique, IP hosts can contact hosts in other networks via translation service provided in the border routers.

The transition proceeds as follows:

7.1. Phase 0:

- a) Using the IPv6 addressing scheme with the exception that the last 32 bit word is reserved for the IPv4 address, implement the routing protocol.
- b) Assign new **Network Numbers** to existing networks.

7.2. Phase 1:

- a) Update all backbone routers and border routers.
- b) Update DNS servers.
- c) Start translation service.

7.3. Phase 2:

- a) Update first the key hosts such as mail servers, DNS servers, FTP servers and central machines.
- b) Update gradually the rest of the hosts, when economically and safe to do so.

7.4. Phase 3:

- a) Update subnet routers.
- b) Withdraw the translation service.

The translation service can be provided as long as the Host IDs (i.e., the 32-bit IP address) are still globally unique. When the IP address space is exhausted, the translation service will be withdrawn and the remaining IP hosts can only communicate with hosts within the the same network. At the same time, networks can use any numbers in the 32-bit space for addressing their hosts.

8. References

- [1] "EIP: The Extended Internet Protocol A Framework for Maintaining Backward Compatibility", Z. Wang, Request for Comments 1385, November 1992.
- [2] Chiappa, N., "The IP Addressing Issue", Work in Progress, October 1990.

- [3] Clark, D., Chapin, L., Cerf, V., Braden, R., and R. Hobby, "Towards the Future Architecture", RFC 1287, MIT, BBN, CNRI, ISI, UC Davis, December 1991.
- [4] Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Cisco, Nokia, December 1998
- [5] "The IAB Routing and Addressing Task Force: Summary Report", work in progress. Ross Callon, Request for Comments 1347, June 1992
- [6] "Supernetting: An Address Assignment and Aggregation Strategy", V.Fuller, T.Li, J.Yu, and K.Varadhan, March 1992.
- [7] "Extending the IP Internet Through Address Reuse", Paul Tsuchiya, December 1991.
- [8] "TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing", Ross Callon, Request for Comments 1347, June 1992
- [9] Potyraj, C., "Firewall Design Considerations for IPv6", National Security Agency Report # I733-041R-2007, October 3, 2007.
- [10] Bellovin, S.M., "Security Problems in the TCP/IP Protocol Suite" AT&T Bell Laboratories, Murray Hill, New Jersey 07974
- [11] Bellovin, S. M., "Security problems in the TCP/IP protocol suite", In Annual Computer Security Applications Conference, December 2004.
- [12] Bellovin, S. M., "Security problems in the TCP/IP protocol suite", Computer Communications Review, 19(2):32-48, April 1989

9. Acknowledgments

The authors would particularly like to thank the following people for their code, data, information and knowledge: Rick Graham, James Ragucci, and Raphael Mudge.

10. Author's Addresses

William J. Chimiak
Laboratory for Telecommunication Sciences
8080 Greenmead Drive
College Park, MD 20740
301-422-5217

+1-301-422-5217
mailto:w.chimiak@ieee.org

Table of contents

Status of this Memo	1
1 Introduction	1
1.1 Motivation	1
1.1.1 IPv4 Address Exhaustion	1
1.1.2 IPv4 Infrastructure and Backward Compatibility	2
1.1.3 IPv6 Network Defense Infrastructure	2
1.2 Goals of IPvX	2
1.2.1 Discussion of the Goals of IPvX	2
2 Advantages	3
3 Assumptions	4
4 IPvX Components	4
4.1 IPvX Header: Simple use of IPv4 Option Space	4
4.1.1 Fields of the IPvX Extension	5
4.1.2 Header Compatibility Features	7
4.1.3 Host Number Compatibility Features	7
4.2 IPvX Super Center (ISC)	8
5 Migration	8
6 IPvX Network Operation	9
6.1 IPvX Network Node Types	9
7 Transition to IPvX	9
7.1 Phase 0:	10
7.2 Phase 1:	10
7.3 Phase 2:	10
7.4 Phase 3:	10
8 References	10
9 Acknowledgments	11
10 Author's Addresses	11