Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2009

R. Despres
November 3, 2008

Stateless Address Mappings (SAMs)
IPv6 & extended IPv4 via local routing domains - possibly multihomed
draft-despres-sam-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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/1id-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 May 7, 2009.

Abstract

Stateless Address Mapping (SAM) is a generic technique to achieve global IPv4 or IPv6 connectivity across local domains where routing is in a different address space. To cope with the IPv4 address shortage, it supports an extension of IPv4 addresses with dynamic-port prefixes. For multi-homed routing domains, it ensures that source addresses that cross domain borders are always routable in the reverse direction (Reverse Path Forwarding). SAM can be used alone as an alternative to NATs, to improve scalability and end-to-end network transparency, or in combination with NATs, to cover a wider range of IPv4-IPv6 coexistence scenarios.

Table of Contents

1. Introduction

Stateless Address Mapping (SAM) is a generic technique to achieve global IPv4 or IPv6 connectivity across local domains where routing is in different address spaces.

The problem statement of Section 2 introduces the context that justifies a SAM approach, and discusses why another approach than NATs is worth standardizing.

Section 3 describes the ~~the~~ proposed specification. It is understood that further work is needed to clarify and polish it, ~~T~~but it is expected to be complete enough to start experimenting with it.

In designing SAM, high attention has paid to algorithmic simplicity and to application generality. It can be viewed as a generalization of [6rd], which itself is derived from the 6to4 of [RFC3056] and of the ISATAP of [RFC5214]. It can also be viewed as an application of a variant of the map and encap principle of [RFC1955], and of a variant of the locator/identifier separation principle of [LISP].

2. Problem Statement

2.1. Existing Internet address spaces

The Internet has two global address spaces, IPv4 and IPv6. A host in a local routing domain that wants to send a packet to an arbitrarily located remote host has to provide its global address.

Comment [DT1]: "obtain the destination address" (it need not be "global" per se)

Due to the lack of IPv4 addresses for all hosts, Internet uses also extensively, in private networks and in some operator networks, IPv4 private addresses [RFC1918]. Network address translations (NATs) are placed at borders between these networks and the global Internet.

Although the need to share global addresses is not pressing in IPv6 as it is in IPv4, considerations on ease of renumbering have le~~a~~d to having~~e~~ private addresses also in IPv6 (ULAs of [RFC4193]).

Standardized solutions are needed for global connectivity to be maintained across routing domains that use private address spaces.

2.2. IPv4 address shortage

Because ~~of~~ a shortage of global IPv4 addresses is now unavoidable before all hosts can support IPv6, global IPv4 addresses will have to be shared among more and more hosts.

They are shared today among hosts of private sites by means of NATs at site entrances, and between mobile phones by means of NAT~~s~~ infrastructures of typical mobile phone operators. Some NATs are even cascaded to increase the statistical efficiency of NAT address sharing.

Assigning an exclusive global IPv4 address to a broadband residential site becomes more and more a luxury, which will have to be charged for. Ordinary customers will have to share more and more with others global IPv4 address they need to communicate in IPv4. More and more devices within ISP infrastructures will therefore have to manage this sharing, one way or another.

Comment [DT2]: Can't parse grammar

2.3. Need for Multihomed routing domains

A routing domain is multihomed if it has several interfaces to the global Internet, typically to different ISPs.

SHIM6 and SCTP are designed to take advantage of such a possibility, in particular to maintain connectivity in case of a single interface failure, but a difficulty remains. Because of the reverse path forwarding principle (RPF) of [RFC3704], hosts of multihomed domains must influence which interface to the global Internet their outgoing packets go through depending on which source address they use. SAMs have to make this possible.

2.4. Translation and Mapping approaches

Where a global packet has to traverse a routing domain having a different address space, two main possibilities exist:

1. A NAT translates the packet. Depending on conditions, the translation may involve several consecutive packets, and may go up to the application layer. It is not in general reversible outside the NAT that did the translation.

2. A SAM derives a locally routable destination address from the global destination address, and encapsulates the global packet to forward it.

Comment [DT3]: I could not understand what a SAM was supposed to do until I got all the way to the pictures in section 4. Suggest moving some topology diagram(s) up into the problem statement section.

Advantages of NATs include the following:

- With the NAPT variant (which translate [address, port] ~~eo~~tuples rather than just addresses), addresses are shared statistically so that their~~e~~ use would in general be more optimized than with static sharing.

- Hosts attached to local routing domains don't need to be dual-stack. They may ignore which is the global address family of remote hosts they communicate with.

Expected advantages that justify SAM deployment include:

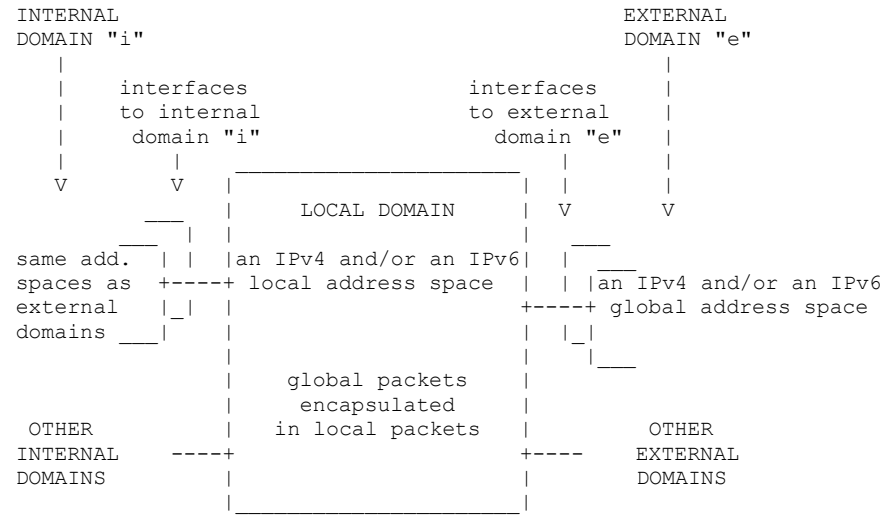
- Good scalability (no need to keep track of transport layer connections)
- End-to-end network transparency: no need for application level translation of addresses exchanged as data; compatibility with transport protocols that use more sophisticated redundancy checks than that of UDP and TCP.
- No DNS implication: global addresses are the only ones to be advertised.
- Functional simplicity (stable specification, low development and operational costs)

The purpose of this document is to propose a specification for the SAM alternative.

3. SAM specification

3.1. Interfaces of SAM local domains

As illustrated in Figure 1, A SAM operates on a local domain which has interfaces to one or several external domains, and to a number of internal domains.



INTERFACES AND ADDRESS SPACES OF SAM DOMAINS

Figure 1

The local domain may be an ISP network, or part of it, or a privately owned network, also in whole or in part.

External domains are in the direction of the global Internet, while internal domains are in the direction of hosts that access the global Internet via the local domain.

A local domain performs its local routing in IPv4, in IPv6, or in both. In each of the two address families it may route in the global address space or in a private address space.

A SAM local domain may support several SAMs. Each one maps a subset of a global address space, to a local address space. In case of a multihomed domain, there may be several mappings from the same global address space.

3.2. SAM Address Spaces

SAMs see global addresses of internal hosts as composed of the global prefix P of the local domain, followed by the local identifier L of the internal domain of the host, followed by a suffix which can be exploited within this internal domain.

3.2.1. Private address (v4P and v6P)

Local address spaces SAMs deal with are the following:

- Private IPv4 (v4P)
- Private IPv6 (v6P)

The v4P address space is that of [RFC1918]. (Addresses addresses have one one of the following prefixes: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/24.)

The v6P address space is that of [RFC4193]? (Addresses have the fc00::/7 prefix).

3.2.2. Non-extended global address spaces (v4G and v6G)

Non-extended global address spaces SAMs deal with are the following:

- Non-extended global IPv4 (v4G)
- Non-extended global IPv6 (v6G)

The non extended global IPv4 address space is~~t~~ the total IPv4 address space minus private addresses of v4P.

The non-extended global IPv6 address space is~~t~~ the total IPv6 address space, minus addresses of v6P, and minus addresses that have in their lower 64 bits an invalid IID. (A valid IID has, in its first octet, either bit 6 is 0 (local significance of the 64-bit IID) or bits 6-7 are "10" (global significance of the 64-bit IID, with an individual organization identifier in other bits of the first 3 octets in EUI-64 format).

Comment [DT4]: Per RFC 4291, this is only true for IPv6 addresses that don't start with binary 000.

3.2.3. Extended IPv4 global address space (v4E)

In the v4E address space, a subnetwork prefix or a host address is a global IPv4 address extended by a port prefix.

In order to avoid interfering with specific interpretations of well known and registered ports (0 to 49,151), only dynamic port numbers are exploited for address extension (49,152 to 65,535).

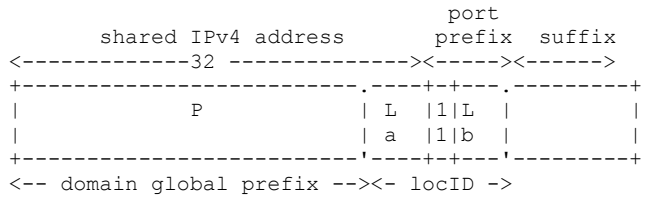
A v4E prefix, always longer than~~t~~ 32 bits, never appears as such in a field of a packet. It is only used to derive from it a local address to be put in an encapsulating packet.

A v4E address can only be used with protocols that use port numbers.

This includes UDP, TCP, DCCP, SCTP, and ICMPv4 unreachability messages in which headers of discarded packets are copied with heir port numbers.

Comment [DT5]: You should point out what common things will break. For example, this means you cannot ping such a node.

Figure 2 illustrates the format of a v4E address, as it is seen in a local domain of prefix P, in the case where the local identifier L spans the address-port boundary. In this case, L has three parts: La and Lb are the useful parts of L to construct the internal domain locator, and bits 0-1 of the port prefix are constant.



V4E ADDRESS FORMAT

Figure 2

Note: the fact that a host having a v4E address may only use some dynamic ports for its incoming connections is not new. Using an SRV record to advertise a dynamic port in the DNS already used in Apple's technology [Bonjour].

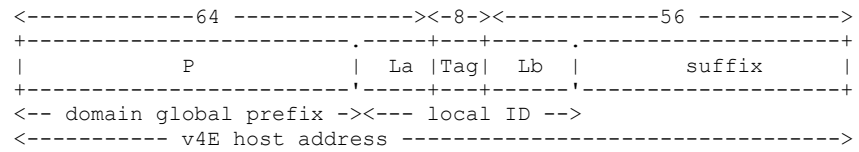
3.2.4. Extended IPv6 global address space (v6E)

An extended IPv6 address format may also be used by SAMs to extend subnet addressing beyond 64 bits. Thus, a private site that has only a /64 (typical for some mobile phones, considered ~~as~~ as independent sites) can thus support several subnets.

Comment [DT6]: Not completely, no. Some of the same issues in RFC 4903 still apply. For example, the required Subnet-Router anycast address (RFC 4291 section 2.6.1) may not work correctly.

The 9th octet is reserved for a v6E tag. Its bits 4-7 are 0xF. This value differs from any value found in v6G addresses. (Bits 6-7 are "00, "01"" or "10" in standard 64-bit IIDs, as detailed in Section 3.2.2). Bits 0 is used for the privacy option of Section 3.6. Other bits are reserved for extensions, of SAMs or others.

Figure 3 illustrates the format of a v6E address, as it is seen in a local domain of prefix P, in the case where the local identifier L spans the 64-IID boundary. In this case, L has three parts: La and Lb are the useful parts of L to construct the internal domain locator, and the .



V6E ADDRESS FORMAT

Figure 3

3.3. The four parameters of a SAM (P, H, E, n)

Each SAM is defined by 4 parameters, P, H, E, and n, where :

- "P" is, in the local-domain global prefix. It is the prefix that, in the global address space, identifies the local domain.
- "H" is the header that is at the beginning of all internal-domain local prefixes.
- "E" is the local anycast address that, in the local domain, is routed toward interfaces to the SAM external domain.
- "n" is the length of local identifiers in the local domain. (The number of possible internal domains is 2 ^ n).

The global address space of a SAM is v4E if E is IPv4 and if p + n exceeds 32, where p is the length of P.

These parameters must at least be administratively configurable. It should also be possible to configure SAM parameters of internal interfaces automatically, e.g. with ad hoc DHCP and DHCPv6 options. Specifying such options is beyond the scope of this document but is easy.

3.4. Mapping rules

3.4.1. Packet encapsulation-decapsulation

Mapping a global packet into a local packet, at its entry to a local domain, is done in the following steps:

1. If the packet is a fragment of an incomplete packet, proceed as indicated in Section 3.5, and proceed.
2. Check that the source global address is realistic at this interface (is not obviously spoofed).

Comment [DT7]: Without a topology picture, this is hard to follow, is this talking about entry from a host, or from the Internet?

3. Find which SAM applies, if any. For this, find the SAM the global prefix P of which matches the internal host address.

4. Derive local source and destination addresses from source and destination global addresses according to Section 3.4.2.

5. Encapsulate the global packet into a local packet having the source and destination derived addresses, and having the protocol field set to 41.

Extracting the global packet contained in a local packet having protocol 41 is done in the following steps:

1. Check that the source address is realistic at this interface (is not obviously spoofed)

2. Check that source and destination addresses of the local packet are, according to Section 3.4.2, those that are derived from source an destination addresses of the encapsulated packet, and that the source address is realistic at this interface (is not obviously spoofed).

3.4.2. Address mappings

The local address mapped from the global address of an external host is the local anycast address E of the SAM .

The local address derived from the global address of an internal host is obtained as follows:

1. Obtain the "local identifier" L of the local domain in p to p+n of the global address).

2. If L contains a constant field of the global address, delete it.

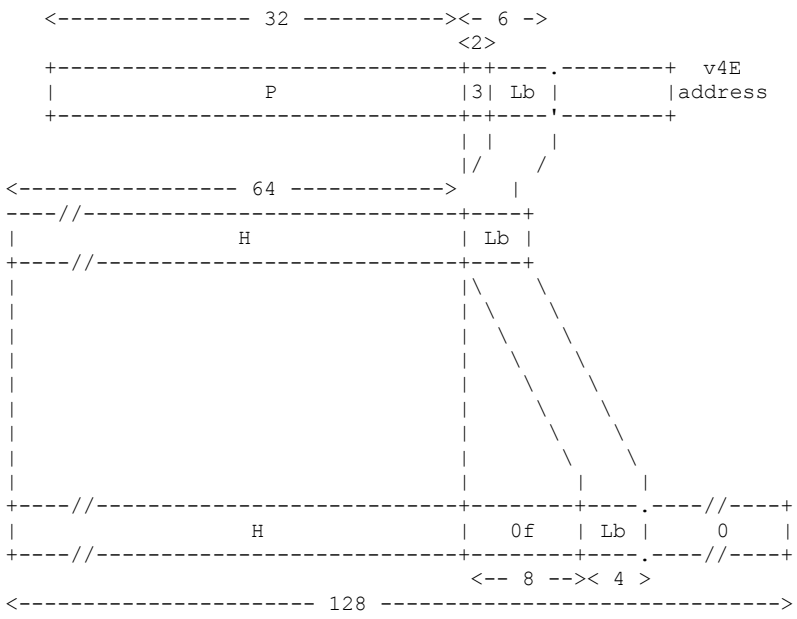
3. Add the header H in front of it.

4. If the local address space is IPv6, add to the ~~the~~ just obtained prefix zeroes up to 120 bits, and insert the 8-bit v6E tag.

5. Else, i.e. if the local address space is IPv4, the header H is normally chosen such that the just obtained prefix has 32 bits. If it has been found useful to have it shorter, complete to 32 bits with zeroes.

Figure 4 illustrates a particular case case where constant fields have to be both deleted and added (a v4E global address mapped to an IPv6 local address).

Comment [DT8]: 41 is for when IPv6 is the inner header. However figures 7 and 8 shows that IPv4 can be inside, in which case it should be protocol 4.



AN EXAMPLE OF V4E GLOBAL PREFIX TO LOCAL ADDRESS MAPPING

Figure 4

3.5. Fragmentation support

Fragmentation is needed when a datagram is too long to fit in the maximum path transmission unit between source and destination hosts (PMTU). TCP has evolved to avoid using fragmentation, but some UDP based applications do use it.

Since SAMs encapsulate global packets, including all fragmentation related information they may contain, destination hosts have all they need to reassemble fragmented datagrams.

Within local domains, precautions must be taken so that no fragmentation of encapsulating packets is needed. (An IPv6 packet of 1280 octets encapsulated with an IPv6 IP header of 40 octets fits largely in generally supported packet sizes.) At its interfaces, a local domain is assumed to discard incoming packets that exceed its supported MTU (and return error ICMP messages to sources).

If global packets are v4G or v6G, address mappings are only based on addresses. They can therefore be performed packet per packet.

If global packets are v4E, a mechanism is needed to forward packets of fragmented datagrams. Since port numbers appear only in the first fragment, the SAM has to record it for reuse when subsequent packets of the same datagram will have to be mapped. These packets being identified by the source address SA and the identification field IF of the IPv4 datagram, a table entry is needed to match the port prefix PP to the [SA, IF]. The entry is created when the first fragment is processed. It is discarded when the last fragment (having the "more fragments" bit = 0) is processed or, for to deal with last fragment losses, after a timeout expires since the last fragment reception.

Comment [DT9]: What is the value?

This mechanism works only if fragments of a same datagram enter a local domain at its same interface, and in their original order. Changing from one interface to another in the middle of a fragmented datagram is acceptable only if it is infrequent, e.g. when routing information bases need to be changed. (If upstream routing would alternate among several interfaces on a per packet basis, the effect would normally be unacceptable but, this problem not being exclusive of SAMs, routing may be assumed to be stable enough in real networks.)

Comment [DT10]: Unfortunately, this is not a safe assumption today. See draft-iab-ip-model-evolution-01.txt section 3.1.7

3.6. On demand privacy protection

IPv6 end-to-end (i.e. without NAT traversal) is the only way to restore both global reachability, at stable address and ports without port restrictions, and the end to end packet preservation which is needed for transport protocols that apply a stronger checksum algorithm than the 16-bit one's complement of UDP and TCP (e.g. SCTP).

On the other hand, NATs are known to provide some privacy protection because individual hosts behind NATs cannot be identified from the outside and because, behind NATs, private routing topologies are hidden. There are consequently some advocates for the deployment of IPv6 to IPv6 NAT to be endorsed by IETF (NAT66s). Without strong caveats, and restrictions on what these NAT66s would do, this could break confidence in IPv~~v~~6 end-to-end capabilities, and encourage a longer use of IPv4, with its NATs and NAT cascades.

Comment [DT11]: IPv6 privacy addresses (RFC4941) provide this in IPv6. Specifically, since a host can have many such IPv6 addresses, you cannot distinguish between one host with many addresses, and several hosts with several addresses each, on the same subnet.

It is therefore proposed to limit address and port translations to outgoing connections of internal hosts that use privacy addresses. Thus, users that consciously request privacy are informed that they implicitly accept some service limitations, which other users don't want to accept, and that the same users may not wish to accept at

different times (then using other local addresses).

In v6G addresses, a privacy demand is already coded as bit 6 of the 9th octet set to 0. In v6E addresses, the proposed coding for privacy demands is in the v6E tag (Section 3.2.4), with bit 0 set to 1.

When a SAM has to forward an IPv6 global packet to an external domain with an IPv6 source expressing a privacy demand, it scrambles, in an arbitrary way provided it is reversible, bits of the internal host address that follow the global prefix P, and bits 2-15 of the internal port if it is a dynamic port (thus performing a locally known 1:1 mapping). The reverse mapping is performed in packets destined to internal hosts that have privacy requirement in their address.

The freedom to choose any reversible scrambling algorithm should make it difficult to discover it from the outside.

Comment [DT12]: No it isn't. The "u" bit is discussed in RFC 4291: "The motivation for inverting the "u" bit when forming an interface identifier is to make it easy for system administrators to hand configure non-global identifiers when hardware tokens are not available." It has nothing to do with privacy demands.

Comment [DT13]: What if the paths are not symmetric? You'd need the same mapping in both directions, and hence in multiple SAMs.

Comment [DT14]: Actually I believe it's the opposite. It would make it easier because if you don't specify a cryptographically safe algorithm, people will pick a far more predictable one because they don't know any better, and de-scrambling will be easier for an attacker.

4. Application examples

The following sections describe a number of SAM application cases.

A SAM that maps a global address space vXX to a local address space vYY is noted SAM(XX/YY). For example, the SAM(6G/4P) of the first example encapsulates global IPv6 packets into private IPV4 packets.

In figures, double arrows "==>" represent routes for prefixes, and single arrows "-->" represent routes for full length addresses. An IPv4 prefix is distinguished from an IPv6 prefix with ".." instead of "::" before the /k which indicates its lengths. The concatenation operator is the dot ".".

4.1. Already deployed configurations

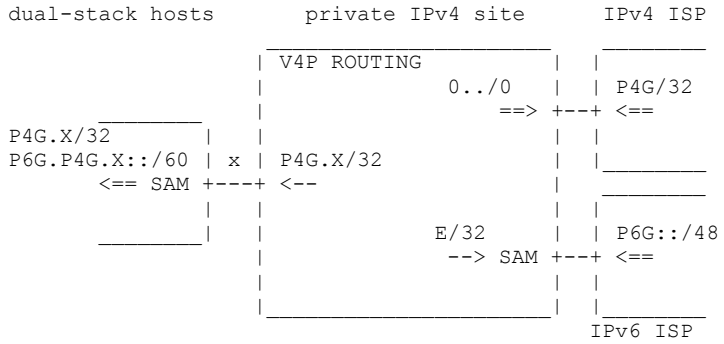
4.1.1. IPv6 across a private IPv4 site (ISATAP=SAM(6G/4P))

Figure 5 shows SAM parameters for a particular case where global IPv6 connectivity is offered, to dual-stack hosts, across a private site where routing is private IPv4 only (a particular application of ISATAP).

The SAM global address prefix P is made of the IPv6 prefix assigned by the ISP to the private site, followed by the ISATAP IID prefix 00:00:5efe::/32.

Interfaces of the private site to IPv4 and IPv6 ISPs are shown

separate, but can be merged if the IPv4 ISP also offers IPv6 on its interfaces (native or with some encapsulation, e.g. that of [6rd]).



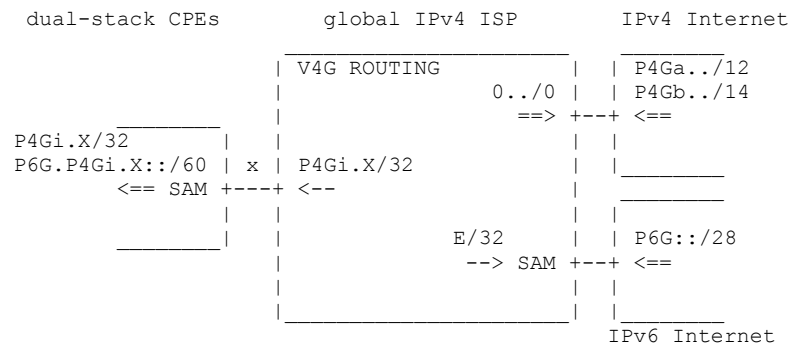
IPv6 ACROSS A PRIVATE IPV4 SITE (ISATAP)
SAM(P=P6G.(00:00:5efe)::/96, H=0../0, E, n=32)

Figure 5

4.1.2. IPv6 across an IPv4 ISP network (6rd=SAM(6G/4G))

Figure 6 shows SAM parameters for a particular case where global IPv6 connectivity, across a global IPv4 ISP network, to customer sites where the CPE is dual stack and supports [6rd].

In this example, the ISP uses one IPv6 prefix, but several IPv4 prefixes (two in the particular case), as typical for an ISP that has progressively increased the number of customers to be supported. Having a /28 IPv6 prefix, it assigns /60 prefixes to its customer sites.



IPv6 ACROSS AN IPV4 ISP NETWORK (6RD)
SAM(P=P6G::, H=0../0, E, n=32)

Figure 6

4.2. New configurations

4.2.1. IPv4 and extended IPv4 across an IPv6 ISP network

This example concerns an ISP that desires to route only IPv6 in its core infrastructure, and that has to provide IPv4 connectivity to its dual-stack customer sites. In view of the IPv4 address shortage, it wishes to distinguish two types of customer sites: a privileged customer site is assigned one IPv4 global address; an ordinary customer is only assigned a port-restricted IPv4 global address.

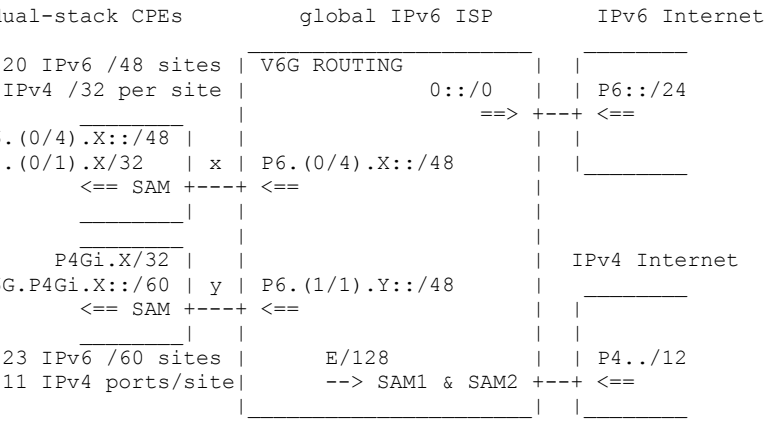
This objective is almost that of [IVI] with its envisaged future support of port multiplexing.

A difference between IVI and SAM objectives is that SAM implies, for this configuration, that CPEs that need IPv4 connectivity be dual stack with SAM support. On the other hand, [IVI] supports CPEs that are IPv6 only and that, despite this, need IPv4 connectivity (accepting as a counterpart a lack of end-to-end transparency). Whether enough customer demand will justify standard solutions for hosts that have IPv6-only stacks, and/or IPv6-only applications, and that need to reach IPv4 only servers is still an open question.

Conversely, while the only IPv4 connectivity of IVI is degraded by IPv6-IPv4 translation, which in particular makes it incompatible with SCTP [RFC3286], SAM provides end-to-end IPv4 transparency (accepting as a counterpart that CPEs work with restricted port ranges). Studies on implications of restricted port ranges are ongoing (see in

particular [Boucadair]).

Figure 7 shows an example of ISP network configuration to satisfy the above requirement. It uses two SAMs, respectively for privileged and for ordinary customer sites.



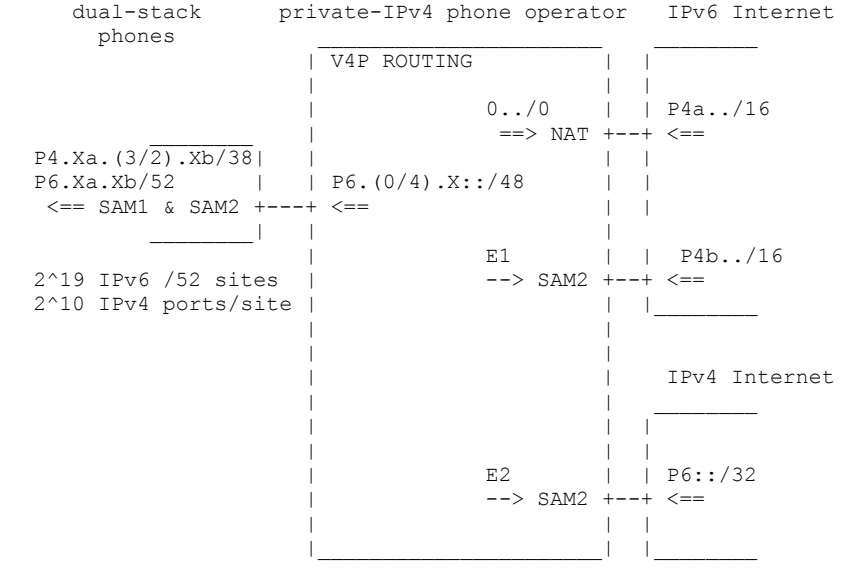
IPv4 AND EXTENDED IPV4 ACROSS AN IPV6 ISP NETWORK
SAM1(P=P4.(0/1).., H=P6.(0/4)::, E/128, n=20)
SAM2(P=P4.(1/1).., H=P6.(1/1)::, E/128, n=25)

Figure 7

4.2.2. IPv6 and extended IPv4 across a private IPv4 mobile operator

This example concerns an ISP that uses private IPv4 as address space of its routing infrastructure and has to provide both IPv6 and extended global IPv4 connectivities to its hosts.

Figure 8 shows an example of ISP network configuration that satisfies this objective. It uses two SAMs, respectively for IPv6 and port restricted IPv4 addresses in mobile phones.



IPv4 AND EXTENDED IPV4 ACROSS AN PRIVATE IPV4 MOBILE OPERATOR
SAM1(P=P4.(0/1).., H=P6.(0/4)::, E/128, n=20)
SAM2(P=P4.(1/1).., H=P6.(1/1)::, E/128, n=25)

Figure 8

4.2.3. Host controlled ISP selection in IPv6 dual-homed sites

This example concerns a private site that has two IPv6 ISP interfaces, and where an internal host must be able to select which outgoing ISP is used, for its outgoing packets, depending on the source address it has chosen.

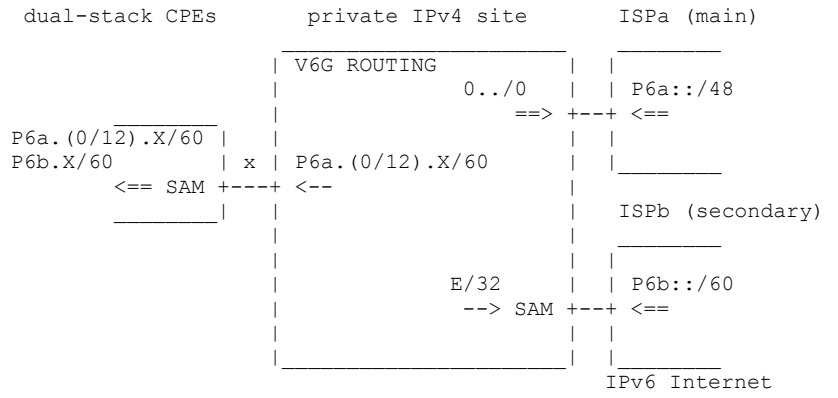
Figure 9 shows an example of private network configuration that satisfies this objective. For dual-homing, it uses one SAM(V6G/v6P). It could use one or several other SAMs for global IPv4 connectivity, but this is ignored in the example.

The SAM in dual-stack hosts, because of its parameters, encapsulates packets that have the secondary IPv6 source address, that which starts with the site prefix assigned by the secondary ISP. If destined to a host outside the private site, its local destination address being that of the SAM, the packet leaves the private site via the ISP that has a return route for the chosen source address. This

is the desired result.

Local routing is, in this example, done in the global IPv6 address space of the main ISP. This choice preserves compatibility with hosts that are not SAM-capable dual-stack hosts. They work as though the site would be single-homed.

Note : another possible choice would have been to use a private IPv6 address space for local routing. This choice has the advantage of suppressing the need to change it if the main ISP changes, or replaces the site prefix by another, but implies that all hosts are dual-stack with SAM support.



IPv6 DUAL HOMING SITE WITH HOST CONTROLLED ISP SELECTION
SAM(P=P6b::, H=P6a.(0/12)::, E, n=32)

Figure 9

4.2.4. End-to-end IPv4 transparency across a home site

The example of Figure 10 concerns a home site that has a IPv4 global address, ad that routes locally in private IPV4. For outgoing connections, some hosts need end-to-end transparency.

To satisfy this requirement, dynamic ports are split into two subsets, one for the NAT and one for the SAM. In the example, the upper half (prefix 7/3) is assigned to the SAM. Then, SAM ports are further split into all permitted hosts. In the example, 13 hosts are supported, each one having 512 dynamic ports for its use. (13 = 2^4 minus three reserved values all 0s, all 1s, and E).

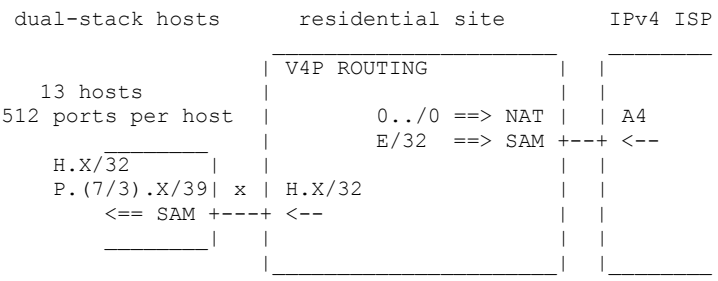


Figure 10

5. Security considerations

Provided consistency checks between local addresses (in encapsulating packets) and global addresses (in encapsulated packets) are systematically done, possibilities global address spoofing is possible, but not more and not less than local addresses spoofing.

As long as SAMs are correctly configured, no other security risk due to SAM operation has been identified.

6. IANA Considerations

TBD

7. Acknowledgements

8. References

8.1. Normative References

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

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

8.2. Informative References

[6rd] Despres, R., "IPv6 Rapid Deployment on IPv4 infrastructures (6rd)" - Work in progress (draft-despres-6rd-02)", October 2008.

[Bonjour] S. Cheshire et al, "Requirements for a Protocol to Replace AppleTalk NBP - Work in progress (draft-cheshire-dnsext-nbp-05)", October 2008.

[Boucadair] M. Boucadair et al, "Provider-Provisioned CPE: IPv4 Connectivity Access in the context of IPv4 address exhaustion - Work in progress (draft-boucadair-port-range-00)", October 2008.

[IVI] Xing Li et al, "Prefix-specific and Stateless Address Mapping (IVI) for IPv4/IPv6 - Work in progress (draft-xli-behave-ivi-00)", July 2008.

[LISP] D. Farinacci et al, "Locator/ID Separation Protocol (LISP) - Work in progress (draft-farinacci-lisp-09)", October 2008.

[RFC1955] Hinden, R., "New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG", RFC 1955, June 1996.

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[RFC3221] Huston, G., "Commentary on Inter-Domain Routing in the Internet", RFC 3221, December 2001.

[RFC3286] Ong, L. and J. Yoakum, "An Introduction to the Stream Control Transmission Protocol (SCTP)", RFC 3286, May 2002.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214,

March 2008.

Author's Address

Remi Despres
3 rue du President Wilson
Levallois,
France

Email: remi.despres@free.fr

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.