Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: January 13, 2011

R. Despres
RD-IPtech

July 12, 2010

Stateless Address Mapping (SAM) - a Simplified Mesh-Softwire Model
draft-despres-softwire-sam-01

Abstract

Stateless Address Mapping (SAM) is a generic mechanism to statelessly establish tunnels, point-to-multipoint, for packets of an address family that traverse domains whose routing is in another address family (mesh softwires). It extends tunneling principles of [6rd] to other address-family combination than IPv6 across IPv4 domains. It thus introduces, for a variety of use cases, a simpler mesh-softwire model than that of [RFC5565].

Among SAM use cases, some are solutions to previously unsolved problems: native IPv6 across IPv4 NATs, with optimized paths; multihoming with independent CPEs and provider-aggregatable prefixes; public IPv4 addresses across IPv6-only domains with optimized paths; static sharing of IPv4 addresses, without impact on routing information bases.

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 http://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 January 13, 2011.

Copyright Notice

Table of Contents

1. Introduction

Stateless Address Mapping (SAM) is a generalization, to other address-family combinations than IPv6 across IPv4 domains, tunneling principles of [6rd]. While the mesh-softwire framework of [RFC5565] depends on a common exterior routing protocol between all potential point-to-multipoint tunnel endpoints, SAM depends only on stateless functions at tunnel endpoints. Domains traversed by SAM tunnels are treated as virtual links, i.e. as links on which no routing link-layer protocol is needed.

A specification of SAM is proposed in Section 2. A number of typical use cases are covered in Section 3. Security considerations are covered in Section 4

2. The SAM model

2.1. Terminology

SAM domain: A SAM domain is a routing domain, or set of routing domains separated by NATs, across which SAM tunnels are statelessly established. They are established between one or several provider domains and a number of customer domains of the SAM domain. Addresses of customer-domain hosts start with prefixes assigned to the SAM domain by its provider domains. A customer domain can range from a single host to a complete network with multiple routers and multiple interior NATs.

P-SAM: A P-SAM is a "provider" stateless-address-mapping function. It is situated in a border node between a SAM domain and one or several of its a provider domains. It encapsulates IP packets or datagrams it receives from its provider domains, and forwards them via the SAM domain to C-SAMs. It also decapsulates IP packets or datagram it receives from the SAM domain, and forwards them either via one of its provider domains, or back via the SAM domain to C-SAMs (hairpin forwarding).

C-SAM: A C-SAM is a "customer" stateless-address-mapping function. It is situated in a border node between a SAM domain and its customer domain. It encapsulates IP packets or datagrams it receives from the customer domain and forwards them via the SAM domain to P-SAMs or C-SAMs. Conversely, it decapsulates IP packets or datagrams it receives from the SAM domain and forwards them via the customer domain.

Mapping Rule: In a C-SAM or P-SAM, a mapping rule derives the interior destination address iDST to be used as interior destination from an exterior destination address eDST.

Exterior Address Families: Exterior address families of a SAM domain are those of prefixes that provider domains of the SAM domain assign to it.

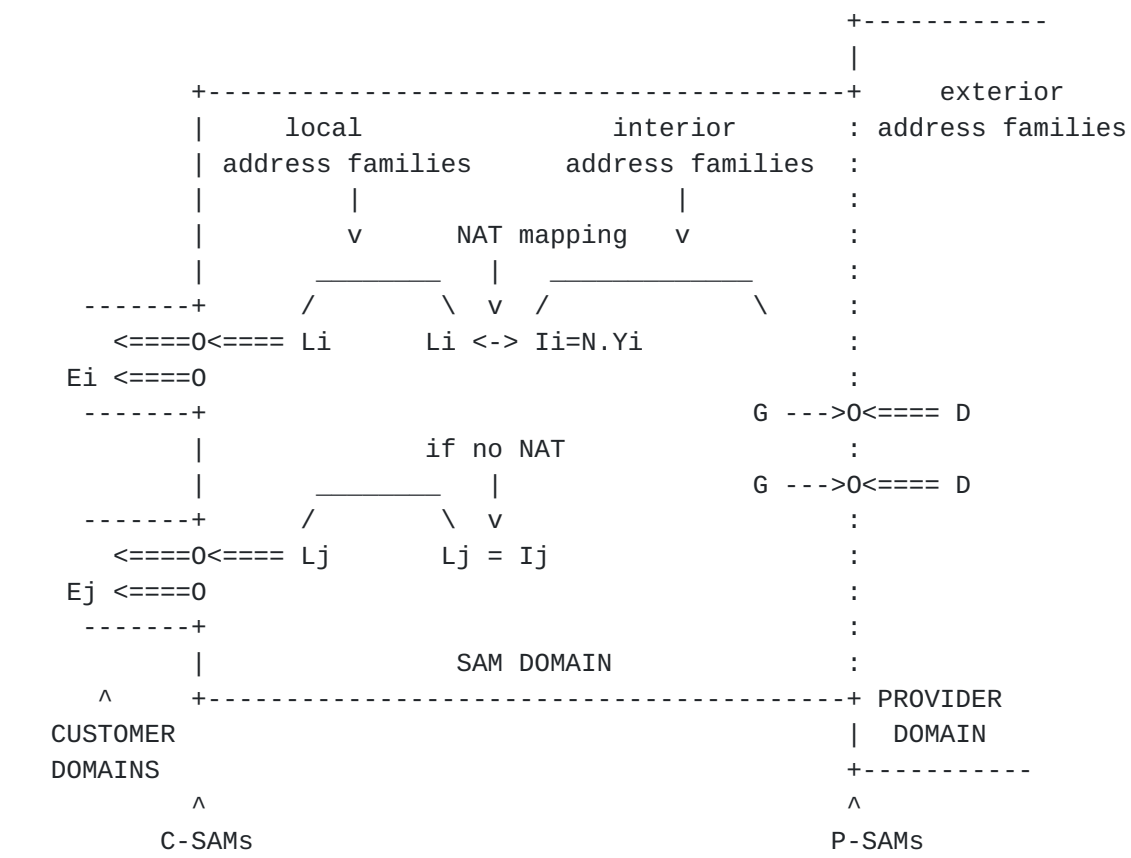
Interior Address Families: In a SAM domain, interior address families are those used for its interior routing. If the SAM domain includes NATs, several independent routing domains are isolated from each other. In this case, interior address families are those used between P-SAMs and NATs that are closest to them.

Local Address Family: For a C-SAM, local address families are those used for interior routing at the interface between the C-SAM and the SAM domain. If there is no NAT between a C-SAM and P-SAMs, local address families of this C-SAM are the interior address families of the SAM domain.

Locator: In a specified address family (IPv4, IPv6 or IPv4E), a locator is either a full address or a prefix.

IPv4E address family: Prefixes of the IPv4E address family are either public IPv4 prefixes, or addresses, or public IPv4 addresses extended up to 47 bits. If it has more than 32 bits, an IPv4E prefix identifies a port set. Ports of this set are those that may be used with the public IPv4 address (see Section 2.4). IPv4E prefixes are only processed in P-SAMs and C-SAMs, never in interior routers of SAM domains.

IPv4+ address: An IPv4+ address has 48-bits. It comprises an IPv4 address and a port number. Such addresses are convenient to identify tunnel endpoints in domains including NAT44s or in domains where public IPv4 addresses have to be shared.



D : Domain exterior prefix
E : C-SAM Exterior locator (starts with D)
L : C-SAM Local locator
I : C-SAM Interior locator
G : P-SAM interior address (default Gateway)
N : NAT interior locator
Y : bits of L after N

C-SAM parameters: {G {E [T]}} [{mapping rule}]
P-SAM parameters: {mapping rule} {G} [{N}]
T : lifetime
Mapping rule: EDP [, IDP][, eds], ced [, IDS]
EDP: Exterior Destination Prefix to be matched
IDP: Interior Destination Prefix to be included
ned: number of bits to be Neglected in the exterior destination
ced: number of bits to be Copied from the exterior destination
IDS: Interior Destination Suffix to be included
=> iDST= IDP . [(eDST - EDP) << eds) / ced] . IDS

THE SAM MODEL

Figure 1

2.2. **C-SAM and P-SAM Parameters -** Mapping Rules

Parameters of C-SAMs and P-SAMs are listed in Figure 1 (square brackets indicate optional contents, and curly brackets contents that may exist in several instances):

a. A CSAM has one or several provider-domain interior addresses G and optionally a number of mapping rules. Each G is assigned one or several C-SAM exterior locators E, and each E may be assigned a time to live T. G addresses are IPv4, IPv6 or IPv4+. E prefixes are provided to C-SAMs with not only their lengths and values, but also with their address families (the length of a prefix is not in general sufficient to determine an address family).

b. A P-SAMs has one or several mapping rules, and the list of provider interior addresses of the domain G (for anti-routing-loop protection - see Section 4). If there are ISP-operated NAT44s in the SAM domain, the P-SAM has also the list of their locators N (see [draft-despres-softwire-6rdplus].

Mapping rules are used to derive interior destination addresses iDST from exterior destination addresses eDST. Each rule comprises:

- EDP: an exterior-destination prefix
- IDP: an optional interior-destination Prefix
- ned: an optional number of bits to be neglected in eDST (default value 0)
- ced: a number of bits to be copied from eDST
- EDP: an optional interior-destination suffix (default length 0)

A rule applies to an eDST if it starts with the rule EDP. The derived iDST then starts with the rule IDP, if present. It continues with a field of length "ced" copied from eDST after its EDP prefix, and after its neglected field of length "ned" if any. It terminates with the rule IDS if present in the rule. (The iDST formula given in Figure 1 uses "." as the concatenation operator, "&lt&lt" as left shift operator, and "/" as truncation operator).

2.3. Encapsulation and Fragmentation Considerations

For IPv4 and IPv6 exterior address families, C-SAMs and P-SAMs forward packets across SAM domains one by one, even if packets only contain fragments of multi-packet datagrams. For the IPv4E address family, though, exterior destination prefixes EDP to be matched imply an analysis of port numbers which appear only in first fragments of multi-packet datagrams. In this case, fragmented IPv4 datagram can be reassembled before being treated as though they would have been received in a single-packet. (More sophisticated solutions than systematic datagram reassembly may be more efficient in some scenarios, but they are beyond the scope of this document.)

Each exterior packet that is tunneled across a SAM domain is encapsulated in an interior datagram whose address family is that of the interior destination iDST. The following considerations apply to maximum transmission units (MTUs):

a. If the interior address family is IPv6, no fragmentation may take place within the SAM domain. C-SAMs and P-SAMs must therefore ensure that no IPv6 packet they transmit exceeds the MTU size known to be accepted on all paths across the SAM domain ([RFC2460]). (at least 1280 octets.) For this, exterior packets can be fragmented in as many packets as needed before each one is encapsulated and transmitted.

b. If the interior destination address iDST is IPv4 or IPv4+, even very large packets may be transmitted in a single datagram. If the exterior address family is IPv4, it may however be preferable to fragment the exterior packet so that each fragment can be transmitted in a datagram that, on its way across the SAM domain, will not be fragmented.

c. If the exterior address family is IPv6, each SAM may, by refusing IPv6 packets that exceed some maximum size, limit the risk that encapsulating datagrams be fragmented on their way across the SAM domain. This maximum size may, for instance, be the packet size known to traverse of the domain without fragmentation or rejection, minus the size of the encapsulation header (provided it is at least 1280 octets).

If the interior destination address is IPv4 or IPv6, encapsulation is IP in IP with the protocol field of the outer header set to 41. If it is IPv4+, the protocol field of the IPv4 header is et to 17 (UDP) and a UDP header is added. Its destination port is that contained in the IPv4+ destination, and the source ports is that contained in the IPv4+ address of the sender.

2.4. Port sets of IPv4E prefixes

Port sets that are assigned to IPv4E prefixes longer than 32 bits must be defined with several constraints:

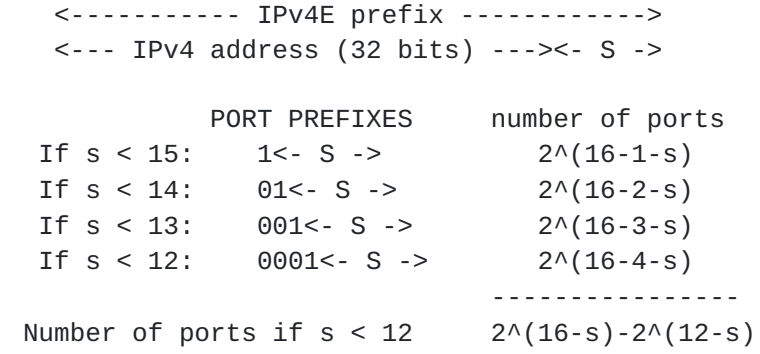
"No administration" The port set must be algorithmically derived from bits added to IPv4 addresses, without any parameters that would have to be administered.

"Fairness-1" Port sets derived of two IPv4E prefixes having the same length must have the same number of ports.

"Fairness-2" Because well-known ports (0 to 1023) have higher value than other ports, and different values from one another, no port set assigned to a domain must contain any of them. Ports from 1024 to 4095 being also avoided by some operating systems when they assign ports to applications, they should also be excluded. The total set of ports to be shared has then 61440 ports (4096 to 65535)

"No waste" The number of ports assigned to hosts should be as large as possible in the context of previous constraints.

The mapping algorithm described in Figure 2 is designed to comply with these constraints. It assigns to each IPv4E prefix up to 4 disjoint port ranges, none of which includes ports 0 to 4095. Each range is defined by a prefix that includes a constant prefix (1, 01, 001 or 0001 respectively) followed by bits that follow the IPv4 address in the IPv4E prefix. IPv4E prefixes of lengths from 33 and to 44 are assigned 4 port ranges. Those of lengths 45, 46, are assigned 3 and 2 port ranges respectively, and those of length 47 are assigned only one port.



PORT SETS OF IPv4E PREFIXES THAT EXCEED 32 BITS

Figure 2

2.5. Acquisition of Parameters by P-SAMs and C-SAMs

For some early experiments, parameters may be administratively configured, but any production deployment makes sense only with automatically-configured C-SAM parameters.

In SAM domains without interior NATs, SAM parameters could be obtained from DHCP or DHCPv6 servers. These servers could statelessly derive specific parameters to be assigned to each C-SAM from the source interior address of the C-SAM, received in its parameter request, and from parameters of the servers themselves.

In SAM domains that include interior NATs, IPv4E has to be used as interior address family. In this case, parameters to be assigned to C-SAMs depend on types of NATs present between them and P-SAMs. DHCP servers are therefore no longer sufficient. The solution described in [draft-despres-softwire-6rdplus] is based on a parameter request being sent by a C-SAM to a well-known IPv4+ address, and on answers to be returned from this well-known address and from a second one.

Having well-known addresses also for SAM parameter servers for IPv4 and IPv6 interior address families permit to collocate parameter server function with P-SAM functions. This can facilitate deployments by avoiding the need to upgrade DHCP servers.

The need of IANA assignments of well-known parameters then amounts to two IPv4 addresses, two UDP ports, and one IPv6 address.

At this stage, more work is needed to specify detailed formats for both DHCP servers and for parameter servers at well-known addresses.

3. Use-Case examples

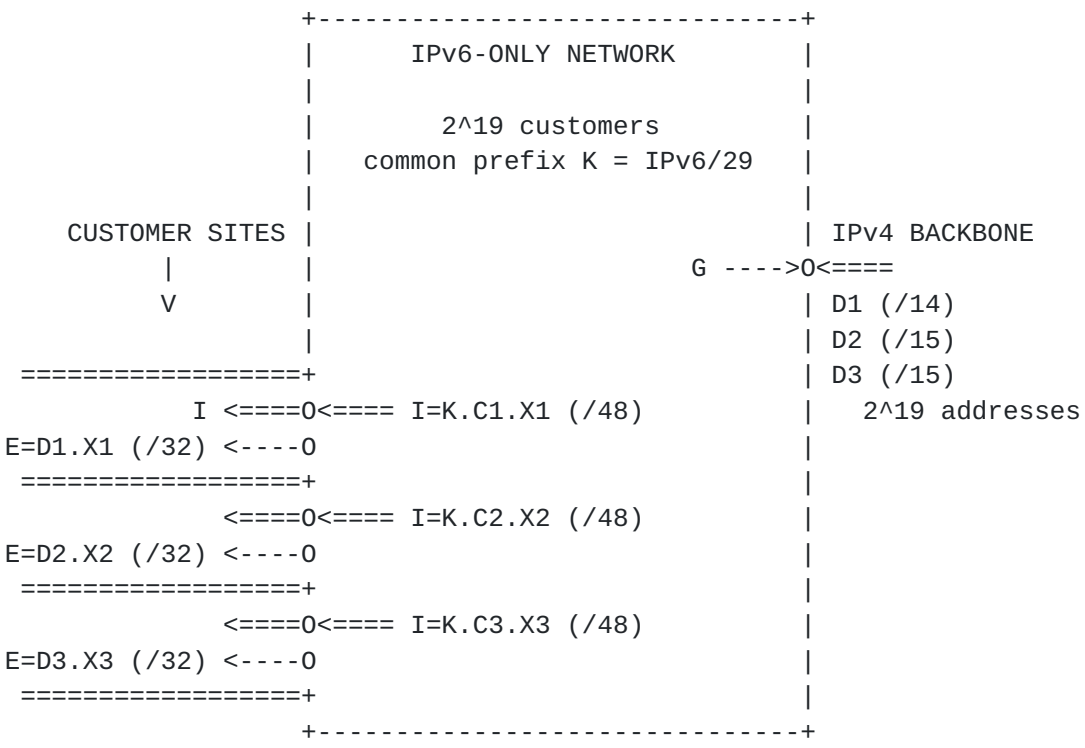
3.1. Native IPv6 across NAT44 CPEs (6rd+)

This use case is now covered in a separate document, [draft-despres-softwire-6rdplus].

Its interior address family is IPv4E.

It uses mapping rules that contain their eds and IDS components, not used in other use cases covered below.

3.2. Public IPv4 addresses and IPv4E prefixes across IPv6-only Domains (4rd)



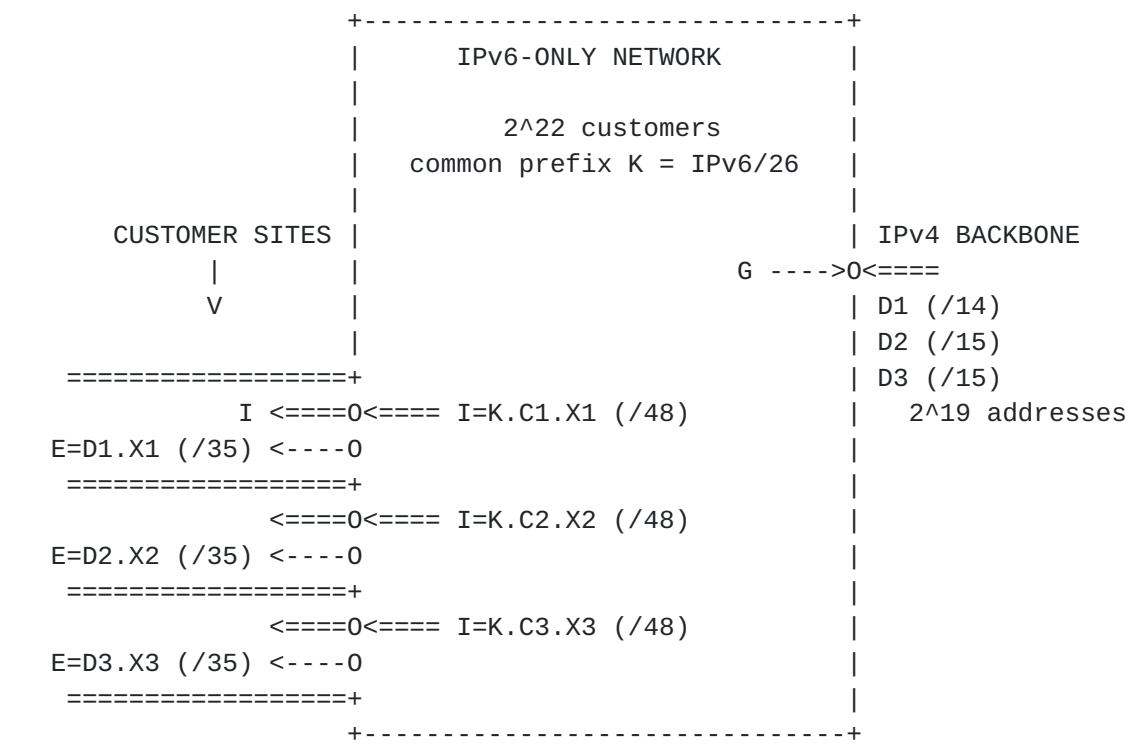
C-SAM PARAMETERS (where C1=0b0, C2=0b10, C3=0b11)
- G
- E(I) = IF I=K.Ci... for some i, THEN E=Di.(I-(K.Ci))
Mapping rule-1 = (EDP=D1, IDP=K.C1, ced=18)
Mapping rule-2 = (EDP=D2, IDP=K.C2, ced=17)
Mapping rule-3 = (EDP=D3, IDP=K.C3, ced=17)

P-SAM PARAMETERS
The three mapping rules, G

IPv4 ACROSS AN IPv6-ONLY NETWORK - ONE IPv4 ADDRESS PER CUSTOMER

Figure 3

As some ISPs have started deploying IPv6-only networks, typically for high bandwidth applications, some of their customers may need connectivity with the IPv4 Internet. Some approaches have been studied to satisfy this need, in particular [DSTM], but they were based on rather complex stateful solutions and were not pursued. A stateless solution, much simpler, is possible with SAM. Being the reverse of that satisfied by 6rd, i.e. native IPv6 across IPv4-only networks, we call it "4rd" (IPv4 "residual deployment").



C-SAM PARAMETERS (where C1=0b0, C2=0b10, C3=0b11)
- G
- E = IF I=K.Ci... for some i, THEN E=Di.(I-(K.Ci))
Mapping rule-1 = (EDP=D1, IDP=K.C1, ced=21)
Mapping rule-2 = (EDP=D2, IDP=K.C2, ced=20)
Mapping rule-3 = (EDP=D3, IDP=K.C3, ced=20)
=> Port prefixes for IPv6 locators E:
0b1xxx, 0b01xxx, 0b001xxx, 0b0001xxx
where xxx = bits of E beyond 32
=> 2^(16-3)-2^(12-3) = 7 680 ports / customer

P-SAM PARAMETERS
The three mapping rules, G

IPv4 ACROSS AN IPv6-ONLY NETWORK - PORT-RESTRICTED ADDRESS PER CUSTOMER

Figure 4

Figure 3 and Figure 4 detail two examples of 4rd SAM configurations. In the first one, the ISP has enough IPv4 addresses for all its IPv6 customers to obtain a public IPv4 address. In the second one, each IPv6 customer only obtains a shared public IPv4 address, with a port set defined by its assigned IPv4E prefix. Note that an ISP, using different IPv6 and IPv4 prefixes, can assign full IPv4 addresses to some of its customers, and shared IPv4 addresses to others, possibly with different sizes of port sets.

In the two examples, the ISP is supposed to have three disjoint IPv4 prefixes, D1, D2, and D3, giving a total of 2^19 IPv4 addresses. It is supposed to assign /48 prefixes I to its customers. In the first example, it uses for this a /29 common IPv6 prefix K. It can thus support 2^19 customers. In the second example, it uses for this a /26 K, thus supporting 2^22 customers. With notations of previous sections, and with 0bxxx meaning the sequence of bits xxx, Figure 3 and Figure 4 are intended to be self explanatory.

3.3. Multihoming and Renumbering with PA Prefixes

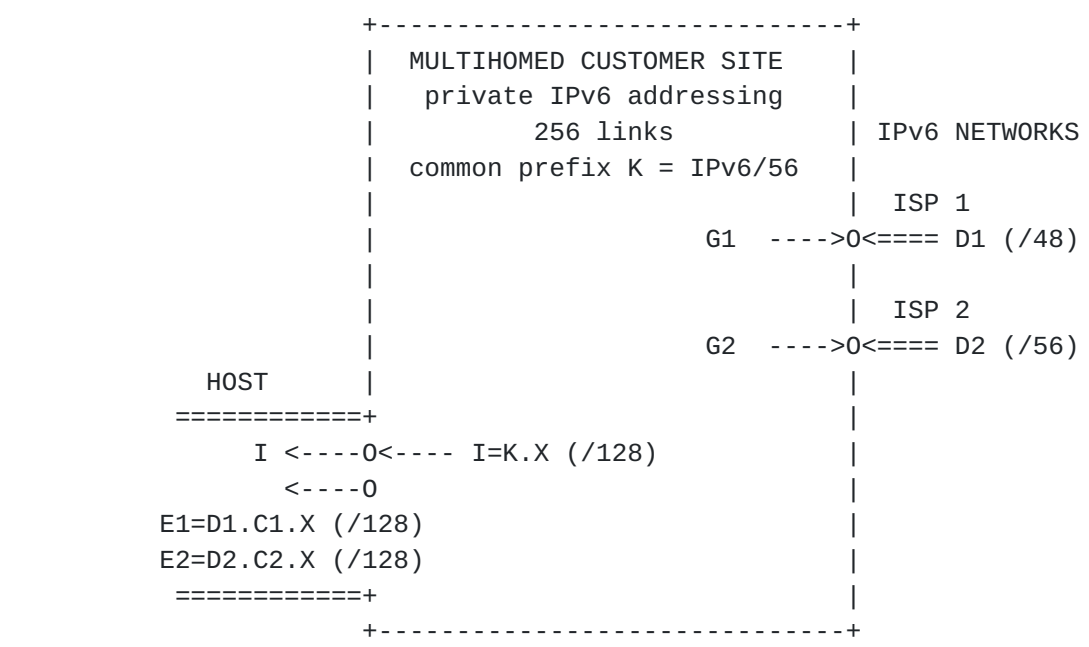
A well known problem of IPv4 is that more and more provider independent prefixes (PI prefixes) are needed to support customer-site multihomings. This has led to a dramatic growth of Internet-core routing tables [RFC3582]. The reason why multihoming is not feasible with independent CPEs having provider-aggregetable prefixes (PA prefixes) is the ingress-filtering protection that ISP support to prevent spoofing. With ingress filtering, a packet transmitted from a multihomed site must go via the ISP network whose prefix is present in the packet source address. No general solution has been specified so far to ensure it, even though IPv6 has been expected to avoid proliferation of PI prefixes. With SAM supported in hosts, a solution is possible, with systematic encapsulation of packets having public IPv6 addresses in interior packets using private addressing. This private addressing may be IPv4 or IPv6. In this configuration, an additional result is that automatic host renumbering can be supported, without any change in interior-routing information bases.

In the example of Figure 5, a customer site uses as interior addressing space an instance of the IPV6 private addressing of [RFC4193]. Its two CPEs, attached to two ISP networks, are assigned a /48 and a /56 respectively. The common prefix K of interior addresses is fdxx:xxxx:xxxx::/56 in which the first 48 bits are obtained according to [RFC4193].

SAM parameters assigned to each host are shown on Figure 5. They include the two provider interior addresses G1 and G2 and, the two customer exterior locators E1 or E2. In this example, locators Ei are full-length IPv6 public addresses. Each one starts with the domain exterior prefix Di assigned to the site by ISPi, followed by a complement Ci such that Di.Ci ha the same length length as the common interior prefix K.

Since D2 is a /56 like K, complement C2 has length 0.

With notations of previous sections, Figure 5 is intended to be self explanatory.



C-SAM PARAMETERS (where C1=0::/8 and C2=0::/0)
- G1
- E1 = I-(K.C1), T1
- G2
- E2 = I-(K.C2), T2

Mapping rule-1 = (EDP=D1.C1, IDP=K, ced=72)
Mapping rule-2 = (EDP=D2.C2, IDP=K, ced=72)

P-SAM PARAMETERS

The same mapping rules, G1, G2

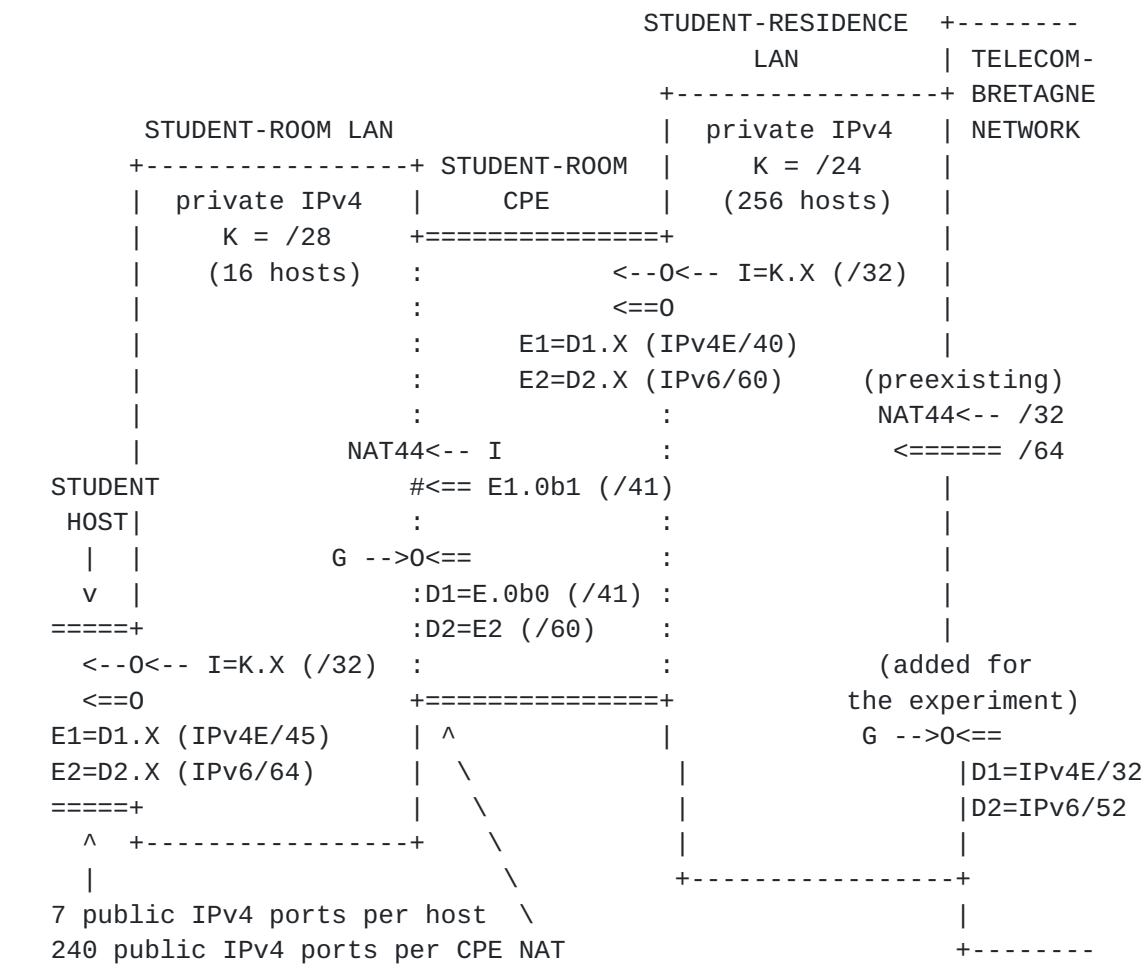
MULTIHOMED SITE WITH IPv6 PROVIDER-AGGREGETABLE PREFIXES

Figure 5

Now, let's assume that ISP2 replaces the assigned D2 by a new one, say a /48 D2'. It does it with a lifetime T2 such that D2 remains valid for some time but D2', having a longer validity, is the preferred one ([RFC2462]). Hosts have to request parameter updates frequently enough to obtain new lifetimes before previous ones expire. Thus, they obtain their exterior locators E2' before the E2 locators expire. When these do expire, hosts have been renumbered, with their E2' as their single exterior locators. (If the new D2' is shorter than /56, the complement C2' that is appended to it in E2' has a non-null length.)

3.4. An Experiment at Telecom Bretagne

An experiment is planned at [Telecom Bretagne], in its student residence.



C-SAM PARAMETERS OF THE STUDENT RESIDENCE
- G
- E1 = D1.(I-K)
- E2 = D2.(I-K)

Mapping rule-1 = (EDP=D, IDP=K, ced=8)
Mapping rule-2 = (EDP=D', IDP=K , ced=8)

P-SAM PARAMETERS OF THE STUDENT RESIDENCE
The same mapping rules

C-SAM PARAMETERS OF A STUDENT ROOM
- G
- E1(I)= D1.(I-K)
- E2(I) = D2.(I-K)

Mapping rule-1 = (EDP=D1, IDP=K, ced=4)
Mapping rule-2 = (EDP=D2, IDP=K, ced=8)

P-SAM PARAMETERS OF A STUDENT ROOM
The same mapping rules

THE TELECOM-BRETAGNE EXPERIMENT

Figure 6

The experiment combines:

- SAM-based address mappings;
- A hierarchy of two levels of SAM domains, with private IPv4 as interior address families in both;
- IPv6 and IPv4E exterior address spaces;
- NATs and hosts that use both their private addresses and their shared public IPv4 addresses.

Figure 6 details the planned configuration. A PC under Linux is used a gateway between the Student-residence LAN and the general Telecom-Bretagne network. It supports the P-SAM of the Student-residence LAN, and has two domain exterior prefixes: D1 is an IPv4E /32 (the public IPv4 address of the gateway), and D2 is an IPv6 /52 used for the experiment. Student-room CPEs are upgraded Linksys routers. Each supports a C-SAM of the student-residence LAN and the P-SAM of the LAN of its student room. Student hosts used for the experiment will be PCs under Linux duly upgraded.

Each student room has, assigned by an IPv4 DHCP server, a private IPv4 address in which the lowest 8 bits are an index that identifies the room (the student-residence LAN has 192.168.0.0/24 as subnet prefix). It also has an IPv6 address (not shown on the figure) starting with the /64 prefix assigned to the Student residence. This address is sufficient for a student rooms in which there is only a host, but insufficient in one having a CPE to support several hosts. SAM will then be used to statelessly delegate a /6O IPv6 prefix to the student room, and to further delegate /64s to hosts in the room.

In an student-room CPE, the NAT44 function is modified so that it uses its two external addresses. Its private IPv4 address is used for outgoing connections to applications assumed to work across NAT cascades (Web, Messaging, the DNS, and possibly some additional ones to be defined). Its public IPv4 address, for which it has a restricted port set, is used for other outgoing connections, and for ports devoted to port forwarding (be it administratively or otherwise, e.g. with UPnP).

Upgraded hosts, also use their two IPv4 addresses (in addition to their IPv6 address constructed with their /64 IPv6 prefix). The private one is, like in CPE NATs, used for outgoing IPv4 connections to NAT-cascade-friendly applications; the other one for other IPv4 outgoing connections and for ports requested by applications for incoming IPv4 connections. The lowest port of the port set is mapped to application port 80 so that hosts can support Web server applications without changing their oncoming port.

At the time of writing this draft, implementation with administratively assigned parameters is well advanced. Real use is planned to be experimented with students in the 4th quarter of 2010.

4. Security Considerations

The general ingress-filtering principle ensures anti-spoofing protection: a packet received at an interface must be silently discarded if the same packet with permuted source and destination would have no route via this interface in the reverse direction.

In the particular case of SAM, it implies that:

- A C-SAM discards a packet:
  - if the packet is received from its customer domain with a source address that doesn't start with an exterior locator of the C-SAM;
  - if the packet is received from the SAM domain with an exterior source address eSRC to which a mapping rule would apply if it would be an exterior destination eDST, and if the source address iSRC of the encapsulating packet differs from the iDST obtained with this mapping rule;
  - if the packet is received from the SAM domain with an exterior source address eSRC to which no mapping rule applies, and if the source address iSRC of the encapsulating packet is not one of the provider interior addresses G.

- A P-SAM discards a packet:
  - if the packet is received from its provider domain domain with a source address eSRC to which a mapping rule would apply if it would be an exterior destination eDST;
  - if the packet is received from the SAM domain with an exterior source address eSRC to which a mapping rule would apply if it would be an exterior destination eDST, and if the source address iSRC in the encapsulating packet differs from the iDST obtained with this mapping rule.

The possibility of routing loop attacks is documented for IPv6-in-IPv4 encapsulationsin [draft-nakibly-v6ops-tunnel-loops-02]. Without precaution, similar attacks would be possible for the more general encapsulations of SAM. The general precaution to be taken is a generalization of that documented for in [6rd]. A P-SAM must silently discard a packet:

- if the packet received from a provider domain would have to be forwarded to an interior address known to be one that of a border node between the SAM domain an this provider domain (such an interior address may be the provider interior address G of any P-SAM of the SAM domain and, in the case of IPv6-in-IPv4 encapsulations that of a 6to4 relay, an ISATAP router, or a 6rd border router, operated by the administrative authority of the SAM domain);
- if the packet is received from the SAM domain with an interior source address known to be one that of a border node between the SAM domain an this provider domain.

With these precautions, no new security risk has been identified so far.

5. IANA Considerations

Section 2.5 indicates which IANA assignments are needed for SAM, namely:

- two well-known IPv4 addresses;
- two well-known UDP ports;
- a well-known IPv6 address.

6. Acknowledgments

Although this specification is mostly the result of a personal work of the author, in continuity with that which led to the 6rd of [RFC5569], recognition is due to a number of colleagues who provided useful comments as the proposal evolved. Mark Townsley gave precious encouragements during early phases of the project, and acted as a convincing advocate for a Cisco Research Grant to be allocated to Telecom Bretagne for the SAM experiment of Section 3.4. Laurent Toutain, who leads the team in charge of this experiment, deserves special gratitude for the confidence he expressed in the concept, and for the time spent for the experiment itself. Dave Thaler has to be thanked for a detailed review made on a very early draft. Satoru Matsushima was first to point out that, because some providers already operate IPv6-only networks, public IPv4 across such networks could become a not-so-long-term application of SAM.

7. References

7.1. Normative References

[RFC1700] Reynolds, J. and J. Postel, "Assigned Numbers", RFC 1700, October 1994.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

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

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

7.2. Informative References

[6rd] Townsley, M. and O. Troan, "IPv6 via IPv4 Service Provider Networks - draft-ietf-softwire-ipv6-6rd-10", May 2010.

[6to4] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", February 2001.

[DNS-SD] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery - draft-cheshire-dnsext-dns-sd-05", September 2008.

[DSTM] Bound, J., Toutain, L., Medina, o., Dupont, F., Afifi, H., and A. Durand, "Dual Stack Transition Mechanism (DSTM)- draft-ietf-ngtrans-dstm-08", June 2002.

[ISATAP] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, March 2008.

[NAT-PMP] Cheshire, S. and M. Krochmal, "NAT Port Mapping Protocol (NAT-PMP) - draft-cheshire-nat-pmp-03", April 2008.

[NatClassification] Jennings, C., "NAT Classification Test Results - draft-jennings-behave-test-results-04", July 2007.

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

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC3068] Huitema, C., "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, June 2001.

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

[RFC3582] Abley, J., Black, B., and V. Gill, "Goals for IPv6 Site-Multihoming Architectures", RFC 3582, August 2003.

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

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

[RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and

E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.

[RFC4925] Li, X., Dawkins, S., Ward, D., and A. Durand, "Softwire Problem Statement", RFC 4925, July 2007.

[RFC5565] Wu, J., Cui, Y., Metz, C., and E. Rosen, "Softwire Mesh Framework", RFC 5565, June 2009.

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

[Telecom Bretagne] "http://international.telecom-bretagne.eu/welcome/".

[draft-despres-softwire-6rdplus] Despres, R., "Rapid Deployment of Native IPv6 Behind IPv4 NATs (6rd+)", July 2010.

[draft-nakibly-v6ops-tunnel-loops-02] Nakibly, G. and F. Templin, "Routing Loops using ISATAP and 6to4: Problem Statement and Proposed Solutions", February 2010.

Author's Address

Remi Despres
RD-IPtech
3 rue du President Wilson
Levallois,
France

Email: remi.despres@free.fr