Stateless 4Via6 Address Sharing
draft-dec-stateless-4v6-01

Abstract

This document discusses the applicability and possible resolution of a number of issues attributed to A+P based solutions, specifically in the context of an IPv6 based solution characterised by this draft as a stateless 4Via6 (4V6) solution. The document presents that the majority of the issues either do not apply to such stateless 4V6 solutions, or are no worse that in alternative NAT44 based solutions. The few remaining issues can be mitigated by the solutions or operators.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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 September 28, 2011.

Copyright Notice

Copyright (c) 2011 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 (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Table of Contents

1. Introduction ........................................ 4
2. Stateless 4-6-4 Technical and Architectual characteristics .. 4
3. Overview of issues and discussion .......................... 7
   3.1. Notion of Unicast Address ............................. 7
      3.1.1. Overview ..................................... 7
      3.1.2. Discussion ................................... 7
   3.2. Implementation on hosts ............................... 8
      3.2.1. Overview ..................................... 8
      3.2.2. Discussion ................................... 8
   3.3. Non TCP/UDP port based IP protocols ..................... 8
      3.3.1. Overview ..................................... 9
      3.3.2. Analysis ..................................... 9
   3.4. Provisioning and Operational Systems .................... 9
      3.4.1. Overview ..................................... 9
      3.4.2. Discussion ................................... 9
   3.5. Training & Education ................................ 11
      3.5.1. Overview ..................................... 11
      3.5.2. Discussion ................................... 11
   3.6. Security ........................................... 11
      3.6.1. Overview ..................................... 11
      3.6.2. Discussion ................................... 12
   3.7. Unknown Failure Modes ................................ 13
      3.7.1. Overview ..................................... 13
      3.7.2. Discussion ................................... 13
   3.8. Possible Impact on NAT66 use & design .................. 13
      3.8.1. Overview ..................................... 13
      3.8.2. Discussion ................................... 13
   3.9. Port statistical multiplexing and monetization of port space ............... 14
      3.9.1. Overview ..................................... 14
      3.9.2. Discussion ................................... 14
   3.10. Readdressing ....................................... 15
      3.10.1. Overview ..................................... 15
      3.10.2. Discussion ................................... 15
   3.11. Ambiguity about communication between devices sharing an IP address ............. 16
      3.11.1. Overview ..................................... 16
      3.11.2. Discussion ................................... 16
4. Conclusion .............................................. 17
5. IANA Considerations ..................................... 17
6. Security Considerations .................................. 17
7. Contributors and Acknowledgements ........................... 17
8. References .............................................. 17
   8.1. Normative References ................................ 17
   8.2. Informative References ............................... 17
Author’s Address ........................................... 19
1. Introduction

As network service providers move towards deploying IPv6 and IPv4 dual stack networks, and further on towards IPv6 only networks, a problem arises in terms of supporting residual IPv4 services, over an infrastructure geared for IPv6-only operations, and doing so in the context of IPv4 address depletion. This class of problem is referred to by the draft as the 4via6 problem, to which a number of solutions have been put forward. The solutions fall largely into two types of architectures characterized by the location of the IPv4 address sharing/overloading function. As an example, the DS-lite solution [I-D.ietf-softwire-dual-stack-lite] relies on the use of a large scale stateful Address Family Transition Router (AFTR), capable of IPv4 address sharing, ie DS-Lite uses a centralized large scale port overloaded stateful NAT44, aka PAT44, that is deployed within the operators’ core network. In contrast, solutions such as a 4rd [I-D.despres-softwire-4rd] and dIVI [I-D.xli-behave-divi] rely on the use of fully distributed NAPT44 functionality located on end user CPEs, keeping the network operators’ core effectively stateless. The latter type of solutions, rely on the same IPv4 address being used by multiple CPEs, each with a different TCP/UDP port range, and are often referred to as being part of the Address+Port (A+P) solution space [I-D.ymbk-aplusp]. A number of issues have been claimed to be attributed to this type of technology & solution, eg [I-D.thaler-port-restricted-ip-issues], [A+P BoF], which have so far delayed standardization progress, and which this draft attempts to discuss and resolve. Specifically, for the analysis the document assumes a number of architectural and technical characteristics, termed as the stateless 4via6 solution, as detailed in the following section.

The term "stateless 4via6 solution" is a general reference to the class of A+P derivative solutions, such as 4rd [I-D.despres-softwire-4rd] and dIVI [I-D.xli-behave-divi], as well a subset of the original A+P solution [I-D.ymbk-aplusp]. The term NAPT44 is used to refer to IPv4-IPv4 Network Address Translation with port overloading.

2. Stateless 4-6-4 Technical and Architectural characteristics

The following architectural and technical characteristics assumed by this document, and evidenced in whole or in part by various stateless 4via6 solution proposals such as 4rd, dIVI, SAM, besides architectural practice. Figure 1 depicts the overall architecture with two IPv4 user networks connected via 4via6 CPEs that share an IPv4 address.
Figure 1 - Generalized Stateless 4via6 system

The stateless 4via6 system has the following characteristics:

1. On user network side the routed IPv6 service provider network is demarcated from the IPv4 user network with a dedicated 4V6 CPE. The CPE externally has only a native IPv6 interface to the SP network, and a native IPv4 interface towards the end user network.

2. Internally, the 4V6 CPE can be modelled as having a port restricted NAPT44 function coupled with a stateless IPv6 adaptation function that is able to ferry the IPv4 traffic in/over the IPv6 interface, besides deriving 4V6 provisioning info from it. The IPv6 adaptation function could be encapsulating packets in IPv4 or translating IPv4 packets, or a combination of both.

3. The IPv4 Internet is demarcated from the operator IPv6 network with one or more operator managed stateless 6v4 gateways that contain an IPv6 adaptation function (not detailed in the diagram) matching the one on the CPE. Note: The stateless 6v4 gateway can be directly at the CPE side edge of the operator.
network, eg in an IP Edge router, or as shown some IP hops removed from the edge network.

4. The service provider has the all the necessary provisioning and accounting infrastructure to support a regular IPv6 deployment. CPE management operations, if any, are done using IPv6, however there is no per CPE or subscriber management required of the stateless 4via6 function, i.e. all stateless 4via6 can share the same service configuration, bar the IPv6 address naturally.

5. The network operator has the ability to assign an IPv6 prefix or IPv6 address to a CPE, and log such address assignment.

6. The shared IPv4 address and any port range is conveyed to the CPE as part of an IPv6 address or prefix, for example using [RFC6052], if not other IPv6 compatible encoding and a port indexing method. For a single shared public IPv4 address and port range, only a single IPv6 address or prefix is assigned irrespective of the port range size, with the mapping between IPv6 and IPv4 domains being entirely algorithmic based on a well known indexing schema.

7. The solution’s architecture does not require customer traffic flows to pass through specific gateways in the network, or do so symmetrically.

8. End user host’s DO NOT implement any of the 4V6, or other address sharing technologies, nor are they addressed directly with a shared IPv4 address. End user IPv4 hosts connected to the CPE receive unique private addresses assigned by the CPE, and it is the CPE that is directly addressed by the shared IPv4 address.

9. The IPv6 Adaptation function is not multi homed to the same IPv6 network. The CPE itself may be multi homed, but it only has one IPv6 addressed interface for the stateless 4via6 application and IPv6 adaptation function.

10. A CPEs NAPT44 function is modified to operate in a shared address port-constrained NAPT44 mode, as per the detailed solution proposals. No DNS64 or IPv6 aware ALGs, nor IPv4 ALGs are used or assumed. Any IPv4 ALG functionality that the CPE may support, remain unaffected. The CPE is expected to act as a DNS resolver proxy, using native DNS over IPv6 to the SP network.

11. Although orthogonal to the discussion of stateless 4V6, it is useful to note that the CPE is expected to have a native IPv6
interface to the end user network, with any of the end user IPv6 hosts (single or dual stack) receiving IPv6 addresses from an IPv6 delegated prefix issued to the CPE.

3. Overview of issues and discussion

This section summarizes the issues attributed to an A+P, or port restricted scheme, along with a discussion of applicability to the assumed system and possible resolutions. The summary of issues stem from [I-D.thaler-port-restricted-ip-issues] and associated discussions.

3.1. Notion of Unicast Address

3.1.1. Overview

The issue, referred to as the "definition of a unicast address", relates to the notion that in a shared IPv4 address system, multiple hosts will be visible as having a single IPv4 address outside of the system. This issue is a general characteristic of any NAPT44 based solution [I-D.ietf-intarea-shared-addressing-issues], including DS-Lite. However, a more specific aspect of this issue in the context of an address sharing system is the possibility that a single host having multiple interfaces will be assigned the same IPv4 address (with different port ranges) on each of its interfaces. It may also be that multiple hosts sharing an address find themselves on the same Layer 2 segment. Either would impede hosts from working within the notion of known host IP stack and protocol implementations.

3.1.2. Discussion

A number of the characteristics of the 4via6 solution architecture cause the issues not to be applicable, key of which is that there is no expectation for any kind of end hosts to be part of the shared IPv4 address system.

In the stateless 4via6 system, CPE nodes are assigned with a shared IPv4 address+port range by means of the unique IPv6 address, containing the embedded IPv4 address + port index, of that CPE node. The CPE node is in addition enabled to be running the port restricted NAPT44 function from the IPv6 derived address, a key characteristic of the solution. On the IPv6 plane, the IPv6 address of the CPE is practically indistinguishable from any "regular" IPv6 address, and in fact any host that is not aware of it conveying an embedded IPv4 address would be able to use this just like any other regular IPv6 address, ie the 4via6 solution uses standard IPv6 addressing. In terms of the IPv4 dimension, since the shared address and port index
are never used to address native IPv4 nodes or hosts, but instead uniquely assigned to a single NAPT44 function that is part of the CPEs, all legacy or other IPv4 hosts are not exposed to the presented issues.

Going beyond the ascribed issue however, it appears desirable to have the 4via6 CPEs that are to be part of the shared system to be able to provide a hint to the network operator in terms of their special capability. Such a hint can be a DHCPv6 Option Request Option, which would be useful to allow the DHCPv6 sub-system to also inform the CPE of any other stateless 4via6 system parameters. A largely similar ORO option is currently being defined as part of [I-D.ietf-softwire-ds-lite-tunnel-option]

Recommendation: Define a suitable DHCPv6 ORO for conveying the 4via6 capability of a CPE.

3.2. Implementation on hosts

3.2.1. Overview

The issue, as presented, relates to the need for modifications on end hosts or devices to support a port constrained mechanism and the overall impossibility of realizing such modifications. Furthermore, host applications that attempt to bind to specific ports that are not part of the allowed port range will fail to do so and may also require modifications.

3.2.2. Discussion

As presented in Section 2 the solution assumes the use of a dedicated CPE implementing the 4via6 functionality within a port constrained mode and NAPT44. Granted, CPE nodes will require to implement new functionality such as the IPv6 adaptation function, that is likely alongside introducing native IPv6 support. However, any and all existing end user IPv4 devices (e.g. PCs, etc) will not affected. Nor are such devices expected to behave in any way different from that of today, where they typically obtain a private rfc1918 address and multiplexed by a CPE using a NAPT44 function.

In summary, the assumed 4via6 solution requires a specific 4via6 CPE but does not require any IPv4 host stack changes.

3.3. Non TCP/UDP port based IP protocols
3.3.1. Overview

This issue relates to the inability of using regular ICMP messages to "ping" an end-host that has been addressed with a shared IPv4 address. The issue can be generalized one applicable to any IP protocol that is not TCP/UDP port based, and also in terms of the ability of using such protocols from end hosts that are assigned a shared IPv4 address.

3.3.2. Analysis

The inability to ping a CPE from the IPv4 Internet is shared by other IPv4 address sharing mechanisms such as DS-Lite. Thus, the issue is no better or worse in the case of the stateless 4via6 solution. The same can be said of end user hosts using other non UDP/TCP port based protocols from behind a NAPT44 function, ie they will not function irrespective of address sharing or not.

In relation to the above another aspect deserves to be highlighted. Throughout, in the 4via6 solution, the IPv6 address of the CPE can be used for operational activities, such as pinging. Also, given that each CPE’s IPv4 address + port range maps deterministically to an IPv6 address and vice versa, the solution actually facilitates customer troubleshooting in contrast to others, eg DS-Lite, where the mapping between IPv6 and IPv4 addresses is indeterminate.

3.4. Provisioning and Operational Systems

3.4.1. Overview

The general claim of this issue is that a service providers’ provisioning and accounting systems would need to [radically] evolve to deal with the notions of shared IPv4 addresses and port range constrains.

3.4.2. Discussion

The stateless 4via6 solution relies on a fully operational IPv6 network, which on the IPv6 plane fundamentally does not differ from a regular IPv6 network, and the stateless 4via6 solution may be seen as an IPv6 application - devices connecting to the network, need unique IPv6 addresses which the network is able to provide. In the 4via6 solution it happens that these unique IPv6 addresses embed an IPv4 address. Hence, additional system enhancements that the stateless 4via6 solution requires, over and above those simply needed to deploy and operate an IPv6 network, lie in the domain of supporting the provisioning of the IPv6 adaptation functionality of the CPEs. This may require the operator to use DHCPv6, or other provisioning methods...
such as IPv6CP, TR-69, in order to configure any relevant 4via6 service parameters to a CPE.

From an IPv4 perspective, an operator will likely want to have a management system capable of the assignment of IPv4 addresses to the shared pool, and tuning the re-use factor. In this, the solution exhibits no grossly different characteristics than those of any system with an operator managed NAT44 function where similar management capabilities need to be introduced.

One additional aspect of the stateless 4via6 solution needs to be highlighted. On a par basis this solution requires less per subscriber management, accounting and logging capabilities than centralized NAPT44 alternatives such as DS-Lite, due to the following:

- The assignment of an IPv6 address that embeds a deterministic IPv4 address and port range removes the need for the operator to perform any NAPT44 binding logging, ie the task of determining which user had a given IPv4 address and port at a given time is simply a matter of determining who had the corresponding IPv6 address, rather than collecting large amounts of dynamic binding data.

- There is no need for the operator to manage NAPT44 binding data access and retention.

- Given the stateless nature of the 4via6 solution, all subscriber CPEs in an operator’s domain can share exactly the same 4via6 service configuration, i.e. The operator does not need to be concerned with managing on a per user basis specific AFTR assignment and/or load balancing such users and throughout ensuring symmetric traffic flows throughout.

- The location of the NAPT44 function on the user’s CPE, allows easy and direct management of the port mappings by the end user removing a need for the operator to introduce PCP [I-D.wing-softwire-port-control-protocol] (or similar) protocols in on AFTRs, and on CPE devices. In effect the end user can retains control of any bindings, which could be via today’s GUI, or UPnP IGDv2, or even PCP.

- As and when needed, a stateless 4via6 solution readily supports the assignment of an unshared IPv4 address, and full port control by the end user. A similar capability with centralised NAPT44 solutions involve onerous management of per subscriber configurations on the operator’s AFTR.
3.5. Training & Education

3.5.1. Overview

The issue claims a concern with the need for developers and support staff to be trained & educated in dealing with a port constrained systems.

3.5.2. Discussion

There appear to be at least two levels of looking at this issue in the stateless 4via6 context. On one level, it is perfectly true that developers and support staff will need to be trained with running/supporting a native IPv6 network, that is now a basis of the solution. This however is an inherent aspect of deploying an IPv6 network and applications. On another level, support and developers need to familiarized with the NAPT44 characteristics of the system, that are not different from those already known about such systems today. More specifically, there appears to be no such thing as a port unconstrained carrier grade NAPT44 system, in either tomorrow’s stateless 4via6 or AFTR guises, or today’s residential CPE NAPT44 implementations that have an inherent hard set translation limit (often 1024 translation, corresponding to a usage of 1024 ports). That application developers should be trained to be reasonably conservative in the usage of ports is thus not an issue of the stateless 4via6 solution, but pretty much of any NAPT44 based solution, even those in use today.

Another useful observation here is that the stateless 4via6 solution, actually allows an operator to retain existing troubleshooting procedures, given which today encompass CPE based NAPT44, rather than changing them radically to an AFTR. Furthermore, it is possible to alleviate any port-range constrains for users by allocating more generous port ranges without the need to manage such users configuration on active core network devices (eg AFTR).

3.6. Security

3.6.1. Overview

The issue relates to port randomization being used as a security mitigation for certain types of specialized attacks, as explained in [RFC6056] and the claim that a system with a restricted port range is grossly more vulnerable.
3.6.2. Discussion

The claim that a stateless 4via6 solution grossly affects security does not appear to be entirely accurate when considering the following i) the actual threat ii) a comparison to a centralized NAPT44 solution, at par value in terms of the number communicating of IP end-points (inside) utilizing the system iii) the ability to use native IPv6 as well as proposed extensions.

Assuming all other information has already been acquired, and also the presence of no exploits, the basic security of IP protocols lies in the computational cost of guessing a combination of a protocol field, eg a TCP sequence number or say a DNS transaction ID, multiplied by the cost of a guess of a source port. Thus, for a TCP brute force attack, the already substantial cost in guessing a sequence number (2^32 possibilities) is multiplied by the port range guess cost. In this context even an increase of say a 2^10 possibilities, corresponding for in a 1K port restricted 4V6 system, is costly enough for most practical purposes. For a UDP/DNS brute force attack, the computational cost required to scan/generate the full range of 2^32 possibilities, corresponding to a port unrestricted system is relatively low/easy - today’s GPUs can do so in a few seconds. UDP/DNS can be said to be inherently vulnerable, with the solution residing in DNSec. A 4V6 port restricted system would indeed lower such a computational cost, but for practical purposes it will still be in the order of seconds. Moreover, for the case of UDP/DNS, the CPE is expected to use its DNS proxy resolver functionality, which acting on native IPv6, is totally unaffected by the port restriction, and thus any of the security claims.

It’s relevant to note that a fully range free random port choice of a centralized NAPT44 system is also something that is unlikely, at least in terms of it being guaranteed, and thus does not form a very strong basis against a port restricted system. When a centralized NAPT44 function is multiplexing N end-points into a given outside IPv4 address, with an average of P ports per end-point, any given next flow from any of the end-points will be assigned to one of the (64k - N *P) available ports. This is dependent on dynamic N and P values, and not just on P, and thus making the port selection a function of the number of end-points as is the case with a stateless 4via6 solution.

Beyond the above, in terms of the avoiding a fixed linear or single port range allocations, extensions to the 4V6 solution provides additional remedy, eg [I-D.bajko-pripaddrassign].

In general thus, with a 4V6 solution it is possible to realize a viable level of security, which for practical purposes offers does
not and extending the 4V6 solution with. It remains an area of possible further proposals for optional port range randomization methods to be combined in a 4V6 solution.

3.7. Unknown Failure Modes

3.7.1. Overview

The issue purports that a system with a port constraints introduces new unknown failure modes, not known with NAT44 or NAPT44 systems, and in general is more complex than such a system.

3.7.2. Discussion

This claim does not appear to have objective technical arguments that can be discussed. A restricted port range system, such as the one assumed in this document, does not appear to have any more or less complexity than any of the other NAPT44 solutions against which the same issue has not been levelled. That is a statement that can be made in consideration of each of those alternative solution network design (eg elaborate routing rules or topologies) and feature implementation complexities, which appear to be no better than that of a stateless 4via6 address port range system. Ultimately, system complexity is something best left adjudicated by the operators choosing to deploy one or the other of these IP based transition solutions.

3.8. Possible Impact on NAT66 use & design

3.8.1. Overview

The notion of a shared address with a constrained port range is seen as possibly bearing influence on use in future schemes involving NAT66, where IPv6 address sharing is in general deemed not to be desired (ie there is good reason to avoid PAT66).

3.8.2. Discussion

The authors do not propose, nor expect to see the IP address sharing characteristic applying to future NAT66/PAT66 discussions and specification. However, having said that it is useful to take a humble step back and consider the general aspect of causality in this context. The direct cause that brought about IPv4 shared address solutions to the fore was a shortage/exhaustion of a limited IPv4 address resource, alongside a failure of the community to migrate IPv4 networks to IPv6 in a timely manner. At the time of writing it is hard to imagine the same occurring with respect to IPv6 address resources, and hopefully the same set of causes will not be allowed
to re-occur. This appears to be the only way to ensure that IPv6 address sharing effect does not come to be, as opposed to precluding such notions within the context of today’s IPv4 world where the causality is rather clear.

3.9. Port statistical multiplexing and monetization of port space

3.9.1. Overview

An issue attributed to port range constrained solutions is that due to their characteristic of assigning a fixed amount of ports to participating system nodes, the overall pool of ports cannot be dynamically/statistically multiplexed.

A corollary of this claimed issue is the claim that port range constraints will lead to monetization by service providers of such port ranges, for example by charging users based on the number of ports assigned or creating some bronze, silver, gold type of port based service categories. This is generally seen as an undesirable prospect due to it leading to "second class" Internet citizens(hip) in terms of a restriction of the ports utilizable by IP users.

3.9.2. Discussion

The 4via6 address shared solution indeed limits the ability to "overload" ie statistically multiplex amongst users, the ports available of a given public IPv4 address. This can be seen as a trade off vs dynamic allocation and the need to log (large amounts) of NAT bindings. Furthermore, the solution is meant to be fundamentally a transitional one for supporting legacy IPv4 users till full migration to IPv6 can occur. As an example, even with a static allocation of ~1000 ports per shared IP user, it allows an operator to effectively multiply by ~64 the current IPv4 unrealizable address space. To put it into a network growth perspective, it allows an operator to support for some 10 years a steady 50% annual increase in users, without requiring new IPv4 addresses. This is likely an alluring (if unlikely) prospect for most, but it demonstrates the fact that even with static port allocations, IPv4 address sharing can go a long way for many operators.

In terms of the corollary of this issue, the monetization of port space, the authors do not consider this claim to apply specifically to the restricted port range solution. It is a possibility that is and/all solutions that utilize NAPT44 technology allow. In essence any operator can, should they choose to do so, "monetize ports" using existing NAT techniques, including DS-Lite AFTR, and thus render their users "second class" citizens. This is a commercial decision, not a technical one, and does not appear to bear relevance to the
technical validity of a stateless 4via6 solution. To draw an analogy, guns and cannons can be used in a reckless manner or not. Thus it appears to be highly unbalanced to claim that one technology (eg cannons/DS-Lite) can to be developed by the community, but not the other (eg guns/a 4via6 address sharing solution).

3.10. Readdressing

3.10.1. Overview

Due to the port range encoding being part of the CPE’s IPv6 address, any change in the range requires a re-configuration of the CPEs 4via6 address. This is said to be an issue given the impact that IP address changes have on existing traffic flows, as well as general IPv6 network routing.

3.10.2. Discussion

It is true that under the assumed notions of the stateless 4via6 solution, IPv6 re-addressing is required to effect a change in terms of the shared IPv4 address or ports. Such changes can and are likely best done using dynamic address configuration methods such as DHCPv6, or alternatively out of band management tools, eg TR-69, especially when the 4via6 address can be derived from a delegated prefix. Using these, the impact of the address change does not translate to a neither a classic IPv6 host renumbering problem nor an unmanageable network renumbering problem. On the CPE, the change only affects the 4via6 address of the CPE and not any end user IPv6 hosts behind the CPE (which would likely continue to derive their IPv6 addresses from an unchanged delegated prefix). On the service provider network side, the change, if any, represents a network renumbering case which the operator can be reasonably expected to handle within their network numbering plan, especially given that the IPv6-prefix of the an IPv4-in-IPv6 address is summarizable.

An addressing change will impacting any existing IPv4 flows that are being NAT’ed by the CPE. This is also analogous to the today’s practice of IPv4 address changes espoused by some operators, which while not being commendable, is established in the market. Nevertheless, as a means of alleviating such an impact it appears desirable for the solutions to investigate the viability of mechanisms that could allow for more graceful addressing changes.

To facilitate IPv6 summarization and operator appears to have two 4V6 deployment choices. When encoding IPv4 addresses in lower order address space bits that are subject to summarization, the operator would need to assign a modest dedicated IPv6 prefix (such as a /64) as an 4V6 IPv6 addressing sub-domain. Alternatively, without
resorting to a separate 4V6 addressing sub-domain, an operator could allow for the IPv4 address embedding to be embedded in a high-order portion of the IPv6 domain address space, one that closely follows the IPv6 domain prefix. These two valid address subnetting and deployment options deserve better description in the solution specifications.

3.11. Ambiguity about communication between devices sharing an IP address.

3.11.1. Overview

A regular IPv4 destination based routed system inherently does not allow two devices to communicate while sharing the same IPv4 address, even if with different ports. Similarly, such a system does not allow on the basis of a IPv4 source address alone to perform address spoofing prevention. These two issues naturally render regular IPv4 based routed networks incapable of supporting a shared address solution.

3.11.2. Discussion

In terms of the IPv4 data plane of the 4via6 solution, the CPE and the stateless gateway components need to be modified in terms of their IPv4 forwarding behaviour. The CPE’s NAPT44 function, must be capable of sending traffic towards the IPv6 adaptation function when the traffic is addressed to its (shared) IPv4 address but a different port than the one assigned to the CPE. Similarly, the CPE’s NAPT44 function must be capable of receiving traffic addressed from its (shared) IPv4 address but a different port than the one assigned to it.

On the IPv6 data plane the stateless 4via6 solution does not suffer from the issue by the nature of relying on regular IPv6 forwarding. Address-spoofing security can be realized on regular IPv6 devices plane, in a way which effectively does not allow a CPE to send IPv6 traffic from a source IPv6 address that it has not been assigned. The spoofing of IPv4 addresses can be prevented in this manner in 4via6 solution relying on translation (dIVI). Tunneling 4via6 solutions (4rd) require IPv6+IPv4 source address validation to be performed at the CPE and stateless gateway, by the IPv6 adaptation function.

The conceptual IPv6 adaptation function has many of its core principles already defined either as part of IPinIP tunneling or stateless NAT64 drafts. However additional work, such as defining the port indexing schemes, is needed and is at the heart of what needs to be covered in the individual solution drafts that fall under
the stateless 4via6 family. Throughout, no legacy IPv4 end-systems are expected to implement these techniques.

4. Conclusion

As per the discussion in this document, the authors believe that the set of issues specifically attributed to A+P based such as the stateless 4via6 solution with characteristics as per Section 2, either do not apply, or can be mitigated. In several aspects, a stateless 4V6 solution represents a reasonable trade off compared to alternatives in areas such as NAT logging, ease as of deployment and operations, all of which are actually facilitated by such a solution.

5. IANA Considerations

This document does not raise any IANA considerations.

6. Security Considerations

This document does not introduce any security considerations over and above those already covered by the referenced stateless 4via6 solution drafts.

7. Contributors and Acknowledgements

The authors thank Dan Wing, Jan Zorz, Satoru Matsushima, Qiong Sun, and Arkadiusz Kaliwoda for their review and feedback on the draft.

8. References

8.1. Normative References


8.2. Informative References

[I-D.despres-softwire-4rd]
Despres, R., "IPv4 Residual Deployment across IPv6-Service networks (4rd) A NAT-less solution",
draft-despres-softwire-4rd-00 (work in progress),
October 2010.

[I-D.ietf-intarea-shared-addressing-issues]
Ford, M., Boucadair, M., Durand, A., Levis, P., and P.
Roberts, "Issues with IP Address Sharing",
draft-ietf-intarea-shared-addressing-issues-05 (work in progress),
March 2011.

[I-D.ietf-softwire-ds-lite-tunnel-option]
Hankins, D. and T. Mrugalski, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual- Stack Lite",
draft-ietf-softwire-ds-lite-tunnel-option-10 (work in progress),
March 2011.

[I-D.ietf-softwire-dual-stack-lite]
Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
Stack Lite Broadband Deployments Following IPv4 Exhaustion",
draft-ietf-softwire-dual-stack-lite-07 (work in progress),
March 2011.

[I-D.thaler-port-restricted-ip-issues]
Thaler, D., "Issues With Port-Restricted IP Addresses",
draft-thaler-port-restricted-ip-issues-00 (work in progress),
February 2010.

[I-D.wing-softwire-port-control-protocol]
Wing, D., Penno, R., and M. Boucadair, "Pinhole Control Protocol (PCP)"

draft-wing-softwire-port-control-protocol-02 (work in progress),
July 2010.

[I-D.xli-behave-divi]
Li, X., Bao, C., and H. Zhang, "Address-sharing stateless
double IVI",
draft-xli-behave-divi-01 (work in progress),
October 2009.

[I-D.ymbk-aplusp]
Bush, R., "The A+P Approach to the IPv4 Address Shortage",
draft-ymbk-aplusp-09 (work in progress),
February 2011.

[RFC6052]
Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X.
Li, "IPv6 Addressing of IPv4/IPv6 Translators",
RFC 6052,
October 2010.

Author’s Address

Wojciech Dec (editor)
Cisco Systems
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands

Email: wdec@cisco.com