

6MAN  
Internet-Draft  
Intended status: Informational  
Expires: July 10, 2014

B. Carpenter, Ed.  
Univ. of Auckland  
T. Chown  
Univ. of Southampton  
F. Gont  
SI6 Networks / UTN-FRH  
S. Jiang  
Huawei Technologies Co., Ltd  
A. Petrescu  
CEA, LIST  
A. Yourtchenko  
cisco  
January 6, 2014

**Analysis of the 64-bit Boundary in IPv6 Addressing**  
**draft-carpenter-6man-why64-00**

Abstract

The IPv6 unicast addressing format includes a separation between the prefix used to route packets to a subnet and the interface identifier used to specify a given interface connected to that subnet. Historically the interface identifier has been defined as 64 bits long, leaving 64 bits for the prefix. This document discusses the reasons for this fixed boundary and the issues involved in treating it as a variable boundary.

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 July 10, 2014.

## Copyright Notice

Copyright (c) 2014 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

|                       |  |                    |
|-----------------------|--|--------------------|
| <a href="#">1.</a>    | Introduction . . . . .                           | <a href="#">2</a>  |
| <a href="#">2.</a>    | Scenarios for prefixes longer than /64 . . . . . | <a href="#">3</a>  |
| <a href="#">2.1.</a>  | Insufficient address space delegated . . . . .   | <a href="#">3</a>  |
| <a href="#">2.2.</a>  | Concerns over ND cache exhaustion . . . . .      | <a href="#">3</a>  |
| <a href="#">3.</a>    | Interaction with IPv6 specifications . . . . .   | <a href="#">4</a>  |
| <a href="#">4.</a>    | Possible areas of breakage . . . . .             | <a href="#">6</a>  |
| <a href="#">5.</a>    | Experimental observations . . . . .              | <a href="#">7</a>  |
| <a href="#">6.</a>    | Privacy issues . . . . .                         | <a href="#">7</a>  |
| <a href="#">7.</a>    | Implementation and deployment issues . . . . .   | <a href="#">8</a>  |
| <a href="#">8.</a>    | Conclusion . . . . .                             | <a href="#">8</a>  |
| <a href="#">9.</a>    | Security Considerations . . . . .                | <a href="#">8</a>  |
| <a href="#">10.</a>   | IANA Considerations . . . . .                    | <a href="#">9</a>  |
| <a href="#">11.</a>   | Acknowledgements . . . . .                       | <a href="#">9</a>  |
| <a href="#">12.</a>   | Change log [RFC Editor: Please remove] . . . . . | <a href="#">9</a>  |
| <a href="#">13.</a>   | References . . . . .                             | <a href="#">9</a>  |
| <a href="#">13.1.</a> | Normative References . . . . .                   | <a href="#">9</a>  |
| <a href="#">13.2.</a> | Informative References . . . . .                 | <a href="#">11</a> |
|                       | Authors' Addresses . . . . .                     | <a href="#">13</a> |

## [1.](#) Introduction

The IPv6 addressing architecture [[RFC4291](#)] specifies that a unicast address is divided into  $n$  bits of subnet prefix followed by  $(128-n)$  bits of interface identifier (IID). Since IPv6 routing is entirely based on variable length subnet masks, there is no architectural assumption that  $n$  has any particular fixed value. However, [RFC 4291](#) also describes a method of forming interface identifiers from IEEE EUI-64 hardware addresses [[IEEE802](#)] and this does specify that such interface identifiers are 64 bits long. Various other methods of forming interface identifiers also specify a length of 64 bits. This has therefore become the de facto length of almost all IPv6 interface



identifiers. One exception is documented in [[RFC6164](#)], which standardises 127-bit prefixes for inter-router links.

Recently it has been clarified that the bits in an IPv6 interface identifier have no particular meaning and should be treated as opaque values [[I-D.ietf-6man-ug](#)]. Therefore, there are no bit positions in the currently used 64 bits that need to be preserved.

The question is often asked why the boundary is set rigidly at /64. This limits the length of a routing prefix to 64 bits, whereas architecturally, and from the point of view of routing protocols, it could be anything (in theory) between /1 and /128 inclusive. Here, we only discuss the question of a shorter IID, allowing a longer routing prefix.

The purpose of this document is to analyse the issues around this question. We make no proposal for change, but we do analyse the possible effects of a change.

## **[2.](#) Scenarios for prefixes longer than /64**

In this section we describe existing scenarios where prefixes longer than /64 have been used or proposed.

### **[2.1.](#) Insufficient address space delegated**

A site may not be delegated a sufficiently large prefix from which to allocate a /64 prefix to all of its internal subnets. In this case the site may either determine that it does not have enough address space to number all its network elements and thus, at the very best, be only partially operational, or it may choose to use internal prefixes longer than /64 to allow multiple subnets and the hosts within them to be configured with addresses.

In this case, the site might choose, for example, to use a /80 per subnet, in combination with hosts using either manually configured addressing or DHCPv6.

It should be noted that the homenet architecture text [[I-D.ietf-homenet-arch](#)] states that a CPE should consider the lack of sufficient address space to be an error condition, rather than using prefixes longer than /64 internally.

### **[2.2.](#) Concerns over ND cache exhaustion**

A site may be concerned that it is open to neighbour discovery (ND) cache exhaustion attacks, whereby an attacker sends a large number of messages in rapid succession to a series of (most likely inactive)



host addresses within a specific subnet, in an attempt to fill a router's ND cache with ND requests pending completion, in so doing denying correct operation to active devices on the network.

An example would be to use a /120 prefix, limiting the number of addresses in the subnet to be similar to an IPv4 /24 prefix, which should not cause any concerns for ND cache exhaustion. Note that the prefix does need to be quite long for this scenario to be valid. The number of theoretically possible ND cache slots on the segment needs to be of the same order of magnitude as the actual number of hosts. Thus small increases from the /64 prefix length do not have a noticeable impact: even  $2^{32}$  potential entries, a factor of two billion decrease compared to  $2^{64}$ , is still more than enough to exhaust the memory on current routers.

As in the previous scenario, hosts would likely be manually configured with addresses, or use DHCPv6.

### 3. Interaction with IPv6 specifications

The precise 64-bit length of the Interface ID is widely mentioned in numerous RFCs describing various aspects of IPv6. It is not straightforward to distinguish cases where this has normative impact or affects interoperability.

First and foremost, the RFCs describing the architectural aspects of IPv6 addressing explicitly state, refer and repeat this apparently immutable value: Addressing Architecture [[RFC4291](#)], Reserved Interface Identifiers [[RFC5453](#)], ILNP [[RFC6741](#)]. Customer Edge routers impose /64 for their interfaces [[RFC7084](#)]. Only the IPv6 Subnet Model [[RFC5942](#)] refers to the assumption of /64 prefix length as a potential implementation error.

Numerous IPv6-over-foo documents make mandatory statements with respect to the 64-bit length of the Interface ID to be used during the Stateless Autoconfiguration. These documents are [[RFC2464](#)] (Ethernet), [[RFC2467](#)] (FDDI), [[RFC2470](#)] (Token Ring), [[RFC2492](#)] (ATM), [[RFC2497](#)] (ARCnet), [[RFC2590](#)] (Frame Relay), [[RFC3146](#)] (IEEE 1394), [[RFC4338](#)] (Fibre Channel), [[RFC4944](#)] (IEEE 802.15.4), [[RFC5072](#)] (PPP), [[RFC5121](#)] [[RFC5692](#)] (IEEE 802.16), [[I-D.ietf-6lowpan-btle](#)], [[I-D.ietf-6man-6lobac](#)], [[I-D.brandt-6man-lowpanz](#)].

To a lesser extent, the address configuration RFCs themselves may in some way assume the 64-bit length of an Interface ID (SLAAC for the link-local addresses, DHCPv6 for the potentially assigned EUI-64-based IP addresses, Default Router Preferences [[RFC4191](#)] for its impossibility of Prefix Length 4, Optimistic Duplicate Address



Detection [[RFC4429](#)] which computes 64-bit-based collision probabilities).

The MLDv2 protocol [[RFC3810](#)] mandates all queries be sent with the fe80::/64 link-local source address prefix and subsequently bases the querier election algorithm on the link-local subnet prefix length of length /64.

The IPv6 Flow Label Specification [[RFC6437](#)] gives an example of a 20-bit hash function generation which relies on splitting an IPv6 address in two equally-sized 64bit-length parts.

IPv6 transition mechanisms such as NAT64 and NPTv6, as well as Basic transition and Teredo rely on the use of IIDs of length 64.

The proposed method [[I-D.ietf-v6ops-64share](#)] of extending an assigned /64 prefix from a smartphone's cellular interface to its WiFi link relies on prefix length, and implicitly on the length of the Interface ID, to be valued at 64.

The HBA, CGA and SeND RFCs rely on the 64bit identifier length, as do the Privacy extensions and some examples in IKEv2bis.

464XLAT [[RFC6877](#)] explicitly mentions acquiring /64 prefixes. However, it also discusses the possibility of using the interface address on the device as the endpoint for the traffic, thus potentially removing this dependency.

[RFC2526] reserves a number of subnet anycast addresses by reserving some anycast IIDs. An anycast IID so reserved cannot be less than 7 bits long. This means that a subnet prefix length longer than /121 is not possible, and a subnet of exactly /121 would be useless since all its identifiers are reserved. It also means that half of a /120 is reserved for anycast. This could of course be fixed in the way described for /127 in [[RFC6164](#)], i.e., avoiding the use of anycast within a /120 subnet.

Other RFCs refer to mandatory alignment on 64-bit boundaries, 64-bit data structures, 64-bit counters in MIB, 64-bit sequence numbers and cookies in security. Finally, the 64 number may be considered 'magic' in some RFCs, (e.g., 64k limits in DNS and Base64 encodings in MIME) but this of course has no influence on the length of the IID. All the same, a programmer might be lulled into assuming a comfortable rule of thumb that an IID is always length 64.





#### **4. Possible areas of breakage**

This section discusses several specific aspects of IPv6 where we can expect operational breakage with subnet prefixes other than /64.

- o Multicast: [[RFC3306](#)] defines a method for generating IPv6 multicast group addresses based on unicast prefixes. This method assumes a longest network prefix of 64 bits. If a longer subnet is used, there is no way to generate a specific multicast group address using this method. In such cases the administrator would need to use a shorter prefix from within their allocation (a /64 or shorter) from which to generate the group address.

Similarly [[RFC3956](#)], which specifies Embedded-RP, allowing IPv6 multicast rendezvous point addresses to be embedded in the multicast group address, would also fail, as the scheme assumes a maximum prefix length of 64 bits.

- o CGA: The Cryptographically Generated Address format (CGA, [[RFC3972](#)]) is heavily based on a /64 interface identifier. [[RFC3972](#)] has defined a detailed algorithm how to generate 64-bit interface identifier from a public key and a 64-bit subnet prefix. Breaking the /64 boundary would certainly break the current CGA definition. However, CGA might benefit in a redefined version if more bits are used for interface identifier (which means shorter prefix length). For now, 59 bits are used for cryptographic purposes. The more bits are available, the stronger CGA could be. Conversely, longer prefixes would weaken CGA.
- o NAT64: Both stateless [[RFC6052](#)] NAT64 and stateful NAT64 [[RFC6146](#)] are flexible for the prefix length. [[RFC6052](#)] has defined multiple address formats for NAT64. In [Section 2](#) "IPv4-Embedded IPv6 Prefix and Format" of [[RFC6052](#)], the network-specific prefix could be one of /32, /40, /48, /56, /64 and /96. The remaining part of the IPv6 address is constructed by a 32-bit IPv4 address, a 8-bit u byte and a variable length suffix (there is no u byte and suffix in the case of 96-bit Well-Known Prefix). NAT64 is therefore OK with a boundary out to /96, but not longer.
- o NPTv6: IPv6-to-IPv6 Network Prefix Translation [[RFC6296](#)] is also bound to /64 boundary. NPTv6 maps a /64 prefix with other /64 prefix. When the NPTv6 Translator is configured with a /48 or shorter prefix, the 64-bit interface identifier is kept unmodified during translation. However, the /64 boundary might be broken as long as the "inside" and "outside" prefix has the same length.
- o ILNP: Identifier-Locator Network Protocol (ILNP) [[RFC6741](#)] is designed around the /64 boundary, since it relies on locally



unique 64-bit interface identifiers. While a re-design to use longer prefixes is not inconceivable, this would need major changes to the existing specification for the IPv6 version of ILNP.

- o shim6: The Multihoming Shim Protocol for IPv6 (shim6) [[RFC5533](#)] in its insecure form treats IPv6 address as opaque 128-bit objects. However, to secure the protocol against spoofing, it is essential to either use CGAs (see above) or Hash-Based Addresses (HBA) [[RFC5535](#)]. Like CGAs, HBAs are generated using a procedure that assumes a 64-bit identifier. Therefore, in effect, secure shim6 is affected by the /64 boundary exactly like CGAs.
- o others?

It goes without saying that if prefixes longer than /64 are to be used, all hosts must be capable of generating IIDs shorter than 64 bits, in order to follow the auto-configuration procedure correctly [[RFC4862](#)]. There is however the rather special case of the link-local prefix. While [RFC 4862](#) is careful not to define any specific length of link-local prefix within fe80::/10, operationally there would be a problem unless all hosts on a link use IIDs of the same length to configure a link-local address during reboot. Typically today the choice of /64 for the link-local prefix length is hard-coded per interface. There might be no way to change this except conceivably by manual configuration, which will be impossible if the host concerned has no local user interface.

## 5. Experimental observations

Still to be written - some experiments are underway, and more input is welcomed. Some points made earlier on the v6ops list can be incorporated here.

## 6. Privacy issues

The length of the interface identifier has implications for privacy [[I-D.ietf-6man-ipv6-address-generation-privacy](#)]. In any case in which the value of the identifier is intended to be hard to guess, whether or not it is cryptographically generated, it is apparent that more bits are better. For example, if there are only 20 bits to be guessed, at most just over a million guesses are needed, today well within the capacity of a low cost attack mechanism. It is hard to state in general how many bits are enough to protect privacy, since this depends on the resources available to the attacker, but it seems clear that a privacy solution needs to resist an attack requiring billions rather than millions of guesses. Trillions would be better, suggesting that at least 40 bits should be available. Thus we can



argue that subnet prefixes longer than say /80 might raise privacy concerns by making the IID guessable.

A prefix long enough to limit the number of addresses comparably to an IPv4 subnet, such as /120, would create exactly the same situation for privacy as IPv4.

## **7. Implementation and deployment issues**

Still to be written - suggestions welcome. Some points made earlier on the v6ops list can be incorporated here.

## **8. Conclusion**

Summary of pros and cons; risks (write this bit last!)

## **9. Security Considerations**

In addition to the privacy issues mentioned in [Section 6](#), and the issues mentioned with CGAs and HBAs in [Section 4](#), the length of the subnet prefix affects the matter of defence against scanning attacks [[RFC5157](#)]. Assuming the attacker has discovered or guessed the prefix length, a longer prefix reduces the space that the attacker needs to scan, e.g., to only 256 addresses if the prefix is /120. On the other hand, if the attacker has not discovered the prefix length and assumes it to be /64, routers can trivially discard attack packets that do not fall within an actual subnet.

However, assume that an attacker finds one valid address A and then starts a scanning attack by scanning "outwards" from A, by trying A+1, A-1, A+2, A-2, etc. This attacker will easily find all hosts in any subnet with a long prefix, because they will have addresses close to A. We therefore conclude that any prefix containing densely packed valid addresses is vulnerable to a scanning attack, without the attacker needing to guess the prefix length. Therefore, to preserve IPv6's advantage over IPv4 in resisting scanning attacks, it is important that subnet prefixes are short enough to allow sparse allocation of identifiers within each subnet. The considerations are similar to those for privacy, and we can again argue that prefixes longer than say /80 might significantly increase vulnerability. Ironically, this argument is exactly converse to the argument for longer prefixes to resist an ND cache attack, as described in [Section 2.2](#).



## **10. IANA Considerations**

This document requests no action by IANA.

## **11. Acknowledgements**

Valuable comments were received from Stig Venaas, ... and other participants in the IETF.

This document was produced using the xml2rfc tool [[RFC2629](#)].

## **12. Change log [RFC Editor: Please remove]**

[draft-carpenter-6man-why64-00](#): original version, 2014-01-06.

## **13. References**

### **13.1. Normative References**

- [I-D.ietf-6man-ug]  
Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", [draft-ietf-6man-ug-06](#) (work in progress), December 2013.
- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", [RFC 2464](#), December 1998.
- [RFC2467] Crawford, M., "Transmission of IPv6 Packets over FDDI Networks", [RFC 2467](#), December 1998.
- [RFC2470] Crawford, M., Narten, T., and S. Thomas, "Transmission of IPv6 Packets over Token Ring Networks", [RFC 2470](#), December 1998.
- [RFC2492] Armitage, G., Schulter, P., and M. Jork, "IPv6 over ATM Networks", [RFC 2492](#), January 1999.
- [RFC2497] Souvatzis, I., "Transmission of IPv6 Packets over ARCnet Networks", [RFC 2497](#), January 1999.
- [RFC2526] Johnson, D. and S. Deering, "Reserved IPv6 Subnet Anycast Addresses", [RFC 2526](#), March 1999.
- [RFC2590] Conta, A., Malis, A., and M. Mueller, "Transmission of IPv6 Packets over Frame Relay Networks Specification", [RFC 2590](#), May 1999.





- [RFC3146] Fujisawa, K. and A. Onoe, "Transmission of IPv6 Packets over IEEE 1394 Networks", [RFC 3146](#), October 2001.
- [RFC3306] Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", [RFC 3306](#), August 2002.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", [RFC 3810](#), June 2004.
- [RFC3956] Savola, P. and B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", [RFC 3956](#), November 2004.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", [RFC 4191](#), November 2005.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.
- [RFC4338] DeSanti, C., Carlson, C., and R. Nixon, "Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel", [RFC 4338](#), January 2006.
- [RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", [RFC 4429](#), April 2006.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.
- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", [RFC 4944](#), September 2007.
- [RFC5072] Varada, S., Haskins, D., and E. Allen, "IP Version 6 over PPP", [RFC 5072](#), September 2007.
- [RFC5121] Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", [RFC 5121](#), February 2008.
- [RFC5157] Chown, T., "IPv6 Implications for Network Scanning", [RFC 5157](#), March 2008.



- [RFC5453] Krishnan, S., "Reserved IPv6 Interface Identifiers", [RFC 5453](#), February 2009.
- [RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", [RFC 5533](#), June 2009.
- [RFC5535] Bagnulo, M., "Hash-Based Addresses (HBA)", [RFC 5535](#), June 2009.
- [RFC5692] Jeon, H., Jeong, S., and M. Riegel, "Transmission of IP over Ethernet over IEEE 802.16 Networks", [RFC 5692](#), October 2009.
- [RFC5942] Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", [RFC 5942](#), July 2010.
- [RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", [RFC 6052](#), October 2010.
- [RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", [RFC 6146](#), April 2011.
- [RFC6164] Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", [RFC 6164](#), April 2011.
- [RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", [RFC 6296](#), June 2011.
- [RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", [RFC 6437](#), November 2011.
- [RFC6741] Atkinson, R., "Identifier-Locator Network Protocol (ILNP) Engineering Considerations", [RFC 6741](#), November 2012.
- [RFC7084] Singh, H., Beebee, W., Donley, C., Stark, B., "Basic Requirements for IPv6 Customer Edge Routers", [RFC 7084](#), November 2013.

### **[13.2.](#) Informative References**



[I-D.brandt-6man-lowpanz]

Brandt, A. and J. Buron, "Transmission of IPv6 packets over ITU-T G.9959 Networks", [draft-brandt-6man-lowpanz-02](#) (work in progress), June 2013.

[I-D.ietf-6lowpan-btle]

Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "Transmission of IPv6 Packets over BLUETOOTH Low Energy", [draft-ietf-6lowpan-btle-12](#) (work in progress), February 2013.

[I-D.ietf-6man-6lobac]

Lynn, K., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over MS/TP Networks", [draft-ietf-6man-6lobac-01](#) (work in progress), March 2012.

[I-D.ietf-6man-ipv6-address-generation-privacy]

Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", [draft-ietf-6man-ipv6-address-generation-privacy-00](#) (work in progress), October 2013.

[I-D.ietf-homenet-arch]

Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", [draft-ietf-homenet-arch-11](#) (work in progress), October 2013.

[I-D.ietf-v6ops-64share]

Byrne, C., Drown, D., and V. Ales, "Extending an IPv6 /64 Prefix from a 3GPP Mobile Interface to a LAN link", [draft-ietf-v6ops-64share-09](#) (work in progress), October 2013.

[IEEE802] IEEE, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", IEEE Std 802-2001 (R2007), 2007.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#), June 1999.

[RFC6741] Atkinson, R., "Identifier-Locator Network Protocol (ILNP) Engineering Considerations", [RFC 6741](#), November 2012.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", [RFC 6877](#), April 2013.



## Authors' Addresses

Brian Carpenter (editor)  
Department of Computer Science  
University of Auckland  
PB 92019  
Auckland 1142  
New Zealand

Email: [brian.e.carpenter@gmail.com](mailto:brian.e.carpenter@gmail.com)

Tim Chown  
University of Southampton  
Southampton, Hampshire S017 1BJ  
United Kingdom

Email: [tjc@ecs.soton.ac.uk](mailto:tjc@ecs.soton.ac.uk)

Fernando Gont  
SI6 Networks / UTN-FRH  
Evaristo Carriego 2644  
Haedo, Provincia de Buenos Aires 1706  
Argentina

Email: [fgont@si6networks.com](mailto:fgont@si6networks.com)

Sheng Jiang  
Huawei Technologies Co., Ltd  
Q14, Huawei Campus  
No.156 Beiqing Road  
Hai-Dian District, Beijing 100095  
P.R. China

Email: [jiangsheng@huawei.com](mailto:jiangsheng@huawei.com)

Alexandru Petrescu  
CEA, LIST  
CEA Saclay  
Gif-sur-Yvette, Ile-de-France 91190  
France

Email: [Alexandru.Petrescu@cea.fr](mailto:Alexandru.Petrescu@cea.fr)





Andrew Yourtchenko

cisco

7a de Kleetlaan

Diegem 1830

Belgium

Email: [ayourtch@cisco.com](mailto:ayourtch@cisco.com)