

Transport Services (taps) Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 22, 2018

F. Gont  
SI6 Networks / UTN-FRH  
G. Gont  
SI6 Networks  
M. Garcia Corbo  
SITRANS  
C. Huitema  
Private Octopus Inc.  
March 21, 2018

**Problem Statement Regarding IPv6 Address Usage  
draft-gont-taps-address-analysis-00**

**Abstract**

This document analyzes the security, privacy, and interoperability implications of IPv6 addresses based on a number of properties (such as address scope, stability, and usage type).

**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 <https://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 22, 2018.

**Copyright Notice**

Copyright (c) 2018 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 (<https://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>	<a href="#">Introduction . . . . .</a>	<a href="#">2</a>
<a href="#">2.</a>	<a href="#">Terminology . . . . .</a>	<a href="#">2</a>
<a href="#">3.</a>	<a href="#">Background . . . . .</a>	<a href="#">3</a>
<a href="#">4.</a>	<a href="#">IPv6 Address Properties . . . . .</a>	<a href="#">3</a>
<a href="#">4.1.</a>	<a href="#">Address Scope Considerations . . . . .</a>	<a href="#">3</a>
<a href="#">4.2.</a>	<a href="#">Address Stability Considerations . . . . .</a>	<a href="#">4</a>
<a href="#">4.3.</a>	<a href="#">Usage Type Considerations . . . . .</a>	<a href="#">5</a>
<a href="#">5.</a>	<a href="#">Issues Associated with Sub-optimal IPv6 Address Usage . . . . .</a>	<a href="#">7</a>
<a href="#">5.1.</a>	<a href="#">Correlation of Network Activity . . . . .</a>	<a href="#">7</a>
<a href="#">5.2.</a>	<a href="#">Testing for the Presence of Node in the Network . . . . .</a>	<a href="#">7</a>
<a href="#">5.3.</a>	<a href="#">Unexpected Address Discovery . . . . .</a>	<a href="#">7</a>
<a href="#">5.4.</a>	<a href="#">Availability Outside the Expected Scope . . . . .</a>	<a href="#">8</a>
<a href="#">6.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">8</a>
<a href="#">7.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">8</a>
<a href="#">8.</a>	<a href="#">Acknowledgements . . . . .</a>	<a href="#">9</a>
<a href="#">9.</a>	<a href="#">References . . . . .</a>	<a href="#">9</a>
<a href="#">9.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">9</a>
<a href="#">9.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">10</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">11</a>

## [1.](#) Introduction

IPv6 addresses may differ in a number of properties, such as address scope (e.g. link-local vs. global), stability (e.g. stable addresses vs. temporary addresses), and intended usage type (outgoing communications vs. incoming communications). While often overlooked, these properties have impact on areas such as security, privacy, and interoperability.

This document analyzes the impact of a number of properties of IPv6 addresses on areas such as security and privacy, and analyzes how IPv6 addresses are currently generated and employed by different operating systems and applications.

## [2.](#) Terminology

This document employs the definitions of "public address", "stable address", and "temporary address" from [Section 2 of \[RFC7721\]](#).

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 \[RFC2119\]](#).



### **3. Background**

Predictable IPv6 addresses result in a number of security and privacy implications. For example, [[Barnes2012](#)] discusses how patterns in network prefixes can be leveraged for IPv6 address scanning. On the other hand, [[RFC7707](#)], [[RFC7721](#)] and [[RFC7217](#)] discuss the security and privacy implications of predictable IPv6 Interface Identifiers (IIDs).

Given the aforementioned previous work in this area, and the formal specification update produced by [[RFC8064](#)], we expect (and assume in the rest of this document) that implementations have replaced any schemes that produce predictable addresses with alternative schemes that avoid such patterns (e.g., [RFC7217](#) in replacement of the traditional SLAAC addresses that embed link-layer addresses).

### **4. IPv6 Address Properties**

There are three parameters that affect the security and privacy properties of an IPv6 address:

- o Scope
- o Stability
- o Usage type (client-like "outgoing connections" vs. server-like "incoming connections")

[Section 4.1](#), [Section 4.2](#), and [Section 4.3](#) discuss the security and privacy implications (and associated tradeoffs) of the scope, stability and usage type properties of IPv6 addresses, respectively.

#### **4.1. Address Scope Considerations**

The IPv6 address scope can, in some scenarios, limit the attack exposure of a node as a result of the implicit isolation provided by a non-global address scope. For example, a node that only employs link-local addresses may, in principle, only be exposed to attack from other nodes in the local link. Hosts employing only Unique Local Addresses (ULAs) may be more isolated from attack than those employing Global Unicast Addresses (GUAs), assuming that proper packet filtering is enforced at the network edge.

The potential protection provided by a non-global addresses should not be regarded as a complete security strategy, but rather as a form of "prophylactic" security (see [[I-D.gont-opsawg-firewalls-analysis](#)]).



We note that the use of non-global addresses is usually limited to a reduced type of applications/protocols that e.g. are only meant to operate on a reduced scope, and hence their applicability may be limited.

A discussion of ULA usage considerations can be found in [\[I-D.ietf-v6ops-ula-usage-considerations\]](#).

#### **4.2. Address Stability Considerations**

The stability of an address has two associated security/privacy implications:

- o Ability of an attacker to correlate network activity
- o Exposure to attack

For obvious reasons, an address that is employed for multiple communication instances allows the aforementioned network activities to be correlated. The longer an address is employed (i.e., the more stable it is), the longer such correlation will be possible. In the worst-case scenario, a stable address that is employed for multiple communication instances over time will allow all such activities to be correlated. On the other hand, if a host were to generate (and eventually "throw away") one new address for each communication instance (e.g., TCP connection), network activity correlation would be mitigated.

##### **NOTE:**

The use of constant IIDs (as in traditional SLAAC) result in addresses that, while not constant as a whole (since the prefix changes), contain a globally-unique value that leaks out the node "identity". Such addresses result in the worst possible security and privacy implications, and their use has been deprecated by [\[RFC8064\]](#).

Typically, when it comes to attack exposure, the longer an address is employed the longer an attacker is exposed to attacks (e.g. an attacker has more time to find the address in the first place [\[RFC7707\]](#)). While such exposure is traditionally associated with the stability of the address, the usage type of the address (see [Section 4.3](#)) may also have an impact on attack exposure.

A popular approach to mitigate network activity correlation is the use of "temporary addresses" [\[RFC4941\]](#). Temporary addresses are typically configured and employed along with stable addresses, with the temporary addresses employed for outgoing communications, and the stable addresses employed for incoming communications.



**NOTE:**

Ongoing work [[I-D.gont-6man-non-stable-iids](#)] aims at updating [[RFC4941](#)] such that temporary addresses can be employed without the need to configure stable addresses.

We note that the extent to which temporary addresses provide improved mitigation of network activity correlation and/or reduced attack exposure may be questionable and/or limited in some scenarios. For example, a temporary address that is reachable for, say, a few hours has a questionable "reduced exposure" (particularly when automated attack tools do not typically require such a long period of time to complete their task). Similarly, if network activity can be correlated for the life of such address (e.g., on the order of several hours), such period of time might be long enough for the attacker to correlate all the network activity he is meaning to correlate.

In order to better mitigate network activity correlation and/or possibly reduce host exposure, an implementation might want to either reduce the preferred lifetime of a temporary address, or even better, generate one new temporary address for each new transport protocol instance. However, the associated lifetime/stability of an address may have a negative impact on the network. For example, if a node were to employ "throw away" IPv6 addresses, or employ temporary addresses [[RFC4941](#)] with a short preferred lifetime, local nodes might need to maintain too many entries in their Neighbor Cache, and a number of devices (possibly enforcing security policies) might also need to cope with such additional state.

Additionally, enforcing a maximum lifetime on IPv6 addresses may cause long-lived TCP connections to fail. For example, an address becoming "Invalid" (after transitioning through the "Preferred" and "Deprecated" states) would cause the TCP connections employing them to break. This, in turn, would cause e.g. long-lived SSH sessions to break/fail.

In some scenarios, attack exposure may be reduced by limiting the usage of temporary addresses to outgoing connections, and prevent such addresses from being used for incoming connections (please see [Section 4.3](#)).

#### **[4.3.](#) Usage Type Considerations**

A node that employs one of its addresses to communicate with an external server (i.e., to perform an "outgoing connection") may cause such address to become exposed to attack. For example, once the external server receives an incoming connection, the corresponding server might launch an attack against the aforementioned address. A





real-world instance of this type of scenario has been documented in [\[Hein\]](#).

However, we note that employing an IPv6 address for outgoing communications need not increase the exposure of local services to other parties. For example, nodes could employ temporary addresses only for outgoing connections, but not for incoming connections. Thus, external nodes that learn about client's addresses could not really leverage such addresses for actively contacting the clients.

There are multiple ways in which this could possibly be achieved, with different implications. Namely:

- o Run a host-based or network-based firewall
- o Bind services to specific (explicit) addresses
- o Bind services only to stable addresses

A client could simply run a host-based firewall that only allows incoming connections on the stable addresses. This is clearly more of an operational way of achieving the desired functionality, and may require good firewall/host integration (e.g., the firewall should be able to tell stable vs. temporary addresses), may require the client to run additional firewall software for this specific purpose, etc. In other scenarios, a network-based firewall could be configured to allow outgoing communications from all internal addresses, but only allow incoming communications to stable addresses. For obvious reasons, this is generally only applicable to networks where incoming communications are allowed to a limited number of hosts/servers.

Services could be bound to specific (explicit) addresses, rather than to all locally-configured addresses. However, there are a number of short-comings associated with this approach. Firstly, an application would need to be able to learn all of its addresses and associated stability properties, something that tends to be non-trivial and non-portable, and that also makes applications protocol-dependent, unnecessarily. Secondly, the BSD Sockets API does not really allow a socket to be bound to a subset of the node's addresses. That is, sockets can be bound to a single address or to all available addresses (wildcard), but not to a subset of all the configured addresses.

Binding services only to stable addresses provides a clean separation between addresses employed for client-like outgoing connections and server-like incoming connections. However, we currently lack an appropriate API for nodes to be able to specify that a socket should only be bound to stable addresses.



## **5. Issues Associated with Sub-optimal IPv6 Address Usage**

### **5.1. Correlation of Network Activity**

As discussed in [[RFC7721](#)], a node that reuses an IPv6 address for multiple communication instances would allow the correlation of such network activities. This could be the case when the same IPv6 address is employed by several instances of the same application (e.g., a browser in "privacy" mode and a browser in "normal" mode), or when the same IPv6 address is employed by two different applications on the same node (e.g., a browser in "privacy" mode, and an email client).

Particularly for privacy-sensitive applications, an application or system might want to limit the usage of a given IPv6 address to a single communication instance, a single application, a single user on the system, etc. However, given current APIs, this is practically impossible.

### **5.2. Testing for the Presence of Node in the Network**

The stable addresses recommended in [[RFC8064](#)] use stable IIDs defined in [[RFC7217](#)]. One key part of that algorithm is that if a device connects to a given network at different times, it will always configure the same IPv6 addresses on that network. If the device hosts a service ready to accept connections on that stable address, adversaries can test the presence of the device on the network by attempting connections to that stable address. Stable addresses used by listening services will thus enable testing whether a specific device is returning to a particular network, which in a number of cases might be considered a privacy issue.

### **5.3. Unexpected Address Discovery**

Systems like DNS-Based Service Discovery [[RFC6763](#)] allow clients to discover services within a limited scope, that can be defined by a domain name. These services are not advertised outside of that scope, and thus do not expect to be discovered by random parties on the Internet. However, such services may be easily discoverable if they listen for connections to IPv6 addresses that a client process also uses as source address when connecting to remote servers.

#### **NOTE:**

An example of such unexpected discovery is described in [[Hein](#)]. A network manager observed scanning traffic directed at the temporary addresses of local devices. The analysis in [[Hein](#)] shows that the scanners learned the addresses by observing the device contact an NTP service ([[RFC5905](#)]). The remote scanning



was possible because the local devices were also accepting connections directed to the temporary addresses.

It should be obvious from the example that the "attack surface" of the services is increased because they are bound to the same IPv6 addresses that are also used by clients for outgoing communications with remote systems. But the overlap between "client" and "server" addresses is only one part of the problem. Suppose that a device hosts both a video game and a home automation application. The video game users will be able to discover the IPv6 address of the game server. If the home automation server listens to the same IPv6 addresses, it is now exposed to connection attempts by all these users. That, too, increases the attack surface of the home automation server.

#### **5.4. Availability Outside the Expected Scope**

The IPv6 addressing architecture [[RFC4291](#)] defines multiple address scopes. In practice, devices are often configured with globally reachable unicast addresses, link local addresses, and Unique Local IPv6 Unicast Addresses (ULA) [[RFC4193](#)]. Availability outside the expected scope happens when a service is expected to be only available in some local scope, but inadvertently becomes available to remote parties. That could happen for example if a service is meant to be available only on a given link, but becomes reachable through ULA or through globally reachable addresses, or if a service is meant to be available only inside some organization's perimeter and becomes reachable through globally reachable addresses. It will happen in particular if a service intended for some local scope is programmed to bind to "unspecified" addresses, which in practice means every address configured for the device.

### **6. IANA Considerations**

There are no IANA registries within this document. The RFC-Editor can remove this section before publication of this document as an RFC.

### **7. Security Considerations**

The security and privacy implications associated with the predictability and lifetime of IPv6 addresses has been analyzed in [[RFC7217](#)] [[RFC7721](#)], and [[RFC7707](#)]. This document complements and extends the aforementioned analysis by considering other IPv6 properties such as the address scope and address usage type, and the associated tradeoffs.



## **8. Acknowledgements**

The authors would like to thank (in alphabetical order) Francis Dupont, Tatuya Jinmei, Erik Kline, Tommy Pauly, and Dave Thaler for providing valuable comments on earlier versions of this document.

Fernando Gont would like to thank Spencer Dawkins for his guidance.

## **9. References**

### **9.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", [RFC 4193](#), DOI 10.17487/RFC4193, October 2005, <<https://www.rfc-editor.org/info/rfc4193>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](#), DOI 10.17487/RFC4941, September 2007, <<https://www.rfc-editor.org/info/rfc4941>>.
- [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", [RFC 5905](#), DOI 10.17487/RFC5905, June 2010, <<https://www.rfc-editor.org/info/rfc5905>>.
- [RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", [RFC 6724](#), DOI 10.17487/RFC6724, September 2012, <<https://www.rfc-editor.org/info/rfc6724>>.
- [RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", [RFC 6763](#), DOI 10.17487/RFC6763, February 2013, <<https://www.rfc-editor.org/info/rfc6763>>.





- [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", [RFC 7217](#), DOI 10.17487/RFC7217, April 2014, <<https://www.rfc-editor.org/info/rfc7217>>.
- [RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", [RFC 8064](#), DOI 10.17487/RFC8064, February 2017, <<https://www.rfc-editor.org/info/rfc8064>>.

## 9.2. Informative References

- [Barnes2012]  
Barnes, R., Altmann, R., and D. Kerr, "Mapping the Great Void Smarter scanning for IPv6", ISMA 2012 AIMS-4 - Workshop on Active Internet Measurements, February 2012, <[https://www.caida.org/workshops/isma/1202/slides/aims1202\\_rbarnes.pdf](https://www.caida.org/workshops/isma/1202/slides/aims1202_rbarnes.pdf)>.
- [Hein] Hein, B., "The Rising Sophistication of Network Scanning", January 2016, <<http://netpatterns.blogspot.be/2016/01/the-rising-sophistication-of-network.html>>.
- [I-D.gont-6man-address-usage-recommendations]  
Gont, F., Gont, G., Corbo, M., and C. Huitema, "Problem Statement Regarding IPv6 Address Usage", [draft-gont-6man-address-usage-recommendations-04](#) (work in progress), October 2017.
- [I-D.gont-6man-non-stable-iids]  
Gont, F., Huitema, C., Krishnan, S., Gont, G., and M. Corbo, "Recommendation on Temporary IPv6 Interface Identifiers", [draft-gont-6man-non-stable-iids-03](#) (work in progress), March 2018.
- [I-D.gont-opsawg-firewalls-analysis]  
Gont, F. and F. Baker, "On Firewalls in Network Security", [draft-gont-opsawg-firewalls-analysis-02](#) (work in progress), February 2016.
- [I-D.ietf-v6ops-ula-usage-considerations]  
Liu, B. and S. Jiang, "Considerations For Using Unique Local Addresses", [draft-ietf-v6ops-ula-usage-considerations-02](#) (work in progress), March 2017.



- [RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6 Networks", [RFC 7707](#), DOI 10.17487/RFC7707, March 2016, <<https://www.rfc-editor.org/info/rfc7707>>.
- [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", [RFC 7721](#), DOI 10.17487/RFC7721, March 2016, <<https://www.rfc-editor.org/info/rfc7721>>.

#### Authors' Addresses

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

Phone: +54 11 4650 8472  
Email: [fgont@si6networks.com](mailto:fgont@si6networks.com)  
URI: <http://www.si6networks.com>

Guillermo Gont  
SI6 Networks  
Evaristo Carriego 2644  
Haedo, Provincia de Buenos Aires 1706  
Argentina

Phone: +54 11 4650 8472  
Email: [ggont@si6networks.com](mailto:ggont@si6networks.com)  
URI: <https://www.si6networks.com>

Madeleine Garcia Corbo  
Servicios de Informacion del Transporte  
Neptuno 358  
Havana City 10400  
Cuba

Email: [madelen.garcia16@gmail.com](mailto:madelen.garcia16@gmail.com)



Christian Huitema  
Private Octopus Inc.  
Friday Harbor, WA 98250  
U.S.A.

Email: [huitema@huitema.net](mailto:huitema@huitema.net)

URI: <http://privateoctopus.com>