# To SLAAC or not to SLAAC

Matjaž Straus Istenič
Academic and Research Network of Slovenia (ARNES)

November 25, 2013

**Keywords**

IPv6 Stateless Address Autoconfiguration, DHCPv6, IPv6 Stable Privacy Addresses, IPv6 First Hop Security, NetFlow version 9

# 1 Introduction

Internet Protocol version 6 (IPv6) was created to improve on IPv4 in many respects. However, security and privacy issues were not treated in a way to fit today's needs. Finding a good balance between security, privacy and complexity is still one of the major concerns in present-day networking. Fortunately, due to a solid design of IPv6, there is enough space to properly address these issues.

It seems that one of the design goals in Internet Protocol version 6 (IPv6) was to lessen the complexity of setting up the networking at hosts. Neighbor Discovery (ND) protocol [2] provides efficient mechanisms for automatic configuration for the hosts, with Stateless Address Autoconfiguration (SLAAC) [3] being intensively used for IPv6 addressing in many local networks. SLAAC is built in the IPv6 protocol itself, therefore widely available and reliable. On the other hand, SLAAC has some drawbacks: it lacks in good balance of privacy and stability of host addressing and, being stateless, it makes monitoring address usage tricky.

In this talk we will focus mainly on host addressing and address usage monitoring. We will discuss the motivation for stable privacy addressing by SLAAC [7] and propose a scalable and efficient technique for tracking the address usage in the local network. We will show that SLAAC can be efficiently and safely used for host autoconfiguration, providing we implement some minor changes and integrate IPv6 first hop security (IPv6 FHS) bindings with standard network flow monitoring.

# 2 Background and Motivation

In this section we will give an introduction to IPv6 ND and SLAAC. We will discuss the security and privacy implications of embedding hardware addresses in the interface identifier which is used in SLAAC (EUI-64 based addressing), and the motivation for privacy extensions to SLAAC [4]. The network administrator's "Better Safe Than Private?" dilemma of choosing a safe but more complex solution over a simple built-in-the-protocol one, which comes with severe security drawbacks, will lead us into discussion of a Dynamic Host Configuration protocol for IPv6 (DHCPv6) [5]. We conclude this section with a motivation to improve security and privacy issues in SLAAC. Then we pursue the scalable solution for network administrators to implement some essential monitoring and auditing of IPv6 address usage.

In this talk we aim for the two goals:

- We support changes in SLAAC for stable and private addressing, depreciating the need for DHCPv6. We always keep in mind to persist with the basics in IPv6 and avoid to introduce any additional protocols and applications.
- We recommend to use some of the existing industry standard technologies for monitoring the local address usage.

# 3 The proposal

We will take a look into some recent and very promising proposals for modification in SLAAC, namely to deprecate the hardware-based IPv6 addressing for hosts and to avoid constantly changing randomized addresses. We will suggest an additional functionality for the networking devices that can be programmed with IPv6 FHS features – we propose to use the industry standard NetFlow version 9 to export IPv6 FHS binding tables to a monitoring system.

### 3.1 Stable privacy addressing

Recently [1], a proposal to deprecate EUI-64 based IPv6 addresses in SLAAC has been published as an IETF draft [6]. The document recommends the use of an alternative scheme for the generation of IPv6 stable addresses [7], which are, however, still composed of a network prefix advertised by a local router, and an interface identifier. The key to mitigate some of the major security and privacy implications, such as network activity correlation, location tracking, address scanning and device-specific vulnerability exploitation, is the proper choice of the interface identifier.

In this section we will explain the proposed technique for generating a stable and private identifier for SLAAC which will gradually diminish the need for privacy extensions in IPv6 addressing. By accepting the stable privacy addressing we achieve our first objective.

### 3.2 Passive Address Usage Monitoring with NetFlow

IPv6 FHS [8] has finally reached the level of maturity adequate enough for implementation in access networking devices that are commonly used in enterprises, small businesses, research & educational networks and campuses. It is expected that IPv6 FHS will soon become a standard feature set in all contemporary networking gear. IPv6 FHS capable device maintains a binding table with sufficient information about active and valid IPv6 systems in the local networks.

There are several ways to export the information from the IPv6 FHS binding table to the monitoring system, like syslog, periodic polling with the use of SNMP or automated scripts, etc. Our idea is to use NetFlow version 9 [9], a technology for exporting statistical data about various types of network flows from a monitoring device (Exporter) to a server (Collector). NetFlow version 9 is expandable with the use of templates. To fulfil our purpose, we would need a few additional field types and define the appropriate flow record. This solution could be easily implemented on both, exporters and collectors.

We will discuss the idea in more detail in this section.

## 4 Conclusion

To SLAAC or not to SLAAC – what will it be? We definitely vote for SLAAC, slightly modified and used with IPv6 FHS.

At the time of writing, deprecation of EUI-64 based addressing and using stable privacy addressing scheme instead has not reached the RFC status yet. We find IPv6 FHS integration in the NetFlow version 9 exporter a good and affordable candidate to provide scalable and efficient way for monitoring IPv6 address usage in the local networks. We will discuss our proposal within the IPv6 networking community and, proven useful, bring it forward to the vendors.

[1] October 2013

# References


[1] Internet Protocol, Version 6 (IPv6) Specification, RFC2460

[2] Neighbor Discovery for IP version 6 (IPv6), RFC4861

[3] IPv6 Stateless Address Autoconfiguration, RFC4862

[4] Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC4941

[5] Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC3315

[6] IPv6 maintenance Working Group: Deprecating EUI-64 Based IPv6 Addresses, http://www.ietf.org/id/draft-gont-6man-deprecate-eui64-based-addresses-00.txt

[7] IPv6 maintenance Working Group: A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC), http://tools.ietf.org/html/draft-ietf-6man-stable-privacy-addresses-14

[8] First Hop IPv6 Security Features in Cisco IOS, http://blog.ipspace.net/2013/07/first-hop-ipv6-security-features-in.html

[9] Cisco Systems NetFlow Services Export Version 9, RFC3954



**Matjaž Straus Istenič** (matjaz.straus@arnes.si) is a network engineer, Internet service provider architect and expert in backbone networks. He worked for ARNES, Slovenia's National Research and Education Network since 1998. Matjaž has advanced and comprehensive technical experience in networking technology and protocols all the way from data link layer up to routing policy. Presently, Matjaž is actively contributing to IPv6 deployment on a national scale and participating in forming and starting-up the Slovenian Network Operaters Forum (SINOG).