

Operational Security Capabilities for
IPv6 Network Infrastructure
Internet-Draft
Intended status: Informational
Expires: January 17, 2013

K. Chittimaneni
Google
M. Kaeo
ISC
E. Vyncke
Cisco Systems
July 16, 2012

Operational Security Considerations for IPv6 Networks
draft-vyncke-opsec-v6-01

Abstract

Network managers know how to operate securely IPv4 network: whether it is the Internet or an enterprise internal network. IPv6 presents some new security challenges. [RFC 4942](#) describes the security issues in the protocol but network managers need also a more practical, operation-minded best common practices.

This document analyzes the operational security issues in all places of a network (service providers, enterprises and residential users) and proposes technical and procedural mitigations techniques.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 17, 2013.

Copyright Notice

Copyright (c) 2012 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
1.1.	Requirements Language	4
2.	Generic Security Considerations	4
2.1.	Addressing Architecture	4
2.1.1.	Overall Structure	4
2.1.2.	Use of ULAs	5
2.1.3.	Point-to-Point Links	5
2.1.4.	Privacy Addresses	5
2.1.5.	DHCP/DNS Considerations	6
2.2.	Link Layer Security	6
2.2.1.	SeND and CGA	6
2.2.2.	DHCP Snooping	7
2.2.3.	ND/RA Rate Limiting	7
2.2.4.	ND/RA Filtering	8
2.3.	Control Plane Security	9
2.3.1.	Control Protocols	10
2.3.2.	Management Protocols	10
2.3.3.	Packet Exceptions	11
2.4.	Routing Security	11
2.4.1.	Authenticating Neighbors/Peers	12
2.4.2.	Securing Routing Updates Between Peers	12
2.4.3.	Route Filtering	12
2.5.	Logging/Monitoring	13
2.5.1.	Data Sources	14
2.5.2.	Use of Collected Data	17
2.5.3.	Summary	18
2.6.	Transition/Coexistence Technologies	19
2.6.1.	Dual Stack	19
2.6.2.	Tunneling Mechanisms	19
2.6.3.	Translation Mechanisms	22
2.7.	General Device Hardening	23
3.	Enterprises Specific Security Considerations	23
3.1.	External Security Considerations:	24
3.2.	Internal Security Considerations:	24
4.	Service Providers Security Considerations	25
4.1.	BGP	25
4.1.1.	Remote Triggered Black Hole	25

4.2.	Transition Mechanism	25
4.2.1.	6PE and 6VPE	25
4.2.2.	6rd	25
4.2.3.	DS-lite	25
4.3.	Lawful Intercept	25
5.	Residential Users Security Considerations	25
6.	Acknowledgements	26
7.	IANA Considerations	26
8.	Security Considerations	26
9.	References	27
9.1.	Normative References	27
9.2.	Informative References	27
	Authors' Addresses	31

1. Introduction

Running an IPv6 network is new for most operators not only because they are not yet used to large scale IPv6 network but also because there are subtle differences between IPv4 and IPv6 especially with respect to security. For example, all layer-2 interactions are now done by Neighbor Discovery Protocol [[RFC4861](#)] rather than by Address Resolution Protocol [[RFC0826](#)]. Moreover, for end-users that usually combination in a single box Customer Premise Equipment (CPE) of firewall and Network Address and Port Translation [[RFC3022](#)] has lead to the common feeling that NATPT equals security and with IPv6 NATPT is no more needed.

The deployment of IPv6 network is commonly done with the dual-stack technique [[RFC4213](#)] which also leads to specific security issues.

This document complements [[RFC4942](#)] by listing all security issues when operating a network.

1.1. 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 [[RFC2119](#)] when they appear in ALL CAPS. These words may also appear in this document in lower case as plain English words, absent their normative meanings.

2. Generic Security Considerations

2.1. Addressing Architecture

IPv6 address allocations and overall architecture are an import part of securing IPV6.

2.1.1. Overall Structure

Once an address allocation has been assigned, there should be some thought given to an overall address allocation plan. A structured address allocation plan can lead to more concise and simpler firewall filtering rules. With the abundance of address space available, an address allocation may be structured around services along with geographic locations, which then can be a basis for more structured network filters to permit or deny services between geographic regions.

An important consideration for manually configured addressing is to make them hard to guess whenever possible. When manually configuring

interface ID's, the more common forms of starting at the beginning or end of a subnet boundary (i.e using a 1 or FF for routers) should be avoided. This will make any potential reconnaissance attack attempt much more difficult. Although some common multicast groups are defined for important networked devices and use of commonly repeated addresses make it easy figure out what the name servers, routers or other critical devices are, a non-random manual address scheme also makes it easy for a potential attacker using a "dictionary attack" of commonly used interface IDs to find your critical infrastructure.

2.1.2. Use of ULAs

ULAs are intended for scenarios where IP addresses will not have global scope. The implicit expectation from the RFC is that all ULAs will be randomly created as /48s. However, in practice some environments have chosen to create ULAs as a /32. While ULAs can be useful for infrastructure hiding, it may create an issue in future if the decision at some point is to make the machines using ULAs globally reachable. This would require renumbering or perhaps even stateful IPv6 Network Address Translation (NAT). The latter would again be problematic in trying to track specific machines that may source malware. It is important to carefully weigh the benefits of using ULAs versus utilizing a section of the global allocation and creating a more effective filtering strategy. A typical argument is that there are too many mistakes made with filters and ULAs make things easier to hide machines.

2.1.3. Point-to-Point Links

[RFC3627](#) indicates that the use of a /64 is the best solution for point-to-point links while a /112 can be used if that's not possible. However, in current deployments where it is felt that using a /64 is wasteful for point-to-point links, many opt to use a /127 or /126 subnet boundary and create manually defined IPv6 addresses for the point-to-point or tunnel endpoints.

2.1.4. Privacy Addresses

Randomly generating an interface ID, as described in [RFC 3041](#), is part of stateless autoconfiguration and used to address some security concerns. Stateless autoconfiguration relies on the automatically generated EUI-64 node address, which together with the /64 prefix make up the global unique IPv6 address. The EUI-64 address is generated from the MAC address. Since MAC addresses for specific vendor equipment can be known, it may be easy for a potential attacker to perform a more directed intelligent scan to try and ascertain specific vendor device reachability for exploitation. Privacy addressing attempts to mitigate this threat.

As privacy addressing could also be used to hide illegal and unsavory activities, privacy addressing can be assigned, audited, and controlled in managed enterprise networks via DHCPv6.

Some people also feel that stateless addressing means that we may not know addresses operating in our networks ahead of time in order to build access control lists (ACLs) of authorized users. While privacy addresses are truly generated randomly to protect against user tracking, but assuming that nodes use the EUI-64 format for global addressing, a list of expected pre-authorized host addresses can be generated.

2.1.5. DHCP/DNS Considerations

Some text

2.2. Link Layer Security

Link layer security is quite possibly the most important and visible security consideration for most operators. IPv6 relied heavily on the Neighbor Discovery protocol (NDP) [[RFC4861](#)] to perform a variety of link operations such as discovering other nodes on the link, resolving their link-layer addresses, and finding routers on the link. If not secured, NDP is vulnerable to various attacks such as router/neighbor message spoofing, redirect attacks, Duplicate Address Detection (DAD) DoS attacks, etc. many of these security threats to NDP have been documented in IPv6 ND Trust Models and Threats [[RFC3756](#)]

2.2.1. SeND and CGA

The original NDP specification called for using IPsec to protect Neighbor Discovery messages. However, manually configuring security associations among multiple hosts on a large network can be very challenging. SEcure Neighbor Discovery (SEND), as described in [[RFC3971](#)], is a mechanism designed to secure ND messages without having to rely on manual IPsec configuration. Cryptographically Generated Addresses (CGA), as described in [[RFC3972](#)], are used to ensure that the sender of a Neighbor Discovery message is the actual "owner" of the claimed address. A new NDP option, the CGA option, is used to carry the public key and associated parameters. Another NDP option, the RSA Signature option, is used to protect all messages relating to neighbor and Router discovery.

SEND protects against:

- o Neighbor Solicitation/Advertisement Spoofing

- o Neighbor Unreachability Detection Failure
- o Duplicate Address Detection DoS Attack
- o Router Solicitation and Advertisement Attacks
- o Replay Attacks
- o Neighbor Discovery DoS Attacks

SEND does NOT:

- o Protect statically configured addresses
- o Protect addresses configured using fixed identifiers (i.e. EUI-64)
- o Provide confidentiality for NDP communications
- o Compensate for an unsecured link - SEND does not require that the addresses on the link and Neighbor Advertisements correspond

2.2.2. DHCP Snooping

Dynamic Host Configuration Protocol for IPv6 (DHCPv6), as detailed in [[RFC3315](#)], enables DHCP servers to pass configuration parameters such as IPv6 network addresses and other configuration information to IPv6 nodes. DHCP plays an important role in any large network by providing robust stateful autoconfiguration and autoregistration of DNS Host Names. Misconfigured (rogue) or malicious DHCP servers can be leveraged to attack IPv6 nodes either by denying nodes from getting a valid address/prefix or by disseminating incorrect information to end nodes for malicious purposes. Some of these scenarios are discussed in [[RFC3315](#)]

The Source Address Validation Improvements (SAVI) group is currently working on ways to mitigate the effects of such attacks. [[I-D.ietf-savi-dhcp](#)] would help in creating bindings between a DHCPv4 [[RFC2131](#)]/DHCPv6 [[RFC3315](#)] assigned source IP address and a binding anchor [[I-D.ietf-savi-framework](#)] on SAVI (Source Address Validation Improvements) device. [[RFC6620](#)] describes how to glean similar bindings when DHCP is not used. The bindings can be used to filter packets generated on the local link with forged source IP address.

2.2.3. ND/RA Rate Limiting

Neighbor Discovery (ND) can be vulnerable to denial of service (DoS) attacks in which a router is forced to perform address resolution for

a large number of unassigned addresses. Possible side effects of this attack preclude new devices from joining the network or even worse rendering the last hop router ineffective due to high CPU usage. Easy mitigative steps include rate limiting Neighbor Solicitations, restricting the amount of state reserved for unresolved solicitations, and clever cache/timer management.

[RFC6583] discusses the potential for DOS in detail and suggests implementation improvements and operational mitigation techniques that may be used to mitigate or alleviate the impact of such attacks.

Additionally, IPv6 ND uses multicast extensively for signaling messages on the local link to avoid broadcast messages for on-the-wire efficiency. However, this has some side effects on wifi networks, especially a negative impact on battery life of smartphones and other battery operated devices that are connected to such networks. The following drafts are actively discussing methods to rate limit RAs and other ND messages on wifi networks in order to address this issue:

- o [[I-D.thubert-savi-ra-throttler](#)]
- o [[I-D.chakrabarti-nordmark-energy-aware-nd](#)]

2.2.4. ND/RA Filtering

Router Advertising spoofing is a well known attack vector and has been extensively documented. The presence of rogue RAs, either intentional or malicious, can cause partial or complete failure of operation of hosts on an IPv6 link. For example, a host can select an incorrect router address which can be used as a man-in-the-middle (MITM) attack or can assume wrong prefixes to be used for stateless address configuration (SLAAC). [[RFC6104](#)] summarizes the scenarios in which rogue RAs may be observed and presents a list of possible solutions to the problem. [[RFC6105](#)] describes a solution framework for the rogue RA problem where network segments are designed around switching devices that are capable of identifying invalid RAs and blocking them before the attack packets actually reach the target nodes. This mechanism is commonly employed as a first line of defense against common attack vectors.

However, several evasion techniques that circumvent the protection provided by RA Guard have surfaced. A key challenge to this mitigation technique is introduced by IPv6 fragmentation. An attacker can conceal the attack by fragmenting his packets into multiple fragments such that the switching device that is responsible for blocking invalid RAs cannot find all the necessary information to perform packet filtering in the same packet.

[I-D.ietf-v6ops-ra-guard-implementation] describes such evasion techniques, and provides advice to RA-Guard implementers such that the aforementioned evasion vectors can be eliminated.

[I-D.gont-6man-nd-extension-headers] attempts to analyze the security implications of using IPv6 Extension Headers with Neighbor Discovery (ND) messages. The ultimate goal of this doc is to update [RFC 4861](#) such that use of the IPv6 Fragmentation Header is forbidden in all Neighbor Discovery messages, thus allowing for simple and effective measures to counter Neighbor Discovery attacks.

2.3. Control Plane Security

[RFC6192] defines the router control plane and this definition is repeated here for the reader's convenience.

Modern router architecture design maintains a strict separation of forwarding and router control plane hardware and software. The router control plane supports routing and management functions. It is generally described as the router architecture hardware and software components for handling packets destined to the device itself as well as building and sending packets originated locally on the device. The forwarding plane is typically described as the router architecture hardware and software components responsible for receiving a packet on an incoming interface, performing a lookup to identify the packet's IP next hop and determine the best outgoing interface towards the destination, and forwarding the packet out through the appropriate outgoing interface.

While the forwarding plane is usually implemented in high-speed hardware, the control plane is implemented by a generic processor (named router processor RP) and cannot process packets at a high rate. Hence, this processor can be attacked by flooding its input queue with more packets than it can process. The control plane processor is then unable to process valid control packets and the router can lose OSPF or BGP adjacencies which can cause a severe network disruption.

The mitigation technique is:

- o To drop non legit control packet before they are queued to the RP (this can be done by a forwarding plane ACL) and
- o To rate limit the remaining packets to a rate that the RP can sustain.

This section will consider several classes of control packets:

- o Control protocols: routing protocols: such as OSPFv3, BGP and by extension Neighbor Discovery and ICMP
- o Management protocols: SSH, SNMP, IPfix, etc
- o Packet exceptions: which are normal data packets which requires a specific processing such as generating a packet-too-big ICMP message or having the hop-by-hop extension header.

2.3.1. Control Protocols

This class includes OSPFv3, BGP, NDP, ICMP.

An ingress ACL to be applied on all the router interfaces SHOULD be configured such as:

- o drop OSPFv3 (identified by Next-Header being 89) and RIPng (identified by UDP port 521) packets from a non link-local address
- o allow BGP (identified by TCP port 179) packets from all BGP neighbors and drop the others
- o allow all ICMP packets (transit and to the router interfaces)

Note: dropping OSPFv3 packets which are authenticated by IPsec could be impossible on some routers which are unable to parse the IPsec ESP or AH extension headers.

Rate limiting of the valid packets SHOULD be done. The exact configuration obviously depends on the power of the Route Processor.

2.3.2. Management Protocols

This class includes: SSH, SNMP, syslog, IPfix, NTP, etc

An ingress ACL to be applied on all the router interfaces SHOULD be configured such as:

- o Drop packets destined to the routers except those belonging to protocols which are used (for example, permit TCP 22 and drop all when only SSH is used);
- o Drop packets where the source does not match the security policy, for example if SSH connections should only be originated from the NOC, then the ACL should permit TCP port 22 packets only from the NOC prefix.

Rate limiting of the valid packets SHOULD be done. The exact

configuration obviously depends on the power of the Route Processor.

2.3.3. Packet Exceptions

This class covers multiple cases where a data plane packet is punted to the route processor because it requires specific processing:

- o generation of an ICMP packet-too-big message when a data plane packet cannot be forwarded because it is too large;
- o generation of an ICMP hop-limit-expired message when a data plane packet cannot be forwarded because its hop-limit field has reached 0;
- o generation of an ICMP destination-unreachable message when a data plane packet cannot be forwarded for any reason;
- o processing of the hop-by-hop extension header. See [\[I-D.krishnan-ipv6-hopbyhop\]](#)

On some routers, not everything can be done by the specialized data plane hardware.. then some packets are 'punted' to the generic RP. This could include for example the processing of a long extension header chain in order to apply an ACL based on layer 4 information.

An ingress ACL cannot help to mitigate a control plane attack using those packet exceptions. The only protection for the RP is to limit the rate of those packet exceptions forwarded to the RP, this means that some data plane packets will be dropped with any ICMP messages back to the source which will cause Path MTU holes. But, there is no other solution.

In addition to limiting the rate of data plane packets queued to the RP, it is also important to limit the generation rate of ICMP messages both the save the RP but also to prevent an amplification attack using the router as a reflector.

2.4. Routing Security

Routing security in general can be broadly divided into three sections:

1. Authenticating neighbors/peers
2. Securing routing updates between peers
3. Route filtering

2.4.1. Authenticating Neighbors/Peers

A basic element of routing is the process of forming adjacencies, neighbor, or peering relationships with other routers. From a security perspective, it is very important to establish such relationships only with routers and/or administrative domains that one trusts. A traditional approach has been to use MD5 passwords, which allows routers to authenticate each other prior to establishing a routing relationship. Most open standard protocols, with the notable exception of OSPFv3, are able to provide this type of authentication mechanism.

OSPFv3 relies on IPSEC to fulfill the authentication function. However, it should be noted that IPSEC support is not standard on all routing platforms. In some cases, this requires specialized hardware that offloads crypto over to dedicated ASICs or enhanced software images (both of which often come with added financial cost) to provide such functionality. [\[RFC6506\]](#) changes OSPFv3's reliance on IPSEC by appending an authentication trailer to the end of the OSPFv3 packets. This document does not specifically provide for a mechanism that will authenticate the specific originator of a packet. Rather, it will allow a router to confirm that the packet has indeed been issued by a router that had access to the authentication key.

2.4.2. Securing Routing Updates Between Peers

IPv6 mandates the provisioning of IPSEC capability in all nodes. Theoretically it is possible, and recommended, that communication between two IPv6 nodes, including routers exchanging routing information be encrypted using IPSEC. In practice however, deploying IPSEC is not always feasible given hardware and software limitations of various platforms deployed, as described in the earlier section. Additionally, most key management mechanisms are designed for a one-to-one communication model. However, in a protocol such as OSPFv3 where adjacencies are formed on a one-to-many basis, IPSEC key management becomes difficult to maintain.

2.4.3. Route Filtering

At a minimum, IPv6 routing policy as it pertains to routing between different administrative domains should aim to maintain parity with IPv4 from a policy perspective e.g.,

- o Filter internal-use, non-globally routable IPv6 addresses at the perimeter
- o Discard packets from and to bogon and reserved space

- o Configure ingress route filters that validate route origin, prefix ownership, etc. through the use of various routing databases, e.g., RADB. There is additional work being done in this area to formally validate the origin ASs of BGP announcements in [[I-D.ietf-sidr-rpki-rtr](#)]

2.5. Logging/Monitoring

In order to perform forensic research in case of any security incident or to detect abnormal behaviors, network operator should log multiple pieces of information.

This includes:

- o logs of all applications when available (for example web servers);
- o use of IP Flow Information Export [[RFC5102](#)]also known as IPfix;
- o use of SNMP MIB [[RFC4293](#)];
- o use of the Neighbor cache;
- o use of stateful DHCPv6 [[RFC3315](#)] lease cache.

Please note that there are privacy issues related to how those logs are collected, kept and safely discarded. Operators are urged to check their country legislation.

All those pieces of information will be used to do:

- o forensic ([Section 2.5.2.1](#)) research to answer questions such as who did what and when?
- o correlation ([Section 2.5.2.3](#)): which IP addresses were used by a specific node (assuming the use of privacy extensions addresses [[RFC4941](#)])
- o inventory ([Section 2.5.2.2](#)): which IPv6 nodes are on my network?
- o abnormal behavior detection ([Section 2.5.2.4](#)): unusual traffic patterns are often the symptoms of a abnormal behavior which is in turn a potential attack (denial of services, network scan, a node being part of a botnet, ...)

2.5.1. Data Sources

This section lists the most important sources of data that are useful for operational security.

2.5.1.1. Logs of Applications

Those logs are usually text files where the remote IPv6 address is stored in all characters (not binary). This can complicate the processing since one IPv6 address, 2001:db8::1 can be written in multiple ways such as:

- o 2001:DB8::1 (in uppercase)
- o 2001:0db8::0001 (with leading 0)
- o and many other ways.

[RFC 5952](#) [[RFC5952](#)] explains this problem in more details and recommends the use of a single canonical format (in short use lower case and suppress leading 0). This memo recommends the use of canonical format [[RFC5952](#)] for IPv6 addresses in all possible cases. If the existing application cannot log under the canonical format, then this memo recommends the use an external program (or filter) in order to canonicalize all IPv6 addresses.

For example, this perl script can be used:

```
#!/usr/bin/perl ?w
use strict ;
use Socket ;
use Socket6 ;

my (@words, $word, $binary_address) ;

## go through the file one line at a time
while (my $line = <STDIN>) {
    @words = split /[ \n]/, $line ;
    foreach $word (@words) {
        $binary_address = inet_pton AF_INET6, $word ;
        if ($binary_address) {
            print inet_ntop AF_INET6, $binary_address ;
        } else {
            print $word ;
        }
        print " " ;
    }
    print "\n" ;
}
```


2.5.1.2. IP Flow Information Export by IPv6 Routers

IPfix [[RFC5102](#)] defines some data elements that are useful for security:

- o in [section 5.4](#) (IP Header fields): nextHeaderIPv6 and sourceIPv6Address;
- o in [section 5.6](#) (Sub-IP fields) sourceMacAddress.

Moreover, IPfix is very efficient in terms of data handling and transport. It can also aggregate flows by a key such as sourceMacAddress in order to have aggregated data associated with a specific sourceMacAddress. This memo recommends the use of IPfix and aggregation on nextHeaderIPv6, sourceIPv6Address and sourceMacAddress.

2.5.1.3. SNMP MIB by IPv6 Routers

[RFC 4293](#) [[RFC4293](#)] defines a Management Information Base (MIB) for the two address families of IP. This memo recommends the use of:

- o ipIfStatsTable table which collects traffic counters per interface;
- o ipNetToPhysicalTable table which is the content of the Neighbor cache, i.e. the mapping between IPv6 and data-link layer addresses.

2.5.1.4. Neighbor Cache of IPv6 Routers

The neighbor cache of routers contains all mappings between IPv4 addresses and data-link layer addresses. It is usually available by two means:

- o the SNMP MIB ([Section 2.5.1.3](#)) as explained above;
- o also by connecting over a secure management channel (such as SSH or HTTPS).

The neighbor cache is highly dynamic as mappings are added when a new IPv6 address appears on the network (could be quite often with privacy extension addresses [[RFC4941](#)] or when they are removed when the state goes from UNREACH to removed (the default time for a removal per Neighbor Unreachability Detection [[RFC4861](#)] algorithm is 38 seconds for a typical host such as Windows 7). This means that the content of the neighbor cache must periodically be fetched every 30 seconds (to be on the safe side) and stored for later use.

This is an important source of information because it is not trivial on a switch using the SAVI [[I-D.ietf-savi-framework](#)] algorithm to defeat the mapping between data-link layer address and IPv6 address.

2.5.1.5. Stateful DHCPv6 Lease

In some networks, IPv6 addresses are managed by stateful DHCPv6 server [[RFC3315](#)] that leases IPv6 addresses to clients. It is indeed quite similar to DHCP for IPv4 so it can be tempting to use this DHCP lease file to discover the mapping between IPv6 addresses and data-link layer addresses as it was usually done in the IPv4 era.

It is not so easy in the IPv6 world because not all nodes will use DHCPv6 (there are nodes which can only do stateless autoconfiguration) but also because DHCPv6 clients are identified not by their hardware-client address as in IPv4 but by a DHCP Unique ID (DUID) which can have several formats: some being the data-link layer address, some being data-link layer address prepended with time information or even an opaque number which is useless for operation security. Moreover, when the DUID is based on the data-link address, this address can be of any interface of the client (such as the wireless interface while the client actually uses its wired interface to connect to the network).

In short, the DHCPv6 lease file is less interesting than in the IPv4 era. DHCPv6 servers that keeps the relayed data-link layer address in addition to the DUID in the lease file do not suffer from this limitation. Special care must be taken to prevent stateless autoconfiguration anyway (and if applicable) by sending RA with all announced prefixes without the A-bit set.

The mapping between data-link layer address and the IPv6 address can be secured by using switches implementing the SAVI [[I-D.ietf-savi-dhcp](#)] algorithms.

2.5.1.6. Other Data Sources

There are other data sources that must be kept exactly as in the IPv4 network:

- o historical mapping of MAC address to RADIUS user authentication in a wireless network or an IPsec-based remote access VPN;
- o historical mapping of MAC address to switch interface in a wired network.

2.5.2. Use of Collected Data

This section leverages the data collected as described before ([Section 2.5.1](#)) in order to achieve several security benefits.

2.5.2.1. Forensic

The forensic use case is when the network operator must locate an IPv6 address that was present in the network at a certain time or is still currently in the network.

The source of information can be, in decreasing order, neighbor cache, DHCP lease file. Then, the procedure is:

1. based on the IPv6 prefix of the IPv6 address find the router(s) which are used to reach this prefix;
2. based on this limited set of routers, on the incident time and on IPv6 address to retrieve the data-link address from live neighbor cache, from the historical data of the neighbor cache, or from the DHCP lease file;
3. based on the data-link layer address, look-up on which switch interface was this data-link layer address. In the case of wireless LAN, the RADIUS log should have the mapping between user identification and the MAC address.

At the end of the process, the interface where the malicious user was connected or the username that was used by the malicious user is found.

2.5.2.2. Inventory

[RFC 5157](#) [[RFC5157](#)] is about the difficulties to scan an IPv6 network due to the vast number of IPv6 addresses per link. This has the side effect of making the inventory task difficult in an IPv6 network while it was trivial to do in an IPv4 network (a simple enumeration of all IPv4 addresses, followed by a ping and a TCP/UDP port scan). Getting an inventory of all connected devices is of prime importance for a secure operation of a network.

There are two ways to do an inventory of an IPv6 network.

The first technique is to use the IPfix information and extract the list of all IPv6 source addresses to find all IPv6 nodes that sent packets through a router. This is very efficient but alas will not discover silent node that never transmitted such packets... Also, it must be noted that link-local addresses will never be discovered by

this means.

The second way is again to use the collected neighbor cache content to find all IPv6 addresses in the cache. This process will also discover all link-local addresses.

2.5.2.3. Correlation

In an IPv4 network, it is easy to correlate multiple logs, for example to find events related to a specific IPv4 address. A simple Unix grep command was enough to scan through multiple text-based files and extract all lines relevant to a specific IPv4 address.

In an IPv6 network, this is slightly more difficult because different character strings can express the same IPv6 address. Therefore, the simple Unix grep command cannot be used. Moreover, an IPv6 node can have multiple IPv6 addresses...

In order to do correlation in IPv6-related logs, it is advised to have all logs with canonical IPv6 addresses. Then, the neighbor cache current (or historical) data set must be searched to find the data-link layer address of the IPv6 address. Then, the current and historical neighbor cache data sets must be searched for all IPv6 addresses associated to this data-link layer address: this is the search set. The last step is to search in all log files (containing only IPv6 address in canonical format) for any IPv6 addresses in the search set.

2.5.2.4. Abnormal Behavior Detection

Abnormal behaviors (such as network scanning, spamming, denial of service) can be detected in the same way as in an IPv4 network

- o sudden increase of traffic detected by interface counter (SNMP) or by aggregated traffic from IPfix records [[RFC5102](#)];
- o change of traffic pattern (number of connection per second, number of connection per host...) with the use of IPfix [[RFC5102](#)]

2.5.3. Summary

While some data sources (IPfix, MIB, switch CAM tables, logs, ...) are also used in the secure operation of an IPv6 network, the DHCPv6 lease file is less reliable and the neighbor cache is of prime importance.

The fact that there are multiple ways to express in a character string the same IPv6 address renders the use of filters mandatory

when correlation must be done.

2.6. Transition/Coexistence Technologies

Some text

2.6.1. Dual Stack

Dual stack has established itself as the preferred deployment choice for most network operators. Dual stacking the network offers many advantages over other transition mechanisms. Firstly, it is easy to turn on without impacting normal IPv4 operations. Secondly, perhaps more importantly, it is easier to troubleshoot when things break. Dual stack allows you to gradually turn IPv4 operations down when your IPv6 network is ready for prime time.

From an operational security perspective, this now means that you have twice the exposure. One needs to think about protecting both protocols now. At a minimum, the IPv6 portion of a dual stacked network should maintain parity with IPv4 from a security policy point of view. Typically, the following methods are employed to protect IPv4 networks at the edge:

- o ACLs to permit or deny traffic
- o Firewalls with stateful packet inspection

It is recommended that these ACLs and/or firewalls be additionally configured to protect IPv6 communications. Also, given the end-to-end connectivity that IPv6 provides, it is also recommended that hosts be fortified against threats. General device hardening guidelines are provided in [Section 2.7](#)

2.6.2. Tunneling Mechanisms

There are many tunnels used for specific use cases. Except when protected by IPsec [[RFC4301](#)], all those tunnels have a couple of security issues (most of them being described in [RFC 6169](#) [[RFC6169](#)]);

- o tunnel injection: a malevolent person knowing a few pieces of information (for example the tunnel endpoints and the used protocol) can forge a packet which looks like a legit and valid encapsulated packet that will gladly be accepted by the destination tunnel endpoint, this is a specific case of spoofing;
- o traffic interception: no confidentiality is provided by the tunnel protocols (without the use of IPsec), therefore anybody on the tunnel path can intercept the traffic and have access to the

clear-text IPv6 packet;

- o service theft: as there is no authorization, even a non authorized user can use a tunnel relay for free (this is a specific case of tunnel injection);
- o reflection attack: another specific use case of tunnel injection where the attacker injects packets with an IPv4 destination address not matching the IPv6 address causing the first tunnel endpoint to re-encapsulate the packet to the destination... Hence, the final IPv4 destination will not see the original IPv4 address but only one IPv4 address of the relay router.
- o bypassing security policy: if a firewall or an IPS is on the path of the tunnel, then it will probably neither inspect nor detect a malevolent IPv6 traffic contained in the tunnel.

To mitigate the bypassing of security policies, it could be helpful to block all default configuration tunnels by denying all IPv4 traffic matching:

- o IP protocol 41: this will block ISATAP ([Section 2.6.2.2](#)), 6to4 ([Section 2.6.2.4](#)), 6rd ([Section 2.6.2.5](#)) as well as 6in4 ([Section 2.6.2.1](#)) tunnels;
- o IP protocol 47: this will block GRE ([Section 2.6.2.1](#)) tunnels;
- o UDP protocol 3544: this will block the default encapsulation of Teredo ([Section 2.6.2.3](#)) tunnels.

Ingress filtering [[RFC2827](#)] should also be applied on all tunnel endpoints if applicable to prevent IPv6 address spoofing.

As several of the tunnel techniques share the same encapsulation (i.e. IPv4 protocol 41) and embed the IPv4 address in the IPv6 address, there are a set of well-known looping attacks described in [RFC 6324](#) [[RFC6324](#)], this RFC also proposes mitigation techniques.

[2.6.2.1](#). Site-to-Site Static Tunnels

Site-to-site static tunnels are described in [RFC 2529](#) [[RFC2529](#)] and in GRE [[RFC2784](#)]. As the IPv4 endpoints are statically configured and are not dynamic they are slightly more secure (bi-directional service theft is mostly impossible) but traffic interception and tunnel injection are still possible. Therefore, the use of IPsec [[RFC4301](#)] in transport mode and protecting the encapsulated IPv4 packets is recommended for those tunnels. Alternatively, IPsec in tunnel mode can be used to transport IPv6 traffic over a non-trusted

IPv4 network.

2.6.2.2. ISATAP

ISATAP tunnels [[RFC5214](#)] are mainly using within a single administrative domain and to connect a single IPv6 host to the IPv6 network. This means that endpoints and the tunnel endpoint are usually managed by a single entity; therefore, audit trail and strict anti-spoofing are usually possible and this raises the overall security.

Special care must be taken to avoid looping attack by implementing the measures of [RFC 6324](#) [[RFC6324](#)] and of [[I-D.templin-v6ops-isops](#)].

IPsec [[RFC4301](#)] in transport or tunnel mode can be used to secure the IPv4 ISATAP traffic to provide IPv6 traffic confidentiality and prevent service theft.

2.6.2.3. Teredo

Teredo tunnels [[RFC4380](#)] are mainly used in a residential environment because that can easily traverse an IPv4 NAT-PT device thanks to its UDP encapsulation and they connect a single host to the IPv6 Internet. Teredo shares the same issues as other tunnels: no authentication, no confidentiality, possible spoofing and reflection attacks.

IPsec [[RFC4301](#)] for the transported IPv6 traffic is recommended.

The biggest threat to Teredo is probably for IPv4-only network as Teredo has been designed to easily traverse IPV4 NAT-PT devices which are quite often co-located with a stateful firewall. Therefore, if the stateful IPv4 firewall allows unrestricted UDP outbound and accept the return UDP traffic, then Teredo actually punches a hole in this firewall for all IPv6 traffic to the Internet and from the Internet. While host policies can be deployed to block Teredo in an IPv4-only network in order to avoid this firewall bypass, it would be more efficient to block all UDP outbound traffic at the IPv4 firewall if deemed possible (of course, at least port 53 should be left open for DNS traffic).

2.6.2.4. 6to4

6to4 tunnels [[RFC3056](#)] require a public routable IPv4 address in order to work correctly. They can be used to provide either one IPv6 host connectivity to the IPv6 Internet or multiple IPv6 networks connectivity to the IPV6 Internet. The 6to4 relay is usually the anycast address defined in [[RFC3068](#)]

They suffer from several technical issues as well as security issues [[RFC3964](#)]. Their use is no more recommended (see [[I-D.ietf-v6ops-6to4-to-historic](#)]).

[2.6.2.5.](#) 6rd

While 6rd tunnels share the same encapsulation as 6to4 tunnels ([Section 2.6.2.4](#)), they are designed to be used within a single SP domain, in other words they are deployed in a more constrained environment than 6to4 tunnels and have little security issues except lack of confidentiality. The security considerations ([Section 12](#)) of [[RFC5969](#)] describes how to secure the 6rd tunnels.

IPsec [[RFC4301](#)] for the transported IPv6 traffic can be used if confidentiality is important.

[2.6.2.6.](#) DS-Lite

DS-lite is more a translation mechanism and is therefore analyzed further ([Section 2.6.3.3](#)) in this document.

[2.6.2.7.](#) Mapping of Address and Port

With the tunnel and encapsulation versions of Mapping of Address and Port (MAP [[I-D.ietf-softwire-map](#)]), the access network is purely an IPv6 network and MAP protocols are used to give IPv4 hosts on the subscriber network to IPv4 hosts on the Internet. The subscriber router does stateful operations in order to map all internal IPv4 addresses and layer-4 ports to the IPv4 address and the set of layer-4 ports received through MAP configuration process. The SP equipment always does stateless operations (either decapsulation or stateless translation). Therefore, as opposed to [Section 2.6.3.3](#) there is no DoS attack against the SP equipment because there is no state and there is no operation caused by a new layer-4 connection (no logging operation).

The SP MAP equipment MUST implement all the security considerations of [[I-D.ietf-softwire-map](#)]; notably, ensuring that the mapping of the IPv4 address and port are consistent with the configuration.

[2.6.3.](#) Translation Mechanisms

Some text

[2.6.3.1.](#) Carrier Grade Nat (CGN)

Some text

2.6.3.2. NAT64/DNS64

Some text

2.6.3.3. DS-lite

Some text

2.7. General Device Hardening

There are many environments which rely too much on the network infrastructure to disallow malicious traffic to get access to critical hosts. In new IPv6 deployments it has been common to see IPv6 traffic enabled but none of the typical access control mechanisms enabled for IPv6 device access. With the possibility of network device configuration mistakes and the growth of IPv6 in the overall Internet it is important to ensure that all individual devices are hardened against miscreant behavior.

The following guidelines should be used to ensure appropriate hardening of the host, be it an individual computer or router, firewall, load-balancer, server, etc device.

- o Restrict access to the device to authenticated and authorized individuals
- o Monitor and audit access to the device
- o Turn off any unused services on the end node
- o Understand which IPv6 addresses are being used to source traffic and change defaults if necessary
- o Use cryptographically protected protocols for device management if possible (SCP, SNMPv3, SSH, TLS, etc)
- o Use host firewall capabilities to control traffic that gets processed by upper layer protocols
- o Use virus scanners to detect malicious programs

3. Enterprises Specific Security Considerations

Enterprises generally have robust network security policies in place to protect existing IPv4 networks. These policies have been distilled from years of experiential knowledge of securing IPv4 networks. At the very least, it is recommended that enterprise

networks have parity between their security policies for both protocol versions.

Security considerations in the enterprise can be broadly categorized into two sections - External and Internal.

3.1. External Security Considerations:

The external aspect deals with providing security at the edge or perimeter of the enterprise network where it meets the service providers network. This is commonly achieved by filtering traffic either by implementing dedicated firewalls with stateful packet inspection or a router with ACLs. A common default IPv4 policy on firewalls that could easily be ported to IPv6 is to allow all traffic outbound while only allowing specific traffic, such as established sessions, inbound. Here are a few more things that could enhance the default policy:

- o Filter internal-use IPv6 addresses at the perimeter
- o Discard packets from and to bogon and reserved space
- o Accept certain ICMPv6 messages to allow proper operation of ND and PMTUD, see also [[RFC4890](#)]
- o Filter specific extension headers, where possible
- o Filter unneeded services at the perimeter
- o Implement Anti-Spoof filtering
- o Implement appropriate rate-limiters and control-plane policers

3.2. Internal Security Considerations:

The internal aspect deals with providing security inside the perimeter of the network, including the end host. The most significant concerns here are related to Neighbor Discovery. At the network level, it is recommended that all security considerations discussed in [Section 2.2](#) be reviewed carefully and the recommendations be considered in-depth as well.

Hosts need to be hardened directly through security policy to protect against security threats. The host firewall default capabilities have to be clearly understood, especially 3rd party ones which can have different settings for IPv4 or IPv6 default permit/deny behavior. In some cases, 3rd party firewalls have no IPv6 support whereas the native firewall installed by default has it. General

device hardening guidelines are provided in [Section 2.7](#)

It should also be noted that many hosts still use IPv4 for transport for things like RADIUS, TACACS+, SYSLOG, etc. This will require some extra level of due diligence on the part of the operator.

[4.](#) Service Providers Security Considerations

[4.1.](#) BGP

tbd

[4.1.1.](#) Remote Triggered Black Hole

tbd

[4.2.](#) Transition Mechanism

tbd: will need to reference the security considerations of relevant RFC.

[4.2.1.](#) 6PE and 6VPE

tbd.

[4.2.2.](#) 6rd

tbd. refer to 6rd section ([Section 2.6.2.5](#))

[4.2.3.](#) DS-lite

tbd.

[4.3.](#) Lawful Intercept

tbd.

[5.](#) Residential Users Security Considerations

The IETF Homenet working group is working on how IPv6 residential network should be done; this obviously includes operational security considerations; but, this is still work in progress.

Residential networks have usually little clue about security or networking. As most of the recent hosts, smartphones, tablets have all IPv6 enabled by default, IPv6 security is important for those

users. Even with an IPv4-only ISP, those users can get IPv6 Internet access with the help of Teredo tunnels. Several peer-to-peer programs (notably Bittorrent) support IPv6 and those programs can initiate a Teredo tunnel through the IPv4 residential gateway, with the consequence of making the internal host reachable from any IPv6 host on the Internet. It is therefore recommended that all host security products (personal firewall, ...) are configured with a dual-stack security policy.

If the Residential Gateway has IPv6 connectivity, [[RFC6204](#)] defines the requirements of an IPv6 CPE and does not take position on the debate of default IPv6 security policy:

- o outbound only: allowing all internally initiated connections and block all externally initiated ones, which is a common default security policy enforced by IPv4 Residential Gateway doing NAT-PT but it also breaks the end-to-end reachability promise of IPv6. [[RFC6092](#)] lists several recommendations to design such a CPE;
- o open: allowing all internally and externally initiated connections, therefore restoring the end-to-end nature of the Internet for the IPv6 traffic but having a different security policy for IPv6 than for IPv4.

[RFC6204] states that a clear choice must be given to the user to select one of those two policies.

[6.](#) Acknowledgements

[7.](#) IANA Considerations

This memo includes no request to IANA.

[8.](#) Security Considerations

This memo attempts to give an overview of security considerations of operating an IPv6 network both in an IPv6-only network but also in a dual-stack environment.

[9.](#) References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", [RFC 6104](#), February 2011.
- [RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", [RFC 6105](#), February 2011.

9.2. Informative References

- [I-D.chakrabarti-nordmark-energy-aware-nd]
Chakrabarti, S., Nordmark, E., and M. Wasserman, "Energy Aware IPv6 Neighbor Discovery Optimizations", [draft-chakrabarti-nordmark-energy-aware-nd-02](#) (work in progress), March 2012.
- [I-D.gont-6man-nd-extension-headers]
Gont, F., "Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery", [draft-gont-6man-nd-extension-headers-03](#) (work in progress), June 2012.
- [I-D.ietf-savi-dhcp]
Bi, J., Wu, J., Yao, G., and F. Baker, "SAVI Solution for DHCP", [draft-ietf-savi-dhcp-14](#) (work in progress), July 2012.
- [I-D.ietf-savi-framework]
Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, "Source Address Validation Improvement Framework", [draft-ietf-savi-framework-06](#) (work in progress), January 2012.
- [I-D.ietf-sidr-rpki-rtr]
Bush, R. and R. Austein, "The RPKI/Router Protocol", [draft-ietf-sidr-rpki-rtr-26](#) (work in progress), February 2012.
- [I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Zhai, Y., Matsushima, S., and T. Murakami, "Mapping of Address and Port (MAP)", [draft-ietf-softwire-map-01](#) (work in progress), June 2012.
- [I-D.ietf-v6ops-6to4-to-historic]

Troan, O., "Request to move Connection of IPv6 Domains via IPv4 Clouds (6to4) to Historic status",
[draft-ietf-v6ops-6to4-to-historic-05](#) (work in progress),
June 2011.

[I-D.ietf-v6ops-ra-guard-implementation]
Gont, F., "Implementation Advice for IPv6 Router
Advertisement Guard (RA-Guard)",
[draft-ietf-v6ops-ra-guard-implementation-04](#) (work in
progress), May 2012.

[I-D.krishnan-ipv6-hopbyhop]
Krishnan, S., "The case against Hop-by-Hop options",
[draft-krishnan-ipv6-hopbyhop-05](#) (work in progress),
October 2010.

[I-D.templin-v6ops-isops]
Templin, F., "Operational Guidance for IPv6 Deployment in
IPv4 Sites using ISATAP", [draft-templin-v6ops-isops-17](#)
(work in progress), May 2012.

[I-D.thubert-savi-ra-throttler]
Thubert, P., "Throttling RAs on constrained interfaces",
[draft-thubert-savi-ra-throttler-01](#) (work in progress),
June 2012.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or
converting network protocol addresses to 48.bit Ethernet
address for transmission on Ethernet hardware", STD 37,
[RFC 826](#), November 1982.

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

[RFC2529] Carpenter, B. and C. Jung, "Transmission of IPv6 over IPv4
Domains without Explicit Tunnels", [RFC 2529](#), March 1999.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P.
Traina, "Generic Routing Encapsulation (GRE)", [RFC 2784](#),
March 2000.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering:
Defeating Denial of Service Attacks which employ IP Source
Address Spoofing", [BCP 38](#), [RFC 2827](#), May 2000.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network
Address Translator (Traditional NAT)", [RFC 3022](#),
January 2001.

- [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", [RFC 3056](#), February 2001.
- [RFC3068] Huitema, C., "An Anycast Prefix for 6to4 Relay Routers", [RFC 3068](#), June 2001.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.
- [RFC3964] Savola, P. and C. Patel, "Security Considerations for 6to4", [RFC 3964](#), December 2004.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", [RFC 4213](#), October 2005.
- [RFC4293] Routhier, S., "Management Information Base for the Internet Protocol (IP)", [RFC 4293](#), April 2006.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.
- [RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", [RFC 4380](#), February 2006.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", [RFC 4890](#), May 2007.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](#), September 2007.
- [RFC4942] Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/

Co-existence Security Considerations", [RFC 4942](#), September 2007.

- [RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", [RFC 5102](#), January 2008.
- [RFC5157] Chown, T., "IPv6 Implications for Network Scanning", [RFC 5157](#), March 2008.
- [RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", [RFC 5214](#), March 2008.
- [RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", [RFC 5952](#), August 2010.
- [RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", [RFC 5969](#), August 2010.
- [RFC6092] Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", [RFC 6092](#), January 2011.
- [RFC6169] Krishnan, S., Thaler, D., and J. Hoagland, "Security Concerns with IP Tunneling", [RFC 6169](#), April 2011.
- [RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", [RFC 6192](#), March 2011.
- [RFC6204] Singh, H., Beebe, W., Donley, C., Stark, B., and O. Troan, "Basic Requirements for IPv6 Customer Edge Routers", [RFC 6204](#), April 2011.
- [RFC6324] Nakibly, G. and F. Templin, "Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations", [RFC 6324](#), August 2011.
- [RFC6506] Bhatia, M., Manral, V., and A. Lindem, "Supporting Authentication Trailer for OSPFv3", [RFC 6506](#), February 2012.
- [RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", [RFC 6583](#), March 2012.
- [RFC6620] Nordmark, E., Bagnulo, M., and E. Levy-Abegnoli, "FCFS

SAVI: First-Come, First-Served Source Address Validation
Improvement for Locally Assigned IPv6 Addresses",
[RFC 6620](#), May 2012.

[evyncke_book]

Hogg and Vyncke, "IPv6 Security", ISBN 1-58705-594-5,
Publisher CiscoPress, December 2008.

Authors' Addresses

Kiran Kumar Chittimaneni
Google
1600 Amphitheater Pkwy
Mountain View 94043
USA

Phone: +16502249772
Email: kk@google.com

Merike Kaeo
ISC
950 Charter Street
Redwood City 94063
USA

Phone: +12066696394
Email: merike@doubleshotsecurity.com

Eric Vyncke
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2 778 4677
Email: evyncke@cisco.com

