

Network Working Group
Internet-Draft
Expires: December 22, 2008

F. Xia
Huawei
S. Krishnan
Ericsson Research
W. Haddad
Qualcomm
J-M. Combes
Orange Labs R&D
Chunqiang. Li
Huawei
June 20, 2008

Distributing a Symmetric Neighbor Discovery Key Using SEND
draft-xia-csi-symmetric-key-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 22, 2008.

Internet-Draft

Distributing a symmetric ND Key

June 2008

Abstract

In this document, a method for provisioning a shared key from the router to the host is defined to protect Neighbor Discovery(ND) signaling between the router and the host. The host sends a Router Solicitation(RS) message with ND Shared Key Request Option to the router. The router encrypts a ND shared key using the host's SEcure Neighbor Discovery(SEND) public key and sends it back to the host through a Router Advertisement(RA) message. The host decrypts the ND shared key using the matching private key. The Neighbor Discovery shared key is then used for protecting the following Neighbor Discovery signaling between the router and the host. The Router Solicitation and Router Advertisement message exchanges are required to have SEND security.

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	Operation Description	4
3.1.	Sending Router Solicitations	4
3.2.	Receiving Router Solicitations and Sending Router Advertisements	4
3.3.	Receiving Router Advertisements	5
3.4.	ND operation secured by a shared key	5
3.5.	Key Generation and Lifetime	6
4.	Message Formats	6
4.1.	ND Shared Key Request Option	6
4.2.	ND Shared Key Reply Option	7
4.3.	Neighbor Discovery Authenticator Option	8
5.	IANA consideration	9
6.	Security Considerations	10
7.	Acknowledgements	10
8.	References	10
8.1.	Normative References	10
8.2.	Informative references	11
	Authors' Addresses	12
	Intellectual Property and Copyright Statements	13

1. Introduction

IPv6 nodes use Neighbor Discovery(ND) protocol [[RFC4861](#)] to discover other nodes on the link, to determine their link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors. [[RFC3971](#)] specifies security mechanisms for ND, that is, Secure Neighbor Discovery (SEND) protocol in which Cryptographically Generated Addresses (CGA) [[RFC3972](#)] are used.

The construction and verification of the RSA Signature option in SEND operation is computationally expensive. In the ND context, however, hosts typically only have to perform a few signature operations as they enter a link, a few operations as they find a new on-link peer with which to communicate, or Neighbor Unreachability Detection with existing neighbors. Routers are required to perform a larger number of operations, particularly when the frequency of router advertisements is high due to mobility requirements. Scalability issue arises when hundreds , even thousands of hosts attach to a router.

In the same way, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) have similar constraints. It is recommended that ND signalling exchanges occur between the 6lowpan host and the PAN coordinator, which is a router in [[I-D.chakrabarti-6lowpan-ipv6-nd](#)]. Another point is 6lowpan hosts may not be able to do asymmetric cryptography all the time because of power/computing consumption.

In this document, a lightweight mechanism is defined by which a shared key for securing ND exchanges between the host and the router is provisioned on the host by the router. The mechanism described in the document utilizes SEND [[RFC3971](#)] public/private key pair to encrypt/decrypt a ND shared key sent from the router to the host. Once the ND shared key is provisioned, all ND exchanges occurring between the host and the router are protected by Message Authentication Codes (MAC) which generally requires much less computational operation. This main idea of the document is in line

with [[I-D.ietf-mipshop-handover-key](#)] in which shared handover key is used for protecting handover signaling between a mobile node and an access router.

The solution is based on and compatible with SEND operation.

[2.](#) Terminology

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](#)].

Xia, et al.

Expires December 22, 2008

[Page 3]

Internet-Draft

Distributing a symmetric ND Key

June 2008

The terminology and messages in this document are based on the definitions in [[RFC3971](#)], in addition to the ones defined below.
ND shared key : A key is shared between a router and a host, and used to protect ND signaling between the router and the host.

[3.](#) Operation Description

[3.1.](#) Sending Router Solicitations

According to SEND [[RFC3971](#)], the CGA option MUST be present in Router Solicitation(RS) messages unless they are sent with the unspecified source address. In this document, RS message with a CGA source address is used for a ND shared key request.

The host MUST send a RS containing a ND Shared Key Request Option defined in [Section 4.1](#) with the SEND's public key. A CGA for the host MUST be the source address of the packet, and the host MUST include the SEND CGA Option and SEND Signature Option with the packet, as specified in [[RFC3971](#)]. The SEND signature covers all fields in the RS, including the 128 bit source and destination addresses and ICMP checksum as described in [[RFC3971](#)], except for the Signature Option itself. The host also sets the authentication Algorithm Type (AT) field in the ND Shared Key Request Option to the host's preferred authentication algorithm. The SEND Nonce MUST also be included for anti-replay protection.

[3.2.](#) Receiving Router Solicitations and Sending Router Advertisements

When the router receives a RS from the host protected with SEND and including a ND Shared Key Request Option, the router MUST first validate the RS using SEND as described in [[RFC3971](#)]. If the RS can not be validated, the router MUST NOT include a ND Shared Key Reply Option [Section 4.2](#) in the reply.

If the RS is validated, the router MUST then determine whether the CGA is already associated with a ND shared key. If the CGA is associated with an existing key, the router MUST return the existing key to the host. If the CGA does not have a ND shared key, the router MUST construct a ND shared key as described in [Section 3.5](#). The router MUST encrypt the key with the host's SEND public key. The router MUST insert the encrypted ND shared key into a ND Shared Key Reply Option and MUST attach the option to the RA. The lifetime of the key MUST also be included in the ND Shared Key Reply Option. The router SHOULD set the AT field of the ND Shared Key Option to the MN's preferred algorithm type indicated in the AT field of the ND Shared Key Request Option, if it is supported; otherwise, the router

MUST select an authentication algorithm which is of equivalent strength or stronger and set the field to that. The router MUST also include the SEND nonce from the RS for anti-replay protection. The router MUST use the CGA constructed from its certified key as the source address for the RA and include a SEND CGA Option and a SEND Signature Option with the SEND signature of the message. The SEND signature covers all fields in the RA, including the 128 bit source and destination addresses and ICMP checksum as described in [[RFC3971](#)], except for the Signature Option itself. The RA is then unicast back to the host. The ND shared key MUST be stored by the router for future use, indexed by the host's CGA, and the authentication AT and a lifetime MUST be recorded with the key.

[3.3](#). Receiving Router Advertisements

Upon receipt of one or more RA secured with SEND and having the ND Shared Key Reply Option, the host MUST first validate the RA as described in [[RFC3971](#)]. Normally the host will have obtained the router's certification path to validate an RA prior to sending the RS and the host MUST check to ensure that the key used to sign the RA is the router's certified public key. If the host does not have the router's certification path cached, it MUST use the SEND

Certification Path Solicitation (CPS) / Certification Path Advertisement (CPA) messages to obtain the certification path to validate the key. If the message is not signed by a certified key , the message MUST be dropped.

The host MUST use it's private key to decrypt the ND shared key. The host MUST use the returned authentication AT indicated in the RA. The host MUST index the ND shared keys with the router's CGA, and the algorithm type and the lifetime are also stored.

When the host moves from a router to another router, it is possible that the new router has no any idea about the ND Shared Key which is provided by the old one. A solution is that the host erases the ND shared key and re-use CGA after a certain number of NS retransmissions.

[3.4.](#) ND operation secured by a shared key

When the host sends Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation(RS) to the router, the host SHOULD check if there is a ND shared key for the router. The host SHOULD utilize the shared key and the corresponding authentication algorithm type to generate an authenticator for the message if a ND shared key exists; otherwise, the host behaves according to[RFC3971], or requests a ND shared key using the procedure defined in this document. The authenticator is conveyed in Neighbor Discovery

Authenticator Option defined in [Section 4.3](#).

When the router sends Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation(RS), Redirect, Router Advertisement(RA) to the host, the router SHOULD check if there is a ND shared key for the host. The router SHOULD utilize the shared key and the corresponding authentication algorithm to generate an authenticator for the message if a ND shared key exists; otherwise, the router behaves according to [[RFC3971](#)]. The authenticator is conveyed in Neighbor Discovery Authenticator Option defined in [Section 4.3](#).

[3.5.](#) Key Generation and Lifetime

The router MUST randomly generate a key having sufficient strength to

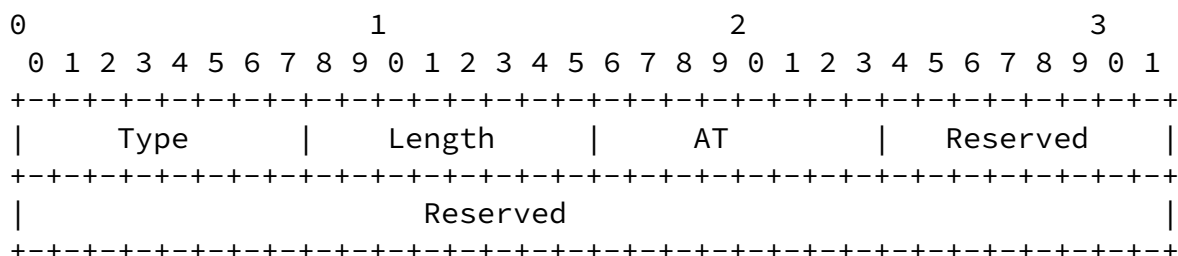
match the authentication algorithm. Some authentication algorithms specify a required key size. The router MUST generate a unique key along with a lifetime for each CGA public key of a host.

Before the lifetime expires, the host SHOULD apply for a new ND shared key using the procedure defined in this document. Once the ND shared key expires, the host and the router SHOULD discard the key.

4. Message Formats

4.1. ND Shared Key Request Option

The ND Shared Key Request Option is a IPv6 Neighbor Discovery [[RFC4861](#)] option in TLV format. The ND Shared Key Request Option is included in the RS message along with the SEND CGA Option, RSA Signature Option, and Nonce Option.



Fields:

Type: To be assigned by IANA.

Length: The length of the option in units of 8 octets, including the Type and Length fields. The value 0 is invalid. The receiver MUST discard a message that contains this value.

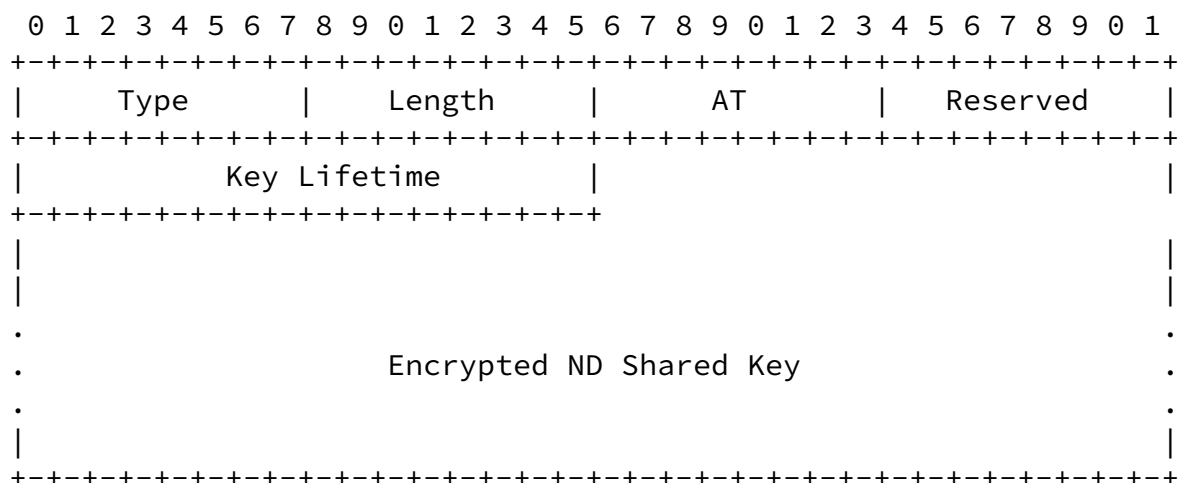
AT: authentication Algorithm Type

- 1 HMAC_SHA1
- 2 HMAC_SHA256
- 3 MD5

Reserved: A 40-bit field reserved for future use.

[4.2.](#) ND Shared Key Reply Option

ND Shared Key Reply Option is a IPv6 Neighbor Discovery [[RFC4861](#)] option in TLV format. The Reply Option is included in the RA message along with the SEND CGA Option, RSA Signature Option, and Nonce Option.

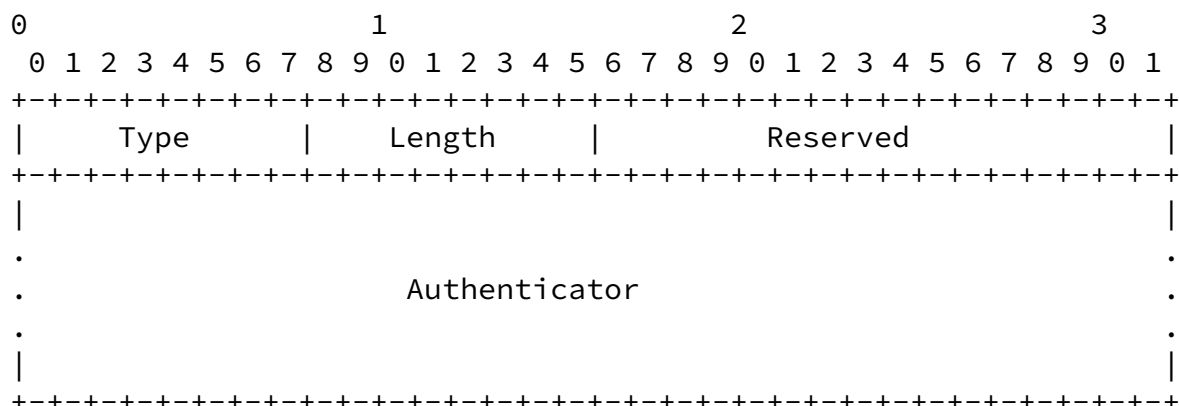


Fields:

- Type: To be assigned by IANA.
- Length: The length of the option in units of 8 octets, including the Type and Length fields. The value 0 is invalid. The receiver MUST discard a message that contains this value.
- AT: authentication Algorithm Type
- 1 HMAC_SHA1
 - 2 HMAC_SHA256
 - 3 MD5
- Reserved: A 8-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.
- Key Lifetime: lifetime of the ND shared key, in seconds.
- Encrypted ND Shared Key:
- The shared key, encrypted with the host's ND shared key encryption public key, using the RSAES-PKCS1-v1_5 format [[RFC3447](#)].

[4.3.](#) Neighbor Discovery Authenticator Option

This option MUST be present all ND signaling between the host and the router. This option specifies how to compute and verify a MAC using the established ND shared key.



Fields:

Type: To be assigned by IANA.

Length: The length of the option in units of 8 octets, including the Type and Length fields. The value 0 is invalid. The receiver MUST discard a message that contains this value.

Reserved: A 8-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Authenticator:

cryptographic value which can be used to determine that the message in question comes from the right authority

Rules for calculating the Authenticator value are the following:

```
ND Data = host's source address | router's address | ICMP Data
Authenticator = First (96, Algorithm( ND Shared Key, ND Data))
```

The algorithm type for authenticator is negotiated between the host and the router through ND Shared Key Request Option and ND Shared Key Reply Option.

5. IANA consideration

Option, ND Shared Key Reply Option, and Neighbor Discovery Authenticator Option, are defined, and require IPv6 Neighbor Discovery option type codes from IANA.

[6.](#) Security Considerations

This document describes a shared key provisioning protocol for the Neighbor Discovery protocol. The key provisioning protocol utilizes a public key of SEND. General security considerations involving CGAs apply to the protocol described in this document, see [[RFC4861](#)] for a discussion of security considerations around CGAs.

[7.](#) Acknowledgements

Jean-Michel Combes is partly funded by MobiSEND, a research project supported by the French 'National Research Agency' (ANR).

[8.](#) References

[8.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [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.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), 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.

- [RFC3314] Wasserman, M., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", [RFC 3314](#), September 2002.

Xia, et al.

Expires December 22, 2008

[Page 10]

Internet-Draft

Distributing a symmetric ND Key

June 2008

[8.2](#). Informative references

- [I-D.ietf-mipshop-handover-key]
Kempf, J., "Distributing a Symmetric FMIPv6 Handover Key using SEND", [draft-ietf-mipshop-handover-key-03](#) (work in progress), October 2007.
- [RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", [RFC 3447](#), February 2003.
- [I-D.chakrabarti-6lowpan-ipv6-nd]
Chakrabarti, S. and E. Nordmark, "LowPan Neighbor Discovery Extensions",
[draft-chakrabarti-6lowpan-ipv6-nd-04](#) (work in progress), November 2007.

Authors' Addresses

Frank Xia
Huawei
1700 Alma Dr. Suite 500
Plano, TX 75075

Phone: +1 972-509-5599
Email: xiayangsong@huawei.com

Suresh Krishnan
Ericsson Research
8400 Decarie Blvd.
Town of Mount Royal, QC Canada

Phone: +1 514 345 7900
Email: Suresh.Krishnan@ericsson.com

Wassim Haddad
Qualcomm

Phone:
Email: whaddad@qualcomm.com

Jean-Michel Combes
Orange Labs R&D
38 rue du General Leclerc
Issy-les-Moulineaux Cedex 9, France 92794

Phone:
Email: jeanmichel.combes@gmail.com

Chunqiang Li
Huawei
No.91 BaiXia Rd.
Nanjing, China 210001

Phone:
Email: li.chunqiang@huawei.com

Xia, et al.	Expires December 22, 2008	[Page 12]
-------------	---------------------------	-----------

Internet-Draft	Distributing a symmetric ND Key	June 2008
----------------	---------------------------------	-----------

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.