

Network Working Group
Internet-Draft
Updates: [3122](#) (if approved)
Intended status: Standards Track
Expires: August 31, 2009

P. Thubert, Ed.
E. Levy-Abegnoli
Cisco
February 27, 2009

IPv6 Inverse Neighbor Discovery Update
draft-thubert-3122bis-01.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

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/1id-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 August 31, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

RFC3122bis

February 2009

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This draft updates the Inverse Discovery Specification [[RFC3122](#)] to provide Secure Neighbor Discovery. The behaviour of the protocol is slightly amended to enable an easier management of the addresses on a link and enable Secure ND.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	4
2.	Inverse Neighbor Discovery Messages	4
2.1.	Inverse Neighbor Discovery Solicitation Message	4
2.2.	Inverse Neighbor Discovery Advertisement Message	5
3.	Inverse Neighbor Discovery Options	6
3.1.	Source/Target Address List	7
4.	Secure Inverse Neighbor Discovery	9
5.	Interface Type and usages	11
5.1.	Point to Multipoint Networks	11
5.2.	Point-to-Point Links	11
5.3.	Broadcast Networks	12
6.	IANA Considerations	12
7.	Security Considerations	12
8.	Acknowledgements	12
9.	References	12
9.1.	Normative References	12
9.2.	Informative References	13
	Authors' Addresses	13

Internet-Draft

RFC3122bis

February 2009

1. Introduction

This draft updates the Inverse Neighbor Discovery Specification [[RFC3122](#)]. Any behaviour or format that is not explicitly changed is preserved.

The behaviour of the protocol is slightly amended :

- o Secure Inverse Neighbor Discovery is added for unicast addresses with a 64bit interface ID. This specification provides the additional options that are required to sign Inverse ND messages with the properties that are defined in [[RFC3971](#)] and details how they may be used to prove the ownership of advertised addresses.
- o Fragmentation of ND messages is accepted but not required. [[RFC3122](#)] requires the use of multiple Advertisement messages when the Target Address List does not fit within MTU. With this specification, it is acceptable to fragment a message, but it is still possible to use multiple Advertisement messages, which can be necessary in particular in the context of Secure Inverse Neighbor Discovery.
- o [[RFC3122](#)] does not allow a crisp management of all Addresses that a peer may use on an interface. When multiple Advertisement messages are used, it is possible to miss one and thus miss some information. With this specification, Address Management is improved in such a way that it is possible to advertise the addition or the deletion of a single address and to get the exhaustive list of all the addresses that a neighbor might use to source packets on an interface.
- o With IPv4, Inverse ARP is traditionally applied to Point to Multipoint networks only. [[RFC3122](#)] claims to apply to "Frame Relay networks", and "also apply to other networks with similar behavior". This specification extends the domain of applicability of Inverse Neighbor Discovery and provides some additional

information on how and why Inverse ND MAY be used on all types of interface.

- o Typos such as the length field in the Source/Target Address List are corrected.

The concept of transaction is introduced to group multiple messages into a single set to enable the advertisement of the complete list of all addresses used to source packets on an interface. Whenever possible, a node should use one message per transaction.

This is problematic when:

- o The list of addresses is so large that it causes the message to be larger than MTU and the node can not fragment.
- o Secure Inverse ND is applied and not all of the addresses are based on a same CGA modifier (see [[RFC3972](#)]).

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 [RFC 2119](#) [[RFC2119](#)].

2. Inverse Neighbor Discovery Messages

This section updates the Inverse Neighbor Discovery Messages defined in [[RFC3122](#)] [section 2](#).

A new field from the ICMP reserved part is used to indicate the version and preserve backward compatibility. Version 0 is [[RFC3122](#)]. Version 1 is this specification. A node proposes a version in the Inverse Neighbor Discovery Solicitation Message and responds with the smallest of its own preferred version and the received proposed version in an Advertisement.

Another new field from the ICMP reserved part is used to indicate the Transaction ID of a Neighbor Discovery Solicitation Message, in order to correlate multiple Advertisement messages that may result from one Solicitation Message. When the information about an address is not

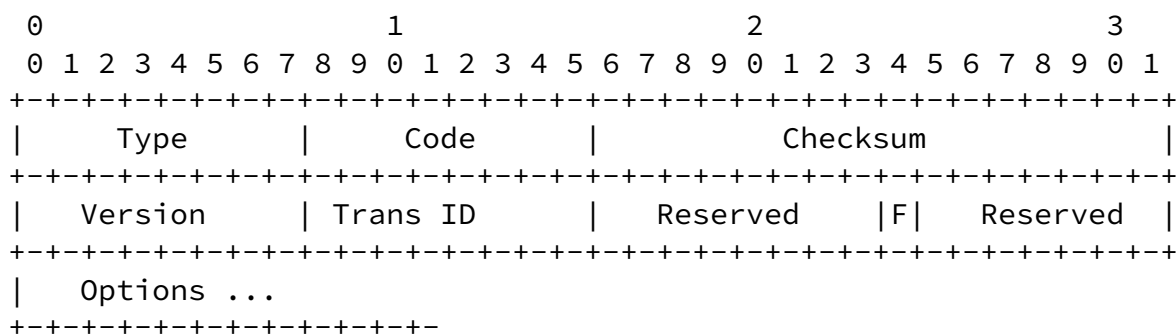
seen after 2 consecutive advertisement of a full List of addresses that address is considered as removed. This decision is made upon the reception of an advertisement with a Transaction ID that is sequentially later then the 2 consecutive advertisements.

2.1. Inverse Neighbor Discovery Solicitation Message

The Inverse Neighbor Discovery Solicitation Message can be used to obtain the full list of IPv6 addresses from the remote end of a Point to Point link such as a PPP link, a tunnel or a Virtual Channel.

The Inverse Neighbor Discovery Solicitation can also be used as a heartbeat mechanism to verify whether a Point to Point link such as a tunnel is still up when there is no signal from the lower layers to indicate a failure.

The Inverse Neighbor Discovery Solicitation Message is changed as follows:



Modified Inverse Neighbor Discovery Solicitation Message

This specification adds the following fields:

Type: 8bit field. Inverse Neighbor Discovery Solicitation.

Version: 8bit field. Version of 0 indicates the support of [RFC3122](#) only. Version of 1 indicates the desire to follow this specification and the backward compatibility with version 0.

F: 1bit field. The "F" flag indicates a request of the Full List of addresses on the peer side of the Link.

The Inverse Neighbor Discovery Advertisement Message is changed as follows:

This specification adds the following fields:

Type: 8bit field. Inverse Neighbor Discovery Advertisement.

Version: 8bit field. Version of 0 indicates the support of [\[RFC3122\]](#) only. Version of 1 indicates the desire to follow this specification. Version can only be set to 1 if the Version in the Solicitation Message was 1 or above.

Transaction ID: 8bit field. The Transaction ID echoes that of the Inverse Neighbor Discovery Solicitation Message that this Message is responding to. The transaction ID zero is used for unsolicited Advertisements.

F: 1bit field. The "F" flag indicates that the Full List of addresses will be provided for that transaction.

Upon a request by the remote peer of the Full List of addresses, this node SHOULD answer with all the addresses that can be used to reach it over this link in the modified Target Address List.

If the IND Solicitation does not request the full list then his node MAY answer with all the addresses that can be used to reach it over this link in the modified Target Address List.

[3.](#) Inverse Neighbor Discovery Options

This section updates the Inverse Neighbor Discovery Options defined in [\[RFC3122\] section 3](#).

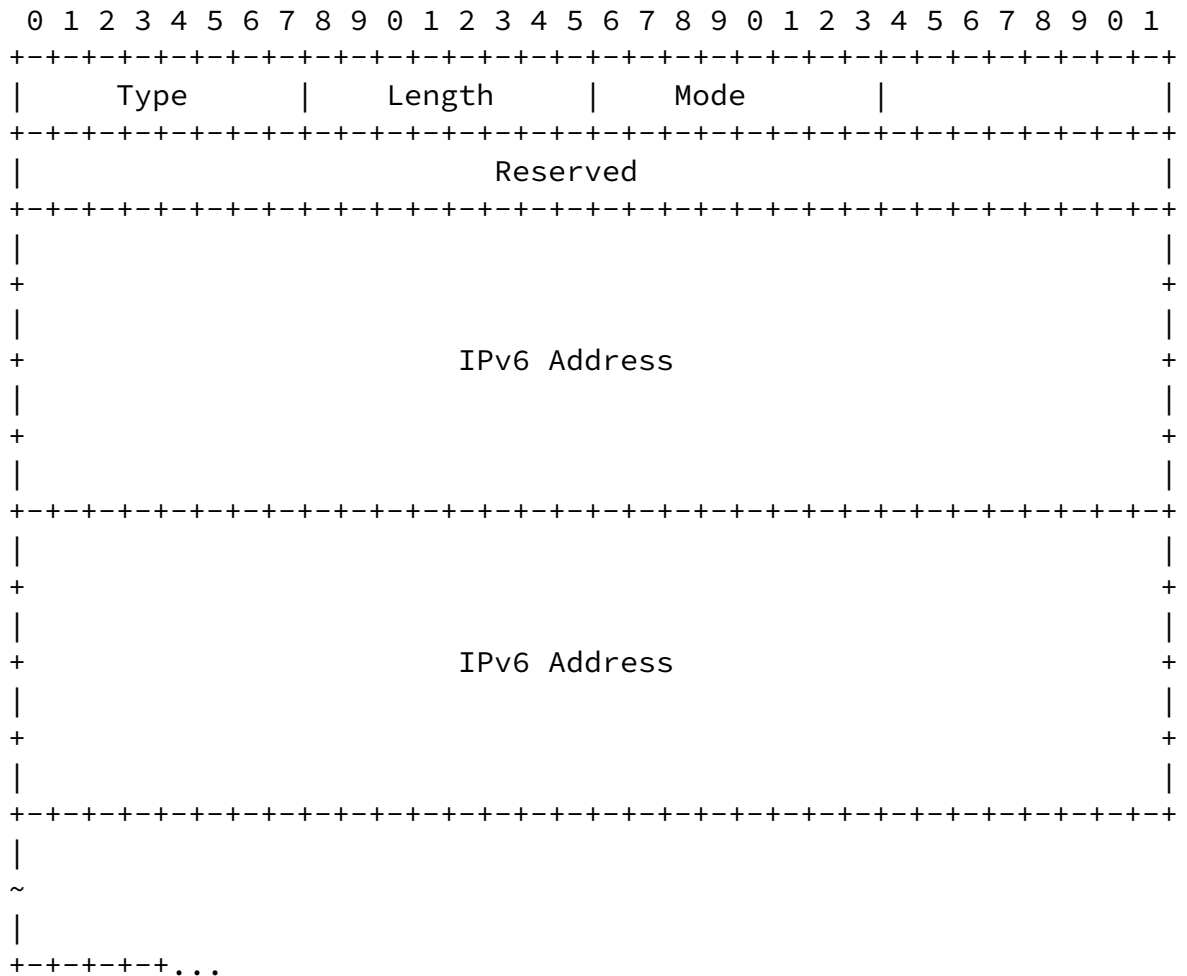
[3.1.](#) Source/Target Address List

With this specification, the Source/Target Address List may be partial or full. It can be used to indicate addition or deletion of individual addresses. This new support can only be used once the first Inverse Neighbor Discovery Solicitation Message is received from the remote peer indicating the support of this specification.

Until the Version that is supported by the peer is known, the only Inverse Neighbor Discovery Messages that this node should send are Solicitations, and this option if present can only be a Source Address List option with a list of addresses that can be used to reach this node over this link.

This specification uses a Length field of 8 bits, assuming that most implementations of [\[RFC3122\]](#) also use a Length field of 8 bits and that the misalignment in [section 3.1](#) is commonly understood as an undetected typo. An error in reading the Length field can be detected when confronting the length of the IPv6 packet and the expected length of this option.

The Inverse Neighbor Discovery Advertisement Message is changed as follows:



Modified Source/Target Address List option

This specification adds the following fields:

Mode 8bit enumeration

[RFC3122](#): Mode of 0 indicates that the list is built conforming to [\[RFC3122\]](#). All the addresses listed are usable but the list might not be complete.

Full: Mode of 1 indicates that the list might contain addresses that are defined on another interface but may be used to source or receive packets over this interface. This is the mode that is used to in reply to a Solicitation with the "F" bit set.

Added: Mode of 2 indicates that the list is a list of recently added addresses but not necessarily part of a full report.

Deleted: Mode of 3 indicates that the list is a list of recently removed addresses that may no more be used on this link.

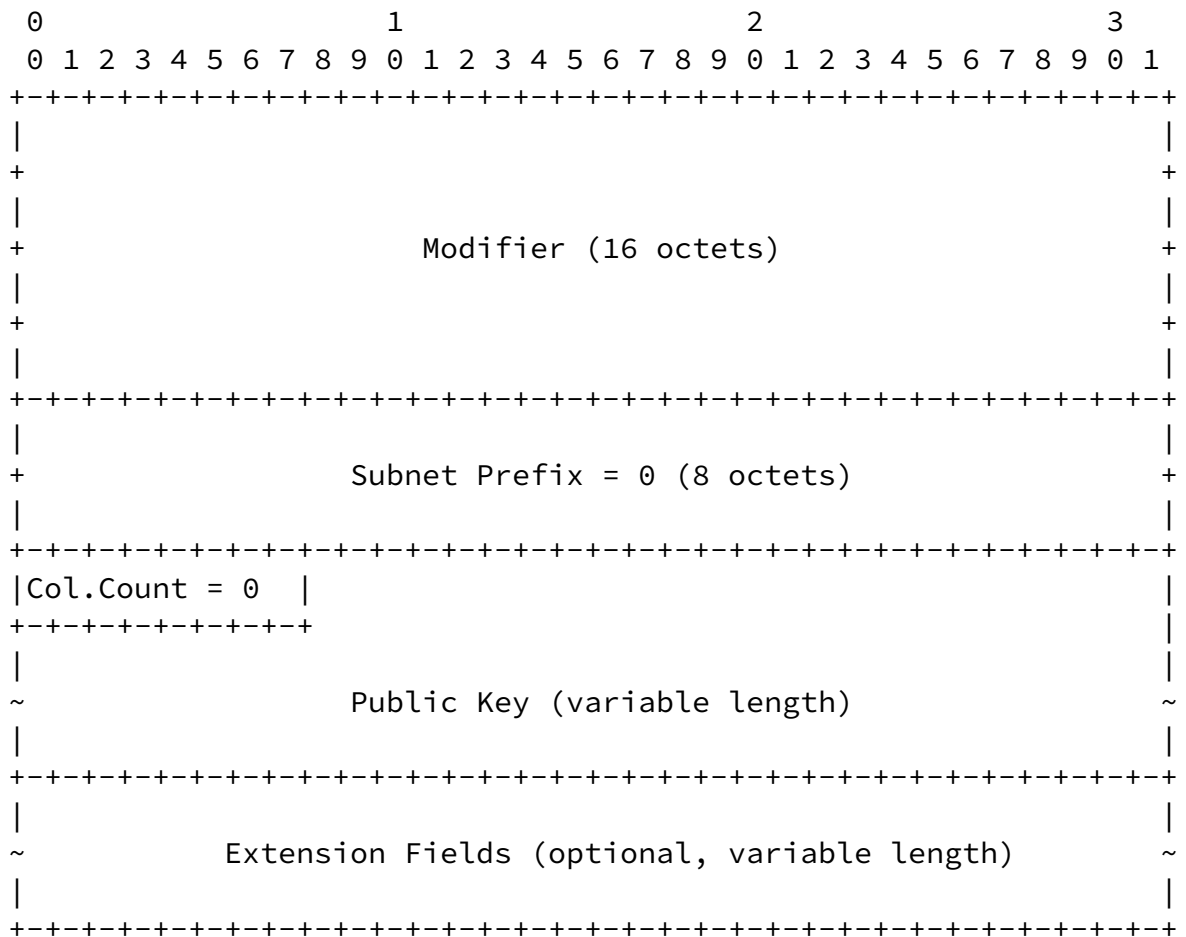
Upon receiving an Address List, a node should verify that the addresses in the list don't collide with any of its own address. In case it does, the duplicate address received in the list will be ignored.

When Secure IND is being used, all the addresses listed in the Target Address List option in one Inverse Neighbor Discovery Advertisement Message must be based on the same CGA modifier. If multiple modifiers are used or some addresses were not built based on CGA, then they must be split in multiple Inverse Neighbor Discovery Advertisement Messages.

4. Secure Inverse Neighbor Discovery

The list of addresses provided in Source/Target address list can be defended using the CGA and the RSA options specified in [[RFC3972](#)] and [[RFC3971](#)]. However, in the case of Secure Inverse Neighbor Discovery, several addresses announced in one message (IND Solicitation or Advertisement) are defended by a single CGA option and a single RSA option. That mandates that all addresses in the list are based on CGA and were computed with the same public key, modifier, collision count, and the same security parameter sec. In this case, the CGA option is as following:

February 2009



The remaining of the CGA algorithm, as described in [\[RFC3972\]](#) applies. The 16*Sec leftmost bits of Hash2 should equal zero. Hash1 is computed separately for each address in the list, using the first 64 bits as the Subnet Prefix, and the interface identifier should

match Hash1 (except for bits 0, 1, 2, 6, and 7, which encode the collision count and the "u" and "g" bits).

The RSA option must also be provided in the message, and the signature must verify with the public key provided in the CGA option

In order to protect against replays, Timestamp and Nonce options, should also be used in the message, with similar rules as one described in [[RFC3971](#)]. When the message is a solicitation (INS), it

should have a nonce option. When the message is solicited (INA as a response to INS), it should repeat the nonce value seen in the solicitation. As far as unsolicited message and solicitation, the timestamp option is required.

[5.](#) Interface Type and usages

Because of IPv4 and the ARP legacy, Inverse Neighbor Discovery is usually associated to Point to Multipoint (P2MP) or Non-Broadcast Multi-Access (NBMA) networks. And certainly, this specification is usable on such networks as Frame Relay or Multidrop tunnels.

But the similarity with IPv4 is limited and this specification enables a lot more:

[5.1.](#) Point to Multipoint Networks

IPv6 Secure Inverse Neighbor Discovery can be applied to P2MP and NBMA networks to prevent the theft an address by another Node.

[5.2.](#) Point-to-Point Links

As opposed to IPv4, using Inverse Neighbor Discovery makes a lot of sense on Point-to-Point link such as PPP or tunnels:

This specification inherits from [[RFC3122](#)] the support of the authentication header to authenticate the remote peer on the link. For P2P links, this might prove more relevant than Secure ND itself.

Because IPv6 operates purely at layer 3, the PPP Network Control Protocol for IPv6 defined in [[RFC5072](#)] provides a way to negotiate a

unique, 64bit interface identifier to be used for the address autoconfiguration but does not enable to advertise an IPv6 address. This would not fit anyway since IPv6 might use many addresses of various lifetimes on a same interface. This specification provides the means to create and maintain the list of addresses that can be used to reach the remote peer at any point of time.

A number of Denial of Service attacks are documented when using [\[RFC4861\]](#) by sending packets to addresses that are not assigned but belong to a prefix that is associated to the P2P link. On those links, Inverse Neighbor Discovery enables a proactive model that defeats those attacks. Any packet that is received for a destination that is not in the ND table is simply dropped.

[5.3.](#) Broadcast Networks

A multihomed host attached to a broadcast network might use an address that belongs to another interface on another subnet to source a packet. This makes the validation of source addresses very problematic. With this specification, a router may solicit the full list of all addresses that this host might use to source packets on that interface, and prove the ownership using SeND. The router might then accept packets that are sourced off-link and may install a host route to that address.

[6.](#) IANA Considerations

This memo includes no request to IANA.

[7.](#) Security Considerations

This draft improves the security model in [\[RFC3122\]](#) by adding the capability to use Secure Neighbor Discovery

[8.](#) Acknowledgements

Thanks to Tony Cheneau and Wojciech Dec for useful feedback and discussion.

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.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.
- [RFC3122] Conta, A., "Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification", [RFC 3122](#), June 2001.
- [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.

9.2. Informative References

- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#), June 1999.
- [RFC5072] S.Varada, Haskin, D., and E. Allen, "IP Version 6 over PPP", [RFC 5072](#), September 2007.

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems
Village d'Entreprises Green Side

400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Phone: +33 4 97 23 26 34
Email: pthubert@cisco.com

Eric Levy-Abegnoli
Cisco Systems
Village d'Entreprises Green Side
400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Phone: +33 4 97 23 26 20
Email: elevyabe@cisco.com