Network Working Group S. Joshi
Internet-Draft S. Ooghe
Intended status: Standards Track Alcatel Lucent
Expires: September 24, 2010 March 23, 2010

Interface Identifier Assignment in IPv6 SLAAC
draft-joshi-6man-neighbor-inform-00

Abstract

This document proposes an optional mechanism as part of IPv6 Stateless Address Autoconfiguration for distribution of unique interface identifiers to IPv6 hosts on a link. Hosts can then use these unique interface identifiers to generate unique autoconfigured link local and global unicast addresses.

This mechanism is intended for use in networks where link layer identifiers are used for generating interface identifiers and where non unique link layer identifiers will result in duplicate link local addresses. An example of such network is Ethernet Broadband access networks.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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/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 September 24, 2010.

Copyright Notice

Copyright (c) 2010 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 BSD License.

Table of Contents

1. Introduction 3

2. Terminology 4
  2.1. General 4
  2.2. Requirements Language 4

3. IPv6 Specification Dependency 5

4. Neighbor Inform Message Format 6

5. Receiving Neighbor INFORM 8
  5.1. Validating of Neighbor Inform Messages 8
  5.2. Node Specification 8
    5.2.1. Host Configuration Variable 8
    5.2.2. Processing Neighbor Inform 9

6. Delegating Interface Identifier 10
  6.1. Delegating Node Specification 10
    6.1.1. Node Configuration Variable 10
    6.1.2. Interface Initialization 10
    6.1.3. Sending Neighbor Inform 10

7. IANA Considerations 12

8. Security Considerations 13

9. Acknowledgements 14

10. References 15
  10.1. Normative References 15
  10.2. Informative References 15

Authors' Addresses 16

1. Introduction

This document introduces an optional mechanism for delegation of interface identifier as part of Stateless Address Autoconfiguration (SLAAC) [RFC4862]. A new optional message Neighbor Inform is introduced to Neighbor Discovery [RFC4861] to enable delegation of interface identifier. A delegating node uses the message as part of SLAAC to delegate unique interface identifiers to hosts on a link.

A typical case is an ethernet based broadband access network consisting of large number of Customer Premise Equiment (CPE) devices conneting to service providers core network. In such a network it's quite likely that either a legitimate or a malicious CPE will have a duplicate MAC address and this would result in two or more hosts on the same link arriving at same EUI-64 based interface identifier as defined in [RFC2464]. Non-unique interface identifier will lead to duplicate link local and global unicast IPv6 addresses and as a result in Denial of Service for legitimate users.

Deploying Network Address Translation is a possible solution to this problem, however it considerably increases the complexity and processing capability required in Broadband Access Nodes. A protocol based solution is desirable as it is scalable and expandable.

2. Terminology

2.1. General

node - a device that implements IPv6.

link - a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IP. Examples are Ethernets (simple or bridged), PPP links or ATM networks as well as Internet-layer (or higher-layer) "tunnels", such as tunnels over IPv4 or IPv6 itself.

neighbors - nodes attached to the same link.

delegating node - a node that distributes interface identifiers to neighbors.

host - any node that is not a router.

proxy - a node that responds to Neighbor Discovery query messages on behalf of another node.

tentative address - an address whose uniqueness on a link is being verified, prior to its assignment to an interface. A tentative address is not considered assigned to an interface in the usual sense. An interface discards received packets addressed to a tentative address, but accepts Neighbor Discovery packets related to Duplicate Address Detection for the tentative address.

solicited-node multicast address - a multicast address to which Neighbor Solicitation messages are sent. The algorithm for computing the address is given in [RFC4291].

2.2. 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].

3. IPv6 Specification Dependency

This document describes a new neighbor discovery message and the processing associated with this message. This document should be read in conjunction with IPv6 Neighbor Discovery [RFC4861] and IPv6 Stateless Address Autoconfiguration [RFC4862].

4. Neighbor Inform Message Format

A delegating node sends Neighbor Inform message in response to Neighbor Solicatation message sent as part of Duplicate Address detection.

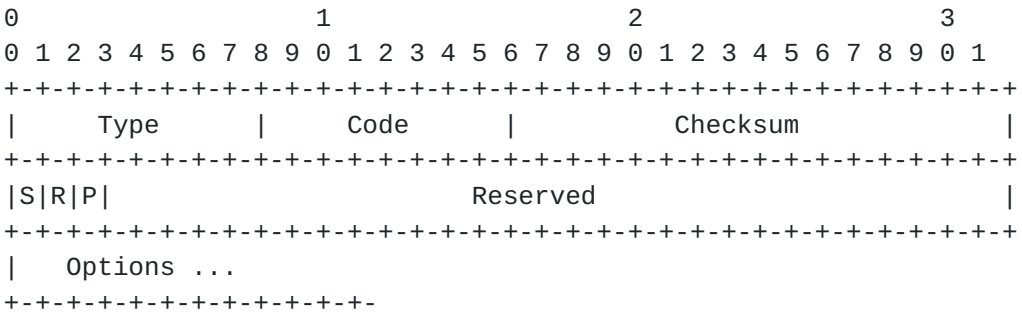


Figure 1: Neighbor Inform Message Format

IP Fields:

Source Address - An address assigned to the interface from which the inform is sent.

Destination Address - The solicited-node multicast address.

Hop Limit - 255

ICMP Fields:

Type - 155

Code 0 - Reconfigure

Checksum - ICMP checksum.

S - Solicited flag. When set, the S-bit indicates that inform was sent in response to a message from Destination address.

R - Router flag. When set, the R-bit indicates that the sender is a router.

P - Proxy flag. When set, the P-bit indicates that the sender is a Neighbor Discovery Proxy.

Reserved- 29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Possible options:

Identifier- Identifier is ICMP code of message that caused this INFORM (e.g. 135 - Solicit)

Target address - The IP address of the target of the solicitation. Option must be included if ICMP Code is 0 and Identifier is SOLICIT.

Interface-ID - Alternative interface ID to be used when reconfiguring link local IPv6 address.

Future versions of this protocol may define new option types. Receivers MUST silently ignore any options they do not recognize and continue processing the message.

5. Receiving Neighbor INFORM

5.1. Validating of Neighbor Inform Messages

A node MUST silently discard any received Neighbor Inform messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.

- ICMP Checksum is valid.

- ICMP Code is 0.

- ICMP length (derived from the IP length) is 24 or more octets.

- Target Address is not solicited node multicast address of tentative address assigned to receiving interface.

- If the IP Destination Address is a multicast address the Solicited flag is zero.

- All included options have a length that is greater than zero.

The contents of the Reserved field, and of any unrecognized options, MUST be ignored. Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values. The contents of any defined options that are not specified to be used with Neighbor Inform messages MUST be ignored and the packet processed as normal. A Neighbor Inform that passes the validity checks is called a "valid inform".

5.2. Node Specification

5.2.1. Host Configuration Variable

A node MUST allow for the following conceptual variables to be configured by system management. The specific variable names are used for demonstration purposes only, and an implementation is not required to have them, so long as its external behavior is consistent with that described in this document. Default values are specified to simplify configuration in common cases.

For each interface:

NbrRcvInform

A flag indicating whether processing of received Neighbor Inform messages is enabled on this interface. Enabling would indicate that node will accept delegated interface identifier for the interface.

Default Value :FALSE

5.2.2. Processing Neighbor Inform

On receipt of a valid Neighbor Inform message on an interface, node behavior depends on whether target address option in message matches a tentative address or an address assigned to the interface.

If the target address is not tentative (i.e., it is assigned to the receiving interface), the Neighbor Inform message is silently discarded by the node.

If the node has not transmitted a Neighbor Solicit with target address. This could be the case where two nodes with same tentative address are attempting DAD and delegating node has responded to other nodes Solicit request. The Neighbor Inform message is silently discarded by the node and node proceeds with DAD for tentative address.

If the target address option in the Inform message matches tentative address of the received interface then the tentative address is determined as duplicate.

A tentative address that is determined to be duplicate SHOULD NOT be assigned to the interface, and the node SHOULD log a system management error.

If Interface-ID option is present in the Inform message, node MUST use the interface identifier provided to regenerate an IPv6 link local or global unicast address and reinitiate Duplicate Address Detection (DAD).

6. Delegating Interface Identifier

6.1. Delegating Node Specification

6.1.1. Node Configuration Variable

A node MUST allow for the following conceptual variables to be configured by system management. The specific variable names are used for demonstration purposes only, and an implementation is not required to have them, so long as its external behavior is consistent with that described in this document. Default values are specified to simplify configuration in common cases.

For each interface:

NbrDelegationEnable

A flag indicating whether sending of Neighbor Inform messages is enabled on this interface. Setting the flag to true would indicate that node will act as a delegating node on that interface.

Default Value :FALSE

6.1.2. Interface Initialization

The node joines all-nodes multicast address on interfaces enabled for delegation.

6.1.3. Sending Neighbor Inform

A delegating node sends a Neighbor Inform in response to a Neighbor Soliciation received as part of Duplicate Addresses Detection initiated by an IPv6 host. Neighbor Solicit messages sent as part of DAD have source address set as unspecified address.

The Target Address of the Inform is copied from the Target Address of the soliciation. The node populates the Interface-ID of the inform either from a database or using a dynamic algorithm. The node may use additional information from received Solicit message e.g. link local address,vlan or physical interface (e.g. DSL) to arrive at a unique Interface-ID to be delegated.

Furthermore, if a node is a router, it MUST set the Router flag to one;otherwise it must set the flag to zero

If a node is a proxy, it MUST set the proxy flag to one;otherwise it must set the flag to zero

The node MUST set the solicited flag to one and multicast the inform to all-nodes address.

7. IANA Considerations

IANA is requested to assign a new ICMPv6 Type (155) for NEIGHBOR INFORM message.

8. Security Considerations

Unsecured Neighbor Discovery has a number of security issues, which are discussed in detail in [RFC3756]. Security mechanisms to protect Neighbor Discovery are described in [RFC3971].

9. Acknowledgements

This document liberally borrows text from RFC4862 and RFC4861.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

10.2. Informative References

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

Authors' Addresses

Shrinivas Joshi
Alcatel Lucent
RR Towers IV, Thiruvika Industrial Estate, Guindy
Chennai, Tamil Nadu 600032
India

Phone: +91-44-3099-8165
Email: shrinivas_ashok.joshi@alcatel-lucent.com

Sven Ooghe
Alcatel Lucent
Copernicuslaan 50
Antwerp 2018
Belgium

Phone: +32-32404226
Email: sven.ooghe@alcatel-lucent.com