Network Working Group
Request for Comments: 3122
Category: Standards Track

A. Conta
Transwitch Corporation

June 2001

Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

This memo describes extensions to the IPv6 Neighbor Discovery that allow a node to determine and advertise an IPv6 address corresponding to a given link-layer address. These extensions are called Inverse Neighbor Discovery. The Inverse Neighbor Discovery (IND) was originally developed for Frame Relay networks, but may also apply to other networks with similar behavior.

Table of Contents

1. Introduction

This document defines extensions to the IPv6 Neighbor Discovery (ND)[IPv6-IND]. The extensions are called IPv6 Inverse Neighbor Discovery (IND). The IPv6 Inverse Neighbor Discovery (IND) allows a node that knows the link-layer address of a directly connected remote node to learn the IPv6 addresses of that node. A node using IND sends solicitations and receives advertisements for one or more IPv6 addresses corresponding to a known link-layer address.

The Inverse Neighbor Discovery (IND) was originally developed for Frame Relay networks, but may also apply to other networks with similar behavior.

The keywords MUST, MUST NOT, MAY, OPTIONAL, REQUIRED, RECOMMENDED, SHALL, SHALL NOT, SHOULD, SHOULD NOT are to be interpreted as defined in [KEYWORDS].

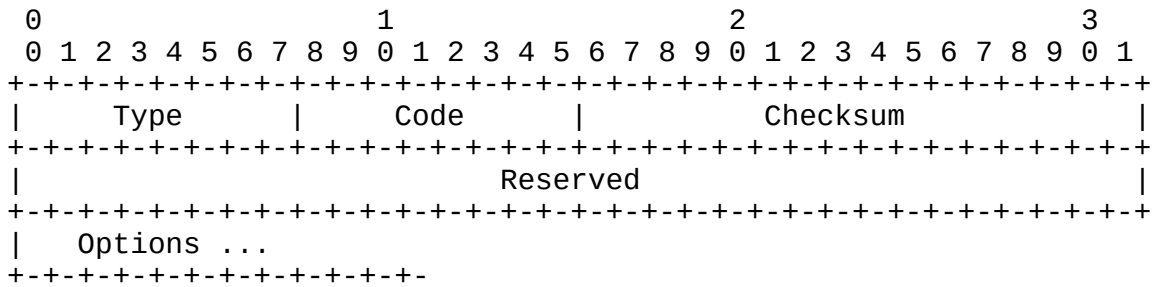
There are a number of similarities and differences between the mechanisms described here and those defined for Inverse ARP for IPv4 in [INV-ARP] or its replacement documents.

2. Inverse Neighbor Discovery Messages

The following messages are defined:

2.1. Inverse Neighbor Discovery Solicitation Message

A node sends an Inverse Neighbor Discovery Solicitation message to request an IPv6 address corresponding to a link-layer address of the target node while also providing its own link-layer address to the target. Since the remote node IPv6 addresses are not known, Inverse Neighbor Discovery (IND) Solicitations are sent as IPv6 all-node multicasts [IPv6], [IPv6-FR], [ENCAPS]. However, at link layer level, an IND Solicitation is sent directly to the target node, identified by the known link-layer address.



Source Address
An IPv6 address assigned to the interface from which this message is sent.

Destination Address
The IPv6 all-node multicast address. This address is specified in its link-scope format, which is FF02::1.

Hop Limit 255

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination, then the sender SHOULD include this header.

ICMP Fields:

Type	141
Code	0
Checksum	The ICMP checksum. See [ICMPv6].
Reserved	This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Required options:

The sender node MUST send the following options in the Solicitation message:

Source Link-Layer Address
The link-layer address of the sender.

Target Link-Layer Address
The link-layer address of the target node.

Other valid options:

The sender node MAY choose to add the following options in the Solicitation message:

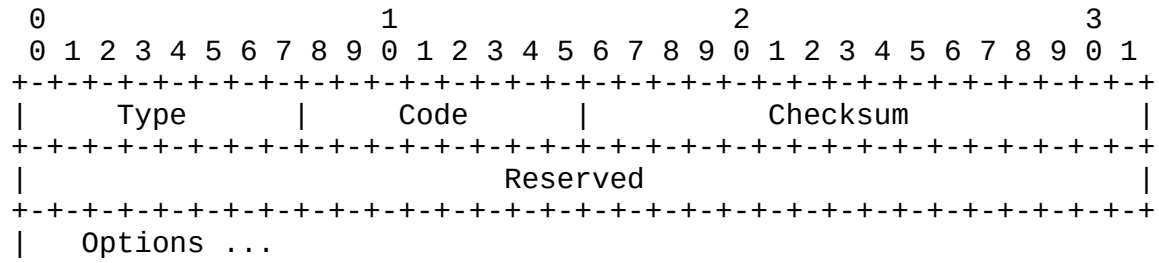
Source Address List
The list of one or more IPv6 addresses of the interface identified by the Source Link-Layer Address. This option is defined in section 3.

MTU
The MTU configured for this link [IPv6-ND].

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

2.2 Inverse Neighbor Discovery Advertisement Message

A node sends Inverse Neighbor Discovery Advertisements in response to Inverse Neighbor Discovery Solicitations.



IP Fields:

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

Destination Address
The Source Address of an invoking Inverse Discovery Neighbor Solicitation.

Hop Limit 255

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header.

ICMP Fields:

Type 142

Code 0

Checksum The ICMP checksum. See [ICMPv6].

Reserved 32-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Required options:

The sender node MUST send the following options in the Advertisement message:

Source Link-Layer Address The link-layer address of the sender.

Target Link-Layer Address
The link-layer address of the target, that is, the sender of the advertisement.

Target Address List
The list of one or more IPv6 addresses of the interface identified by the Target Link-Layer Address in the Inverse Neighbor Discovery Solicitation message that prompted this advertisement. This option is defined in Section 3.

Other valid options:

The sender node MAY choose to add the following option in the Advertisement message:

MTU
The MTU configured for this link [IPv6-ND].

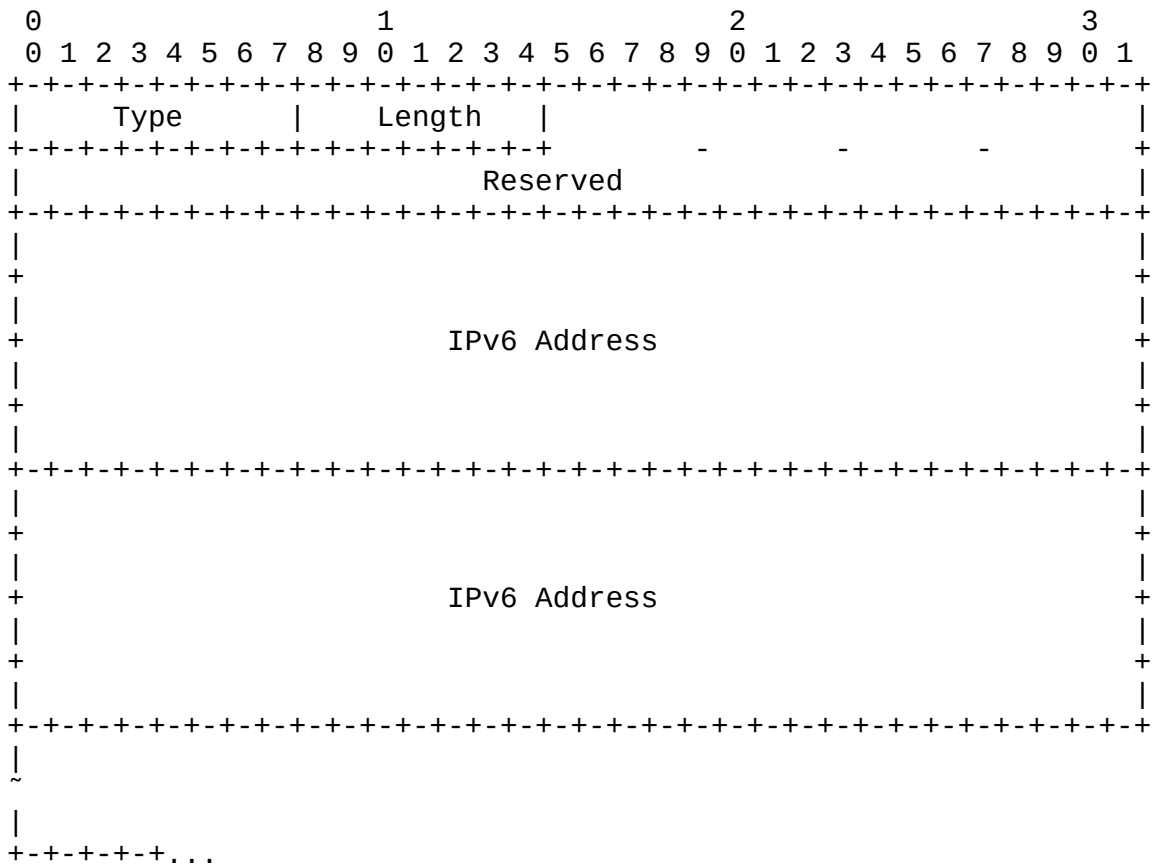
Future versions of this protocol may add other option types. Receivers MUST silently ignore any options they do not recognize and continue processing the message.

3. Inverse Neighbor Discovery Options Formats

Inverse Neighbor Discovery messages include Neighbor Discovery options [IPv6-ND] as well as an Inverse Neighbor Discovery specific options: the Source Address List and the Target Address List.

3.1 Source/Target Address List

The Source Address List and the Target Address List option are TLV options (type, length, variable size field) (see Section 4.6 of [IPv6-ND] with the following fields:



Fields:

Type 9 for Source Address List
10 for Target Address List

Note: These Option Type values should be assigned from the IPv6 Neighbor Discovery family of values.

Length The length of the option (including the Type, Length, and the Reserved fields) in units of 8 octets. The minimum value for Length is 3, for one IPv6 address.

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

IPv6 Addresses One or more IPv6 addresses of the interface.

Description:

The Source Address List contains a list of IPv6 addresses of the interface identified by the Source Link-Layer Address.

The Target Address List contains a list of IPv6 addresses of the interface identified by the Target Link-Layer Address.

The number of addresses "n" in the list is calculated based on the length of the option:

n = (Length - 1)/2 (Length is the number of groups of 8 octets)

The Source Address List MUST fit in one IND Solicitation message. Therefore in case all IPv6 addresses of an interface do not fit in one messages, the option does not contain a complete list. For a complete list of IPv6 addresses, a node should rely on the IND Advertisement message.

The Target Address List SHOULD be the complete list of addresses of the interface identified by the Target Link-Layer Address. If the list of IPv6 addresses of an interface does not fit in one IND Advertisement message, one or more IND Advertisement messages, with the same fields as the first message, SHOULD follow. The Target Address List option(s) of the second, and subsequent message(s) SHOULD contain the rest of the IPv6 addresses of the interface identified by the Target Link-Layer Address, which did not fit in the first message.

Note 1: The scope of the Inverse Neighbor Discovery mechanism is limited to IPv6 address discovery, that is, providing address mapping information. Therefore, it does not make any provisions or rules regarding how a node uses the addresses that were returned in an Inverse Discovery message. Furthermore, it does not exclude any particular type of IPv6 address from the Source or Target Address

List. For example, if an interface has manually configured, and autoconfigured addresses, including temporary ones, unicast, multicast, etc..., the list should not exclude any.

Note 2: An implementation MUST NOT send duplicates in the IPv6 address list.

4. Inverse Neighbor Discovery Protocol

IND operates essentially the same as ND [IPv6-ND]: the solicitor of a target IP address sends on an interface a solicitation message, the target node responds with an advertisement message containing the information requested. The information learned MAY be stored in the Neighbor Discovery cache [IPv6-ND], as well as IPv6 address structures which may be associated with the interface.

4.1 Sender Node Processing

A soliciting node formats an IND Solicitation message as defined in a previous section, encapsulates the packet for the specific link-layer and sends it directly to the target node. Although the destination IP address is the all-node multicast address, the message is sent only to the target node. The significant fields for the IND protocol are the Source IP address, the Source link-layer address, the Target link-layer address, and the MTU. The latter can be used in setting the optimum value of the MTU for the link.

While awaiting a response, the sender SHOULD retransmit IND Solicitation messages approximately every RetransTimer (expiration)[IPv6-ND], even in the absence of additional traffic to the neighbor. Retransmissions MUST be rate-limited to at most one solicitation per neighbor every RetransTimer.

If no IND Advertisement is received after MAX_MULTICAST_SOLICIT [IPv6-ND] solicitations, inverse address resolution has failed. If the sending of the Solicitation was required by an upper-layer, the sender module MUST notify the error to the upper-layer through an appropriate mechanism (e.g., return value from a procedure call).

4.2 Receiver Node Processing

4.2.1 Processing Inverse Neighbor Solicitation Messages

For every IND Solicitation, the receiving node SHOULD format in response a proper IND Advertisement using the link-layer source and target address pair as well as the IPv6 source address from the IND Solicitation message.

If a node updates the Neighbor Discovery Cache with information learned from IND messages, the receiver node of the IND Solicitation SHOULD put the sender’s IPv6 address/link-layer address mapping - i.e., the source IP address and the Source link-layer address from the solicitation message - into its ND cache [IPv6-ND] as it would for a ND solicitation.

Because IPv6 nodes may have multiple IPv6 addresses per interface, a node responding to an IND Solicitation SHOULD return in the Target Address List option a list containing one or more IPv6 addresses corresponding to the interface identified by the Target Link-Layer Address field in the solicitation message. The list MUST not contain duplicates.

4.2.2 Processing Inverse Neighbor Advertisement Messages

If a node updates The Neighbor Discovery Cache with information learned from IND messages, the receiver node of the IND advertisement SHOULD put the sender's IPv6 address/link-layer address mapping - i.e., the IP addresses from Target addresses list and the Source link-layer address from the IND advertisement message - into its ND cache [IPv6-ND] as it would for a ND advertisement.

4.3 Message Validation

Inverse Neighbor Discovery messages are validated as follows:

4.3.1 Validation of Inverse Neighbor Discovery Solicitations

A node MUST silently discard any received Inverse Neighbor Solicitation 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.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- The Target Link-Layer Address is a required option and MUST be present.
- The Source Link-Layer Address is a required option and MUST be present.
- All included options have a length that is greater than zero.

The content 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 Neighbor Discovery [IPv6-ND] options that are not specified to be used with Inverse Neighbor Discovery Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear besides the required options is the MTU option.

An Inverse Neighbor Solicitation that passes the validity checks is called a "valid solicitation".

4.3.2 Validation of Inverse Neighbor Discovery Advertisements

A node MUST silently discard any received Inverse Neighbor Discovery Advertisement 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.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 48 or more octets.
- Source Link-Layer Address option is present.
- Target Link-Layer Address option is present.
- The Target Address List option is present.
- The length of the Target Address List option is at least 3.
- All other included options have a length that is greater than zero.

The contents of the Reserved fields, and of any unrecognized options, MUST be ignored. Future, backward-compatible changes to the protocol may specify the contents of the Reserved fields or add new options; backward-incompatible changes may use different Code values.

The contents of any defined options [IPv6-ND] that are not specified to be used with Inverse Neighbor Advertisement messages MUST be ignored and the packet processed as normal. The only defined option that may appear besides the required options is the MTU option.

An Inverse Neighbor Advertisement that passes the validity checks is called a "valid advertisement".

5. Security Considerations

When being employed on point to point virtual circuits, as it is the case with Frame Relay networks, Inverse Neighbor Discovery messages are less sensitive to impersonation attacks from on-link nodes, as it would be the case with broadcast links.

Like Neighbor Discovery, the protocol reduces the exposure to threats from off-link nodes in the absence of authentication by ignoring IND packets received from off-link senders. The Hop Limit field of all received packets is verified to contain 255, the maximum legal value. Because routers decrement the Hop Limit on all packets they forward, received packets containing a Hop Limit of 255 must have originated from a neighbor.

Inverse Neighbor Discovery protocol packet exchanges can be authenticated using the IP Authentication Header [IPSEC-Auth]. A node SHOULD include an Authentication Header when sending Inverse Neighbor Discovery packets if a security association for use with the IP Authentication Header exists for the destination address. The security associations may have been created through manual configuration or through the operation of some key management protocol.

Received Authentication Headers in Inverse Neighbor Discovery packets MUST be verified for correctness and packets with incorrect authentication MUST be ignored.

In case of use with Frame Relay, to avoid an IP Security Authentication verification failure, the Frame Relay specific preprocessing of a Neighbor Discovery Solicitation message that contains a DLCI format Source link-layer address option, MUST be done by the receiver node after it completed IP Security processing.

It SHOULD be possible for the system administrator to configure a node to ignore any Inverse Neighbor Discovery messages that are not authenticated using either the Authentication Header or Encapsulating Security Payload. Such a switch SHOULD default to allowing unauthenticated messages.

Confidentiality issues are addressed by the IP Security Architecture and the IP Encapsulating Security Payload documents [IPSEC], [IPSEC-ESP].

6. IANA Considerations

IANA was requested to assign two new ICMPv6 type values, as described in Section 2.1 and 2.2. They were assigned from the Informational range of messages, as defined in Section 2.1 of RFC 2463. There were no ICMPv6 code values defined for these types (other than 0); future assignments are to be made under Standards Action as defined in RFC 2434.

IANA was also requested to assign two new ICMPv6 Neighbor Discovery Option types as defined in Section 3.1. No outside reviewing was necessary.

7. Acknowledgments

Thanks to Steve Deering, Thomas Narten and Erik Nordmark for discussing the idea of Inverse Neighbor Discovery. Thanks to Thomas Narten, and Erik Nordmark, and also to Dan Harrington, Milan Merhar, Barbara Fox, Martin Mueller, and Peter Tam for a thorough reviewing.

Also it should be acknowledged that parts of the text in this specification derived from the IPv6 Neighbor Discovery text [IPv6-ND].

8. References

[IPv6] Deering, S. and R. Hinden, "Internet Protocol Version 6 Specification", RFC 2460, December 1998.

[IPv6-ND] Narten, T., Nordmark, E. and W. Simpson "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[ICMPv6] Conta, A., and S. Deering "Internet Control Message Protocol for the Internet Protocol Version 6", RFC 2463, December 1998.

[IPv6-FR] Conta, A., Malis, A. and M. Mueller, "Transmission of IPv6 Packets over Frame Relay Networks", RFC 2590, May 1999. December 1997.

[IPSEC] Atkinson, R. and S. Kent, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[IPSEC-Auth] Atkinson, R. and S. Kent, "IP Authentication Header", RFC 2402, December 1998.

[IPSEC-ESP] Atkinson, R. and S. Kent, "IP Encapsulating Security Protocol (ESP)", RFC 2406, November 1998.

[ASSIGN] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, March 1994.

[ENCAPS] Brown, C. and A. Malis, "Multiprotocol Interconnect over Frame Relay", RFC 2427, November 1998.

[INV-ARP] Bradley, T., Brown, C. and A. Malis "Inverse Address Resolution Protocol", RFC 2390, August 1998.

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

9. Authors' Addresses

Alex Conta
Transwitch Corporation
3 Enterprise Drive
Shelton, CT 06484

Phone: +1-203-929-8810
EMail: aconta@txc.com

Appendix A

A. Inverse Neighbor Discovery with Frame Relay Networks

This appendix documents the details of using the Inverse Neighbor Discovery on Frame Relay Networks, which were too specific to be part of the more general content of the previous sections.

A.1 Introduction

The Inverse Neighbor Discovery (IND) specifically applies to Frame Relay nodes. Frame Relay permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) are identified in a Frame Relay network by a Data Link Connection Identifier (DLCI). Each DLCI defines for a Frame Relay node a single virtual connection through the wide area network (WAN). A DLCI has in general a local significance.

By way of specific signaling messages, a Frame Relay network may announce to a node a new virtual circuit with its corresponding DLCI. The DLCI identifies to a node a virtual circuit, and can be used as the equivalent of a remote node link-layer address, allowing a node to identify at link layer level the node at the other end of the virtual circuit. For instance in Figure 1., node A (local node) identifies the virtual circuit to node B (remote node) by way of DLCI = 30. However, the signaling message does not contain information about the DLCI used by a remote node to identify the virtual circuit to the local node, which could be used as the equivalent of the local link-layer address. For instance in Figure 1., node B (remote node) may identify the virtual circuit to node A by way of DLCI = 62.

Furthermore, the message being transmitted at link-layer level and completely independent of the IPv6 protocol does not include any IPv6 addressing information. The Inverse Neighbor Discovery is a protocol that allows a Frame Relay node to discover the equivalent of a local link layer address, that is, the identifier by way of which remote nodes identify the node, and more importantly discover the IPv6 addresses of the interface at the other end of the virtual circuit, identified by the remote link-layer address.

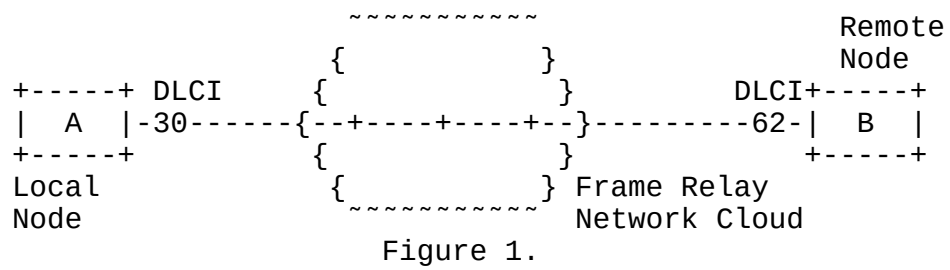


Figure 1.

The IPv6 Inverse Neighbor Discovery (IND) protocol allows a Frame Relay node to discover dynamically the DLCI by which a remote node identifies the virtual circuit. It also allows a node to learn the IPv6 addresses of a node at the remote end of a virtual circuit.

A.2. Inverse Neighbor Discovery Messages

Frame Relay nodes generate Inverse Neighbor Discovery messages as follows:

A.2.1. Inverse Neighbor Discovery Solicitation Message

The sender of an Inverse Neighbor Discovery Solicitation does not know the remote node's IPv6 addresses, but knows the equivalent of a remote node link-layer address. Inverse Neighbor Discovery (IND) Solicitations are sent as IPv6 all-node multicasts [IPv6], [IPv6-FR], [ENCAPS]. However, at link layer level, an IND Solicitation is sent directly to the target node, identified by the known link-layer address (DLCI).

The fields of the message, which are filled following considerations specific to Frame Relay are:

Source Link-Layer Address
: For the sender Frame Relay node, the Source Link-Layer Address is the equivalent of the link-layer address by which the remote node identifies the source of this message. The sender may have no knowledge of this information. If the sender knows the information, it SHOULD include it in the field, otherwise it SHOULD live it zero (empty). This information, if present, can be used for network debugging purposes. Regardless of the sender's action on this field, prior to any Inverse Neighbor Discovery processing, the receiver of this message replaces this field, whether filled in or not by the sender, with information carried by the Frame Relay header in the DLCI field. The field is encoded in DLCI format as defined by [IPv6-FR].

Target Link-Layer Address
For sender Frame Relay node, the Target Link-Layer Address field is filled with the value known as the equivalent of the target node link-layer address. This value is the DLCI of the VC to the target node. It is encoded in DLCI format [IPv6-FR].

To illustrate the generating of a IND Solicitation message by a Frame Relay node, let's consider as an example Node A (Figure 1.) which sends an IND solicitation to Node B. The Solicitation message fields will have the following values:

At Node A (sender of the IND solicitation message).

Source Link-Layer Address
DLCI=unknown (overwritten by the receiver).

Target Link-Layer Address
DLCI=30.

At Node B (receiver of the IND solicitation message).

Source Link-Layer Address
DLCI=62 (filled in by the receiver).

Target Link-Layer Address
DLCI=30.

Note: For Frame Relay, both the above addresses are in Q.922 format (DLCI), which can have 10 (default), or 23 significant addressing bits [IPv6-FR]. The option length (link-layer address) is expressed in 8 octet units, therefore, the DLCI will have to be extracted from the 8 bytes based on the EA field (bit 0) of the second, third, or forth octet (EA = 1). The C/R, FECN, BECN, DE fields in the Q.922 address have no significance for IND and are set to 0 [IPv6-FR].

MTU
The value filled in the MTU option is the MTU for the virtual circuit identified by the known DLCI [IPv6-FR].

A.2.2 Inverse Neighbor Discovery Advertisement Message

A Frame Relay node sends Inverse Neighbor Discovery Advertisements in response to Inverse Neighbor Discovery Solicitations.

The fields of the message, which are filled following considerations specific to Frame Relay are:

Source Link-Layer Address
For Frame Relay, this field is copied from the Target link-layer address field of the Inverse Neighbor Discovery Solicitation. It is encoded in DLCI format [IPv6-FR].

Target Link-Layer Address
For Frame Relay, this field is copied from the Source link-layer address field of the Inverse Neighbor Discovery Solicitation. It is encoded in DLCI format [IPv6-FR].

For example if Node B (Figure 1.) responds to an IND solicitation sent by Node A. with an IND advertisement, these fields will have the following values:

At Node B (sender of the advertisement message):

Source Link-Layer Address
DLCI=30 (was Target in Solicitation Message).

Target Link-Layer Address
DLCI=62 (was Source in Solicitation Message).

At Node A (receiver of the advertisement message from B).

Source Link-Layer Address
DLCI=30 (was Target in Solicitation Message).

Target Link-Layer Address
DLCI=62 (was Source in Solicitation Message).

Target Address List
The list of one or more IPv6 addresses of the interface identified by the Target Link-Layer Address in the Inverse Neighbor Discovery Solicitation message that prompted this advertisement.

MTU The MTU configured for this link (virtual circuit) [IPv6-ND].

Note: In case of Frame Relay networks, the IND messages are sent on a virtual circuit, which acts like a virtual-link. If the virtual circuit breaks, all participants to the circuit receive appropriate link layer signaling messages, which can be propagated to the upper layers, including IPv6.

A.3. Inverse Neighbor Discovery Protocol

This section of the appendix documents only the specific aspects of Inverse Neighbor Discovery with Frame Relay Networks.

A.3.1 Sender Node Processing

A soliciting Frame Relay node formats an IND solicitation message as defined in a previous section, encapsulates the packet for the Frame Relay link-layer [IPv6-FR] and sends it to the target Frame Relay node. Although the destination IP address is the IPv6 all-node multicast address, the message is sent only to the target Frame Relay node. The target node is the known remote node on the link represented by the virtual circuit.

A.3.2 Receiver Node Processing

A.3.2.1 Processing Inverse Neighbor Solicitation Messages

A Frame Relay node, before further processing, is replacing in the Source link-layer address the existent DLCI value with the DLCI value from the Frame Relay header of the frame containing the message. The DLCI value has to be formatted appropriately in the Source link-layer address field [IPv6-FR]. This operation is required to allow a correct interpretation of the fields in the further processing of the IND solicitation message.

For a Frame Relay node, the MTU value from the solicitation message MAY be used to set the receiver's MTU to a value that is more optimal, in case that was not already done at the interface configuration time.

A.3.2.2 Processing Inverse Neighbor Advertisement Messages

The receiver Frame Relay node of the IND Advertisement MAY put the sender's IPv6 address/link-layer address mapping - i.e., the Target IP addresses and the Source link-layer address from the IND advertisement message - into its ND cache [IPv6-ND] as it would for a ND Advertisement.

Further, the receiver Frame Relay node of the IND Advertisement MAY store the Target link-layer address from the message as the DLCI value at the remote end of the VC. This DLCI value is the equivalent of the link-layer address by which the remote node identifies the receiver.

If the receiver node of the IND Advertisement has a pool of IPv6 addresses, and if the implementation allows, it may take decisions to pairing specific local IPv6 addresses to specific IPv6 addresses from the target list in further communications on the VC. More specifically, such a pairing may be based on IPv6 addresses being on the same subnet, that is having the same prefix.

Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.