Network Working Group
Internet-Draft
Expires: January 19, 2006

G. Daley
Monash University CTIE
E. Nordmark
Sun Microsystems
N. Moore
Monash University CTIE

July 18, 2005

Tentative Source Link-Layer Address Options for IPv6 Neighbour Discovery

draft-daley-ipv6-tsllao-02.txt

Status of this Memo

Copyright Notice

Abstract

The proposed IPv6 Duplicate Address Detection (DAD) Optimization "Optimistic DAD" defines a set of recoverable procedures which allow a node to make use of an address before DAD completes. Essentially, Optimistic DAD forbids usage of certain Neighbour Discovery options which could pollute active neighbour cache entries, while an address is tentative.

This document defines a new option and procedures to replace cache polluting options, in a way which is useful to tentative nodes. These procedures are designed to be to backward compatible with existing devices which support IPv6 Neighbour Discovery.

Table of Contents

1. Introduction

Source Link-Layer Address Options (SLLAOs) are sent in Neighbour discovery messages in order to notify neighbours of a mapping between a specific IPv6 Network layer address and a link-layer (or MAC) address. Upon reception of a neighbour discovery message containing such an option, nodes update their neighbour cache entries with the IP to link-layer address mapping in accordance with procedures defined in IPv6 Neighbour Discovery [2].

Optimistic DAD [4] prevents usage of these options in Router and Neighbour Solicitation messages from a tentative address (while Duplicate Address Detection is occurring). This is because receiving a Neighbour Solicitation (NS) or Router Solicitation (RS) containing an SLLAO would otherwise overwrite an existing cache entry, even if the cache entry contained the legitimate address owner, and the solicitor was a duplicate address.

Neighbour Advertisement (NA) messages don't have such an issue, since the Advertisement message contains a flag which explicitly disallows overriding of existing cache entries, by the target link-layer address option carried within.

The effect of preventing SLLAOs for tentative addresses is that communications with these addresses are sub-optimal for the tentative period. Sending solicitations without these options causes an additional round-trip for neighbour discovery if the advertiser does not have an existing neighbour cache entry for the solicitor. In some cases, multicast advertisements will be scheduled, where neighbour discovery is not possible on the advertiser.

Tentative Source Link-Layer Address Options are designed to replace the existing Source Link-Layer Address Options available in IPv6 Neighbour Discovery, when a device is performing Optimistic DAD.

1.1 Tentative Source Link-Layer Address Option Format

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 5 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     |    Link-Layer Address ...
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
   Fields:
     Type   TBD    (Requires IANA Allocation) suggest 33 (0x21)

     Length         The length of the option (including the type and
                    length fields) in units of 8 octets.

     Link-Layer Address
                    The variable length link-layer address.

     Description
                    The Tentative Source Link-Layer Address option
                    contains the link-layer address of the sender of
                    the packet.  It is used in the Neighbour
                    Solicitation and Router Solicitation packets.
```

1.2 Tentative Source Link-Layer Address Option Semantics

The Tentative Source Link-Layer Address option (TSLLAO) functions in the same role as the Source Link-Layer Address option defined for [2], but it MUST NOT override an existing neighbour cache entry.

The differing neighbour cache entry MUST NOT be affected by the reception of the Tentative Source Link-Layer Address option. This ensures that tentative addresses are unable to modify legitimate neighbour cache entries.

In the case where an entry is unable to be added to the neighbour cache, a node MAY send responses direct to the link-layer address specified in the TSLLAO.

For these messages, no Neighbour Cache entry may be created, although response messages may be directed to a particular unicast address.

These procedures are discussed further in Section 3.3.

2. Sending Solicitations containing TSLLAO

Tentative Source Link-Layer Address Options may be sent in Router and Neighbour Solicitations, as described below.

In a case where it is safe to send a Source Link-Layer Address

Option, a host SHOULD NOT send a TSLLAO, since the message may be misinterpreted by legacy nodes.

Importantly, a node MUST NOT send a TSLLAO in the same message where a Source Link-Layer Address Option is sent.

2.1 Sending Neighbour Solicitations with TSLLAO

Neighbour Solicitations sent to unicast addresses MAY contain a TSLLAO.

Since delivery of a packet to a unicast destination requires prior knowledge of the destination's hardware address, unicast Neighbour Solicitation packets may only be sent to destinations for which a neighbour cache entry already exists.

For example, if checking bidirectional reachability to a router, it may be possible to send a Neighbour Solicitation with TSLLAO to the router's advertised address.

As discussed in [2], the peer device may not have a cache entry even if the soliciting host does, in which case reception of TSLLAO may create a neighbour cache entry, without the need for neighbour discovering the original solicitor.

2.2 Sending Router Solicitations with TSLLAO

Any Router Solicitation from a Preferred, Deprecated or Optimistic address MAY be sent with a TSLLAO [4].

An extension which allows Router Solicitations to be sent with a TSLLAO from the unspecified address is described in Appendix C.

3. Receiving Tentative Source Link-Layer Address Options

Receiving a Tentative Source Link-Layer Address Option allows nodes to unicast responses to solicitations without performing neighbour discovery.

It does this by allowing the solicitation to create STALE neighbour cache entries if one doesn't exist, but only update an entry if the link-layer address in the option matches the entry.

Additionally, TSLLAO messages may be used to direct advertisements to particular link-layer destinations without updating neighbour cache entries. This is described in Appendix C.

3.1 Handling Tentative Source Link-Layer Address Options

Use of Tentative Source Link-Layer Address Options is only defined for Neighbour and Router Solicitation messages.

In any other received message, the presence of the option is silently ignored, that is, the packet is processed as if the option was not present.

It is REQUIRED that the same validation algorithms for Neighbour and Router Solicitations received with TSLLAO as in the IPv6 Neighbour Discovery specification [2], are used.

In the case that a solicitation containing a TSLLAO is received, The only processing differences occur in checking and updating the neighbour cache entry. Particularly, there is no reason to believe that the host will remain tentative after receiving a responding advertisement.

As defined in Section 1.1, Tentative Source Link-Layer Address Options do not overwrite existing neighbour cache entries where the link-layer addresses of the option and entry differ.

If a solicitation from a unicast source address is received where no difference exists between the TSLLAO and an existing neighbour cache entry, the option MUST be treated as if it were an SLLAO after message validation, and processed accordingly.

In the case that a cache entry is unable to be created or updated due to existence of a conflicting neighbour cache entry, it MUST NOT update the neighbour cache entry.

An extension which allows a direct advertisement to the soliciting host without modifying the neighbour cache entry is described in Appendix C.

3.2 Receiving Neighbour Solicitations containing TSLLAO

The TSLLAO option is only allowed in Neighbour Solicitations with specified source addresses for which SLLAO is not required.

A Neighbour Solicitation message received with TSLLAO and an unspecified source address MUST be silently discarded.

Upon reception of a Tentative Source Link-Layer Address Option in a Neighbour Solicitation for which the receiver has the Target Address configured, a node checks to see if there is a neighbour cache entry with conflicting link-layer address.

If no such entry exists, the neighbour cache of the receiver SHOULD be updated, as if the Tentative Source Link-Layer Address Option was a SLLAO.

Sending of the solicited Neighbour Advertisement then proceeds normally, as defined in section 7.2.4 of [2].

If there is a conflicting neighbour cache entry, the node processes the solicitation as defined in Section 7.2.4 of [2], except that the Neighbour Cache entry MUST NOT be modified.

3.3 Receiving a Router Solicitation containing TSLLAO

In IPv6 Neighbour Discovery [2], responses to Router Solicitations are either sent to the all-nodes multicast address, or may be sent to the solicitation's source address if it is a unicast address.

Including a TSLLAO in the solicitation allows a router to choose to send a packet directly to the link-layer address even in situations where this would not normally be possible.

For Router Solicitations with unicast source addresses, neighbour caches SHOULD be updated with the link-layer address from a TSLLAO if there is no differing neighbour cache entry. In this case, Router Advertisement continues as in Section 6.2.6 of [2].

For received solicitations with a differing link-layer address to that stored in the neighbour cache, the node processes the solicitation as defined in Section 6.2.6 of [2], except that the Neighbour Cache entry MUST NOT be modified.

4. IANA Considerations

For standardization, it would be required that the IANA provide allocation of the Tentative Source Link-Layer Address Option (Section 1.1) from the IPv6 Neighbour Discovery options for IPv6.

Current experimental implementations have used the value 0x11 (17) for the Tentative Source Link-Layer Address Option.

Potential details of the allocation process for these options is detailed in the expired draft [5].

5. Security Considerations

The use of the TSLLAO in Neighbour and Router Solicitation messages acts in a similar manner to SLLAO, updating neighbour cache entries, in a way which causes packet transmission.

Particular care should be taken that transmission of messages complies with existing IPv6 Neighbour Discovery Procedures, so that unmodified hosts do not receive invalid messages.

An attacker may cause messages may be sent to another node by an advertising node (a reflector), without creating any ongoing state on the reflector.

This is attack requires one solicitation for each advertisement and the advertisement has to go to a unicast MAC destination. That said, the size of the advertisement may be significantly larger than the solicitation, or the attacker and reflector may be on a medium with greater available bandwidth than the victim.

For link-layers where it isn't possible to spoof the link-layer source address this allows a slightly increased risk of reflection attacks from nodes which are on-link.

Additionally, since a SEND host must always advertise using SEND options and signatures, a non-SEND attacker may cause excess computation on both a victim node and a router by causing SEND advertisement messages to be transmitted to a particular MAC address and the all-nodes multicast. [3] specifies guidelines to hosts receiving unsolicited advertisements in order to mitigate such attacks.

While this is the same effect as experienced when accepting SLLAO from non-SEND nodes, the lack of created neighbour cache entries on the advertiser may make such attacks more difficult to trace.

Modification of Neighbour Discovery messages on the network is possible, unless SEND is used. [3] provides a protocol specification in which soliciting nodes sign ND messages with a private key and use addresses generated from this key.

Even if SEND is used, the lifetime of a neighbour cache entry may be extended by continually replaying a solicitation message to a particular router or hosts. Since this may be achieved for any Neighbour or Router Solicitation message, corresponding advertisements to the original transmitters of these solicitation messages may occur.

SEND defines use of Timestamp values to protect a device from attack through replay of previously sent messages. Although this applies to Neighbour and Router Solicitation messages, granularity of the timestamp allows the messages to be used for up to five minutes [3].

All Router and Neighbour Solicitations using SEND contain a Nonce

option, containing a random identifier octet string. Since SEND messages are digitally signed, and may not be easily modified, replay attacks will contain the same Nonce option, as was used in the original solicitation.

While the Nonce Option included in a transmission to another node may not vary within one short solicitation period (the host may itself replay solicitations in the case of packet loss), the presence of the timestamp option ensures that for later solicitations, a different Timestamp and Nonce will be used.

Therefore, a receiver seeing a solicitation with the same Timestamp and Nonce (and signature) for more than either of MAX_RTR_SOLICITATIONS (for Router Solicitations), MAX_UNICAST_SOLICIT or MAX_MULTICAST_SOLICIT (for Neighbour Solicitations), SHOULD ignore further solicitations with this (Nonce,Timestamp,Source) triple, ensuring that no modification is made to neighbour cache entries. This applies to any solicitation packet capable of carrying a SEND payload, whether they use TSLLAO or SLLAO.

Stations noticing such an attack SHOULD notify their administrator of the attempt at Denial-of-service.

6. Acknowledgments

Erik Nordmark coined a proposal for TSLLAO during a conversation with JinHyeock Choi and Greg Daley.

7. References

7.1 Normative References

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

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

[3] Arkko, J., Kempf, J., Sommerfeld, B., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ndopt-06 (work in progress), July 2004.

[4] Moore, N., "Optimistic Duplicate Address Detection for IPv6", draft-ietf-ipv6-optimistic-dad-03 (work in progress), January 2005.

7.2 Informative References

[5] Narten, T., "IANA Allocation Guidelines for Values in IPv6 and Related Headers", draft-narten-ipv6-iana-considerations-00 (work in progress), October 2002.

[6] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

Authors' Addresses

Greg Daley
Centre for Telecommunications and Information Engineering
Department of Electrical and Computer Systems Engineering
Monash University
Clayton, Victoria 3800
Australia

Phone: +61 3 9905 4655
Email: greg.daley@eng.monash.edu.au

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Mountain View, CA
USA

Phone: +1 650 786 2921
Email: erik.nordmark@sun.com

Nick "Sharkey" Moore
Centre for Telecommunications and Information Engineering
Department of Electrical and Computer Systems Engineering
Monash University
Clayton, Victoria 3800
Australia

Email: nick.moore@eng.monash.edu.au

Appendix A. Constraints imposed by IPv6 Neighbour Discovery

Hosts which send and receive Tentative Source Link Layer Address Options may be interacting with legacy nodes which support IPv6 Neighbour Discovery procedures, but do not understand the new option.

For these nodes, the presence of the option is silently ignored, that is, the packet is processed as if the option was not present. Therefore all messages sent with TSLLAO options MUST be compliant with the existing requirements for options and addressing specified in the IPv6 Neighbour Discovery RFC [2].

A.1 Constraints on Neighbour Solicitations

As described in Section 7.2.2 of [2], packets sent to solicited nodes' multicast addresses MUST contain Source Link-Layer Address options.

> Neighbour solicitations to multicast addresses MUST NOT contain TSLLAO

Neighbour Solicitations to unicast addresses SHOULD include a link-layer address (if the sender has one has one) as a Source Link-Layer Address option.

> Unicast neighbour solicitations without Source Link-Layer Address Options MAY contain TSLLAO, if the solicitor has a Link-Layer address.

A.2 Constraints on Router Solicitations

As described in Section 6.3.7 of [2], Router Solicitations SHOULD contain Source Link-Layer Address Options.

> Router Solicitations without Source Link-Layer Address options MAY contain a TSLLAO.

Appendix B. Interactions with legacy nodes

Devices which do not implement Tentative Source Link Layer address options will act as if no option was placed within the Neighbour Discovery message. The following sections summarize how legacy hosts will interact with messages containing TSLLAO.

Appendix B.1 Legacy Neighbour Solicitation processing

A node can include the TSLLAO option in a unicast NS (and no SLLAO option) when the transmitter's address is either tentative or optimistic.

> An RFC 2461 host receiving such a packet will "see" a packet without an SLLAO option, which is allowed in RFC2461.

If the recipient host has an existing neighbour cache entry for the transmitter, it can then send a Neighbour Advertisement.

Where no neighbour cache entry exists, the recipient will send a multicast NS (containing its own SLLAO) in order for the original transmitter to respond with an NA. Upon reception of the original transmitter's NA, an NA is sent back to the origin.

The TSLLAO option MUST NOT be included in an NS message which has no source address.

An RFC 2461 host sees an NS without a source address as a Duplicate Address Detection message.

Reception of duplicate address detection messages may cause side-effects on other hosts, which may cause them to treat addresses as invalid.

Appendix B.2 Legacy Router Solicitation Processing

A node can include the TSLLAO option in an RS with a unicast source address (and no SLLAO option) when the transmitter's address is either tentative or optimistic.

An RFC 2461 router receiving such a packet will "see" a packet without an SLLAO option, which is allowed in RFC2461.

If the router has an existing neighbour cache entry for this host, it may send a Unicast RA in response, but may send a multicast in preference.

If no neighbour cache entry exists, some routers will not be able to provide a unicast response. These routers will schedule a multicast response.

Other routers may attempt to perform neighbour discovery (by sending a multicast NS), and unicast a response when a neighbour cache entry has been created.

A node can include the TSLLAO option in an RS with an unspecified source address (and no SLLAO option) when the transmitter's address is tentative. This is described in Appendix C.

RFC 2461 routers receiving this solicitation will "see" a message without a SLLAO (such options are not allowed in RFC2461).

These routers will schedule a multicast RA response.

Appendix C. Sending Directed Advertisements without the Neighbour Cache

In the case where an entry is unable to be added to the neighbour cache, a node MAY send responses direct to the link-layer address specified in the TSLLAO. Also, RS packets sent without a specificed source address may potentially contain a TSLLAO.

In this case the unicast link-layer address from the solicitation MAY be extracted from the TSLLAO option and used as the destination of the link-layer frame for a responding Router Advertisment.

Sending such a packet MUST NOT consult the neighbour or destination caches for address.

Such packets SHOULD scheduled as if they were unicast advertisements as specified in [2].

If an implementation can not send a Router Advertisement using information from the TSLLAO i.e, without consulting the neighbour cache, then it SHOULD behave as if the TSLLAO option was not present in the solicitation message.

Intellectual Property Statement

Disclaimer of Validity

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 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.

Copyright Statement

Acknowledgment

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