Network Working Group
Internet-Draft
Expires: September 29, 2005

G. Daley
Monash University CTIE
March 31, 2005

Nonce response matching for router reachability in IPv6
draft-daley-dna-nonce-resp-01.txt

Status of this Memo

Copyright Notice

Abstract

IPv6 Neighbour Discovery does not provide a mechanism which allows a node to match its router solicitations to advertised responses.

The Nonce Neighbour Discovery Option was originally defined for Secured Neighbour Discovery. This draft describes the use of the Nonce Option for generic router reachability testing.

Table of Contents

1. Introduction

Secured Neighbour Discovery (SEND) defines an extension to IPv6 Neighbour Discovery which supports signed message exchanges between neighbours, in order to secure neighbour cache construction [2][3].

In SEND, nodes must copy a Nonce Option from a solicitation into a responding advertisement, in order to identify that an advertisement is fresh and generated due to a particular solicitation.

This property of unambiguous router response detection is useful when detecting network reachability changes, and may be used as part of a configuration change detection scheme, even for non-SEND hosts and routers.

2. Necessity of nonces

Responses to Router Solicitations are often multicast (section 6.2.6 of [2]). Although procedures for responding to solicitations require transmission of all configuration options in solicited Router Advertisements, In many cases the contents of Router Advertisements will not substantially change between solicited and unsolicited messages.

Therefore it is impossible for a host to determine between a solicited and an unsolicited RA.

Even if a host can tell between multicast solicited and unsolicited router advertisements, it may not know which host solicited it, if multiple nodes exist on the same link. For example, a host may believe that its own router solicitation was received and processed to create the RA, even if its solicitation was lost. Therefore some form of response matching is valuable.

It is possible for a router to identify either the origin of the solicitation by its address, or to match a chosen random number from the solicitation. While each approach is viable, both have have drawbacks. Address based matches require addresses to already be configured on the solicitor, whereas random number matching schemes have the potential for solicitation identifier collision if the matching space is too small.

SEND nonces are an existing non-address dependent response matching mechanism which allow a host to ask that a router if their solicitation was seen. They provide a large enough identifier space to ensure very low numbers of identifier collisions, and may be used even without completed address configuration on solicitors.

3. SEND response matching

Existing SEND nodes will send Nonce Options in response to options received in solicitations. A nonce received in a signed SEND message is therefore a response to a solicitation, if the nonce contained in the option matches.

This occurs regardless of whether the response is unicast or multicast, a Neighbour Advertisement or a Router Advertisement.

4. Sending Nonce Options for router response

In order to provide response matching for hosts performing router discovery, hosts MAY send Nonce Options containing a random number as described in [3] section 5.3.2 and 5.3.3, even if it has not been configured to use SEND.

When receiving a Nonce Option in an RS message which causes an advertisement, a router SHOULD copy the nonce into the response RA in order to provide response matching for solicitors.

Upon reception of a Nonce Option with a random number matching that which was transmitted, a host knows that the router received the message, and that bidirectional packet flow was successful.

When processing a SEND host's solicitation, a router can send a Nonce Option in responding Router Advertisements, even if it cannot sign the message, or prove its right to be a router. This will not affect the security of the message, still resulting in an unsecured neighbour cache entry, but provides analogous router reachability proofs to SEND in the absence of a SEND capable router.

When a SEND router processes a Nonce Option in an unsecured RS, it SHOULD include the Nonce Option into a secured Router Advertisement if it responds to the solicitation.

If the length of the received Nonce Option in this case is more than 16 Octets, the router MUST NOT transmit the responding nonce. In most cases, the additional load of transmitting 16 extra solicited octets and performing a hash over these values is unlikely to be problematic. In order to protect SEND resources though, priority MAY be given to computation of responses to soliciting SEND nodes.

5. Router responses to unicast destinations

In most cases, it is possible to identify that a Router Advertisement is solicited if received at a unicast address, since unicast Router Advertisements are typically only sent in response to solicitation.

It may not be possible to identify if the received Router Advertisement is a fresh one though. In order to provide a weak liveness proof, it is valuable to include received nonces in Router Advertisements. This doesn't prove message authenticity, origin or authorization, although it requires a live responder.

Since the router has a choice to respond either unicast or multicast, where the solicitor's source address is specified in the Router Solicitation, a host does not know if it is going to receive a unicast response. In this case, a host SHOULD send a Nonce Option in its solicitation anyway.

In order to prove the freshness of its response, a router SHOULD include a received Nonce Option into a Router Advertisement, even if it is unicast.

6. Nonces and unspecified source addresses

Except for on Duplicate Address Detection (DAD) Neighbour Solicitations (NSs), SEND is not used where the source IPv6 address of a message is unspecified [4][3]. Responses to router solicitations from unspecified source addresses are therefore not typically covered by SEND nonces.

Since any RA response to an unspecified address is multicast, this is exactly where Nonce Options would be useful. In detection of network attachment, it is important not to harm any existing hosts when detecting connection to a new network. In performing router discovery it is therefore possible that hosts will treat existing addresses as unconfirmed, and transmit solicitations from unspecified addresses.

Nonce Options in packets transmitted from unspecified source addresses allow response matching for hosts which solicit on a particular link, even though they do not yet have any non-tentative addresses.

Hosts SHOULD send Nonce Options in Router Solicitations from the unspecified address, even though these cannot be protected using SEND.

Routers SHOULD respond to Nonce Options from the unspecified address, this aids in response matching from tentatively addressed hosts.

7. Duplicate MAC Frames

In wireless environments with MAC layer acknowledgments, it is possible that ACKs at the MAC layer are not received for packets,

causing successful transmission of the same frame multiple times.

Where this occurs for Router Solicitations, it is possible that a host can cause multiple Router Advertisements to be sent based on a single solicitation being enqueued at the transmitter.

In order to ensure that a particular solicitation packet is not already responded to, a router MAY keep a small cache of received nonces (or nonces and public keys for SEND routers), to ensure that responses aren't transmitted multiple times for the same solicitation.

This cache SHOULD time out quickly (possibly dependent on the MAC) in order to ensure that the number of Nonce collisions (where nodes each choose the same nonce) is small.

8. Deferred responses

In section 6.2.6 of the IPv6 Neighbour Discovery RFC [2], cancellation of a Router Advertisement responding to solicitation is described, considering that the next scheduled Router Advertisement is sufficiently close.

Where a router decides to defer responding to the next scheduled multicast RA, it MAY include the solicitor's Nonce Option into the scheduled advertisement.

9. Multiple nonce response

Particularly where multiple solicitations have been deferred due to close scheduling of a multicast RA, a router MAY include more than one Nonce Option into a multicast Router Advertisement.

This allows the router to indicate reception of multiple Router Solicitations with only one Router Advertisement.

In order to prevent resource depletion attacks, routers SHOULD ensure that only limited resources are used for storage of Nonce Options. In order to limit resource utilization, and prevent unfair nonce buffer utilization, Nonce Options of greater than 16 octets SHOULD NOT be stored in this manner and cannot be deferred for multiple nonce response. This may mean that no nonce response is given for large nonces, if resources are otherwise unavailable.

10. Interaction with legacy routers

Legacy routers which do not recognise Nonce Options will not provide responding nonces when router advertising.

A host SHOULD not assume that a router is sending an unsolicited Router Advertisement if a received multicast advertisement contains no Nonce Options and the solicitor has never seen a nonce from that router before.

In this case, legacy procedures (i.e. guesswork) or ND probing may be required to confirm reachability with a router.

11. IPR Considerations

This document defines a use for nonces in Detecting Network Attachment. IBM holds a patent describing use of Nonces in authentication protocols (5,148,479). In the patent, nonces are used as a mechanism to protect against replay of messages. This patent has been cited on many occasions within the IETF's documents and standardization process.

The use of nonces described by this draft is considered by the author not intentionally or usefully applied to replay protection, rather it is applicable only to response matching. Therefore, the author believes that this patent is not applicable to the document here described.

12. IANA Considerations

This document defines another use case for an existing allocated IPv6 Neighbour Discovery Option.

No IANA action is needed.

13. Security Considerations

It is important to consider that Nonce Options were designed for security purposes within a framework which supplied robust message authenticity and authorization.

Using these nonces in unsecured messages will not provide any additional security over messages without nonces.

Additional procedures defining interactions between SEND and non-SEND nodes are outlined above. Since SEND was not designed to interact with non-SEND nodes using its option formats, there is a possibility that SEND nodes may interpret Nonce Option presence in non-SEND RS or RA incorrectly.

As there are no known field deployments of SEND today, the effect of this issue is unknown at this time.

Inclusion of additional text into a SEND message may cause additional computation on a router, at limited computational cost to the soliciting hosts. SEND routers MAY make use of deferred transmissions and multiple nonce responses to mitigate this effect, potentially reducing the number of signatures to be performed, as well as the number of packet and bit transmissions.

As mentioned above, it may be possible to separate the responses to nonces from secured and unsecured devices. Responses to secured devices MAY be given priority in order to prevent resource starvation for SEND Routers.

The addition of generic text (a reflected Nonce Option) for inclusion into SEND Router Advertisement messages lowers the cost, and potentially widens the scope for chosen-plaintext attacks on SEND routers. Currently this is limited due to an SHA-1 hash over the SEND message contents. Nevertheless, SEND Routers SHOULD monitor their secured and unsecured nonce reception, and SHOULD log unusually high levels of nonce activity to the administrator.

14. Acknowledgments

15. References

15.1 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.

15.2 Informative References

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

Author's Address

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

Appendix A. Implementation status

A simple implementation of this operation without SEND is under development for RADVD.

Currently multiple nonce responses in a single RA are not supported.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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