Internet Engineering Task Force (IETF)
Request for Comments: 5909
Category: Informational
ISSN: 2070-1721

J-M. Combes
France Telecom Orange
S. Krishnan
Ericsson
G. Daley
Netstar Logicalis

July 2010

Securing Neighbor Discovery Proxy: Problem Statement

Abstract

Neighbor Discovery Proxies are used to provide an address presence on a link for nodes that are no longer present on the link. They allow a node to receive packets directed at its address by allowing another device to perform Neighbor Discovery operations on its behalf.

Neighbor Discovery Proxy is used in Mobile IPv6 and related protocols to provide reachability from nodes on the home network when a Mobile Node is not at home, by allowing the Home Agent to act as proxy. It is also used as a mechanism to allow a global prefix to span multiple links, where proxies act as relays for Neighbor Discovery messages.

Neighbor Discovery Proxy currently cannot be secured using Secure Neighbor Discovery (SEND). Today, SEND assumes that a node advertising an address is the address owner and in possession of appropriate public and private keys for that node. This document describes how existing practice for proxy Neighbor Discovery relates to SEND.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5909.

Table of Contents

1. Introduction

Neighbor Discovery Proxy is defined in IPv6 Neighbor Discovery [RFC4861]. It is used in networks where a prefix has to span multiple links [RFC4389] but also in Mobile IPv6 [RFC3775] (and so in Mobile-IPv6-based protocols like Network Mobility (NEMO) [RFC3963], Fast Handovers for Mobile IPv6 (FMIPv6) [RFC5568], or Hierarchical Mobile IPv6 (HMIPv6) [RFC5380]) and in the Internet Key Exchange Protocol (IKE) version 2 (IKEv2) [RFC4306]. It allows a device that is not physically present on a link to have another advertise its presence, and forward packets to the off-link device.

Neighbor Discovery Proxy relies upon another device, the proxy, to monitor for Neighbor Solicitations (NSs), and answer with Neighbor Advertisements (NAs). These proxy Neighbor Advertisements direct data traffic through the proxy. Proxied traffic is then forwarded to the end destination.

2. Scenarios

This section describes the different scenarios where the interaction between Secure Neighbor Discovery (SEND) and ND Proxy raises issues.

2.1. IPv6 Mobile Nodes and Neighbor Discovery Proxy

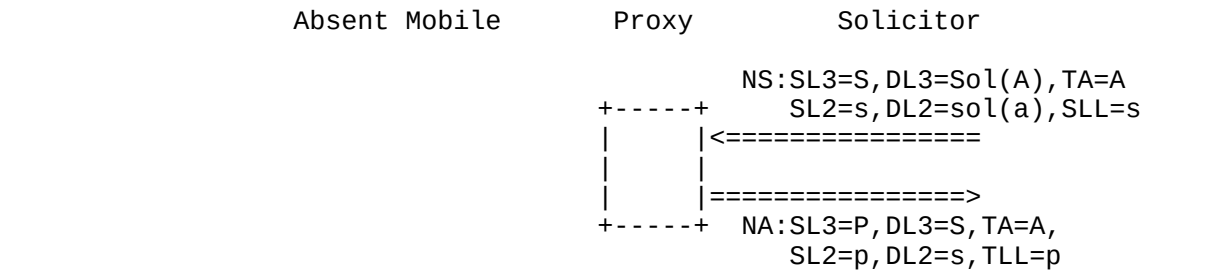
The goal of IPv6 mobility is to allow nodes to remain reachable while moving around in the IPv6 Internet. The following text is focused on Mobile IPv6 but the issue raised by the interaction between SEND and ND Proxy may be the same with Mobile IPv6 based protocols (e.g., NEMO, HMIPv6).

For Mobile IPv6 Mobile Nodes (MNs), it is necessary to keep existing sessions going or to allow new sessions even when one leaves the home network.

In order to continue existing sessions, when nodes are present on the home link, the Proxy (i.e., the Home Agent in Mobile IPv6) sends an unsolicited NA to the all-nodes multicast address on the home link as specified [RFC3775].

For new sessions, the Proxy, which listens to the MN’s address responds with a Neighbor Advertisement that originates at its own IPv6 address and has the proxy’s address as the Target Link-Layer Address, but contains the absent mobile in the Target Address field of the Neighbor Advertisement. In this case, SEND cannot be applied because the address in the Target Address field is not the same as the one in the Source Address field of the IP header.

As seen in Figure 1, solicitors send a multicast solicitation to the solicited nodes multicast address (based on the unicast address) of the absent node (a mobile node that is away from the home link).



Legend:

SL3: Source IPv6 Address	NS: Neighbor Solicitation
DL3: Destination IPv6 Address	NA: Neighbor Advertisement
SL2: Source Link-Layer Address	RS: Router Solicitation
DL2: Destination Link-Layer Address	RA: Router Advertisement
TA: Target Address	
SLL/TLL: Source/Target Link-Layer Address Option	

Figure 1

While at home, if the MN has configured Cryptographically Generated Addresses (CGAs) [RFC3972], it can secure establishment by its on-link neighbors of Neighbor Cache Entries (NCEs) for its CGAs by using SEND [RFC3971]. SEND security requires a node sending Neighbor Advertisements for a given address to be in possession of the public/private key pair that generated the address.

When an MN moves away from the home link, a proxy has to undertake Neighbor Discovery signaling on behalf of the MN. In Mobile IPv6, the role of the proxy is undertaken by the Home Agent. While the Home Agent has a security association with the MN, it does not have access to the public/private key pair used to generate the MN’s CGA. Thus, the Home Agent acting as an ND proxy cannot use SEND for the address it is proxying [RFC3971].

When an MN moves from the home network to a visited network, the proxy will have to override the MN’s existing Neighbor Cache Entries that are flagged as secure [RFC3971]. This is needed for the Home Agent to intercept traffic sent on-link to the MN that would otherwise be sent to the MN’s link-layer address.

With the current SEND specification, any solicitation or advertisement sent by the proxy will be unsecure and thus will not be able to update the MN’s NCE for the home address because it is flagged as secured. These existing Neighbor Cache Entries will only time-out after Neighbor Unreachability Detection [RFC4861] concludes the Home Address is unreachable at the link layer recorded in the NCE.

Where secured proxy services are not able to be provided, a proxy's advertisement may be overridden by a rogue proxy without the receiving host realizing that an attack has occurred. This is identical to what happens in a network where SEND is not deployed.

2.2. IPv6 Fixed Nodes and Neighbor Discovery Proxy

This scenario is a sub-case of the previous one. In this scenario, the IPv6 node will never be on the link where the ND messages are proxied. For example, an IPv6 node gains remote access to a network protected by a security gateway that runs IKEv2 [RFC4306]. When a node needs an IP address in the network protected by a security gateway, the security gateway assigns an address dynamically using Configuration Payload during IKEv2 exchanges. The security gateway then needs to receive packets sent to this address; one way to do so would be to proxy ND messages.

2.3. Bridge-Like ND Proxies

The Neighbor Discovery (ND) Proxy specification [RFC4389] defines an alternative method to classic bridging. Just as with classic bridging, multiple link-layer segments are bridged into a single segment, but with the help of proxying at the IP layer rather than link-layer bridging. In this case, the proxy forwards messages while modifying their source and destination MAC addresses, and it rewrites their solicited and override flags and Link-Layer Address Options.

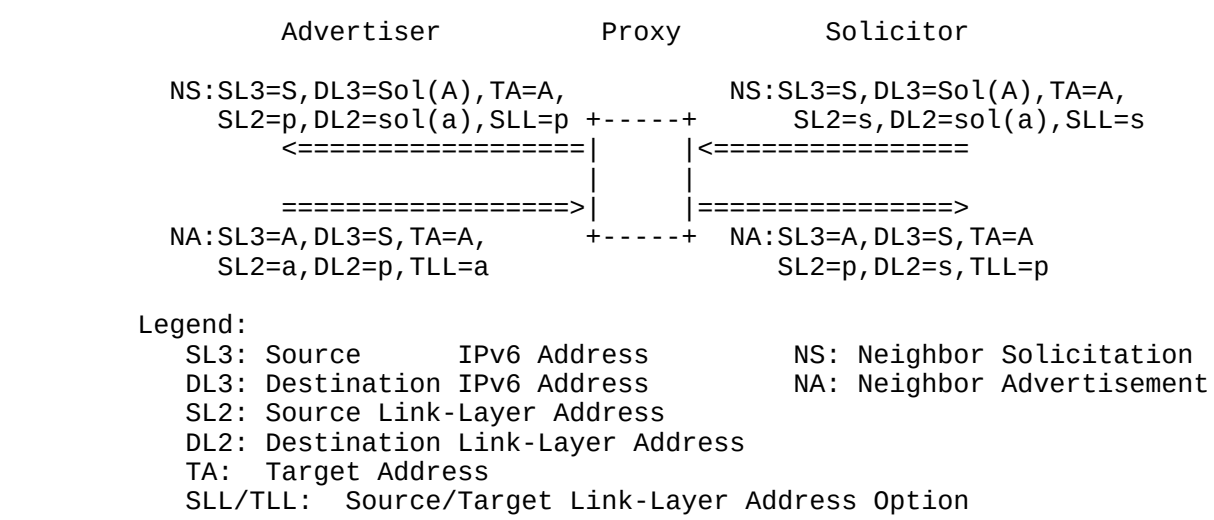
This rewriting is incompatible with SEND signed messages for a number of reasons:

- Rewriting elements within the message will break the digital signature.
- The source IP address of each packet is the packet's origin, not the proxy's address. The proxy is unable to generate another signature for this address, as it doesn't have the CGA private key [RFC3971].

Thus, proxy modification of SEND solicitations may require sharing of credentials between the proxied node and the proxying node or creation of new options with proxying capabilities.

While bridge-like ND proxies aim to provide as little interference with ND mechanisms as possible, SEND has been designed to prevent modification or spoofing of advertisements by devices on the link.

Of particular note is the fact that ND Proxy performs a different kind of proxy Neighbor Discovery to Mobile IPv6 [RFC3775] [RFC4389]. RFC 3775 (Mobile IPv6) specifies that the Home Agent as proxy sends Neighbor Advertisements from its own address with the Target Address set to the absent Mobile Node's address. The Home Agent's own link-layer address is placed in the Target Link-Layer Address Option [RFC3775]. On the other hand, ND Proxy resends messages containing their original address, even after modification (i.e., the IP source address remains the same) [RFC4389]. Figure 2 describes packet formats for proxy Neighbor solicitation and advertisement as specified by RFC 4389.



Legend:
SL3: Source IPv6 Address
DL3: Destination IPv6 Address
SL2: Source Link-Layer Address
DL2: Destination Link-Layer Address
TA: Target Address
SLL/TLL: Source/Target Link-Layer Address Option
NS: Neighbor Solicitation
NA: Neighbor Advertisement

Figure 2

In order to use the same security procedures for both ND Proxy and Mobile IPv6, changes may be needed to the proxying procedures in [RFC4389], as well as changes to SEND.

An additional (and undocumented) requirement for bridge-like proxying is the operation of router discovery. Router discovery packets may similarly modify Neighbor Cache state, and require protection from SEND.

In Figure 3, the router discovery messages propagate without modification to the router address, but elements within the message change. This is consistent with the description of Neighbor Discovery above.

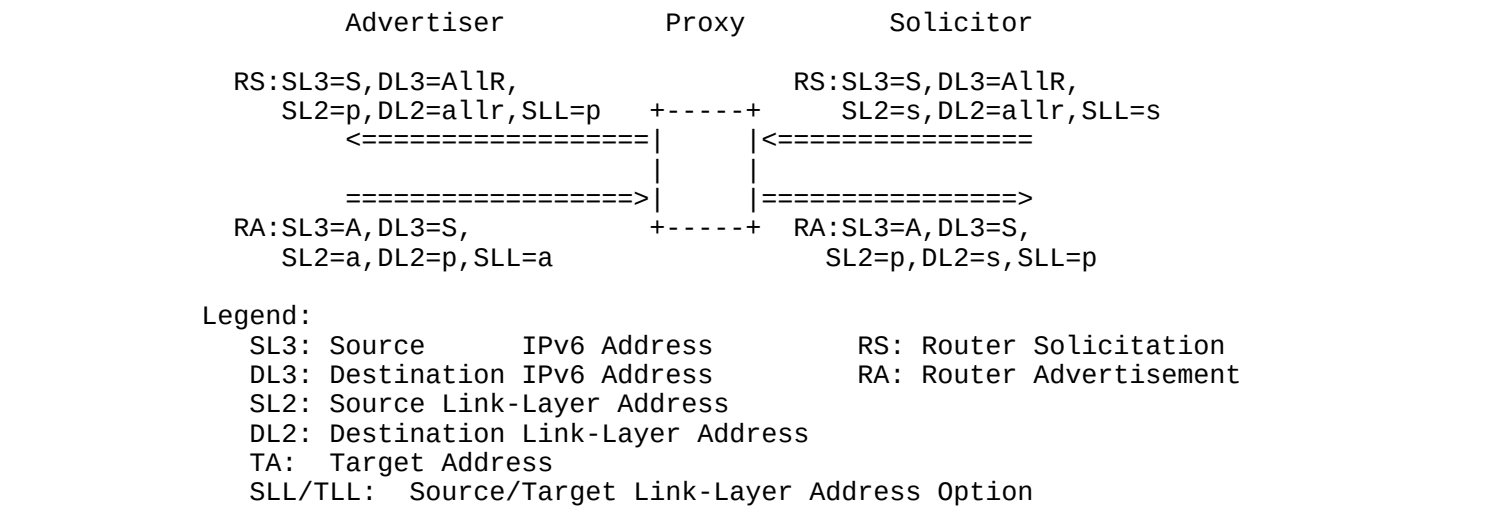


Figure 3

Once again, these messages may not be signed with a CGA signature by the proxy, because it does not own the source address.

Additionally, Authorization Delegation Discovery messages need to be exchanged for bridge-like ND proxies to prove their authority to forward. Unless the proxy receives explicit authority to act as a router, or the router knows of its presence, no authorization may be made. This explicit authorization requirement may be at odds with the zero configuration goal of ND proxying [RFC4389].

An alternative (alluded to in an appendix of ND Proxy [RFC4389]) suggests that the proxy send Router Advertisements (RAs) from its own address. As described by ND Proxy, this is insufficient for providing proxied Neighbor Advertisement service, but may be matched with Neighbor solicitation and advertisement services using the proxy's source address in the same way as Mobile IPv6 [RFC4389] [RFC3775]. This means that all router and Neighbor advertisements would come from the proxied address, but may contain a target address that allows proxied Neighbor presence to be established with peers on other segments. Router discovery in this case has the identity of the original (non-proxy) router completely obscured in router discovery messages.

The resultant proxy messages would have no identifying information indicating their origin, which means that proxying between multiple links would require state to be stored on outstanding solicitations (effectively a ND only NAT). This level of state storage may be undesirable.

Mobile IPv6 does not experience this issue when supplying its own address, since ND messages are never forwarded on to the absent node (the Home Agent having sufficient information to respond itself).

Authorization from a router may still be required for Router Advertisement, and will be discussed in Section 4.2.

3. Proxy Neighbor Discovery and SEND

There are currently no existing secured Neighbor Discovery procedures for proxied addresses, and all Neighbor Advertisements from SEND nodes are required to have equal source and target addresses, and be signed by the transmitter (Section 7.4 of [RFC3971]).

Signatures over SEND messages are required to be applied on the CGA source address of the message, and there is no way of indicating that a message is proxied.

Even if the message is able to be transmitted from the original owner, differences in link-layer addressing and options require modification by a proxy. If a message is signed with a CGA-based signature, the proxy is unable to regenerate a signature over the changed message as it lacks the keying material.

Therefore, a router wishing to provide proxy Neighbor Advertisement service cannot use existing SEND procedures on those messages.

A host may wish to establish a session with a device that is not on-link but is proxied. As a SEND host, it prefers to create Neighbor Cache Entries using secured procedures. Since SEND signatures cannot be applied to an existing proxy Neighbor Advertisement, it must accept non-SEND advertisements in order to receive proxy Neighbor Advertisements.

Neighbor Cache spoofing of another node therefore becomes trivial, as any address may be proxy-advertised to the SEND node, and overridden only if the node is there to protect itself. When a node is present to defend itself, it may also be difficult for the solicitor determine the difference between a proxy-spoofing attack, and a situation where a proxied device returns to a link and overrides other proxy advertisers [RFC4861].

3.1. CGA Signatures and Proxy Neighbor Discovery

SEND defines one public-key and signature format for use with Cryptographically Generated Addresses (CGAs) [RFC3972]. CGAs are intended to tie address ownership to a particular public/private key pair.

In SEND as defined today, Neighbor Discovery messages (including the IP Addresses from the IPv6 header) are signed with the same key used to generate the CGA. This means that message recipients have proof that the signer of the message owned the address.

When a proxy replaces the message's source IPv6 address with its own CGA, the existing CGA option and RSA signature option would need to be replaced with ones that correspond to the CGA of the proxy. To be valid according to the SEND specification, the Target Address of the Neighbor Advertisement message would need to be replaced also to be equal to the Source Address [RFC3971].

Additional authorization information may be needed to prove that the proxy is indeed allowed to advertise for the target address, as is described in Section 4.

3.2. Non-CGA Signatures and Proxy Neighbor Discovery

Where a proxy retains the original source address in a proxied message, existing security checks for SEND will fail, since fields within the message will be changed. In order to achieve secured proxy Neighbor Discovery in this case, extended authorization mechanisms may be needed for SEND.

SEND provides mechanisms for extension of SEND to non-CGA-based authorization. Messages are available for Authorization Delegation Discovery, which is able to carry arbitrary PKIX/X.509 certificates [RFC5280].

There is, however, no specification of keying information option formats analogous to the SEND CGA Option [RFC3971]. The existing option allows a host to verify message integrity by specifying a key and algorithm for digital signature, without providing authorization via mechanisms other than CGA ownership.

The digital signature in SEND is transported in the RSA Signature Option. As currently specified, the signature operation is performed over a CGA Message type, and allows for CGA verification. Updating the signature function to support non-CGA operations may be necessary.

Within SEND, more advanced functions such as routing may be authorized by certificate path verification using Authorization Delegation Discovery.

With non-CGA signatures and authentication, certificate contents for authorization may need to be determined, as outlined in Section 4.

While SEND provides for extensions to new non-CGA methods, existing SEND hosts may silently discard messages with unverifiable RSA signature options (Section 5.2.2 of [RFC3971]), if configured only to accept SEND messages. In cases where unsecured Neighbor Cache Entries are still accepted, messages from new algorithms will be treated as unsecured.

3.3. Securing Proxy DAD

Initiation of proxy Neighbor Discovery also requires Duplicate Address Detection (DAD) checks of the address [RFC4862]. These DAD checks need to be performed by sending Neighbor Solicitations, from the unspecified source address, with the target being the proxied address.

In existing SEND procedures, the address that is used for CGA tests on DAD NS is the target address. A Proxy that originates this message while the proxied address owner is absent is unable to generate a CGA-based signature for this address and must undertake DAD with an unsecured NS. It may be possible that the proxy can ensure that responding NAs are secured though.

Where bridge-like ND proxy operations are being performed, DAD NSs may be copied from the original source, without modification (considering they have an unspecified source address and contain no link-layer address options) [RFC4389].

If non-CGA-based signatures are available, then the signature over the DAD NS doesn’t need to have a CGA relationship to the Target Address, but authorization for address configuration needs to be shown using certificates.

In case there is a DAD collision between two SEND nodes on different interfaces of the proxy, it is possible that the proxy may not have the authority to modify the NA defending the address. In this case, the proxy still needs to modify the NA and pass it onto the other interfaces even if it will fail SEND verification on the receiving node.

3.4. Securing Router Advertisements

While Router Solicitations are protected in the same manner as Neighbor Solicitations, the security for Router Advertisements is mainly based on the use of certificates. Even though the mechanism for securing RAs is different, the problems that arise due to the modification of the L2 addresses are exactly the same: the proxy needs to have the right security material (e.g., certificate) to sign the RA messages after modification.

4. Potential Approaches to Securing Proxy ND

SEND nodes already have the concept of delegated authority through requiring external authorization of routers to perform their routing and advertisement roles. The authorization of these routers takes the form of delegation certificates.

Proxy Neighbor Discovery requires a delegation of authority (on behalf of the absent address owner) to the proxier. Without this authority, other devices on the link have no reason to trust an advertiser.

For bridge-like proxies, it is assumed that there is no preexisting trust between the host owning the address and the proxy. Therefore, authority may necessarily be dynamic or based on topological roles within the network [RFC4389].

Existing trust relationships lend themselves to providing authority for proxying in two alternative ways.

First, the SEND router authorization mechanisms described above provide delegation from the organization responsible for routing in an address domain to the certified routers. It may be argued that routers so certified may be trusted to provide service for nodes that form part of a link's address range, but are themselves absent. Devices which are proxies could either be granted the right to proxy by the network's router, or be implicitly allowed to proxy by virtue of being an authorized router.

Second, where the proxied address is itself a CGA, the holder of the public and private keys is seen to be authoritative about the address's use. If this address owner was able to sign the proxier's address and public key information, it would be possible to identify that the proxy is known and trusted by the CGA address owner for proxy service. This method requires that the proxied address know or learn the proxy's address and public key, and that the certificate signed by the proxied node's is passed to the proxy, either while they share the same link, or at a later stage.

In both methods, the original address owner's advertisements need to override the proxy if it suddenly returns, and therefore timing and replay protection from such messages need to be carefully considered.

4.1. Secured Proxy ND and Mobile IPv6

Mobile IPv6 has a security association between the Mobile Node and Home Agent. The Mobile Node sends a Binding Update to the Home Agent, to indicate that it is not at home. This implies that the

Mobile Node wishes the Home Agent to begin proxy Neighbor Discovery operations for its home address(es).

4.1.1. Mobile IPv6 and Router-Based Authorization

A secured Proxy Neighbor Advertisements proposal based on existing router trust would require no explicit authorization signaling between HA and MN to allow proxying. Hosts on the home link will believe proxied advertisements solely because they come from a trusted router.

Where the home agent operates as a router without explicit trust to route from the advertising routing infrastructure (such as in a home, with a router managed by an ISP), more explicit proxying authorization may be required, as described in Section 4.2.

4.1.2. Mobile IPv6 and Per-Address Authorization

Where proxy Neighbor Discovery is delegated by the MN to the home agent, the MN needs to learn the public key for the Home Agent, so that it can generate a certificate authorizing the public/private key pair to be used in proxying. It may conceivably do this using Certificate Path Solicitations either over a home tunnel, when it is away from home, or during router discovery while still at home [RFC3971] [RFC3775].

When sending its Binding Update to the HA, the MN would need to provide a certificate containing the subject's (i.e., proxy HA's) public key and address, the issuer's (i.e., MN's) CGA and public key, and timestamps indicating when the authority began and when it ends. This certificate would need to be transmitted at binding time. Messaging or such an exchange mechanism would have to be developed.

4.1.3. Cryptographic-Based Solutions

Specific cryptographic algorithms may help to allow trust between entities of a same group.

This is the case, for example, with ring signature algorithms. These algorithms generate a signature using the private key of any member from the same group, but to verify the signature the public keys of all group members are required. Applied to SEND, the addresses are cryptographically generated using multiple public keys, and the Neighbor Discovery messages are signed with an RSA ring signature [RING]. (Note that the cryptographic algorithms that are the foundation for [RING] and other similar solutions are not widely accepted in the security community; additional research is needed before a Standards Track protocol could be developed.)

4.1.4. Solution Based on the 'Point-to-Point' Link Model

Another approach is to use the 'Point-to-Point' link model.

In this model, one prefix is provided per MN, and only an MN and the HA are on a same link. The consequence is the HA no longer needs to act as ND Proxy.

One way to design such a solution is to use virtual interfaces, on the MN and the HA, and a virtual link between them. Addresses generated on the virtual interfaces will only be advertised on the virtual link. For Mobile IPv6, this results in a virtual Home Network where the MN will never come back.

4.2. Secured Proxy ND and Bridge-Like Proxies

In link-extension environments, the role of a proxy is more explicitly separated from that of a router. In SEND, routers may expect to be authorized by the routing infrastructure to advertise and may provide this authority to hosts in order to allow them to change forwarding state.

Proxies are not part of the traditional infrastructure of the Internet, and hosts or routers may not have an explicit reason to trust them, except that they can forward packets to regions where otherwise those hosts or routers could not reach.

4.2.1. Authorization Delegation

If a proxy can convince a device that it should be trusted to perform proxying function, it may require that device to vouch for its operation in dealing with other devices. It may do this by receiving a certificate, signed by the originating device that the proxy is believed capable of proxying under certain circumstances.

This allows nodes receiving proxied Neighbor Discovery packets to quickly check if the proxy is authorized for the operation. There are several bases for such trust, and requirements in proxied environments, which are discussed below.

4.2.2. Unauthorized Routers and Proxies

Routers may be advertising on networks without any explicit authorization, and SEND hosts will register these routers if there are no other options [RFC3971]. While proxies may similarly attempt to advertise without authority, this provides no security for the routing infrastructure. Any device can be setup as a SEND proxy/ router so long as it signs its own ND messages from its CGA.

This may not help in the case that a proxy attempts to update Neighbor Cache Entries for a SEND node that moves between links, since the SEND node's authority to advertise its own CGA address would not be superseded by a proxy with no credentials.

4.2.3. Multiple Proxy Spans

Proxies may have multiple levels of nesting, which allow the network to connect between non-adjacent segments.

In this case, authority delegated at one point will have to be redelegated (possibly in a diluted form) to proxies further away from the origin of the trust.

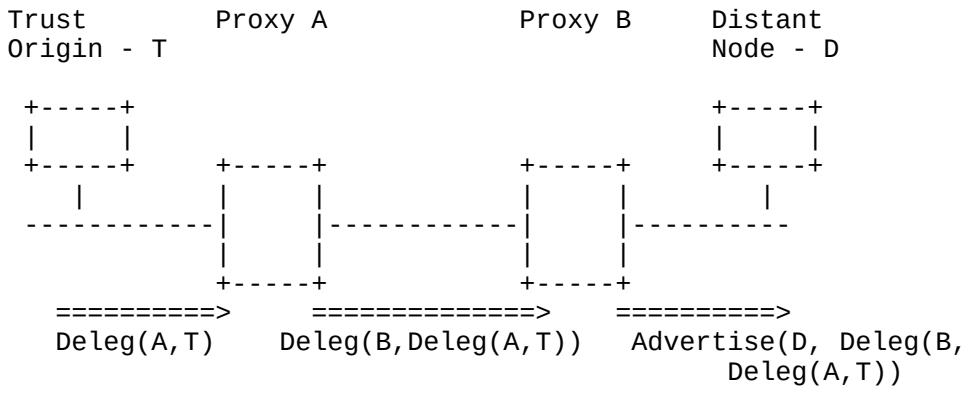


Figure 4

As shown in Figure 4, the Proxy A needs to redelegate authority to proxy for T to Proxy B; this allows it to proxy advertisements that target T back to D.

4.2.4. Routing Infrastructure Delegation

Where it is possible for the proxy to pre-establish trust with the routing infrastructure, or at least to the local router, it may be possible to authorize proxying as a function of routing within the subnet. The router or CA may then be able to certify proxying for only a subset of the prefixes for which it is itself certified.

If a router or CA provides certification for a particular prefix, it may be able to indicate that only proxying is supported, so that Neighbor Cache Entries of routers connected to Internet infrastructure are never overridden by the proxy, if the router is present on a segment.

Hosts understanding such certificates may allow authorized proxies and routers to override the host when assuming proxy roles, if the host is absent.

Proxy certificate signing could be done either dynamically (requiring exchanges of identity and authorization information) or statically when the network is set up.

4.2.5. Local Delegation

Where no trust tie exists between the authority that provides the routing infrastructure and the provider of bridging and proxying services, it may still be possible for SEND hosts to trust the bridging provider to authorize proxying operations.

SEND itself requires that routers be able to show authorization, but doesn’t require routers to have a single trusted root.

A local bridging/proxying authority trust delegation may be possible. It would be possible for this authority to pass out local-use certificates, allowing proxying on a specific subnet or subnets, with a separate authorization chain to those subnets for the routers with Internet access.

This would require little modification to SEND, other than the addition of router-based proxy authority (as in Section 4.2.4), and proxies would in effect be treated as routers by SEND hosts [RFC3971]. Distribution of keying and trust material for the initial bootstrap of proxies would not be provided though (and may be static).

Within small domains, key management and distribution may be a tractable problem, so long as these operations are simple enough to perform.

Since these domains may be small, it may be necessary to provide certificate chains for trust anchors that weren’t requested in Certificate Path Solicitations, if the proxy doesn’t have a trust chain to any requested trust anchor.

This is akin to ’suggesting’ an appropriate trusted root. It may allow for user action in allowing trust extension when visiting domains without ties to a global keying infrastructure. In this case, the trust chain would have to start with a self-signed certificate from the original CA.

4.2.6. Host Delegation of Trust to Proxies

Unlike Mobile IPv6, for bridge-like proxied networks, there is no existing security association upon which to transport proxying authorization credentials.

Thus, proxies need to convince Neighbors to delegate proxy authority to them, in order to proxy-advertise to nodes on different segments. It will be difficult without additional information to distinguish between legitimate proxies and devices that have no need or right to proxy (and may want to make two network segments appear connected).

When proxy advertising, proxies must not only identify that proxying needs to occur, but provide proof that they are allowed to do so, so that SEND Neighbor Cache Entries may be updated. Unless the authorization to update such entries is tied to address ownership proofs from the proxied host or the verifiable routing infrastructure, spoofing may occur.

When a host received a proxied Neighbor advertisement, it would be necessary to check authorization in the same way that authorization delegation discovery is performed in SEND.

Otherwise, certificate transport will be required to exchange authorization between proxied nodes and proxies.

Proxies would have to be able to delegate this authorization to downstream proxies, as described in Section 4.2.3.

4.3. Proxying Unsecured Addresses

Where the original Neighbor Discovery message is unsecured, there is an argument for not providing secured proxy service for that node.

In both the Mobile IPv6 and extended networks cases, the node may arrive back at the network and require other hosts to map their existing Neighbor Cache Entry to the node’s link-layer address. The re-arriving node’s overriding of link-layer address mappings will occur without SEND in this case.

It is notable that without SEND protection any node may spoof the arrival, and effectively steal service across an extended network. This is the same as in the non-proxy case, and is not made significantly worse by the proxy’s presence (although the identity of the attacker may be masked if source addresses are being replaced).

If signatures over the proxied messages were to be used, re-arrival and override of the Neighbor Cache Entries would have to be allowed, so the signatures would indicate that at least the proxy wasn't spoofing (even if the original sender was).

For non-SEND routers, though, it may be possible for secured proxies to send signed router advertisement messages, in order to ensure that routers aren't spoofed, and subsequently switched to different parts of the extended network.

This has problems in that the origin is again unsecured, and any node on the network could spoof router advertisement for an unsecured address. These spoofed messages may become almost indistinguishable (except for the non-CGA origin address) from unspoofed messages from SEND routers.

Given these complexities, the simplest method is to allow unsecured devices to be spoofed from any port on the network, as is the case today.

5. Two or More Nodes Defending the Same Address

All the previous sections of this document focused on the case where two nodes defend the same address (i.e., the node and the proxy). However, there are also cases where two or more nodes are defending the same address. This is at least the case for:

- Nodes having the same address, as the Mobile Access Gateway's (MAG's) ingress link-local address in Proxy Mobile IPv6 (PMIPv6) [RFC5213].

- Nodes having a common anycast address [RFC4291].

The problem statement, described previously in this document, applies for these cases, and the issues are the same from a signaling point of view.

Multicast addresses are not mentioned here because Neighbor Discovery Protocol is not used for them.

In the first case, [RFC5213] assumes that the security material used by SEND (i.e., public-private key pair) is shared between all the MAGs. For the second case, there is no solution today. But, in the same way, it should be possible to assume that the nodes having a common anycast address could also share the security material.

It is important to notice that when many nodes defending the same address are not in the same administrative domain (e.g., MAGs in different administrative domains but in the same PMIPv6 domain [RFC5213]), sharing the security material used by SEND may raise a security issue.

6. Security Considerations

6.1. Router Trust Assumption

Router-based authorization for Secured Proxy ND may occur without the knowledge or consent of a device. It is susceptible to the 'Good Router Goes Bad' attack described in [RFC3756].

6.2. Certificate Transport

Certificate delegation relies upon transfer of the new credentials to the proxying HA in order to undertake ND proxy on its behalf. Since the binding cannot come into effect until DAD has taken place, the delegation of the proxying authority necessarily predates the return of the Binding Ack, as described in [RFC3775]. In the case above described, the home tunnel that comes into creation as part of the binding process may be required for transport of Certificate Path Solicitations or Advertisements [RFC3971]. This constitutes a potential chicken-and-egg problem. Either modifications to initial home binding semantics or certificate transport are required. This may be trivial if certificates are sent in the clear between the MN's Care-of Address (CoA) and the HA without being tunneled.

6.3. Timekeeping

All of the presented methods rely on accurate timekeeping on the receiver nodes of Neighbor Discovery Timestamp Options.

For router-authorized proxy ND, a Neighbor may not know that a particular ND message is replayed from the time when the proxied host was still on-link, since the message's timestamp falls within the valid timing window. Where the router advertises its secured proxy NA, a subsequent replay of the old message will override the NCE created by the proxy.

Creating the NCE in this way, without reference to accurate subsequent timing, may only be done once. Otherwise, the receiver will notice that the timestamp of the advertisement is old or doesn't match.

One way of creating a sequence of replayable messages that have timestamps likely to be accepted is to pretend to do an unsecured DAD on the address each second while the MN is at home. The attacker saves each DAD defense in a sequence. The granularity of SEND timestamp matching is around one second, so the attacker has a set of SEND NAs to advertise, starting at a particular timestamp, and valid for as many seconds as the original NA gathering occurred.

This sequence may then be played against any host that doesn't have a timestamp history for that MN, by tracking the number of seconds elapsed since the initial transmission of the replayed NA to that victim, and replaying the appropriate cached NA.

Where certificate-based authorization of ND proxy is in use, the origination/starting timestamp of the delegated authority may be used to override a replayed (non-proxy) SEND NA, while also ensuring that the Proxy NA's timestamp (provided by the proxy) is fresh. A returning MN would advertise a more recent timestamp than the delegated authority and thus override it. This method is therefore not subject to the above attack, since the proxy advertisement's certificate will have a timestamp greater than any replayed messages, preventing it from being overridden.

7. Acknowledgments

James Kempf and Dave Thaler particularly contributed to work on this document. Contributions to discussion on this topic helped to develop this document. The authors would also like to thank Jari Arkko, Vijay Devarapalli, Mohan Parthasarathy, Marcelo Bagnulo, Julien Laganier, Tony Cheneau, Michaela Vanderveen, Sean Shen, and Sheng Jiang for their comments and suggestions.

Jean-Michel Combes is partly funded by MobiSEND, a research project supported by the French 'National Research Agency' (ANR).

8. References

8.1. Normative References

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[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.

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

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4389] Thaler, D., Talwar, M., and C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389, April 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.

8.2. Informative References

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

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[RING] Kempf, J. and C. Gentry, "Secure IPv6 Address Proxying using Multi-Key Cryptographically Generated Addresses (MCGAs)", Work in Progress, August 2005.

Authors' Addresses

Jean-Michel Combes
France Telecom Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

EMail: jeanmichel.combes@orange-ftgroup.com

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal
QC Canada

EMail: Suresh.Krishnan@ericsson.com

Greg Daley
Netstar Logicalis
Level 6/616 St Kilda Road
Melbourne, Victoria 3004
Australia

Phone: +61 401 772 770
EMail: hoskuld@hotmail.com