csi Working Group
Internet-Draft
Intended status: Informational
Expires: November 28, 2008

G. Daley

J-M. Combes
Orange Labs R&D
May 27, 2008

Securing Neighbour Discovery Proxy Problem Statement
draft-daley-csi-sndp-prob-00.txt

Status of this Memo

This Internet-Draft will expire on November 28, 2008.

Abstract

Neighbour Discovery Proxy is used to provide an address presence on a link from nodes which are no themselves present. It allows a node to receive packets directed at its address by allowing another device to neighbour advertise on its behalf.

Neighbour 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 neighbour discovery messages.

Neighbour Discovery Proxy currently cannot be secured using 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 Neighbour Discovery relates to Secured Neighbour Discovery.

Table of Contents

1. Introduction

Neighbour Discovery Proxy is defined in IPv6 Neighbour 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 NEMO [RFC3963], FMIPv6 [RFC4068] or HMIPv6 [RFC4140]) and in IKEv2 [RFC4306]. It allows a device which is not physically present on a link to have another advertise its presence, and forward on packets to the off-link device.

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

2. Scenarios

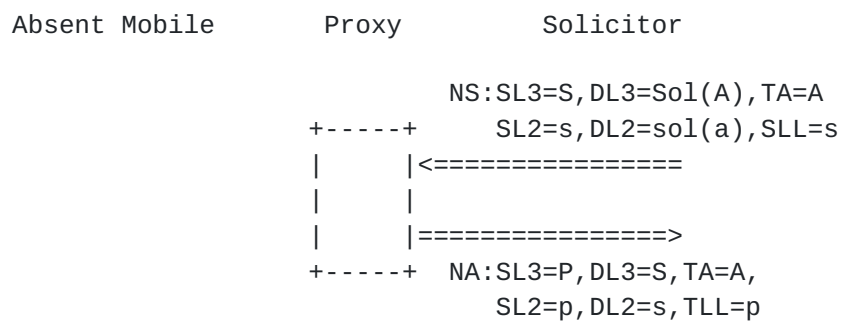
This section describes the different scenarios where the interaction between SEND and ND-Proxy raises issues.

2.1. IPv6 Mobile Nodes and Neighbour Discovery Proxy

When moving in the Internet, the aim of IPv6 mobility is to allow a device continued packet delivery, whether present on its home network or not. The following text is focused on Mobile IPv6 but the issue is the same with Mobile IPv6 based protocols (e.g. NEMO, HMIPv6).

For Mobile IPv6 Mobile Nodes (MN), it is necessary to keep existing sessions going even when one leaves the home network. If a neighbour is actively delivering packets to a Mobile Node which is at home, this neighbour will have a valid neighbour cache entry pointed at the MN's link-layer address on the Home link.

As seen in Figure 1, solicitors send a multicast solicitation to the solicited nodes address of the absent node (based on the unicast address).



Legend:

SL3: Source	IPv6 Address	NS: Neighbour Solicitation
DL3: Destination	IPv6 Address	NA: Neighbour 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

The Proxy, which listens to this address responds with a Neighbour Advertisement which 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 Neighbour Advertisement. In this case, no solicitations are proxied, as the advertisements originate within the proxy itself.

If Cryptographically Generated Addressing (CGA) [RFC3972] is available, the MN may be able to secure its neighbour cache bindings while at home using Secured Neighbour Discovery (SEND) [RFC3971]. SEND assumes that the address owner is the advertiser and therefore has access to the keys required to sign advertisements about the address. Movement away from the home link requires that a proxy undertake Neighbour Discovery.

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 as proxy will not have access to the public-private key pair used to generate the MN's cryptographic address. This prevents Proxy Neighbour Discovery from using SEND as defined [RFC3971].

Where a host moves from the home network to a visited network, the proxy needs to override existing valid neighbour cache entries which may have SEND protection. This is needed in order to redirect traffic to use the proxy's link-layer address, allowing packets to flow onto the tunnel connecting the Home Agent/Proxy and the MN. With current specifications, any solicitation or advertisement sent by the proxy will not be able to update the MN's home address if the

existing NC entry is protected by SEND. Such existing neighbour cache entries will time-out after Neighbour Unreachability Detection [RFC4861].

Where secured proxy services are not able to be provided, a proxy's advertisement may be overridden by a bogus proxy without it even knowing the attack has occurred.

2.2. IPv6 Fixed Nodes and Neighbor Discovery Proxy

This scenario is a sub-case from the previous one. The IPv6 node will never be on the link where the ND messages are proxied. This is case with IKEv2 [RFC4306] when a node needs an IP address in the network protected by a security gateway and this latest assigns it dynamically using Configuration Payload during IKEv2 exchanges. The security gateway will have to proxy ND messages to be able to intercept messages, sent to the node, to tunnel them to this latest.

2.3. Bridge-like ND proxies

Where proxies exist between two segments, messages may be sent by the proxy on the far link, in order to gain or pass on neighbour information. The proxy in this case forwards messages while modifying their source and destination MAC addresses, and rewrites their Link-Layer Address Options solicited and override flags. This is defined in Bridge Like ND Proxy (ND Proxy) [RFC4389].

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 the packets 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].

Proxy modification of SEND solicitations and advertisements require removal of (at least) CGA and Signature options, and may also need new options with proxy capabilities if non-CGA signatures are added to SEND.

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 neighbour discovery to Mobile IPv6 [RFC3775] [RFC4389]. The Mobile IPv6 RFC specifies that the Home Agent as proxy sends Neighbour 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].

ND Proxy resends messages containing their original address, even after modification [RFC4389]. Figure 2 describes packet formats for proxy neighbour solicitation and advertisement as specified by the specification.

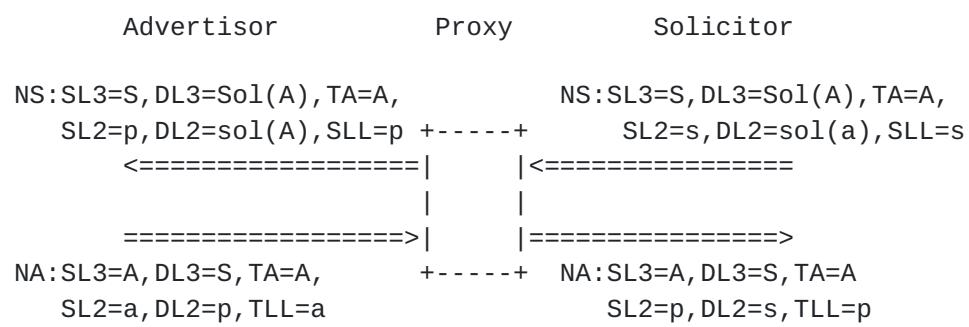


Figure 2

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 neighbour 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 Neighbour Discovery above.

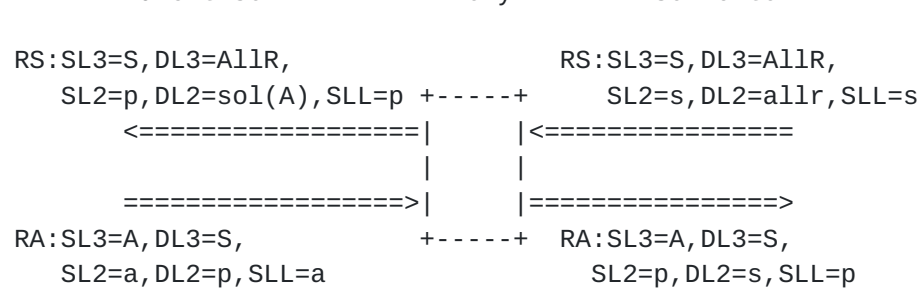


Figure 3

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

Additionally, multicast Authorization Delegation Discovery ICMPv6 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 zero configuration goal of ND proxying [RFC4389].

An alternative (alluded to in an appendix of ND Proxy) suggests that the proxy send Router Advertisements (RA) from its own address. As described by ND Proxy, this is insufficient for providing proxied Neighbour Advertisement service, but may be matched with neighbour 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 neighbour advertisements would come from the proxied address, but may contain a target address which allows proxied neighbour 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 5.2.

3. Proxy ND and Mobility

Whenever a mobile device moves off a link and requires another device to forward packets from that address to the MN's new location, proxy Neighbour Discovery is required.

In the Mobile IPv6 case, where the Mobile Node moves away from home, a Home Agent needs to be able to override existing neighbour cache entries in order to redirect packet flow over a tunnel to the Mobile

Node's Care-of-Address (CoA) [RFC3775].

In Fast Handovers for Mobile IPv6, local neighbours or routers with existing valid neighbour cache states need to be told the PAR's link-layer address when the MN is departing for a new link, or after arrival on the new link when tunnel forwarding begins [RFC4068]. This allows the MN to maintain reachability to the hosts on that link until it is able to send Mobile IPv6 Binding signalling subsequent to address configuration on the new network.

As shown in Figure 4, after the mobile node departs, the Home Agent or Proxy sends an overriding Neighbour advertisement, in order to update existing neighbour cache entries.

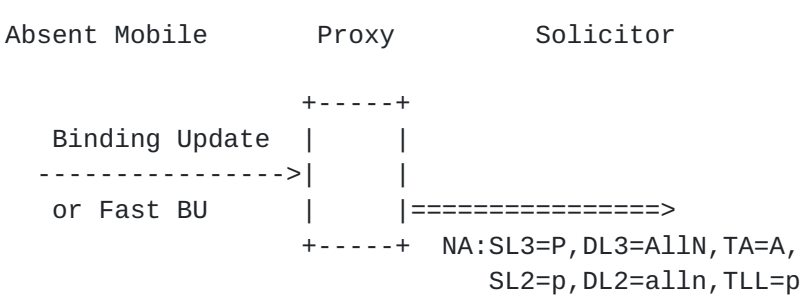


Figure 4

Where the proxy forwards between segments of a network, nodes may move between segments [RFC4389]. For this scenario, the proxy is responsible for updating neighbour cache entries as incorrect state is left in them after the move.

Devices which were on the same segment as the moving node, subsequently have incorrect neighbour cache state, as they now need to traverse the proxy to get to the other node. Devices which were previously being proxied may now be on the same segment as the mobile node, and may go direct.

As illustrated in Figure 5, the nodes may have incorrect neighbour cache state, even if the proxy knows of the departure to another segment.

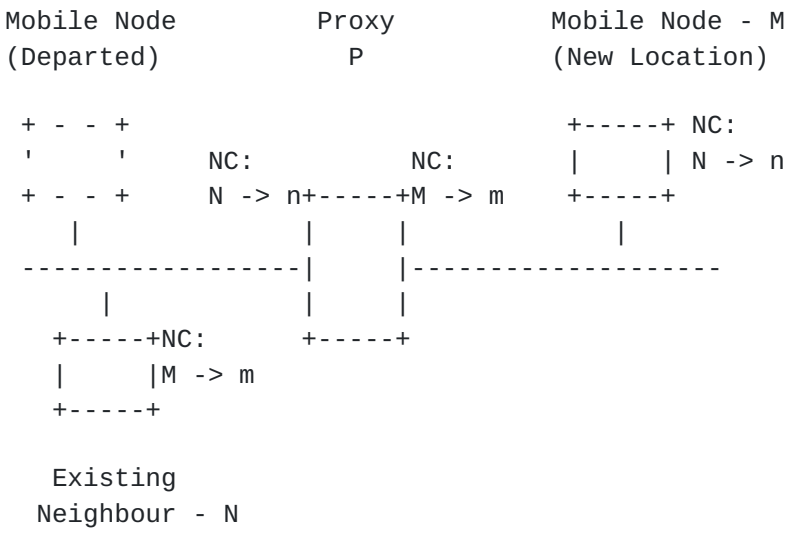


Figure 5

While neighbour cache state times out, and causes devices to probe for the location of a peer, long delays may occur before timeouts of neighbour cache state [RFC4861]. In cases where these delays are too long, the proxy may have to override the neighbour cache entries of hosts which were previously on the same segment as the moving node.

Those devices now resident on the same segment as the mobile node will have the proxy's link-layer address in its neighbour cache. In ND Proxy, it is indicated that packets are never forwarded back to the same segment upon which they arrived (potentially to prevent forwarding loops) [RFC4389].

Similarly, if the mobile node is unaware of its movement, it too may have incorrect neighbour cache entries for devices which it is now on the same segment as. This is shown below in Figure 6.

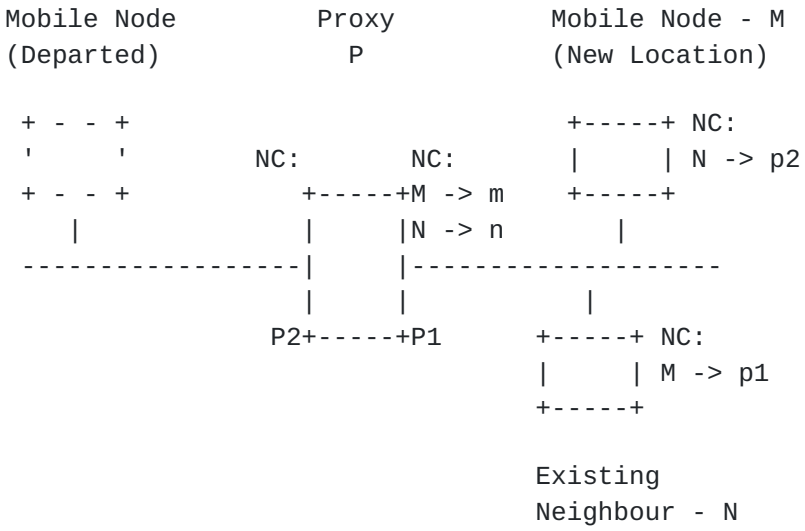


Figure 6

For the remaining duration of their incorrect neighbour cache entry (up to around 35 seconds), all packets will be dropped. Therefore, these devices may need to be updated with the present node's link-layer address.

Procedures regarding updating caches rely upon Section 7.2.6 of IPv6 Neighbour Discovery [RFC4861], which allows proxies to neighbour advertise to all-nodes with the override flag set when becoming a proxy or addresses change.

For either environment, updates are required to neighbour cache entries which may be for SEND nodes. These advertisements must therefore have enough authority to override neighbour cache entries even though they are secured.

4. Proxy Neighbour Discovery and SEND

There are currently no existing secured Neighbour Discovery procedures for proxied addresses, and all Neighbour 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 Neighbour Advertisement service can not use existing SEND procedures on those messages.

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

Neighbour 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].

4.1. CGA signatures and Proxy Neighbour Discovery

SEND defines one public-key and signature format for use with Cryptographically Generated Addresses (CGAs) [RFC3971]. CGAs are intended to tie address ownership to a particular Public/Private key pair.

In SEND as defined today, Neighbour 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.

Where a proxy replaces the message source with its own CGA, the existing CGA option and RSA signature option need to be replaced with the proxy's. Such a message will validate using SEND, except that the Target Address field will not match the IPv6 Source Address in Neighbour Advertisements [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 5.

4.2. Non-CGA signatures and Proxy Neighbour Discovery

Where a proxy retains the original source address in a proxied message, existing SEND-CGA checks will fail, since fields within the

message will be changed. In order to achieve secured proxy neighbour discovery in this case, new signature authentication mechanisms may be needed for SEND.

SEND provides interfaces 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 no specification though 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 for functions 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 infers support for CGA verification. Clarification or changing of this issue for 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 5.

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 neighbour cache entries are still accepted, messages from new algorithms will be treated as unsecured.

4.3. Securing proxy DAD

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

In existing SEND procedures, the address which is used for CGA tests on DAD NS is the target address. A Proxy which 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 NA's are secured though.

Where bridge-like ND proxy operations are being performed, DAD NS's 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. Where SEND-only nodes do not understand the signature format.

5. 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 Neighbour 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 which 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' 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.

5.1. 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 Neighbour Discovery operations for its home address(es).

5.1.1. Mobile IPv6 and Router-based authorization

A secured Proxy Neighbour Advertisements proposal based on existing router trust would require no explicit authorization signalling 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 5.2.

5.1.2. Mobile IPv6 and per-address authorization

Where proxy Neighbour 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 either do this using Certificate Path Solicitations over a home tunnel, over the Internet, or 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(proxy-HA)'s public key and address, the issuer(MN)'s CGA and public key, and timestamps indicating when the authority began and when it ends. This certificate would need to be passed near to binding time, possibly in a Certificate Path Advertisement [RFC3971]. Messaging or such an exchange mechanism would have to be developed.

5.1.3. 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, a type of signature generated using the private key of any entity from the same group but to check 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.

5.1.4. 'Point-to-Point' link model based solution

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

In this model, one prefix is provided per MN and only a MN and the HA are on a same link. The consequence is the HA no more 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 to use a virtual Home Network where the MN will never come back.

5.2. 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 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 they could not reach.

5.2.1. 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 neighbour 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.

5.2.2. Unauthorized routers and proxies

Routers advertising on networks without routers may have to operate with no explicit authorization, and SEND hosts will configure these if there's no other option [RFC3971]. While proxies may similarly attempt to advertise without authority, this provides no security for the routing infrastructure. Any device can set up to be 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 neighbour cache entries for SEND node which moves between links, since the SEND node's authority to advertise its own CGA address would not be superceded by a proxy with no credentials.

5.2.3. 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.

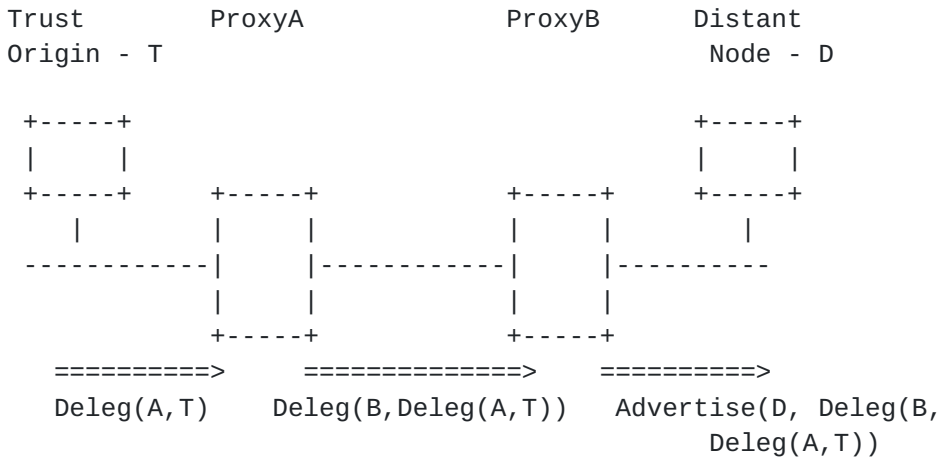


Figure 7

As shown in Figure 7, the Proxy A needs to redelegate authority to proxy for T to B, this allows it to proxy advertisements back to D, which target T.

5.2.4. 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 which is itself certified for.

If a router or CA provides certification for a particular prefix, it may be able to indicate that only proxying is supported, so that neighbour 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 host SEND/CGA 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.

5.2.5. Local Delegation

Where no trust tie exists between the authority which 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 that for the routers with Internet access.

This would require little modification to SEND, other than addition of router based proxy authority (as in Section 5.2.4), 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 are simple enough to perform.

Since these domains may be small, it may be necessary to provide certificate chains for trust anchors which 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.

5.2.6. 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.

Proxies need then to convince neighbours 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 which have no need or right to proxy (and may wish two network segments to appear to be 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 Neighbour 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 neighbour 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 5.2.3.

Movement between segments could be controlled with increasing certificate sequence numbers and timestamps. The timestamp of the root authority (in this case, the CGA address owner) would be most significant. Where ties exist, the shortest chain would supercede, as this would indicate a proxy closer to the proxied node.

5.3. Proxying unsecured addresses

Where the original neighbour 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 neighbour 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 neighbour 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/CGA 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 being on 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.

6. Two or more nodes defending a same address

The previous part of this document focused on the case where two nodes defend a same address (i.e. the node and the proxy). But, there are scenarios where two or more nodes are defending a same address. This is at least the case for:

- Nodes having the same address, as the MAG's ingress link-local address in PMIPv6 [I-D.ietf-netlmm-mn-ar-if].

o 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 signalling point of view.

In the first case, [I-D.ietf-netlmm-mn-ar-if] 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 a 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 a same address are not in the same administrative domain (e.g. MAGs in different administrative domains but in a same PMIPv6 domain [I-D.ietf-netlmm-proxymip6]), sharing the security material used by SEND may raise a security issue.

7. IANA Considerations

No new options or messages are defined in this document.

8. Security Considerations

8.1. 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].

8.2. Certificate Transport

The certification 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 above described case, the home tunnel which comes into creation as part of the binding process may be required for Certificate Path Solicitation or Advertisement transport [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 signed, non-repudiable certificates are sent in the clear between the MN's CoA and the HA without being tunneled.

8.3. Timekeeping

All of the presented methods rely on accurate timekeeping on the receiver nodes of Neighbour Discovery Timestamp Options and certificates.

For router-authorized proxy ND, a neighbour 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 NC entry created by the proxy.

Creating the neighbour cache entry 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 which 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 defence in a sequence. The granularity of SEND timestamp matching is around 1 second, so the attacker has a set of SEND NA's 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 which 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.

9. Acknowledgments

James Kempf and Dave Thaler particularly contributed to work on this document. Contributions to discussion on this topic helped to develop this document. Thanks go to Jari Arkko, Vijay Devarapalli, and Mohan Parthasarathy.

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

10. References

10.1. Normative References

[I-D.ietf-netlmm-mn-ar-if]
Laganier, J., Narayanan, S., and P. McCann, "Interface between a Proxy MIPv6 Mobility Access Gateway and a Mobile Node", draft-ietf-netlmm-mn-ar-if-03 (work in progress), February 2008.

[I-D.ietf-netlmm-proxymip6]
Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-16 (work in progress), May 2008.

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

[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.

10.2. 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.

[RFC4068] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[RFC4140] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

[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.

Appendix A. Changes from the previous versions

To be removed prior to publication as an RFC.

Previous version: draft-daley-send-spnd-prob-02

- Integration of the "Two or more nodes defending a same address" section in the core document.
- Addition of the "Cryptographic based solutions" section.
- Addition of the "'Point-to-Point' link model based solution" section.
- Update of the references.

Previous version: draft-daley-send-spnd-prob-01

- Reorganisation of the draft structure.
- Addition of the "Fixed Nodes and Neighbor Discovery Proxy" section.
- Update of the references.

- Addition of the "Two or more nodes defending a same address" Appendix

- Addition of the "Changes from the previous version" Appendix.

Authors' Addresses

Greg Daley
55 Pakington St
Kew, Victoria 3101
Australia

Phone: +61 405 494849
Email: hoskuld@hotmail.com

Jean-Michel Combes
Orange Labs R&D
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Email: jeanmichel.combes@gmail.com

Full Copyright Statement

Intellectual Property