Network Working Group J. Arkko
Internet-Draft Ericsson
Expires: December 18, 2003 June 19, 2003

SEcure Neighbor Discovery (SEND)
draft-arkko-send-ndopt-00.txt

Status of this Memo

Copyright Notice

Abstract

IPv6 nodes use the Neighbor Discovery (ND) protocol to discover other nodes on the link, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. If not secured, ND protocol is vulnerable to various attacks. This document specifies security mechanisms for ND. Contrary to the original ND specifications, these mechanisms do not make use of IPsec.

The purpose of this draft is to present an alternative to the current approach in the Working Group.

Table of Contents

1. Introduction

IPv6 defines the Neighbor Discovery (ND) protocol in RFC 2461 [6]. Nodes on the same link use the ND protocol to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. The ND protocol is used both by hosts and routers. Its functions include Router Discovery (RD), Address Auto-configuration, Address Resolution, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and Redirection.

RFC 2461 called for the use of IPsec for protecting the ND messages. However, it turns out that in this particular application IPsec can only be used with a manual configuration of security associations due to chicken-and-egg problems in using IKE [23, 21] before ND is operational. Furthermore, the number of such manually configured security associations needed for protecting ND is impractically large [24]. Finally, RFC 2461 did not specify detailed instructions for using IPsec to secure ND.

Section 4 describes our overall approach to securing ND. This approach involves the use of new ND options to carry public-key based signatures. A zero-configuration mechanism is used for showing address ownership, and routers are certified by a trusted root. The formats, procedures, and cryptographic mechanisms for the zero-configuration mechanism are described in a related specification [27].

Section 6 describes the mechanism for distributing certificate chains to establish authorization delegation chain to a common trusted root. The new ND options are discussed in Section 5, and Section 8 show how to apply these components to securing Neighbor and Router Discovery.

Finally, Section 9 discusses the co-existence of secure and non-secure Neighbor Discovery on the same link, Section 10 discusses performance considerations, and Section 11 discusses security considerations for SEND.

2. Terms

Authorization Certificate (AC)

The signer of an authorization certificate has authorized the entity designated in the certificate for a specific task or service.

Authorization Delegation Discovery (ADD)

This is a process through which SEND nodes can acquire a certificate chain from a peer node to a trusted root.

Cryptographically Generated Addresses (CGAs)

A technique [27, 31] where the address of the node is cryptographically generated from the public key of the node and some other parameters using a one-way hash function.

Duplicate Address Detection (DAD)

This mechanism defined in RFC 2462 [7] assures that two IPv6 nodes on the same link are not using the same addresses.

Internet Control Message Protocol version 6 (ICMPv6)

The IPv6 control signaling protocol. Neighbor Discovery is a part of ICMPv6.

Neighbor Discovery (ND)

The IPv6 Neighbor Discovery protocol [6].

Neighbor Unreachability Detection (NUD)

This mechanism defined in RFC 2461 [6] is used for tracking the reachability of neighbors.

Nonce

Nonces are random numbers generated by a node. In SEND, they are used to ensure that a particular advertisement is linked to the solicitation that triggered it.

3. Neighbor and Router Discovery Overview

IPv6 Neighbor and Router Discovery have several functions. Many of these functions are overloaded on a few central message types such as the ICMPv6 Neighbor Discovery message. In this section we explain some of these tasks and their effects in order to understand better how the messages should be treated. Where this section and the original Neighbor Discovery RFCs are in conflict, the original RFCs take precedence.

In IPv6, many of the tasks traditionally done at lower layers such as ARP have been moved to the IP layer. As a consequence, unified mechanisms can be applied across link layers, security mechanisms or other extensions can be adopted more easily, and a clear separation of the roles between the IP and link layer can be achieved.

The main functions of IPv6 Neighbor Discovery are as follows:

- Neighbor Unreachability Detection (NUD) is used for tracking the reachability of neighbors, both hosts and routers. NUD is defined in Section 7.3 of RFC 2461 [6]. NUD is security-sensitive, because an attacker could falsely claim that reachability exists when it in fact does not.

- Duplicate Address Detection (DAD) is used for preventing address collisions [7]. A node that intends to assign a new address to one of its interfaces runs first the DAD procedure to verify that other nodes are not using the same address. Since the outlined rules forbid the use of an address until it has been found unique, no higher layer traffic is possible until this procedure has completed. Thus, preventing attacks against DAD can help ensure the availability of communications for the node in question.

- Address Resolution is similar to IPv4 ARP [20]. The Address Resolution function resolves a node's IPv6 address to the corresponding link-layer address for nodes on the link. Address Resolution is defined in Section 7.2 of RFC 2461 [6] and it is used for hosts and routers alike. Again, no higher level traffic can proceed until the sender knows the hardware address of the destination node or the next hop router. Note that like its predecessor in ARP, IPv6 Neighbor Discovery does not check the source link layer address against the information learned through Address Resolution. This allows for an easier addition of network elements such as bridges and proxies, and eases the stack implementation requirements as less information needs to be passed from layer to layer.

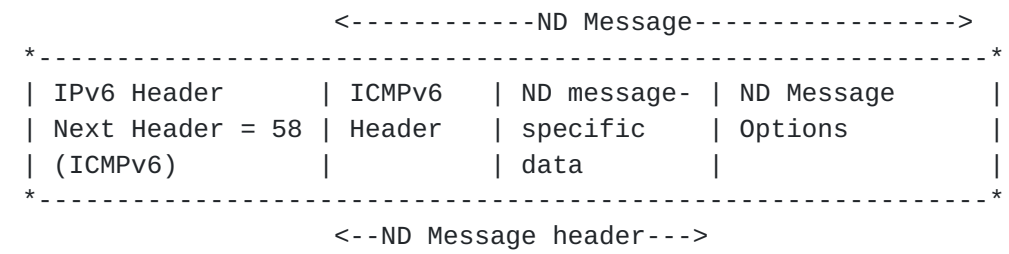
- Address Autoconfiguration is used for automatically assigning

addresses to a host [7]. This allows hosts to operate without configuration related to IP connectivity. The Address Autoconfiguration mechanism is stateless, where the hosts use prefix information delivered to them during Router Discovery to create addresses, and then test these addresses for uniqueness using the DAD procedure. A stateful mechanism, DHCPv6 [25], provides additional Autoconfiguration features. Router and Prefix Discovery and Duplicate Address Detection have an effect to the Address Autoconfiguration tasks.

- The Redirect function is used for automatically redirecting hosts to an alternate router. Redirect is specified in Section 8 of RFC 2461 [6]. It is similar to the ICMPv4 Redirect message [19].

- The Router Discovery function allows IPv6 hosts to discover the local routers on an attached link. Router Discovery is described in Section 6 of RFC 2461 [6]. The main purpose of Router Discovery is to find neighboring routers that are willing to forward packets on behalf of hosts. Prefix discovery involves determining which destinations are directly on a link; this information is necessary in order to know whether a packet should be sent to a router or to the destination node directly. Typically, address autoconfiguration and other tasks can not proceed until suitable routers and prefixes have been found.

The Neighbor Discovery messages follow the ICMPv6 message format and ICMPv6 types from 133 to 137. The IPv6 Next Header value for ICMPv6 is 58. The actual Neighbor Discovery message includes an ND message header consisting of ICMPv6 header and ND message-specific data, and zero or more ND options:



The ND message options are formatted in the Type-Length-Value format.

All IPv6 ND protocol functions are realized using the following messages:

ICMPv6 Type	Message
133	Router Solicitation (RS)
134	Router Advertisement (RA)
135	Neighbor Solicitation (NS)
136	Neighbor Advertisement (NA)
137	Redirect

The functions of the ND protocol are realized using these messages as follows:

- Router Discovery uses the RS and RA messages.
- Duplicate Address Detection uses the NS and NA messages.
- Address Autoconfiguration uses the NS, NA, RS, and RA messages.
- Address Resolution uses the NS and NA messages.
- Neighbor Unreachability Detection uses the NS and NA messages.
- Redirect uses the Redirect message.

The destination addresses used in these messages are as follows:

- Neighbor Solicitation: The destination address is either the solicited-node multicast address, unicast address, or an anycast address.
- Neighbor Advertisement: The destination address is either a unicast address or the All Nodes multicast address [1].
- Router Solicitation: The destination address is typically the All Routers multicast address [1].
- Router Advertisement: The destination address can be either a unicast or the All Nodes multicast address [1]. Like the solicitation message, the advertisement is also local to the link only.
- Redirect: This message is always sent from the router's link-local address to the source address of the packet that triggered the Redirect. Hosts verify that the IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address. Rules in [1] dictate that unspecified, anycast, or multicast addresses may not be used as source addresses. Therefore, the destination address will always be a unicast address.

4. Secure Neighbor Discovery Overview

New Neighbor Discovery options are used in to protect Neighbor and Router Discovery messages. This specification introduces these options, an authorization delegation discovery process, an address ownership proof mechanism, and requirements for the use of these components for Neighbor Discovery.

The components of the solution specified in this document are as follows:

- Trusted roots are expected to certify the authority of routers. A host and a router must have at least one common trusted root before the host can adopt the router as its default router. Optionally, an authorization certificate can specify the prefixes for which the router is allowed to act as a router. Delegation Chain Solicitation and Advertisement messages are used to discover a certificate chain to the trusted root without requiring the actual Router Discovery messages to carry lengthy certificate chains.

- Cryptographically Generated Addresses are used to assure that the sender of a Neighbor or Router Advertisement is the owner of an the claimed address. A public-private key pair needs to be generated by all nodes before they can claim an address.

- A new Neighbor Discovery option, the Signature option is used to protect all messages relating to Neighbor and Router discovery.

  Public key signatures are used. The trust to the public key is established either with the authorization delegation process or the address ownership proof mechanism, depending on configuration and the type of the message protected.

- In order to prevent replay attacks, the new Neighbor Discovery options Timestamp and Nonce are used. Given that Neighbor and Router Discovery messages are in some cases sent to multicast addresses, the Timestamp option offers replay protection without previously established state or sequence numbers. In addition, solicitation - advertisement pairs are protected through the Nonce option.

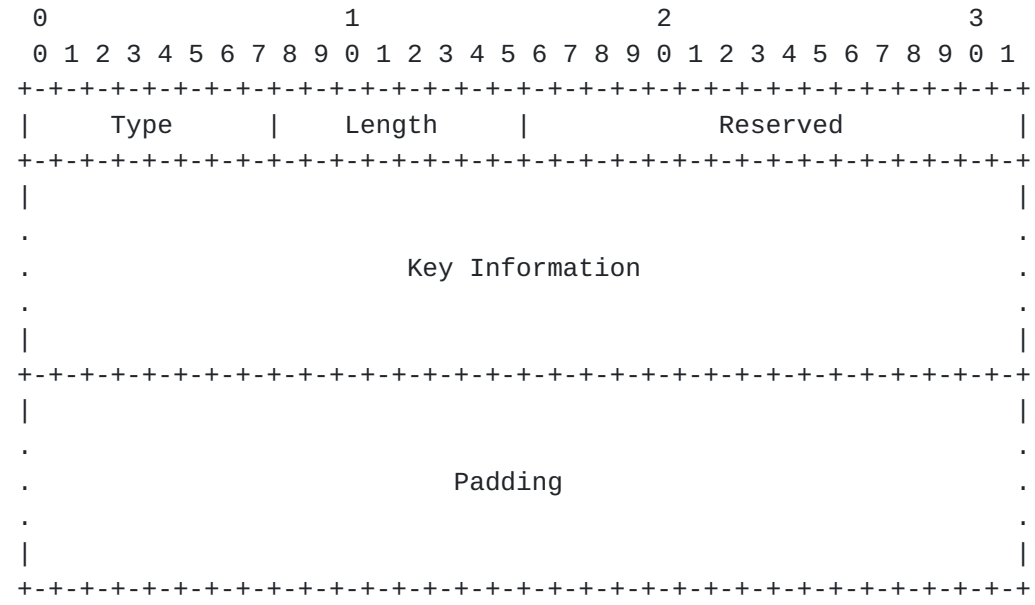
5. Neighbor Discovery Options

The following new ND mechanisms are required in SEND:

- The CGA option can be present in all Neighbor Discovery messages.
- The Signature option is required in all Neighbor Discovery messages.
- The Timestamp option is required in all Neighbor Discovery advertisements and Redirects.
- The Nonce option is required in all Neighbor Discovery solicitations, and for all solicited advertisements.
- Proxy Neighbor Discovery is not supported in this specification (it will be specified in a future document).

5.1 CGA Option

The CGA option allows the verification of the sender's CGA. The format of the CGA option is described in the following:



The meaning of the fields is described below:

Type

TBD <To be assigned by IANA> for CGA.

Length

The length of the option in units of 8 octets, i.e., 2.

Reserved

This is an 16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver..

Key Information

This variable length field contains the public key of the sender. It also may contain some other additional information which is necessary when CGA is used.

The contents of the Key Information field are represented as ASN.1 DER-encoded data item of the following type:

```
SendKeyInformation ::= CGAParameters

CGAParameters ::= SEQUENCE {
  publicKey      SubjectPublicKeyInfo,
  auxParameters  CGAAuxParameters }
```

(The normative definition of the type CGAParameters is in in [27]).

The verification of the CGA is based on the contents of the CGAParameters structure.

This specification requires that if both the CGA option and the Signature option are present, then the publicKey field in the former option MUST be the public key referred to in the Key Hash field in the latter option. Packets received with two different keys MUST be silently discarded. Note that a future extension may provide a mechanism which allows the owner of an address and the signer to be different parties.

The length of the Key Information field is determined by the ASN.1 encoding.

Padding

This variable length field begins after the ASN.1 encoding of the previous field has ends, and continues to the end of the option, as specified by the Length field.

5.1.1 Processing Rules for Senders

A node sending a message using the CGA option MUST construct the message as follows:

The Key Information field in the Authentication Data field is set to the SendKeyInformation structure according to the rules presented above and in [27]. The used public key is taken from configuration.

An address MUST be constructed as specified in [27]. Depending on the type of the message, this address appears in different places:

Redirect

The address MUST be the source address of the message.

Neighbor Solicitation

The address MUST be the Target Address for solicitations sent for the purpose of Duplicate Address Detection, and source address of the message otherwise.

Neighbor Advertisement

The address MUST be the source address of the message.

Router Solicitation

The address MUST be the source address of the message, unless it is the unspecified address.

Router Advertisement

The address MUST be the source address of the message.

5.1.2 Processing Rules for Receivers

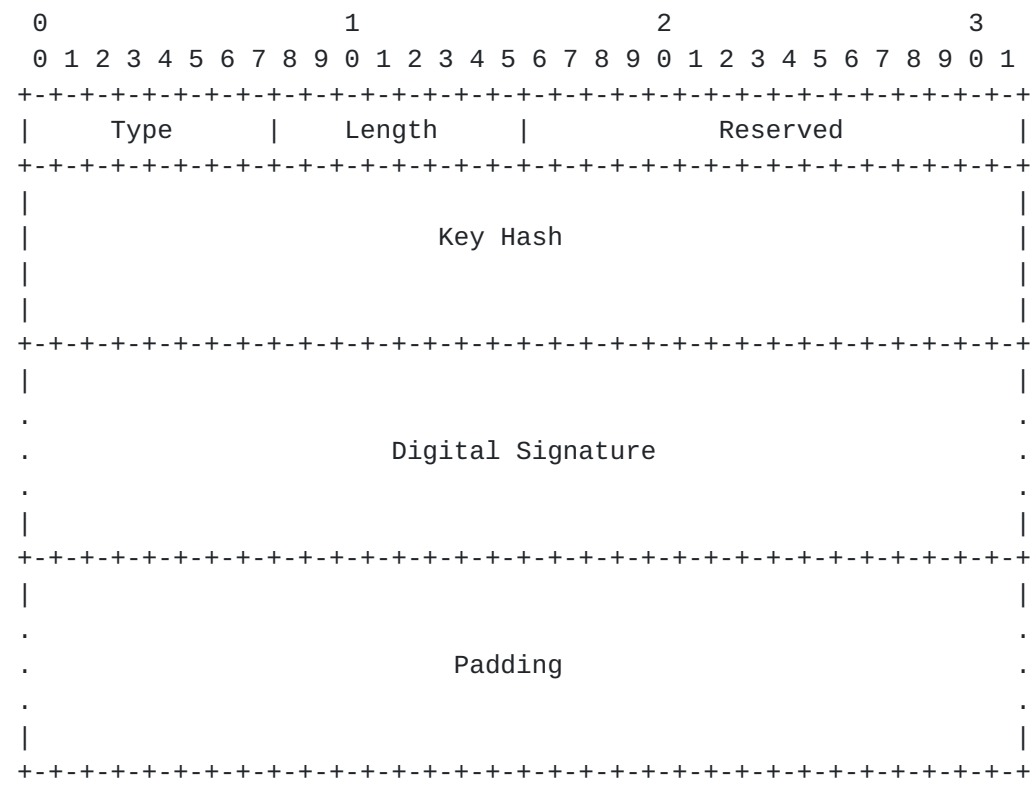
A message containing a Signature option MUST be checked as follows:

If the use of CGA has been configured, we require the receiving node to verify the source address of the packet using the algorithm described in Section 5 of [27]. The inputs for the algorithm are the contents of the CGAParameters structure from the Key Information field, the source address of the packet, and the minimum acceptable Sec value from the security association. If the CGA verification is successful, the recipient proceeds with the cryptographically more time consuming check of the signature.

Note that a receiver which does not support CGA or has not specified its use in its security associations can still verify packets using trusted roots, even if CGA had been used on a packet. The CGA property of the address is simply left untested.

5.2 Signature Option

The Signature option allows public-key based signatures to be attached to Neighbor Discovery messages. Both trusted root authentication and CGAs can be used. The format of the Signature option is described in the following:



The meaning of the fields is described below:

Type

TBD <To be assigned by IANA> for Signature.

Length

The length of the option in units of 8 octets, i.e., 2.

Reserved

This is an 16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver..

Key Hash

This 128 bit field contains a SHA1 hash of the public key used for the constructing the signature. Its purpose is to associate the signature to a particular key known by the receiver. Such a key can be either stored in the certificate cache of the receiver, or be received in the CGA option in the same message.

Digital Signature

This variable length field contains the signature made using the sender's private key, over the the whole packet as defined by the usual AH rules [3]. The signature is made using the RSA algorithm and MUST be encoded as private key encryption in PKCS #1 format [17].

This field starts after the Key Hash field. The length of the Digital Signature field is determined by the PKCS #1 encoding.

Padding

This variable length field begins after the PKCS #1 encoding of the previous field has ends, and continues to the end of the option, as specified by the Length field.

5.2.1 Processing Rules for Senders

A node sending a message using the Signature option MUST construct the message as follows:

- The message is constructed in its entirety.
- The Signature option is added as the last option in the message.
- For the purpose of constructing a signature, the following data items are appended:
  - The source address of the message.
  - The destination address of the message.
  - The contents of the message, starting from the ICMPv6 header, up to and including the Key Information field in the Signature option. The Signature and the Padding fields are not included.
- The message, in the form defined above, is signed using the configured private key, and the resulting PCKS #1 signature is put

to the Digital Signature field.

5.2.2 Processing Rules for Receivers

A message containing a Signature option MUST be checked as follows:

- The Signature option appears as the last option.
- The Key Information and Digital Signature fields have correct encoding, and do not exceed the length of the Authentication Data field.
- The Digital Signature verification shows that it has been calculated as specified in the previous section.
- If the use of a trusted root has been configured, a valid authorization delegation chain is known between the receiver's trusted root and the sender's public key.

  Note that the receiver may verify just the CGA property of a packet, even if the sender has used a trusted root as well.

Messages that do not pass all the above tests MUST be silently discarded.

5.2.3 Configuration

All nodes that support the reception of the Signature option MUST record the following configuration information:

authorization method

This parameter determines the mechanisms through which the authority of the sender is determined. It can have four values:

trusted root

The authority of the sender is verified as described in Section 6.5. The sender may have additional authorization through the use of CGAs, but this is neither required nor verified.

CGA

The CGA property of the sender's address is verified as described in [27]. The sender may have additional authority through a trusted root, but this is neither required nor verified.

trusted root and CGA

Both the trusted root and the CGA verification is required.

trusted root or CGA

Either the trusted root or the CGA verification is required.

root

The public key of the trusted root, if authorization method is not set CGA.

minbits

The minimum acceptable key length for peer public keys (and any intermediaries between the trusted root and the peer). The default SHOULD be 1024 bits. Implementations MAY also set an upper limit in order to limit the amount of computation they need to perform when verifying packets that use these security associations.

minSec

The minimum acceptable Sec value, if CGA verification is required (see Section 2 in [27]. This parameter is intended to facilitate future extensions and experimental work. The minSec value SHOULD always be set to zero.

All nodes that support the sending of the Signature option MUST record the following configuration information:

keypair

A public-private key pair. If authorization delegation is in use, there must exist a delegation chain from a trusted root to this key pair.

CGA flag

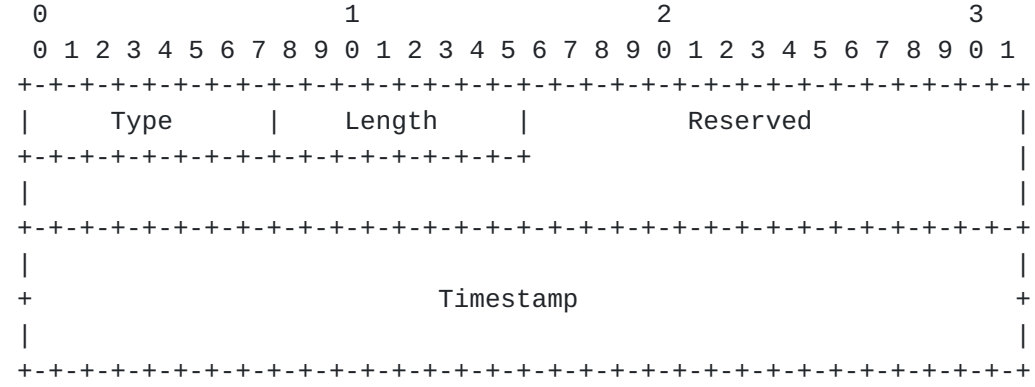
A flag that indicates whether or not the CGA is used.

CGA parameters

Optionally any information required to construct CGAs, including the used Sec value and nonce, and the CGA itself.

5.3 Timestamp Option

The purpose of the Timestamp option is to ensure that unsolicited advertisements and redirects have not been replayed. The format of the Timestamp option is described in the following:



Where the fields are as follows:

Type

TBD <To be assigned by IANA> for Timestamp.

Length

The length of the option in units of 8 octets, i.e., 2.

Reserved

This is a 48-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver..

Timestamp

This 64 bit unsigned integer field contains a timestamp. The format is 64 bits, and the contents are the number of milliseconds since January 1, 1970 00:00 UTC.

Senders SHOULD set the Timestamp field to the current time.

Receivers SHOULD be configured with an allowed Delta value. They SHOULD maintain a cache of the last received timestamp value from each specific source address within this time period. Receivers SHOULD then check the Timestamp field as follows:

o A packet with a Timestamp field value beyond the current time plus

or minus the allowed Delta value MUST be silently discarded.

Recommended default value for the allowed Delta is 3,600 seconds.

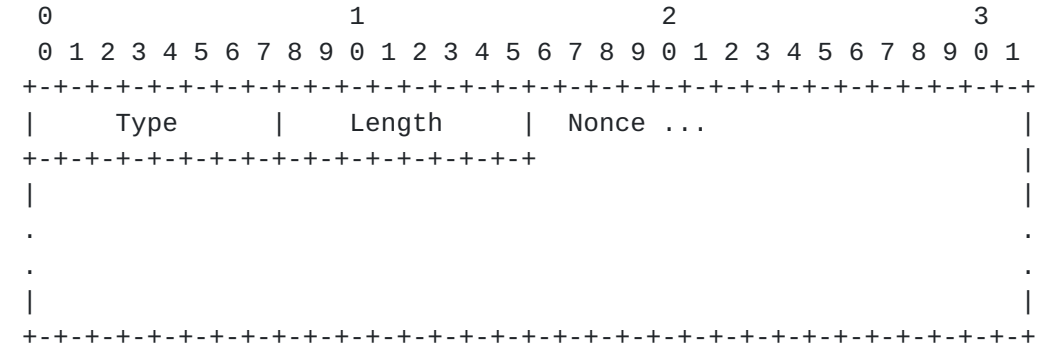
- A packet accepted according to the above rule MUST be checked against the last received timestamp value from the given source address. A packet that has already been seen from the same source with the same or lower Timestamp field value MUST be silently discarded.

- If packet passes both of the above tests, a new timestamp value MUST be registered in the cache for the given source address.

- If the cache becomes full, the receiver SHOULD temporarily reduce the Delta value for that source address so that all messages within that value can still be stored.

5.4 Nonce Option

The purpose of the Nonce option is to ensure that an advertisement is a fresh response to a solicitation sent earlier by this same node. The format of the Nonce option is as described in the following:



Where the fields are as follows:

Type

TBD <To be assigned by IANA> for Nonce.

Length

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

Nonce

This field contains a random number selected by the sender of the solicitation message. The length of the number MUST be at least 6 bytes.

5.5 Proxy Neighbor Discovery

The Target Address in Neighbor Advertisement is required to be equal to the source address of the packet, except in the case of proxy Neighbor Discovery. Proxy Neighbor Discovery is discussed in another specification.

6. Authorization Delegation Discovery

Several protocols, including IPv6 Neighbor Discovery, allow a node to automatically configure itself based on information it learns shortly after connecting to a new link. It is particularly easy for "rogue" routers to be configured, and it is particularly difficult for a network node to distinguish between valid and invalid sources of information when the node needs this information before communicating off-link.

Since the newly-connected node likely can not communicate off-link, it can not be responsible for searching information to help validate the router; however, given a chain of appropriately signed certificates, it can check someone else's search results and conclude that a particular message comes from an authorized source. Similarly, the router, which is already connected to the network, can if necessary communicate off-link and construct the certificate chain.

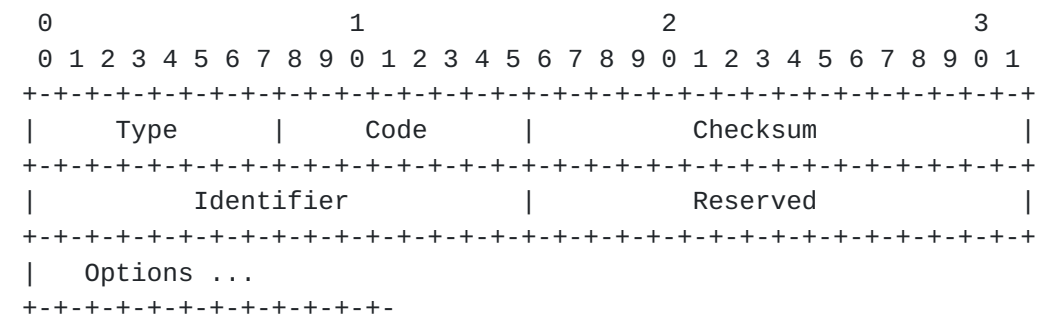
The Secure Neighbor Discovery protocol introduces two new ICMPv6 messages that are used between hosts and routers to allow the client to learn the certificate chain with the assistance of the router. Where hosts have certificates from a trusted root, these messages MAY also optionally be used between hosts to acquire the peer's certificate chain.

The Delegation Chain Solicitation message is sent by hosts when they wish to request the certificate chain between a router and the one of the hosts' trusted roots. The Delegation Chain Advertisement message is sent as an answer to this message, or periodically to the All Nodes multicast address. These messages are separate from the rest of the Neighbor Discovery in order to reduce the effect of the potentially voluminous certificate chain information to other messages.

The Authorization Delegation Discovery process does not exclude other forms of discovering the certificate chains. For instance, during fast movements mobile nodes may learn information - including the certificate chains - of the next router from the previous router.

6.1 Delegation Chain Solicitation Message Format

Hosts send Delegation Chain Solicitations in order to prompt routers to generate Delegation Chain Advertisements quickly.



IP Fields:

Source Address

An IP address assigned to the sending interface, or the unspecified address if no address is assigned to the sending interface.

Destination Address

Typically the all-routers multicast address, the solicited-node multicast address, or the address of the hosts' default router.

Hop Limit

255

ICMP Fields:

Type

TBD <To be assigned by IANA> for Delegation Chain Solicitation.

Code

0

Checksum

The ICMP checksum [8]..

Identifier

This 16 bit unsigned integer field acts as an identifier to help match advertisements to solicitations. The Identifier field MUST NOT be zero.

Reserved

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

Valid Options:

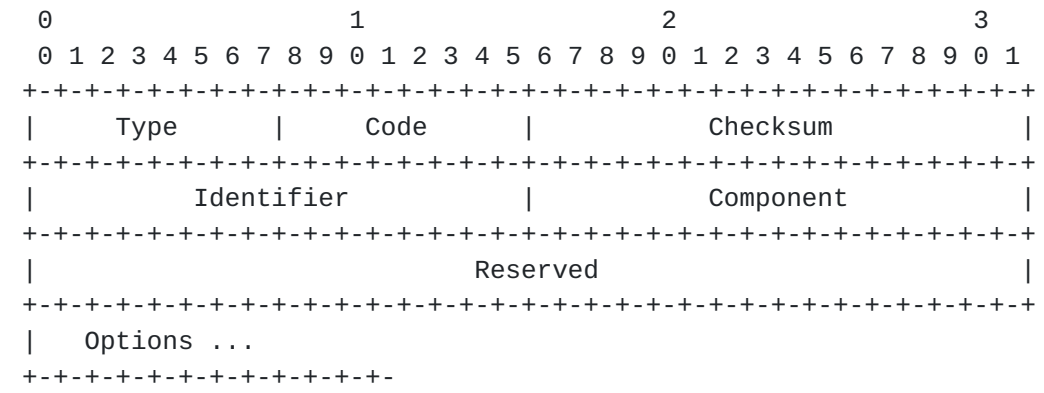
Trusted Root

One or more trusted roots that the client is willing to accept.

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

6.2 Delegation Chain Advertisement Message Format

Routers send out Delegation Chain Advertisement messages periodically, or in response to a Delegation Chain Solicitation.



IP Fields:

Source Address

MUST be a unicast address assigned to the interface from which this message is sent.

Destination Address

Either the solicited-node multicast address of the receiver or the all-nodes multicast address.

Hop Limit

255

ICMP Fields:

Type

TBD <To be assigned by IANA> for Delegation Chain Advertisement.

Code

0

Checksum

The ICMP checksum [8]..

Identifier

This 16 bit unsigned integer field acts as an identifier to help match advertisements to solicitations. The Identifier field MUST be zero for unsolicited advertisements and MUST NOT be zero for solicited advertisements.

Component

This is a 16 bit unsigned integer field used for informing the receiver which certificate is being sent, and how many are still left to be sent in the whole chain.

A single advertisement MUST be broken into separately sent components if there is more than one Certificate option, in order to avoid excessive fragmentation at the IP layer. Unlike the fragmentation at the IP layer, individual components of an advertisement may be stored and taken in use before all the components have arrived; this makes them slightly more reliable and less prone to Denial-of-Service attacks.

The first message in a N-component advertisement has the Component field set to N-1, the second set to N-2, and so on. Zero indicates that there are no more components coming in this advertisement.

The components MUST be ordered so that the trusted root end of the chain is the one sent first, each certificate sent after it can be verified with previously sent certificates, and the certificate of the sender comes last.

Reserved

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

Valid Options:

Certificate

One certificate is provided in Certificate option, to establish a (part of) certificate chain to a trusted root.

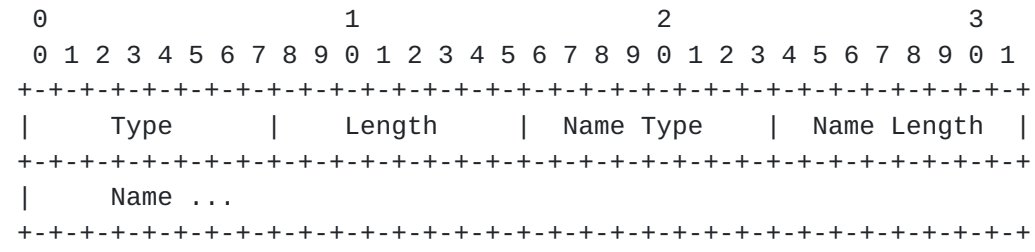
Trusted Root

Zero or more Trusted Root options may be included to help receivers decide which advertisements are useful for them. If present, these options MUST appear in the first component of a multi-component advertisement.

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

6.3 Trusted Root Option

The format of the Trusted Root option is as described in the following:



Where the fields are as follows:

Type

TBD <To be assigned by IANA> for Trusted Root.

Length

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

Name Type

The type of the name included in the Name field. This specification defines only one legal value for this field:

1 FQDN

Name Length

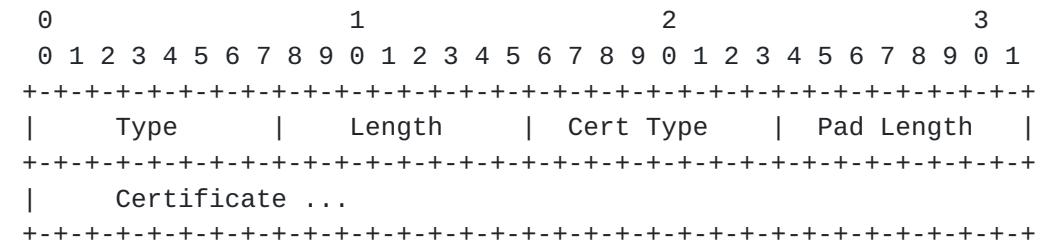
The length of the Name field, in bytes. Octets beyond this length but within the length specified by the Length field are padding and MUST be set to zero by senders and ignored by receivers.

Name

When the Name Type field is set to 1, the Name field contains the Fully Qualified Domain Name of the trusted root, for example "trustroot.operator.com".

6.4 Certificate Option

The format of the certificate option is as described in the following:



Where the fields are as follows:

Type

TBD <To be assigned by IANA> for Certificate.

Length

The length of the option (including the Type, Length, Cert Type, Pad Length, and Certificate fields) in units of 8 octets.

Cert Type

The type of the certificate included in the Name field. This specification defines only one legal value for this field:

1 X.509 Certificate

Pad Length

The amount of padding beyond the end of the Certificate field but within the length specified by the Length field. Padding MUST be set to zero by senders and ignored by receivers.

Certificate

When the Cert Type field is set to 1, the Certificate field contains an X.509 certificate [16].

6.5 Router Authorization Certificate Format

The certificate chain of a router terminates in a router authorization certificate that authorizes a specific IPv6 node as a router. Because authorization chains are not common practice in the Internet at the time this specification is being written, the chain MUST consist of standard Public Key Certificates (PKC, in the sense of [11]) for identity from the trusted root shared with the host to the router. This allows the host to anchor trust for the router's public key in the trusted root. The last item in the chain is an Authorization Certificate (AC, in the sense of [12]) authorizing the router's right to route. Stronger certification is necessary here than for CGAs because the right to route must be granted by an authorizing agency. Future versions of this specification may include provision for full authorization certificate chains, should they become common practice.

SEND nodes MUST support the RFC 3281 X.509 attribute certificate format [12] as the default format for router authorization certificates, and MAY support other formats. Router authorization certificates MUST be signed by the network operator or other trusted third party whose PKC is above the router's PKC in the delegation chain. Routers MAY advertise multiple ACs if the trust delegation obtains from different trust roots, and the authorized prefixes in those certificates MAY be disjoint. A router SHOULD only advertise one AC corresponding to one trust root and all interfaces and prefixes covered by that trust root MUST be in the AC.

In the attribute certificate, the GeneralName type MUST be either a dNSName or iPAddress for the router, unless otherwise specified by RFC 3281. If the GeneralName attribute is a dNSName, it MUST be resolvable to a global unicast address assigned to the router. If the GeneralName attribute is an iPAddress, it MUST be a global unicast address assigned to the router. For purposes of facilitating

renumbering, a dNSName SHOULD be used. However, hosts MUST NOT use a dNSName or iPAddress for validating the certificate. The router's public key hash, stored in the acinfo.holder.objectDigestInfo.objectDigest field of the certificate provides the definitive validation. As explained in Section 8.2, the addresses from the certificate can be matched against the global addresses claimed in the Router Advertisement.

6.5.1 Field Values

acinfo.holder.entityName

This field MAY contain one or several entityNames, of type dNSName or iPAddress, referring to global address(es) belonging to the router.

acinfo.objectDigestInfo.digestedObjectType

This field MUST be present and of type (1), publicKey.

acinfo.holder.digestAlgorithm

This field MUST indicate id-sha1 as indicated in RFC 3279 [10].

acinfo.objectDigestInfo.objectDigest

This field MUST be a SHA-1 digest over either a PKCS#1 [17] (RSA) or an RFC 3279 Section 2.3.2 representation [10] (DSA) representation of the router's public key. If this digest does not match the digest of the router's public key from its PKC, a node MUST discard the certificate.

acinfo.issuer.v2form.issuerName

The field MUST contain the distinguished name from the PKC used to sign the router AC.

acinfo.attrCertValidityPeriod

A node MUST NOT accept a certificate if the validity period has ended or has not yet started.

acinfo.attributes

This field MUST contain a list of prefixes that the router is authorized to route, or the unspecified prefix if the router is allowed to route any prefix. The field has the following type:

```
  name: AuthorizedSubnetPrefix
   OID: {id-rcert}
Syntax: iPAddress
values: Multiple allowed
        Multiple prefix values are allowed.
```

The details of the above syntax are specified in Section 2.2.3.8 of [14].

If the router is authorized only to route specific prefixes, the ipAddress values consist of IPv6 addresses in standard RFC 3513 [13] prefix format. One iPAddress value appears for each prefix routed by the router. If the router is authorized to route any prefix, a single ipAddress value appears with the value of the unspecified address.

6.6 Processing Rules for Routers

Routers SHOULD possess a key pair and certificate from at least one certificate authority.

A router MUST silently discard any received Delegation Chain Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 8 or more octets.
- Identifier field is non-zero.
- All included options have a length that is greater than zero.

The contents of the Reserved field, and of any unrecognized options, MUST be ignored. Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values. The contents of any defined options that are not specified to be used

with Router Solicitation messages MUST be ignored and the packet processed in the normal manner. The only defined option that may appear is the Trusted Root option. A solicitation that passes the validity checks is called a "valid solicitation".

Routers MAY send unsolicited Delegation Chain Advertisements for their trusted root. When such advertisements are sent, their timing MUST follow the rules given for Router Advertisements in RFC 2461 [6]. The only defined option that may appear is the Certificate option. At least one such option MUST be present. Router SHOULD also include at least one Trusted Root option to indicate the trusted root on which the Certificate is based.

In addition to sending periodic, unsolicited advertisements, a router sends advertisements in response to valid solicitations received on an advertising interface. A router MUST send the response to the all-nodes multicast address, if the source address in the solicitation was the unspecified address. If the source address was a unicast address, the router MUST send the response to the solicited-node multicast address corresponding to the source address.

In a solicited advertisement, the router SHOULD include suitable Certificate options so that a delegation chain to the solicited root can be established. The root is identified by the FQDN from the Trusted Root option being equal to an FQDN in the AltSubjectName field of the root's certificate. The router SHOULD include the Trusted Root option(s) in the advertisement for which the delegation chain was found.

If the router is unable to find a chain to the requested root, it SHOULD send an advertisement without any certificates. In this case the router SHOULD include the Trusted Root options which were solicited.

Rate limitation of Delegation Chain Advertisements is performed as specified for Router Advertisements in RFC 2461 [6].

6.7 Processing Rules for Hosts

Hosts SHOULD possess the certificate of at least one certificate authority, and MAY possess their own key pair and certificate from this authority.

A host MUST silently discard any received Delegation Chain Advertisement messages that do not satisfy all of the following validity checks:

o IP Source Address is a unicast address. Note that routers may use

multiple addresses, so this address not sufficient for the unique identification of routers.

- IP Destination Address is either the all-nodes multicast address or the solicited-node multicast address corresponding to one of the unicast addresses assigned to the host.
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 16 or more octets.
- All included options have a length that is greater than zero.

The contents of the Reserved field, and of any unrecognized options, MUST be ignored. Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values. The contents of any defined options that are not specified to be used with Delegation Chain Advertisement messages MUST be ignored and the packet processed in the normal manner. The only defined option that may appear is the Certificate option. An advertisement that passes the validity checks is called a "valid advertisement".

Hosts SHOULD store certificate chains retrieved in Delegation Chain Discovery messages if they start from a root trusted by the host. The certificates chains SHOULD be verified before storing them. Routers are required to send the certificates one by one, starting from the trusted root end of the chain. Except for temporary purposes to allow for message loss and reordering, hosts SHOULD NOT store certificates received in a Delegation Chain Advertisement unless they contain a certificate which can be immediately verified either to the trusted root or to a certificate which has been verified earlier.

Note that it may be useful to cache this information and implied verification results for use over multiple attachments to the network. In order to use an advertisement for the verification of a specific Neighbor Discovery message, the host matches the key hash in acinfo.Holder.objectDigestInfo to the public key carried in the IPsec AH Authentication Data field.

When an interface becomes enabled, a host may be unwilling to wait for the next unsolicited Delegation Chain Advertisement. To obtain such advertisements quickly, a host SHOULD transmit up to MAX_RTR_SOLICITATIONS Delegation Chain Solicitation messages each separated by at least RTR_SOLICITATION_INTERVAL seconds. Delegation Chain Solicitations SHOULD be sent after any of the following events:

- The interface is initialized at system startup time.
- The interface is reinitialized after a temporary interface failure or after being temporarily disabled by system management.
- The system changes from being a router to being a host, by having its IP forwarding capability turned off by system management.
- The host attaches to a link for the first time.
- A movement has been indicated by lower layers or has been inferred from changed information in a Router Advertisement.
- The host re-attaches to a link after being detached for some time.
- A Router Advertisement has been received with a public key that is not stored in the hosts' cache of certificates, or there is no authorization delegation chain to the host's trusted root.

Delegation Chain Solicitations MUST NOT be sent if the host has a currently valid certificate chain for the router to a trusted root, including the Attribute Certificate for the desired router (or host).

A host MUST send Delegation Chain Solicitations either to the All-Routers multicast address, if it has not selected a default router yet, or to the default router's IP address if it has already been selected.

If two hosts communicate with the solicitations and advertisements, the solicitations MUST be sent to the solicited-node multicast address of the receiver. The advertisements MUST be sent as specified above for routers.

Delegation Chain Solicitations SHOULD be rate limited and timed similarly with Router Solicitations, as specified in RFC 2461 [6].

When processing a possible advertisement sent as a response to a solicitation, the host MAY prefer to process first those advertisements with the same Identifier field value as in the solicitation. This makes Denial-of-Service attacks against the mechanism harder (see Section 11.3).

7. Securing Neighbor Discovery with SEND

This section describes how to use the mechanisms from Section 5, Section 6, and the reference [27] in order to provide security for Neighbor Discovery.

7.1 Neighbor Solicitation Messages

All Neighbor Solicitation messages are protected with SEND.

7.1.1 Sending Secure Neighbor Solicitations

Secure Neighbor Solicitation messages are sent as described in RFC 2461 and 2462, with the additional requirements listed in the following.

All Neighbor Solicitation messages sent MUST contain the Nonce, Timestamp and Signature options, and MAY contain the CGA option. The Signature option MUST be configured with the sender's key pair, setting the authorization method and additional information as is desired.

7.1.2 Receiving Secure Neighbor Solicitations

Received Neighbor Solicitation messages are processed as described in RFC 2461 and 2462, with the additional SEND-related requirements listed in the following.

Neighbor Solicitation messages received without the Nonce, Timestamp, or Signature option MUST be silently discarded. The Signature option MUST be configured with the expected authorization method, the minimum allowable key size, and optionally with the information related to the trusted root and the acceptable minSec value.

7.2 Neighbor Advertisement Messages

All Neighbor Advertisement messages are protected with SEND.

7.2.1 Sending Secure Neighbor Advertisements

Secure Neighbor Advertisement messages are sent as described in RFC 2461 and 2462, with the additional requirements listed in the following.

All Neighbor Advertisement messages sent MUST be sent with the Timestamp and Signature options and MAY be sent with the CGA option. The Signature option MUST be configured with the sender's key pair, setting the authorization method and additional information as is

desired.

Neighbor Advertisements sent in response to a Neighbor Solicitation MUST contain a copy of the Nonce option included in the solicitation.

7.2.2 Receiving Secure Neighbor Advertisements

Received Neighbor Advertisement messages are processed as described in RFC 2461 and 2462, with the additional SEND-related requirements listed in the following.

Neighbor Advertisement messages received without the Timestamp and Signature options MUST be silently discarded. The Signature option MUST be configured with the expected authorization mechanism (CGA or trusted root), the minimum allowable key size, and optionally with the information related to the trusted root and the acceptable minSec value.

Received Neighbor Advertisements sent to a unicast destination address without a Nonce option MUST be silently discarded.

7.3 Other Requirements

Upon receiving a message for which the receiver has no certificate chain to a trusted root, the receiver MAY use Authorization Delegation Discovery to learn the certificate chain of the peer.

Hosts that use stateless address autoconfiguration MUST generate a new CGA as specified in Section 4 of [27] for each new autoconfiguration run.

It is outside the scope of this specification to describe the use of trusted root authorization between hosts with dynamically changing addresses. Such dynamically changing addresses may be the result of stateful or stateless address autoconfiguration or through the use of RFC 3041 [9]. If the CGA method is not used, hosts would be required to exchange certificate chains that terminate in a certificate authorizing a host to use an IP address having a particular interface identifier. This specification does not specify the format of such certificates, since there are currently a few cases where such certificates are required by the link layer and it is up to the link layer to provide certification for the interface identifier. This may be the subject of a future specification. It is also outside the scope of this specification to describe how stateful address autoconfiguration works with the CGA method.

8. Securing Router Discovery with SEND

This section describes how to use the mechanisms from Section 5, Section 6, and the reference [27] in order to provide security for Router Discovery.

8.1 Router Solicitation Messages

All Router Solicitation messages are protected with SEND.

8.1.1 Sending Secure Router Solicitations

Secure Router Solicitation messages are sent as described in RFC 2461, with the additional requirements listed in the following.

Router Solicitation messages sent with an unspecified source address MUST have the Nonce and Timestamp options. Other Router Solicitations MUST have the Nonce, Timestamp, and Signature options. The Signature option MUST be configured with the sender's key pair, setting the authorization method and additional information as is desired.

8.1.2 Receiving Secure Router Solicitations

Received Router Solicitation messages are processed as described in RFC 2461, with the additional SEND-related requirements listed in the following.

Router Solicitation message sent with an unspecified source address and without the Nonce and Timestamp options MUST be silently discarded. Router Solicitation messages received with another type of source address but without the Nonce, Timestamp, and Signature options MUST be silently discarded. The Signature option MUST be configured with the expected authorization mechanism (CGA or trusted root), the minimum allowable key size, and optionally with the information related to the trusted root and the acceptable minSec value.

8.2 Router Advertisement Messages

All Router Advertisement messages are protected with SEND.

8.2.1 Sending Secure Router Advertisements

Secure Router Advertisement messages are sent as described in RFC 2461, with the additional requirements listed in the following.

All Router Advertisement messages sent MUST contain a Timestamp and

Signature options. The Signature option SHOULD be configured to protect the advertisement with the trusted root authorization method and MAY be configured to additionally protect it with the CGA authorization method.

Router Advertisements sent in response to a Router Solicitation MUST contain a copy of the Nonce option included in the solicitation.

8.2.2 Receiving Secure Router Advertisements

Received Router Advertisement messages are processed as described in RFC 2461, with the additional SEND-related requirements listed in the following.

Router Advertisement messages received without the Timestamp and Signature options MUST be silently discarded. The Signature option SHOULD be configured to require the trusted-root authorization method and they MAY additionally be configured to require CGA authentication.

Received Router Advertisements sent to a unicast destination address without a Nonce option MUST be silently discarded.

8.3 Redirect Messages

All Redirect messages are protected with SEND.

8.3.1 Sending Redirects

Secure Redirect messages are sent as described in RFC 2461, with the additional requirements listed in the following.

All Redirect messages sent MUST contain the Timestamp and Signature options. The security associations used for this MUST be configured with the sender's key pair, setting the authorization method and additional information as is desired.

8.3.2 Receiving Redirects

Received Redirect messages are processed as described in RFC 2461, with the additional SEND-related requirements listed in the following.

Redirect messages received without the Timestamp and Signature options MUST be silently discarded. The Signature option MUST be configured with the expected authorization mechanism (CGA or trusted root), the minimum allowable key size, and optionally with the information related to the trusted root and the acceptable minSec

value.

If only CGA-based security associations are used, hosts MUST follow the rules defined below when receiving Redirect messages:

1. The Redirect message MUST be protected as discussed above.

2. The receiver MUST verify that the Redirect message comes from an IP address to which the host may have earlier sent the packet that the Redirect message now partially returns. That is, the source address of the Redirect message must be the default router for traffic sent to the destination of the returned packet. If this is not the case, the message MUST be silently discarded.

   This step prevents a bogus router from sending a Redirect message when the host is not using the bogus router as a default router.

8.4 Other Requirements

The certificate for a router MAY specify the global IP address(es) of the router. If so, only these addresses can appear in advertisements where the Router Address (R) bit [15] is set. All hosts MUST have the certificate of a trusted root.

Hosts SHOULD use Authorization Delegation Discovery to learn the certificate chain of their default router or peer host, as explained in Section 6. The receipt of a protected Router Advertisement message for which no router Authorization Certificate and certificate chain is available triggers Authorization Delegation Discovery.

9. Co-Existence of SEND and ND

During the transition to secure links or as a policy consideration, network operators may want to run a particular link with a mixture of secure and insecure nodes. However, all routers are required to support SEND. The following behaviour is mandated:

- Router Solicitations SHOULD be accepted without the Nonce, Timestamp, CGA, and Signature options. The router SHOULD respond according to the rules outlined in Section 8.2 except that a Nonce option is not sent.

- Neighbor Solicitations SHOULD be accepted without the Nonce, Timestamp, CGA, and Signature options. The receiver SHOULD respond according to the rules outlined in Section 7.2 except that a Nonce option is not sent.

- Neighbor Advertisements SHOULD be accepted without the Timestamp, CGA and Signature options. The receiver SHOULD act according to the RFC 2461 [6] and RFC 2462 [7] rules, but take precedence for information sent using SEND over plain ND.

10. Performance Considerations

The computations related to AH_RSA_Sig transform are computationally relatively expensive operations.

In the application for which AH_RSA_Sig has been designed, however, hosts typically have the need to perform only a few operations as they enter a link, and a few operations as they find a new on-link peer with which to communicate.

Routers are required to perform a larger number of operations, particularly when the frequency of router advertisements is high due to mobility requirements. Still, the number of operations on a router is on the order of a few dozen operations per second, some of which can be precomputed as discussed below. A large number of router solicitations may cause higher demand for performing asymmetric operations, although RFC 2461 limits the rate at which responses to solicitations can be sent.

Signatures related to the use of the AH_RSA_Sig transform MAY be precomputed for Multicast Neighbor and Router Advertisements. Typically, solicited advertisements are sent to the unicast address from which the solicitation was sent. Given that the IPv6 header is covered by the AH integrity protection, it is typically not possible to precompute solicited advertisements.

11. Security Considerations

11.1 Threats to the Local Link Not Covered by SEND

SEND does not compensate for an insecure link layer. In particular, there is no cryptographic binding in SEND between the link layer frame address and the IPv6 address. On an insecure link layer that allows nodes to spoof the link layer address of other nodes, an attacker could disrupt IP service by sending out a Neighbor Advertisement having the source address on the link layer frame of a victim, a valid CGA with valid AH signature corresponding to itself, and a Target Link-layer Address extension corresponding to the victim. The attacker could then proceed to cause a traffic stream to bombard the victim in a DoS attack. To protect against such attacks, link layer security MUST be used. An example of such for 802 type networks is port-based access control [35].

Prior to participating in Neighbor Discovery and Duplicate Address Detection, nodes must subscribe to the All Nodes Multicast Group and Solicited Node Multicast Group for the address that they are claiming RFC 2461 [6]. Subscribing to a multicast group requires that the nodes use MLD [22]. MLD contains no provision for security. An attacker could send an MLD Done message to unsubscribe a victim from the Solicited Node Multicast address. However, the victim should be able to detect such an attack because the router sends a Multicast-Address-Specific Query to determine whether any listeners are still on the address, at which point the victim can respond to avoid being dropped from the group. This technique will work if the router on the link has not been compromised. Other attacks using MLD are possible, but they primarily lead to extraneous (but not overwhelming) traffic.

11.2 How SEND Counters Threats to Neighbor Discovery

The SEND protocol is designed to counter the threats to IPv6 Neighbor Discovery outlined in [29]. The following subsections contain a regression of the SEND protocol against the threats, to illustrate what aspects of the protocol counter each threat.

11.2.1 Neighbor Solicitation/Advertisement Spoofing

This threat is defined in Section 4.1.1 of [29]. The threat is that a spoofed Neighbor Solicitation or Neighbor Advertisement causes a false entry in a node's Neighbor Cache. There are two cases:

1. Entries made as a side effect of a Neighbor Solicitation or Router Solicitation. There are two cases:

1. A router receiving a Router Solicitation with a firm IPv6 source address and a Target Link-Layer Address extension inserts an entry for the IPv6 address into its Neighbor Cache.

2. A node doing Duplicate Address Detection (DAD) that receives a Neighbor Solicitation for the same address regards the situation as a collision and ceases to solicit for the address.

2. Entries made as a result of a Neighbor Advertisement sent as a response to a Neighbor Solicitation for purposes of on-link address resolution.

11.2.1.1 Solicitations with Effect

SEND counters the threat of solicitations with effect in the following ways:

1. As discussed in Section 5, SEND nodes preferably send Router Solicitations with a firm IPv6 address and AH header, which the router can verify, so the Neighbor Cache binding is correct. If a SEND node must send a Router Solicitation with the unspecified address, the router will not update its Neighbor Cache, as per RFC 2461.

2. When SEND nodes are performing DAD, they use the tentative address as the source address on the Neighbor Solicitation packet, and include an IPv6 AH header. This allows the receiving SEND node to verify the solicitation.

See Section 11.2.5, below, for discussion about replay protection and timestamps.

11.2.1.2 Address Resolution

SEND counters attacks on address resolution by requiring that the responding node include an AH header with a signature on the packet, and that the node's interface identifier either be a CGA or that the node be able to produce a certificate authorizing that node to use the interface identifier.

The Neighbor Solicitation and Advertisement pairs implement a challenge-response protocol, as explained in Section 7 and discussed in Section 11.2.5 below.

11.2.2 Neighbor Unreachability Detection Failure

This attack is described in Section 4.1.2 of [29]. SEND counters this attack by requiring a node responding to Neighbor Solicitations sent as NUD probes to include an AH header and proof of authorization to use the interface identifier in the address being probed. If these prerequisites are not met, the node performing NUD discards the responses.

11.2.3 Duplicate Address Detection DoS Attack

This attack is described in Section 4.1.3 of [29]. SEND counters this attack by requiring the Neighbor Advertisements sent as responses to DAD to include an AH header and proof of authorization to use the interface identifier in the address being tested. If these prerequisites are not met, the node performing DAD discards the responses.

When a SEND node is used on a link that also connects to non-SEND nodes, the SEND node defends its addresses by sending unprotected Neighbor Solicitations with an unspecified address, as explained in Section 9. However, the SEND node ignores any unprotected Neighbor Solicitations or Advertisements that may be send by the non-SEND nodes. This protects the SEND node from DAD DoS attacks by non-SEND nodes or attackers simulating to non-SEND nodes, at the cost of a potential address collision between a SEND node and non-SEND node. The probability and effects of such an address collision are discussed in [27].

11.2.4 Router Solicitation and Advertisement Attacks

These attacks are described in Sections 4.2.1, 4.2.4, 4.2.5, 4.2.6, and 4.2.7 of [29]. SEND counters these attacks by requiring Router Advertisements to contain an AH header, and that the signature in the header be calculated using the public key of a host that can prove its authorization to route the subnet prefixes contained in any Prefix Information Options. The router proves it authorization by showing an attribute certificate containing the specific prefix or the indication that the router is allowed to route any prefix. A Router Advertisement without these protections is dropped as part of the IPsec processing.

SEND does not protect against brute force attacks on the router, such as DoS attacks, or compromise of the router, as described in Sections 4.4.2 and 4.4.3 of [29].

11.2.5 Replay Attacks

This attack is described in Section 4.3.1 of [29]. SEND protects against attacks in Router Solicitation/Router Advertisement and Neighbor Solicitation/Neighbor Advertisement transactions by including a Nonce option in the solicitation and requiring the advertisement to include a matching option. Together with the signatures this forms a challenge-response protocol. SEND protects against attacks from unsolicited messages such as Neighbor Advertisements, Router Advertisements, and Redirects by including a timestamp into the AH header. A window of vulnerability for replay attacks exists until the timestamp expires.

When timestamps are used, SEND nodes are protected against replay attacks as long as they cache the state created by the message containing the timestamp. The cached state allows the node to protect itself against replayed messages. However, once the node flushes the state for whatever reason, an attacker can re-create the state by replaying an old message while the timestamp is still valid. Since most SEND nodes are likely to use fairly coarse grained timestamps, as explained in Section 5.3, this may affect some nodes.

11.2.6 Neighbor Discovery DoS Attack

This attack is described in Section 4.3.2 of [29]. In this attack, the attacker bombards the router with packets for fictitious addresses on the link, causing the router to busy itself with performing Neighbor Solicitations for addresses that do not exist. SEND does not address this threat because it can be addressed by techniques such as rate limiting Neighbor Solicitations, restricting the amount of state reserved for unresolved solicitations, and clever cache management. These are all techniques involved in implementing Neighbor Discovery on the router.

11.3 Attacks against SEND Itself

The CGAs have a 59-bit hash value. The security of the CGA mechanism has been discussed in [27].

Some Denial-of-Service attacks against ND and SEND itself remain. For instance, an attacker may try to produce a very high number of packets that a victim host or router has to verify using asymmetric methods. While safeguards are required to prevent an excessive use of resources, this can still render SEND non-operational.

Security associations based on the use of asymmetric cryptography can be vulnerable to Denial-of-Service attacks, particularly when the attacker can guess the SPIs and destination addresses used in the security associations. In SEND this is easy, as both the SPIs and the addresses (such as all nodes multicast address) are standardized.

Due to the use of multicast, one packet sent by the attacker will be processed by multiple receivers.

When CGA protection is used, SEND deals with these attacks using the verification process described in Section 5.2.2. In this process a simple hash verification of the CGA property of the address is performed first before performing the more expensive signature verification.

When trusted roots and certificates are used for address validation in SEND, the defenses are not quite as effective. Implementations SHOULD track the resources devoted to the processing of packets received with the AH_RSA_Sig transform, and start selectively dropping packets if too many resources are spent. Implementations MAY also drop first packets that are not protected with CGA.

The Authorization Delegation Discovery process may also be vulnerable to Denial-of-Service attacks. An attack may target a router by request a large number of delegation chains to be discovered for different roots. Routers SHOULD defend against such attacks by caching discovered information (including negative responses) and by limiting the number of different discovery processes they engage in.

Attackers may also target hosts by sending a large number of unnecessary certificate chains, forcing hosts to spend useless memory and verification resources for them. Hosts defend against such attacks by limiting the amount of resources devoted to the certificate chains and their verification. Hosts SHOULD also prioritize advertisements sent as a response to their requests above multicast advertisements.

12. IANA Considerations

This document defines two new ICMP message types, used in Authorization Delegation Discovery. These messages must be assigned ICMPv6 type numbers from the informational message range:

- The Delegation Chain Solicitation message, described in Section 6.1.
- The Delegation Chain Advertisement message, described in Section 6.2.

This document defines two new Neighbor Discovery [6] options, which must be assigned Option Type values within the option numbering space for Neighbor Discovery messages:

- The Trusted Root option, described in Section 6.3.
- The Certificate option, described in Section 6.4.
- The CGA option, described in Section 5.1.
- The Signature option, described in Section 5.2.
- The Timestamp option, described in Section 5.3.
- The Nonce option, described in Section 5.4.

This document defines a new name space for the Name Type field in the Trusted Root option. Future values of this field can be allocated using standards action [5].

Another new name space is allocated for the Cert Type field in the Certificate option. Future values of this field can be allocated using standards action [5].

13. Comparison to AH-Based Approach

This approach has the following benefits compared to the current Working Group document approach:

- The full implementation of the security mechanism, including Nonces and CGAs, exists within one module. There is no need to analyze the security of the mechanism across ND, IPsec, and possibly the CGA layers.

- The CGA part of the solution can easily be separated into its own optional specification, if IPR concerns can not be resolved. This is possible because the CGA handling is done in its own option. (The authorization method configuration flag is the only thing common to the CGA and Signature options.)

- No extensions or modifications of IPsec processing are required: SPD entries are not required to distinguish ICMP types, AH does not need to support public keys or CGAs, and destination address acgnostic security associations are not needed.

- It is not necessary to allocate a new multicast address to represent the solicited-node multicast address for SEND nodes.

- It is not necessary to change the Neighbor Discovery behavior with regards to the use of the unspecified address. Since all information is available within the Neighbor Discovery messages, unspecified source addresses can be used, still being able to correlate the CGA property with the Target Address in a Neighbor Solicitation during Duplicate Address Detection.

- The transition mechanisms for links with both SEND and non-SEND nodes are significantly simpler. In particular, non-SEND nodes will be able to receive DAD probes and other messages sent by the SEND nodes.

- Only a single set of Neighbor Discovery messages from the router needs to be transmitted on a link. This helps avoid extra overhead for mobility beacons and other frequently occurring messaging.

- Given that the asymmetric computations required in SEND are computationally expensive, it is necessary to control the number of these operations in order to avoid Denial-of-Service attacks. This control is easier to arrange with "application layer" information. For instance, a router need not verify more Router Solicitations with an unspecified source address than it can respond to according to the RFC 2461 rules.

- There is no need for an API to communicate certificate chains requests and certificate chains between the IPsec and Neighbor Discovery modules.

  Also, a good implementation of SEND would not require the user to configure it (beyond perhaps enabling it). In order to achieve this with IPsec, a set of policy entries needs to be automatically created upon system start. This may require an additional API.

- There is no need for the CGA parameters to be stored both in the IPsec and Neighbor Discovery modules, where they are needed for the construction of AH headers and addresses, respectively.

- It is not necessary to change existing BITS or BITW IPsec implementations to support SEND and AH_RSA_Sig. There are two problems associated with such changes:

  * A SEND implementation in such environment can not proceed until this modification has been completed.

  * Typical hardware that processes IPsec packets may not be easily changed to process asymmetric transforms. (Of course such packets can be passed to the main CPU at the node, assuming this can easily be done in the given implementation.)

- In addition, many IPsec implementations are highly optimized because they are on the fast path for packet processing. For example, the Linux implementation runs in the kernel interrupt thread. Some of the SEND modifications might require IPsec processing to wait on a semaphore while, for example, a certificate chain is fetched, an operation that takes place out of band in regular IPsec processing because it is done using IKE. While it is possible that the implemenation can be arranged so that general IPsec processing isn't impacted, the resulting code could increase in complexity.

The use of IPsec to protect ND is possible, but the limits and capabilities of IPsec have to be stretched. Small changes in the ND protocol (or our understanding of the issues) may cause a situation which is no longer easily handled when the "application" and the security exist at different layers. Although IPsec as defined in RFC 2402 just defines a header format, RFC 2401 and the ensuing years of implementation have evolved a complex interconnected set of components for IPsec which will require some modification to accommodate SEND.

On the other hand, IPsec is the current solution for securing ND in the original ND RFCs. Even if the current IPsec can be used only in

very limited networks to secure ND, it could be argued that it is logical to continue its use. Also, the existence of an asymmetric transform in IPsec would be potentially useful in other contexts as well.

Normative References

[1] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

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

[3] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[4] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[5] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

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

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

[8] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[9] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[10] Bassham, L., Polk, W. and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

[11] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[12] Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[13] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[14] Lynn, C., "X.509 Extensions for IP Addresses and AS Identifiers", Internet-Draft (expired)

draft-ietf-pkix-x509-ipaddr-as-extn-00, February 2002.

[15] Perkins, C., Johnson, D. and J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-22 (work in progress), May 2003.

[16] International Organization for Standardization, "The Directory - Authentication Framework", ISO Standard X.509, 2000.

[17] RSA Laboratories, "RSA Encryption Standard, Version 1.5", PKCS 1, November 1993.

[18] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

Informative References

[19] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[20] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[21] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[22] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[23] Arkko, J., "Effects of ICMPv6 on IKE and IPsec Policies", draft-arkko-icmpv6-ike-effects-01 (work in progress), June 2002.

[24] Arkko, J., "Manual SA Configuration for IPv6 Link Local Messages", draft-arkko-manual-icmpv6-sas-01 (work in progress), June 2002.

[25] Droms, R., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-dhcpv6-28 (work in progress), November 2002.

[26] Kent, S., "IP Encapsulating Security Payload (ESP)", draft-ietf-ipsec-esp-v3-04 (work in progress), March 2003.

[27] Aura, T., "Cryptographically Generated Addresses (CGA)", draft-ietf-send-cga-00.txt (work in progress), May 2003.

[28] Arkko, J., Kempf, J., Sommerfeld, B. and B. Zill, "SEcure Neighbor Discovery (SEND) Protocol", draft-ietf-send-ipsec-00.txt (work in progress), February 2003.

[29] Nikander, P., "IPv6 Neighbor Discovery trust models and threats", draft-ietf-send-psreq-00 (work in progress), October 2002.

[30] Montenegro, G. and C. Castelluccia, "SUCV Identifiers and Addresses", draft-montenegro-sucv-03 (work in progress), July 2002.

[31] O'Shea, G. and M. Roe, "Child-proof Authentication for MIPv6", Computer Communications Review, April 2001.

[32] Nikander, P., "Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World", Proceedings of the Cambridge Security Protocols Workshop, April 2001.

[33] Arkko, J., Aura, T., Kempf, J., Mantyla, V., Nikander, P. and M. Roe, "Securing IPv6 Neighbor Discovery", Wireless Security Workshop, September 2002.

[34] Montenegro, G. and C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses", NDSS, February 2002.

[35] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", IEEE Standard 802.1X, September 2001.

Author's Address

Jari Arkko
Ericsson
Jorvas 02420
Finland

EMail: jari.arkko@ericsson.com

Appendix A. Contributors

Most of the substantive material in this document has been derived from the current official Working Group item [28]. The authors of that document have deserve full credit for this document as well. All errors are mine, however.

Appendix B. Acknowledgements

The author would like to thank James Kempf, Pekka Nikander, Tuomas Aura, Ran Atkinson for interesting discussions in this problem space.

Appendix C. IPR Considerations

The optional CGA part of SEND uses public keys and hashes to prove address ownership. Several IPR claims have been made about such methods.

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

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