



# Implementing IPv6 Secure Neighbor Discovery

---

**First Published: February 27, 2009**

**Last Updated: February 27, 2009**

This document provides information about configuring the Secure Neighbor Discovery (SeND) protocol for IPv6.

The SeND feature is designed to counter the threats of the Neighbor Discovery Protocol (NDP). SeND defines a set of neighbor discovery options and two neighbor discovery messages. SeND also defines a new autoconfiguration mechanism to establish address ownership.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Implementing SeND for IPv6”](#) section on page 35.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS, image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Implementing SeND for IPv6, page 2](#)
- [Information About Implementing SeND for IPv6, page 2](#)
- [How to Implement SeND for IPv6, page 7](#)
- [Configuration Examples for Implementing SeND for IPv6, page 28](#)
- [Additional References, page 33](#)
- [Feature Information for Implementing SeND for IPv6, page 35](#)
- [Glossary, page 36](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

# Prerequisites for Implementing SeND for IPv6

SeND feature is available on crypto images because it involves using cryptographic libraries.

## Information About Implementing SeND for IPv6

To configure the SeND protocol for IPv6, you should understand the following concepts:

- [IPv6 Neighbor Discovery Trust Models and Threats, page 2](#)
- [SeND Protocol, page 2](#)
- [SeND Deployment Models, page 3](#)

## IPv6 Neighbor Discovery Trust Models and Threats

There are three IPv6 neighbor discovery trust models, which are described as follows:

- All authenticated nodes trust each other to behave correctly at the IP layer and not to send any neighbor discovery or router discovery (RD) messages that contain false information. This model represents a situation where the nodes are under a single administration and form a closed or semiclosed group. A corporate intranet is an example of this model.
- A router trusted by the other nodes in the network to be a legitimate router that routes packets between the local network and any connected external networks. This router is trusted to behave correctly at the IP layer and not to send any neighbor discovery or RD messages that contain false information. This model represents a public network run by an operator. The clients pay the operator, have the operator's credentials, and trust the operator to provide the IP forwarding service. The clients do not trust each other to behave correctly; any other client node must be considered able to send falsified neighbor discovery and RD messages.
- A model where the nodes do not directly trust each other at the IP layer. This model is considered suitable where a trusted network operator is not available.

Nodes on the same link use NDP to discover each other's presence and link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors. NDP is used by both hosts and routers. The original NDP specifications used IPsec to protect NDP messages. However, not many detailed instructions for using IPsec are available. The number of manually configured security associations needed for protecting NDP can be very large, which makes that approach impractical for most purposes. These threats need to be considered and eliminated.

## SeND Protocol

The SeND protocol counters NDP threats. It defines a set of new ND options, and two new ND messages (Certification Path Solicitation (CPS) and Certification Path Answer (CPA)). It also defines a new autoconfiguration mechanism to be used in conjunction with the new ND options to establish address ownership.

SeND defines the mechanisms defined in the following sections for securing the NDP:

- [Cryptographically Generated Address, page 3](#)
- [Authorization Delegation Discovery, page 3](#)

## Cryptographically Generated Address

Cryptographically generated addresses (CGAs) are IPv6 addresses generated from the cryptographic hash of a public key and auxiliary parameters. This provides a method for securely associating a cryptographic public key with an IPv6 address in the SeND protocol.

The node generating a CGA address must first obtain a Rivest, Shamir, and Adelman (RSA) key pair (SeND uses an RSA public/private key pair). The node then computes the interface identifier part (which is the rightmost 64 bits) and appends the result to the prefix to form the CGA address.

CGA address generation is a one-time event. A valid CGA cannot be spoofed and the CGA parameters received associated to it is reused because the message must be signed with the private key that matches the public key used for CGA generation, which only the address owner will have.

A user cannot replay the complete SeND message (including the CGA address, CGA parameters, and CGA signature) because the signature has only a limited lifetime.

## Authorization Delegation Discovery

Authorization delegation discovery is used to certify the authority of routers by using a trust anchor. A trust anchor is a third party that the host trusts and to which the router has a certification path. At a basic level, the router is certified by the trust anchor. In a more complex environment, the router is certified by a user that is certified by the trust anchor. In addition to certifying the router identity (or the right for a node to act as a router), the certification path contains information about prefixes that a router is allowed to advertise in router advertisements. Authorization delegation discovery enables a node to adopt a router as its default router.

## SeND Deployment Models

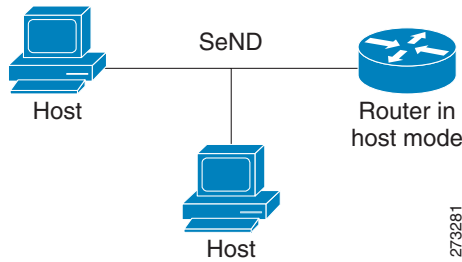
This section describes the following SeND deployment models:

- [Host-to-Host Deployment Without a Trust Anchor, page 3](#)
- [Neighbor Solicitation Flow, page 4](#)
- [Host-Router Deployment Model, page 5](#)
- [Router Advertisement and Certificate Path Flows, page 5](#)
- [Single CA Model, page 6](#)

### Host-to-Host Deployment Without a Trust Anchor

Deployment for SeND between hosts is straightforward. The hosts can generate a pair of RSA keys locally, autoconfigure their CGA addresses, and use them to validate their sender authority, rather than using a trust anchor to establish sender authority. [Figure 1](#) illustrates this model.

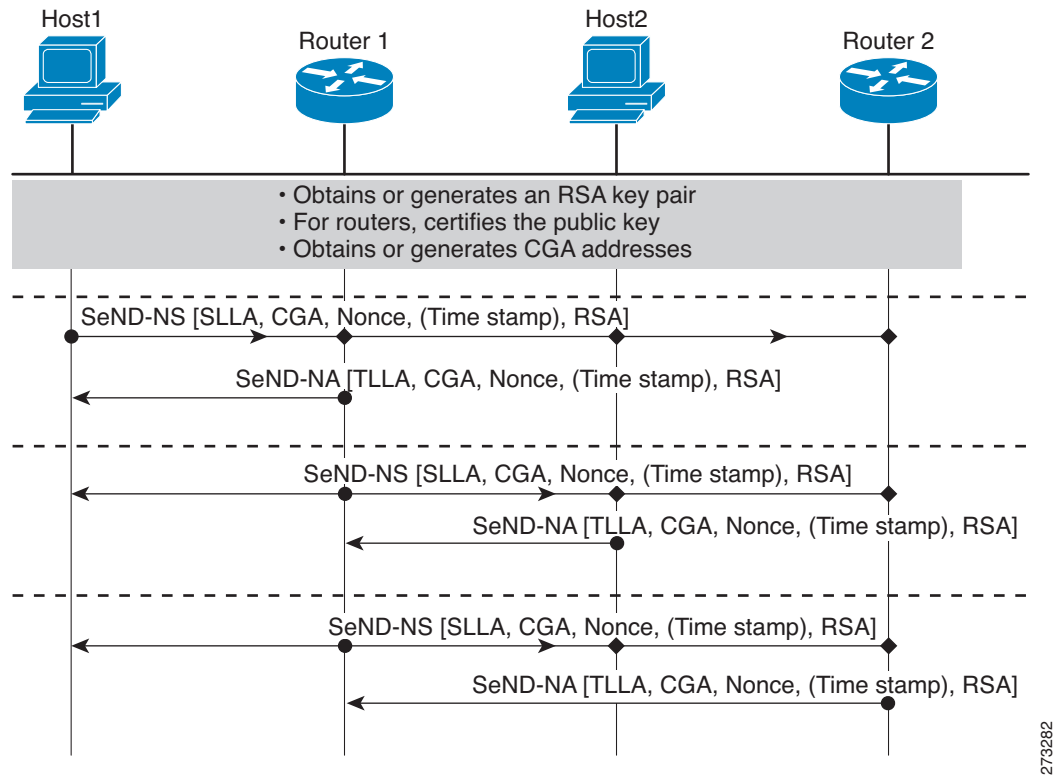
**Figure 1** *Host-to-Host Deployment Model*



## Neighbor Solicitation Flow

In a neighbor solicitation scenario, hosts and routers in host mode exchange neighbor solicitations and neighbor advertisements. These neighbor solicitations and neighbor advertisements are secured with CGA addresses and CGA options, and have nonce, time stamp, and RSA neighbor discovery options. [Figure 2](#) illustrates this scenario.

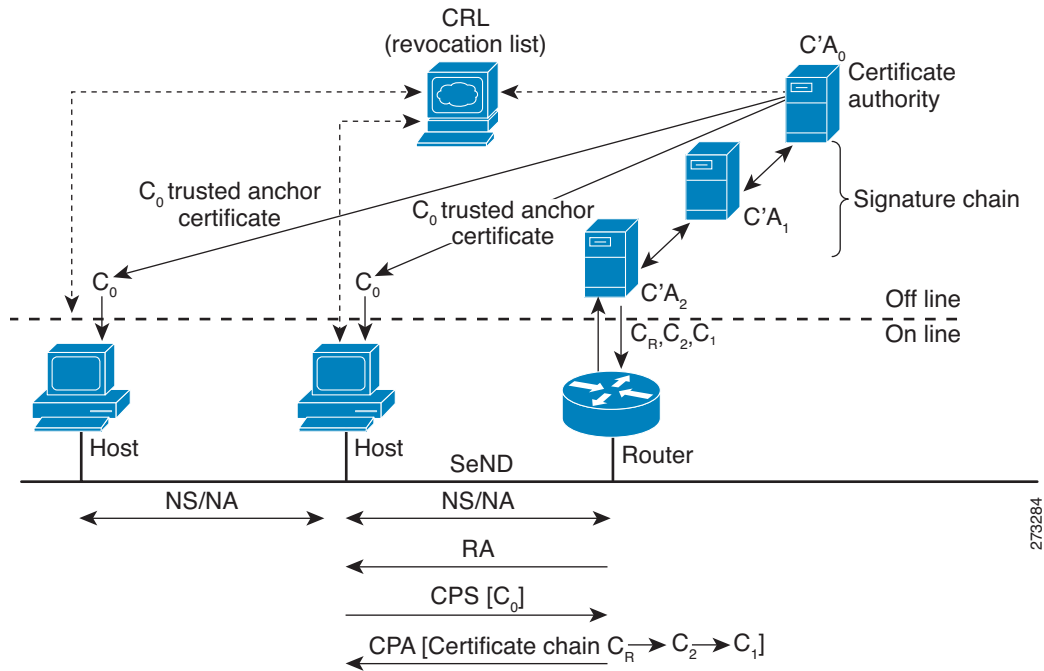
**Figure 2** *Neighbor Solicitation Flow*



## Host-Router Deployment Model

In many cases, hosts will not have access to the infrastructure that will enable them to obtain and announce their certificates. In these situations, hosts will secure their relationship using CGA, and secure their relationship with routers using a trusted anchor. When using router advertisements (RAs), SeND mandates that routers are authenticated through a trust anchor. Figure 3 illustrates this scenario.

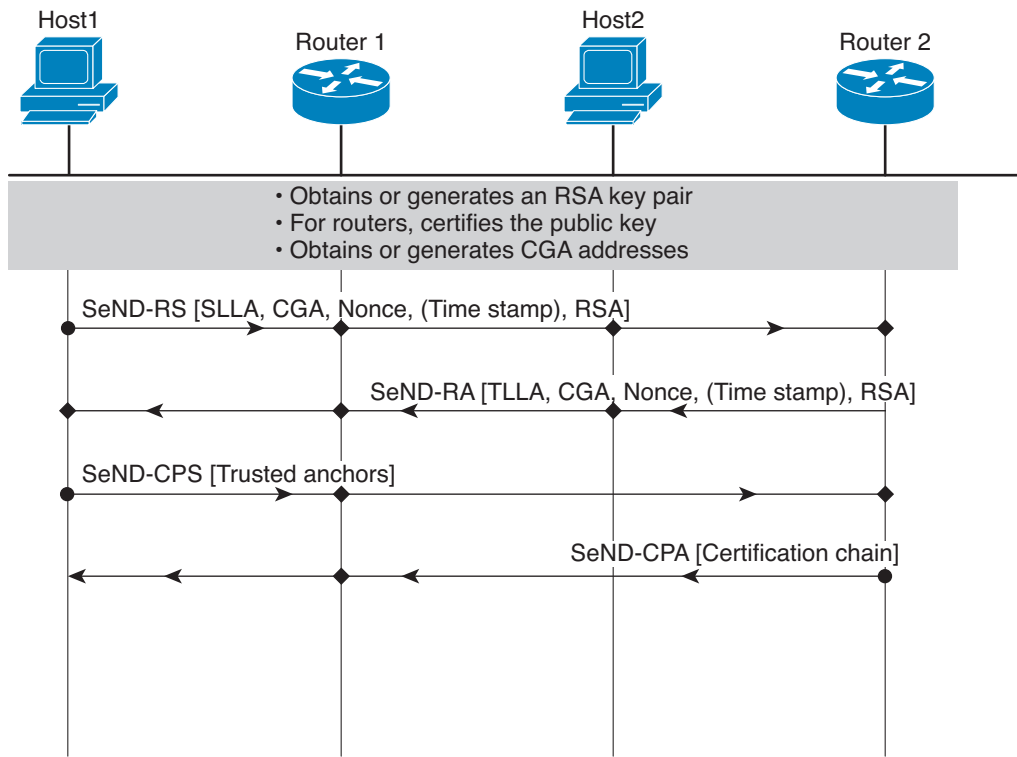
Figure 3 Host-Router Deployment Model



## Router Advertisement and Certificate Path Flows

Figure 4 shows the certificate exchange performed using certification path solicitation CPS/CPA SeND messages. In the illustration, Router R is certified (using an X.509 certificate) by its own CA (certificates C<sub>R</sub>). The CA itself (CA<sub>2</sub>) is certified by its own CA (certificates C<sub>2</sub>), and so on, up to a CA (CA<sub>0</sub>) that the hosts trusts. The certificate C<sub>R</sub> contains IP extensions per RFC 3779, which describes which prefix ranges the router R is allowed to announce (in RAs). This prefix range, certified by CA<sub>2</sub>, is a subset of CA<sub>2</sub>'s own range, certified by CA<sub>1</sub>, and so on. Part of the validation process when a certification chain is received consists of validating the certification chain and the consistency of nested prefix ranges.

**Figure 4 Router Advertisement and Certificate Path Flows**

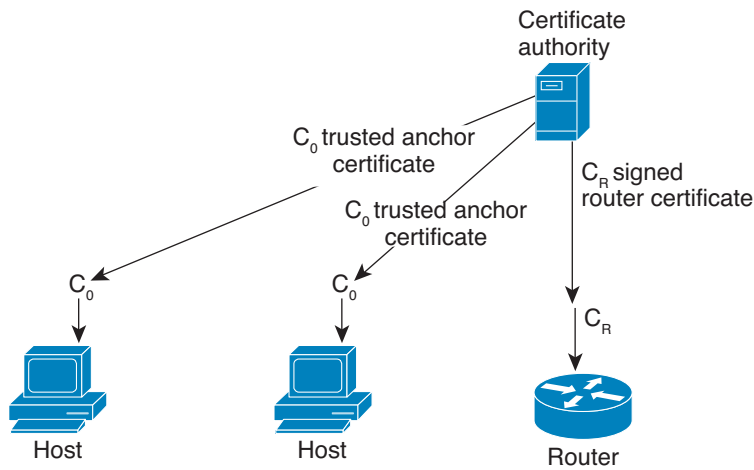


273285

## Single CA Model

The deployment model shown in Figure 3 can be simplified in an environment where both hosts and routers trust a single CA such as the Cisco certification server (CS). Figure 5 illustrates this model.

**Figure 5 Single CA Deployment Model**



273286

# How to Implement SeND for IPv6

The following sections describe how to configure the certificate server, the host and the router:

- [Configuring Certificate Servers to Enable SeND, page 8](#) (required)
- [Configuring a Host to Enable SeND, page 10](#) (required)
- [Configuring a Router to Enable SeND, page 12](#) (required)

To configure SeND on a Cisco device, you must understand the following concepts:

- [Certificate Servers, page 7](#)
- [Host, page 7](#)
- [Router, page 7](#)

## Certificate Servers

Certificate servers are used to grant certificates after validating or certifying key pairs. A tool for granting certificates is mandatory in any SeND deployment. Many tools are available to grant certificates, for example, Open Secure Sockets Layer (OpenSSL) on Linux. However, very few certificate servers support granting certificates containing IP extensions. Cisco IOS certificate servers support every kind of certificate including the certificates containing the IP extensions. For more information on Cisco IOS certificates, refer to the [Configuring and Managing a Cisco IOS Certificate Server](#) module in the *Cisco IOS Security Configuration Guide*.

## Host

SeND is available in host mode. The set of available functions on a host will be a subset of SeND functionality. CGA will be fully available and the prefix authorization delegation will be supported on the host side (sending CPS and receiving CPA).

To implement SeND, configure the host with the following parameters:

- An RSA key pair used to generate CGA addresses on the interface.
- A SeND modifier that is computed using the RSA key pair.
- A key on the SeND interface.
- CGAs on the SeND interface.
- A Public Key Infrastructure (PKI) trustpoint, with minimum content; for example, the URL of the certificate server. A trust anchor certificate must be provisioned on the host.

## Router

SeND is available in router mode. You can use the **ipv6 unicast-routing** command to configure a node to a router. To implement SeND, configure routers with the same elements as that of the host. The routers will need to retrieve certificates of their own from a certificate server. The RSA key and subject name of the trustpoint are used to retrieve certificates from a certificate server. Once the certificate has been obtained and uploaded, the router generates a certificate request to the certificate server and installs the certificate.

Following is a summary of operations to be performed before SeND is configured on the host or router:

- Hosts are configured with one or more trust anchors.

- Hosts are configured with an RSA key pair or configured with the capability to locally generate it. Note that for hosts not establishing their own authority via a trust anchor, these keys are not certified by any CA.
- Routers are configured with RSA keys and corresponding certificate chains, or the capability to obtain these certificate chains that match the host trust anchor at some level of the chain.

While booting, hosts and routers must either retrieve or generate their CGAs. Typically, routers will autoconfigure their CGAs once and save them (along with the key pair used in the CGA operation) into their permanent storage. At a minimum, link-local addresses on a SeND interface should be CGAs. Additionally, global addresses can be CGAs.

## Configuring Certificate Servers to Enable SeND

Hosts and routers must be configured with RSA key pairs and corresponding certificate chains before the SeND parameters are configured. Perform the following task to configure the certificate server to grant certificates. Once the certificate server is configured, other parameters for the certificate server can be configured.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki trustpoint *name***
5. **ip-extension [multicast | unicast] {inherit [ipv4 | ipv6] | prefix *ipaddress* | range *min-ipaddress* *max-ipaddress*}**
6. **revocation-check {[crl] [none] [ocsp]}**
7. **exit**
8. **crypto pki server *name***
9. **grant auto**
10. **cdp-url *url-name***
11. **no shutdown**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>ip http server</code>  <b>Example:</b> Router(config)# ip http server	Configures the HTTP server.
Step 4	<code>crypto pki trustpoint name</code>  <b>Example:</b> Router(config)# crypto pki trustpoint CA	(Optional) Declares the trustpoint that your certificate server should use and enters ca-trustpoint configuration mode.  <ul style="list-style-type: none"> <li>If you plan to use X.509 IP extensions, use this command. To automatically generate a CS trustpoint, go to <a href="#">Step 8</a>.</li> </ul>
Step 5	<code>ip-extension [multicast   unicast] {inherit [ipv4   ipv6]   prefix ipaddress   range min-ipaddress max-ipaddress}</code>  <b>Example:</b> Router(ca-trustpoint)# ip-extension prefix 2001:100::/32	(Optional) Specifies that the IP extensions are included in a certificate request either for enrollment or generation of a certificate authority (CA) for the Cisco IOS CA.
Step 6	<code>revocation-check {[crl] [none] [ocsp]}</code>  <b>Example:</b> Router(ca-trustpoint)# revocation-check crl	(Optional) Sets one or more methods for revocation checking.
Step 7	<code>exit</code>  <b>Example:</b> Router(ca-trustpoint)# exit	Returns to global configuration mode.
Step 8	<code>crypto pki server name</code>  <b>Example:</b> Router(config)# crypto pki server CA	Configures the PKI server and places the router in server configuration mode.
Step 9	<code>grant auto</code>  <b>Example:</b> Router(config-server)# grant auto	(Optional) Grants all certificate requests automatically.
Step 10	<code>cdp-url url-name</code>  <b>Example:</b> Router(config-server)# cdp-url http://209.165.202.129/CA.crl	(Optional) Sets the URL name if the host is using a Certificate Revocation List (CRL).
Step 11	<code>no shutdown</code>  <b>Example:</b> Router(config-server)# no shutdown	Enables the certificate server.

## Configuring a Host to Enable SeND

SeND is available in host mode. Before you can configure SeND parameters in host mode, first configure the host using the following commands. Once the host has been configured, SeND parameters can be configured on it.

### Summary Steps

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** [general-keys | usage-keys | signature | encryption] [label *key-label*] [exportable] [modulus *modulus-size*] [storage *devicename:*] [on *devicename:*]
4. **ipv6 cga modifier rsakeypair** *key-label* sec-level {0 | 1}
5. **crypto pki trustpoint** *name*
6. **enrollment** [mode] [retry period *minutes*] [retry count *number*] url *url* [pem]
7. **revocation-check** {[crl] [none] [ocsp]}
8. **exit**
9. **crypto pki authenticate** *name*
10. **ipv6 nd secured sec-level minimum** *value*
11. **interface** *type number*
12. **ipv6 cga rsakeypair** *key-label*
13. **ipv6 address** *ipv6-address/prefix-length* link-local cga
14. **ipv6 nd secured trustanchor** *trustanchor-name*
15. **ipv6 nd secured timestamp** {delta *value* | fuzz *value*}
16. **exit**
17. **ipv6 nd secured full-secure**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Host> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Host# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p><b>crypto key generate rsa</b> [general-keys   usage-keys   signature   encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename:] [on devicename:]</p> <p><b>Example:</b> Host(config)# crypto key generate rsa label SEND modulus 1024</p>	Configures the RSA key.
Step 4	<p><b>ipv6 cga modifier rsakeypair</b> key-label sec-level {0   1}</p> <p><b>Example:</b> Host(config)# ipv6 cga modifier rsakeypair SEND sec-level 1</p>	Enables the RSA key to be used by SeND (generates the modifier).
Step 5	<p><b>crypto pki trustpoint</b> name</p> <p><b>Example:</b> Host(config)# crypto pki trustpoint SEND</p>	Specifies the node trustpoint and enters ca-trustpoint configuration mode.
Step 6	<p><b>enrollment</b> [mode] [retry period minutes] [retry count number] url url [pem]</p> <p><b>Example:</b> Host(ca-trustpoint)# enrollment url http://209.165.200.254</p>	Specifies the enrollment parameters of a CA.
Step 7	<p><b>revocation-check</b> {[crl] [none] [ocsp]}</p> <p><b>Example:</b> Host(ca-trustpoint)# revocation-check none</p>	Sets one or more methods of revocation.
Step 8	<p><b>exit</b></p> <p><b>Example:</b> Host(ca-trustpoint)# exit</p>	Returns to global configuration mode.
Step 9	<p><b>crypto pki authenticate</b> name</p> <p><b>Example:</b> Host(config)# crypto pki authenticate SEND</p>	Authenticates the certification authority (by getting the certificate of the CA).
Step 10	<p><b>ipv6 nd secured sec-level minimum</b> value</p> <p><b>Example:</b> Host(config)# ipv6 nd secured sec-level minimum 1</p>	<p>(Optional) Configures CGA.</p> <ul style="list-style-type: none"> <li>You can provide additional parameters such as security level and key size.</li> <li>In the example, the security level accepted by peers is configured.</li> </ul>
Step 11	<p><b>interface</b> type number</p> <p><b>Example:</b> Host(config)# interface fastethernet 0/0</p>	Specifies an interface type and number, and places the router in interface configuration mode.

	Command or Action	Purpose
Step 12	<code>ipv6 cga rsakeypair key-label</code>  <b>Example:</b> Host(config-if)# ipv6 cga rsakeypair SEND	(Optional) Configures CGA on interfaces.
Step 13	<code>ipv6 address ipv6-address/prefix-length link-local cga</code>  <b>Example:</b> Host(config-if)# ipv6 address FE80::260:3EFF:FE11:6770/23 link-local cga	Configures an IPv6 link-local address for the interface and enables IPv6 processing on the interface.
Step 14	<code>ipv6 nd secured trustanchor trustanchor-name</code>  <b>Example:</b> Host(config-if)# ipv6 nd secured trustanchor SEND	(Optional) Configures trusted anchors to be preferred for certificate validation.
Step 15	<code>ipv6 nd secured timestamp {delta value   fuzz value}</code>  <b>Example:</b> Host(config-if)# ipv6 nd secured timestamp delta 300	(Optional) Configures the timing parameters.
Step 16	<code>exit</code>  <b>Example:</b> Host(config-if)# exit	Returns to global configuration mode.
Step 17	<code>ipv6 nd secured full-secure</code>  <b>Example:</b> Host(config)# ipv6 nd secured full-secure	(Optional) Configures general SeND parameters. <ul style="list-style-type: none"> <li>In the example, secure mode is configured on SeND.</li> </ul>

## Configuring a Router to Enable SeND

SeND is available in the router mode. Before you can configure SeND parameters in router mode, first configure the router using the following commands. Once the router has been configured, the SeND parameters can be configured on it.

### Summary Steps

- enable
- configure terminal
- crypto key generate rsa [general-keys | usage-keys | signature | encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename:] [on devicename:]
- ipv6 cga modifier rsakeypair key-label sec-level {0 | 1}
- crypto pki trustpoint name
- subject-name [attr tag] [eq | ne | co | nc] string

7. **rsa**keypair *key-label*
8. **revocation-check** {[crl] [none] [ocsp]}
9. **exit**
10. **crypto pki authenticate** *name*
11. **crypto pki enroll** *name*
12. **ipv6 nd secured sec-level** [minimum *value*]
13. **interface** *type number*
14. **ipv6 cga rsa**keypair *key-label*
15. **ipv6 address** *ipv6-address/prefix-length link-local cga*
16. **ipv6 nd secured trustanchor** *trustanchor-name*
17. **ipv6 nd secured timestamp** {delta *value* | fuzz *value*}
18. **exit**
19. **ipv6 nd secured full-secure**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>crypto key generate rsa</b> [general-keys   usage-keys   signature   encryption] [label <i>key-label</i> ] [exportable] [modulus <i>modulus-size</i> ] [storage <i>devicename:</i> ] [on <i>devicename:</i> ]  <b>Example:</b> Router(config)# crypto key generate rsa label SEND modulus 1024	Configures the RSA key.
<b>Step 4</b>	<b>ipv6 cga modifier rsa</b> keypair <i>key-label</i> <b>sec-level</b> {0   1}  <b>Example:</b> Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1	Enables the RSA key to be used by SeND (generates the modifier).
<b>Step 5</b>	<b>crypto pki trustpoint</b> <i>name</i>  <b>Example:</b> Router(config)# crypto pki trustpoint SEND	Configures PKI for a single or multiple-tier CA, specifies the router trustpoint, and places the router in ca-trustpoint configuration mode.

	Command or Action	Purpose
Step 6	<p><b>subject-name</b> [<i>attr tag</i>] [<i>eq</i>   <i>ne</i>   <i>co</i>   <i>nc</i>] <i>string</i></p> <p><b>Example:</b> Router(ca-trustpoint)# subject-name C=FR, ST=PACA, L=Example, O=Cisco, OU=NSSTG, CN=router</p>	Creates a rule entry.
Step 7	<p><b>rsa</b>keypair <i>key-label</i></p> <p><b>Example:</b> Router(ca-trustpoint)# rsa</p>	Binds the RSA key pair for SeND.
Step 8	<p><b>revocation-check</b> {[<i>cr1</i>] [<i>none</i>] [<i>ocsp</i>]}</p> <p><b>Example:</b> Router(ca-trustpoint)# revocation-check none</p>	Sets one or more methods of revocation.
Step 9	<p><b>exit</b></p> <p><b>Example:</b> host(ca-truspoint)# exit</p>	Returns to global configuration mode.
Step 10	<p><b>crypto pki authenticate</b> <i>name</i></p> <p><b>Example:</b> host(config)# crypto pki authenticate SEND</p>	Authenticates the certification authority (by getting the certificate of the CA).
Step 11	<p><b>crypto pki enroll</b> <i>name</i></p> <p><b>Example:</b> Router(config)# crypto pki enroll SEND</p>	Obtains the certificates for the router from the CA.
Step 12	<p><b>ipv6 nd secured sec-level minimum</b> <i>value</i></p> <p><b>Example:</b> Router(config)# ipv6 nd secured sec-level minimum 1</p>	<p>(Optional) Configures CGA and provides additional parameters such as security level and key size.</p> <ul style="list-style-type: none"> <li>In the example, the minimum security level that SeND accepts from its peers is configured.</li> </ul>
Step 13	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b> Router(config)# interface fastethernet 0/0</p>	Specifies an interface type and number, and places the router in interface configuration mode.
Step 14	<p><b>ipv6 cga rsa</b>keypair <i>key-label</i></p> <p><b>Example:</b> Router(config-if)# ipv6 cga rsa</p>	<p>(Optional) Configures CGA on interfaces.</p> <ul style="list-style-type: none"> <li>In the example, CGA is generated.</li> </ul>
Step 15	<p><b>ipv6 address</b> <i>ipv6-address/prefix-length</i> <b>link-local cga</b></p> <p><b>Example:</b> Router(config-if)# ipv6 address fe80::link-local cga</p>	Configures an IPv6 link-local address for the interface and enables IPv6 processing on the interface.

	Command or Action	Purpose
Step 16	<code>ipv6 nd secured trustanchor trustpoint-name</code>  <b>Example:</b> Router(config-if)# ipv6 nd secured trustanchor SEND	(Optional) Configures trusted anchors to be preferred for certificate validation.
Step 17	<code>ipv6 nd secured timestamp {delta value   fuzz value}</code>  <b>Example:</b> Router(config-if)# ipv6 nd secured timestamp delta 300	(Optional) Configures the timing parameters.
Step 18	<code>exit</code>  <b>Example:</b> Router(config-if)# exit	Returns to global configuration mode.
Step 19	<code>ipv6 nd secured full-secure</code>  <b>Example:</b> Router(config)# ipv6 nd secured full-secure	(Optional) Configures general SeND parameters, such as secure mode and authorization method. <ul style="list-style-type: none"> <li>In the example, SeND security mode is enabled.</li> </ul>

## How to Implement SeND

The tasks in the following sections explain how to implement SeND:

- [Creating the RSA Key Pair and CGA Modifier for the Key Pair, page 15](#) (required)
- [Configuring Certificate Enrollment for a PKI, page 16](#) (required)
- [Configuring a Cryptographically Generated Address, page 19](#) (required)
- [Configuring SeND Parameters, page 21](#) (optional)

### Creating the RSA Key Pair and CGA Modifier for the Key Pair

To create the RSA key pair and the CGA modifier for the key pair, perform the following task.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto key generate rsa [general-keys | usage-keys | signature | encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename:] [on devicename:]`
4. `ipv6 cga modifier rsakeypair key-label sec-level {0 | 1}`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto key generate rsa</b> [general-keys   usage-keys   signature   encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename:] [on devicename:]  <b>Example:</b> Router(config)# crypto key generate rsa label SeND	Generates RSA key pairs.
Step 4	<b>ipv6 cga modifier rsakeypair</b> key-label sec-level {0   1}  <b>Example:</b> Router(config)# ipv6 cga modifier rsakeypair SeND sec-level 1	Generates the CGA modifier for a specified RSA key, which enables the key to be used by SeND.

## Configuring Certificate Enrollment for a PKI

Certificate enrollment, which is the process of obtaining a certificate from a CA, occurs between the end host that requests the certificate and the CA. Each peer that participates in the PKI must enroll with a CA.

In IPv6, you can autoenroll or manually enroll the device certificate. The following task describes how to configure certificate enrollment for a PKI.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** name
4. **subject-name** [x.500-name]
5. **enrollment** [mode] [retry period minutes] [retry count number] url url [pem]
6. **serial-number** [none]
7. **auto-enroll** [percent] [regenerate]
8. **password** string
9. **rsakeypair** key-label [key-size [encryption-key-size]]
10. **fingerprint** ca-fingerprint

11. **ip-extension** [multicast | unicast] {inherit [ipv4 | ipv6] | prefix *ipaddress* | range *min-ipaddress* *max-ipaddress*}
12. **exit**
13. **crypto pki authenticate** *name*
14. **exit**
15. **copy** [/erase] [/verify | /noverify] *source-url* *destination-url*
16. **show crypto pki certificates**
17. **show crypto pki trustpoints** [status | label [status]]

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>crypto pki trustpoint</b> <i>name</i>  <b>Example:</b> Router(config)# crypto pki trustpoint trustpoint1	Declares the trustpoint that your router should use and enters ca-trustpoint configuration mode.
<b>Step 4</b>	<b>subject-name</b> [ <i>x.500-name</i> ]  <b>Example:</b> Router(ca-trustpoint)# subject-name name1	Specifies the subject name in the certificate request.
<b>Step 5</b>	<b>enrollment</b> [mode] [retry period <i>minutes</i> ] [retry count <i>number</i> ] url <i>url</i> [pem]  <b>Example:</b> Router(ca-trustpoint)# enrollment url http://name1.example.com	Specifies the URL of the CA on which your router should send certificate requests.
<b>Step 6</b>	<b>serial-number</b> [none]  <b>Example:</b> Router(ca-trustpoint)# serial-number	(Optional) Specifies the router serial number in the certificate request.
<b>Step 7</b>	<b>auto-enroll</b> [percent] [regenerate]  <b>Example:</b> Router(ca-trustpoint)# auto-enroll	(Optional) Enables autoenrollment, allowing you to automatically request a router certificate from the CA.

	Command or Action	Purpose
Step 8	<b>password</b> <i>string</i>  <b>Example:</b> Router(ca-trustpoint)# password password1	(Optional) Specifies the revocation password for the certificate.
Step 9	<b>rsakeypair</b> <i>key-label</i> [ <i>key-size</i> [ <i>encryption-key-size</i> ]]  <b>Example:</b> Router(ca-trustpoint)# rsakeypair SEND	Specifies which key pair to associate with the certificate.
Step 10	<b>fingerprint</b> <i>ca-fingerprint</i>  <b>Example:</b> Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E	(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.
Step 11	<b>ip-extension</b> [ <b>multicast</b>   <b>unicast</b> ] { <b>inherit</b> [ <b>ipv4</b>   <b>ipv6</b> ]   <b>prefix</b> <i>ipaddress</i>   <b>range</b> <i>min-ipaddress max-ipaddress</i> }	Add IP extensions (IPv6 prefixes or range) to verify prefix list the router is allowed to advertise.
Step 12	<b>exit</b>  <b>Example:</b> Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 13	<b>crypto pki authenticate</b> <i>name</i>  <b>Example:</b> Router(config)# crypto pki authenticate name1	Retrieves and authenticates the CA certificate. <ul style="list-style-type: none"> <li>This command is optional if the CA certificate is already loaded into the configuration.</li> </ul>
Step 14	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 15	<b>copy</b> [ <b>/erase</b> ] [ <b>/verify</b>   <b>/noverify</b> ] <i>source-url destination-url</i>  <b>Example:</b> Router# copy system:running-config nvram:startup-config	(Optional) Copies the running configuration to the NVRAM startup configuration.

	Command or Action	Purpose
Step 16	<code>show crypto pki certificates</code>  <b>Example:</b> Router# show crypto pki certificates	(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.
Step 17	<code>show crypto pki trustpoints [status   label [status]]</code>  <b>Example:</b> Router# show crypto pki trustpoints name1	(Optional) Displays the trustpoints configured in the router.

## Configuring a Cryptographically Generated Address

To configure a CGA, perform the following tasks:

- [Configuring General CGA Parameters, page 19](#) (required)
- [Configuring CGA Address Generation on an Interface, page 20](#) (required)

## Configuring General CGA Parameters

To configure general CGA parameters such as security level and key size, perform the following task.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 nd secured sec-level [minimum value]`
4. `ipv6 nd secured key-length [[minimum | maximum] value]`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>ipv6 nd secured sec-level [minimum value]</code>  <b>Example:</b> Router(config)# ipv6 nd secured sec-level minimum 1	Configures the SeND security level.
Step 4	<code>ipv6 nd secured key-length [[minimum   maximum] value]</code>  <b>Example:</b> Router(config)# ipv6 nd secured key-length minimum 512	Configures SeND key-length options.

## Configuring CGA Address Generation on an Interface

To configure CGA address generation on an interface, perform the following task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 cga rsakeypair** *key-label*
5. **ipv6 address** {*ipv6-address/prefix-length [cga]* | *prefix-name sub-bits/prefix-length [cga]*}

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type number</code>  <b>Example:</b> Router(config)# interface Ethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.

	Command or Action	Purpose
Step 4	<pre>ipv6 cga rsakeypair key-label</pre> <p><b>Example:</b> Router(config-if)# ipv6 cga rsakeypair SEND</p>	Specifies which RSA key pair should be used on a specified interface.
Step 5	<pre>ipv6 address { ipv6-address/prefix-length [cga]   prefix-name sub-bits/prefix-length [cga] }</pre> <p><b>Example:</b> Router(config-if)# ipv6 address 2001:0DB8:1:1::/64 cga</p>	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface. <ul style="list-style-type: none"> <li>The <b>cga</b> keyword generates a CGA address.</li> </ul> <p><b>Note</b> The CGA link-local addresses must be configured by using the <b>ipv6 address link-local</b> command.</p>

## Configuring SeND Parameters

To configure SeND, perform the following tasks:

- [Configuring the SeND Trustpoint, page 21](#) (optional)
- [Configuring SeND Trust Anchors on the Interface, page 24](#) (optional)
- [Configuring Secured and Nonsecured Neighbor Discovery Message Coexistence Mode, page 25](#) (optional)
- [Configuring SeND Parameters Globally, page 26](#) (optional)
- [Configuring the SeND Time Stamp, page 27](#) (optional)

## Configuring the SeND Trustpoint

In the router mode, the key pair used to generate the CGA addresses on an interface must be certified by the CA and the certificate sent on demand over the SeND protocol. One RSA key pair and associated certificate is enough for SeND to operate; however, users may use several keys, identified by different labels. SeND and CGA refer to a key directly by label or indirectly by trustpoint.

Multiple steps are required to bind SeND to a trustpoint. First a key pair is generated. Then the device refers to it in a trustpoint. Then the SeND interface configuration points to the trustpoint. There are two reasons for the multiple steps:

- The same key pair can be used on several SeND interfaces
- The trustpoint contains additional information, such as the certificate, required for SeND to perform authorization delegation

A CA certificate must be uploaded for the referred trustpoint. The referred trustpoint is in reality a trusted anchor.

Several trustpoints can be configured, pointing to the same RSA keys, on a given interface. This function is useful if different hosts have different trusted anchors (that is, CAs that they trust). The router can provide each host with the certificate signed by the CA they trust.

To configure the SeND trustpoint, perform the following task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]
4. **ipv6 cga modifier rsakeypair** *key-label* **sec-level** {0 | 1}
5. **crypto pki trustpoint** *name*
6. **subject-name** [*x.500-name*]
7. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
8. **enrollment terminal** [**pem**]
9. **ip-extension** [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress* *max-ipaddress*}
10. **exit**
11. **crypto pki authenticate** *name*
12. **crypto pki enroll** *name*
13. **crypto pki import** *name* **certificate**
14. **interface** *type number*
15. **ipv6 nd secured trustpoint** *trustpoint-name*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto key generate rsa</b> [ <b>general-keys</b>   <b>usage-keys</b>   <b>signature</b>   <b>encryption</b> ] [ <b>label</b> <i>key-label</i> ] [ <b>exportable</b> ] [ <b>modulus</b> <i>modulus-size</i> ] [ <b>storage</b> <i>devicename:</i> ] [ <b>on</b> <i>devicename:</i> ]  <b>Example:</b> Router(config)# crypto key generate rsa label SEND	Generates RSA key pairs.
Step 4	<b>ipv6 cga modifier rsakeypair</b> <i>key-label</i> <b>sec-level</b> {0   1}  <b>Example:</b> Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1	Generates the CGA modifier for a specified RSA key, which enables the key to be used by SeND.

	Command or Action	Purpose
Step 5	<p><b>crypto pki trustpoint</b> <i>name</i></p> <p><b>Example:</b> Router(config)# crypto pki trustpoint trustpoint1</p>	Declares the trustpoint that your router should use and enters ca-trustpoint configuration mode.
Step 6	<p><b>subject-name</b> [<i>x.500-name</i>]</p> <p><b>Example:</b> Router(ca-trustpoint)# subject-name name1</p>	Specifies the subject name in the certificate request.
Step 7	<p><b>rsa</b>keypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]]</p> <p><b>Example:</b> Router(ca-trustpoint)# rsa keypair SEND</p>	Specifies which key pair to associate with the certificate.
Step 8	<p><b>enrollment terminal</b> [<i>pem</i>]</p> <p><b>Example:</b> Router(ca-trustpoint)# enrollment terminal</p>	Specifies manual cut-and-paste certificate enrollment.
Step 9	<p><b>ip-extension</b> [<i>multicast</i>   <i>unicast</i>] {<i>inherit</i> [<i>ipv4</i>   <i>ipv6</i>]   <i>prefix ipaddress</i>   <i>range min-ipaddress max-ipaddress</i>}</p> <p><b>Example:</b> Router(ca-trustpoint)# ip-extension unicast prefix 2001:100:1::/48</p>	Adds IP extensions to the router certificate request.
Step 10	<p><b>exit</b></p> <p><b>Example:</b> Router(ca-trustpoint)# exit</p>	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 11	<p><b>crypto pki authenticate</b> <i>name</i></p> <p><b>Example:</b> Router(config)# crypto pki authenticate trustpoint1</p>	Authenticates the certification authority (by getting the certificate of the CA).
Step 12	<p><b>crypto pki enroll</b> <i>name</i></p> <p><b>Example:</b> Router(config)# crypto pki enroll trustpoint1</p>	Obtains the certificates for your router from the CA.
Step 13	<p><b>crypto pki import</b> <i>name certificate</i></p> <p><b>Example:</b> Router(config)# crypto pki import trustpoint1 certificate</p>	Imports a certificate manually via TFTP or as a cut-and-paste at the terminal.

	Command or Action	Purpose
Step 14	<code>interface type number</code>  <b>Example:</b> Router(config)# interface Ethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 15	<code>ipv6 nd secured trustpoint trustpoint-name</code>  <b>Example:</b> Router(config-if)# ipv6 nd secured trustpoint trustpoint1	Enables SeND on an interface and specifies which trustpoint should be used.

## Configuring SeND Trust Anchors on the Interface

This task can be performed only in host mode. The host must be configured with one or more trust anchors. As soon as SeND is bound to a trustpoint on an interface (see [“Configuring the SeND Trustpoint” section on page 21](#)), this trustpoint is also a trust anchor.

A trust anchor configuration consists of the following items:

- A public key signature algorithm and associated public key, which may include parameters
- A name
- An optional public key identifier
- An optional list of address ranges for which the trust anchor is authorized

Because PKI has already been configured, the trust anchor configuration is accomplished by binding SeND to one or several PKI trustpoints. PKI is used to upload the corresponding certificates, which contain the required parameters (such as name and key).

This is an optional task. It allows you to select trust anchors listed in the CPS when requesting for a certificate. If you opt not to configure trust anchors, all the PKI trustpoints configured on the host will be considered.

To configure a trusted anchor on the interface perform the following task:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto pki trustpoint name`
4. `enrollment terminal [pem]`
5. `exit`
6. `crypto pki authenticate name`
7. `interface type number`
8. `ipv6 nd secured trustanchor trustanchor-name`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto pki trustpoint name</b>  <b>Example:</b> Router(config)# crypto pki trustpoint anchor1	Declares the trustpoint that your router should use and enters ca-trustpoint configuration mode.
Step 4	<b>enrollment terminal [pem]</b>  <b>Example:</b> Router(ca-trustpoint)# enrollment terminal	Specifies manual cut-and-paste certificate enrollment.
Step 5	<b>exit</b>  <b>Example:</b> Router(ca-trustpoint)# exit	Returns to global configuration.
Step 6	<b>crypto pki authenticate name</b>  <b>Example:</b> Router(config)# crypto pki authenticate anchor1	Authenticates the certification authority (by getting the certificate of the CA).
Step 7	<b>interface type number</b>  <b>Example:</b> Router(config)# interface Ethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 8	<b>ipv6 nd secured trustanchor trustanchor-name</b>  <b>Example:</b> Router(config-if)# ipv6 nd secured trustanchor anchor1	Specifies a trusted anchor on an interface and binds SeND to a trustpoint.

## Configuring Secured and Nonsecured Neighbor Discovery Message Coexistence Mode

During the transition to SeND secured interfaces, network operators may want to run a particular interface with a mixture of nodes accepting secured and unsecured neighbor discovery messages. To configure the coexistence mode for secure and nonsecure neighbor discovery messages on the same interface, perform the following task.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd secured trustpoint** *trustpoint-name*
5. **no ipv6 nd secured full-secure**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface Ethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
<b>Step 4</b>	<b>ipv6 nd secured trustpoint</b> <i>trustpoint-name</i>  <b>Example:</b> Router(config-if)# ipv6 nd secured trustpoint trustpoint1	Enables SeND on an interface and specifies which trustpoint should be used.
<b>Step 5</b>	<b>no ipv6 nd secured full-secure</b>  <b>Example:</b> Router(config-if)# no ipv6 nd secured full-secure	Provides the coexistence mode for secure and nonsecure neighbor discovery messages on the same interface.

**Configuring SeND Parameters Globally**

To configure SeND parameters globally, perform the following optional task.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ipv6 nd secured key-length** [[**minimum** | **maximum**] *value*]
4. **ipv6 nd secured sec-level minimum** *value*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 nd secured key-length</b> [[minimum   maximum] value]  <b>Example:</b> Router(config)# ipv6 nd secured key-length minimum 512	Configures the SeND key-length options.
Step 4	<b>ipv6 nd secured sec-level minimum</b> value  <b>Example:</b> Router(config)# ipv6 nd secured sec-level minimum 2	Configures the minimum security level value that can be accepted from peers.

## Configuring the SeND Time Stamp

To configure SeND time stamp on an interface, perform the following optional task.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd secured timestamp** { **delta** *value* | **fuzz** *value* }

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>interface type number</code>  <b>Example:</b> Router(config)# interface Ethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	<code>ipv6 nd secured timestamp {delta value   fuzz value}</code>  <b>Example:</b> Router(config-if)# ipv6 nd secured timestamp delta 600	Configures the SeND time stamp.

## Configuration Examples for Implementing SeND for IPv6

This section provides the following configuration examples:

- [Configuring Certificate Servers: Example, page 28](#)
- [Configuring a Host to Enable SeND: Example, page 29](#)
- [Configuring a Router to Enable SeND: Example, page 30](#)
- [Configuring a SeND Trustpoint in Router Mode: Example, page 32](#)
- [Configuring SeND Trust Anchors in the Host Mode: Example, page 32](#)
- [Configuring CGA Address Generation on an Interface: Example, page 32](#)

### Configuring Certificate Servers: Example

The following example shows how to configure certificate servers:

```
crypto pki server CA
 issuer-name C=FR, ST=fr, L=example, O=cisco, OU=nsstg, CN=CA0 lifetime ca-certificate
 700 !
crypto pki trustpoint CA
 ip-extension prefix 2001::/16
 revocation-check crl
 rsakeypair CA
 no shutdown
```



#### Note

If you need to configure certificate servers without IP extensions, do not use the **ip-extension** command.

To display the certificate servers with IP extensions, use the **show crypto pki certificates verbose** command:

```
Router# show crypto pki certificates verbose

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    c=FR
    st=fr
```

```

l=example
o=cisco
ou=nsstg
cn=CA0
Subject:
c=FR
st=fr
l=example
o=cisco
ou=nsstg
cn=CA0
Validity Date:
start date: 09:50:52 GMT Feb 5 2009
end date: 09:50:52 GMT Jan 6 2011
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: MD5 with RSA Encryption
Fingerprint MD5: 87DB764F 29367A65 D05CEE3D C12E0AC3
Fingerprint SHA1: 04A06602 86AA72E9 43F2DB33 4A7D40A2 E2ED3325
X509v3 extensions:
X509v3 Key Usage: 86000000
Digital Signature
Key Cert Sign
CRL Signature
X509v3 Subject Key ID: 75B477C6 B2CA7BBE C7866657 57C84A32 90CEFB5A
X509v3 Basic Constraints:
CA: TRUE
X509v3 Authority Key ID: 75B477C6 B2CA7BBE C7866657 57C84A32 90CEFB5A
Authority Info Access:
X509v3 IP Extension:
IPv6:
2001::/16
Associated Trustpoints: CA

```

## Configuring a Host to Enable SeND: Example

The following example shows how to configure a host to enable SeND:

```

enable
configure terminal
crypto key generate rsa label SEND modulus 1024
The name for the keys will be: SEND
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
ipv6 cga modifier rsakeypair SEND sec-level 1
crypto pki trustpoint SEND
enrollment url http://209.165.200.254
revocation-check none
exit
crypto pki authenticate SEND
Certificate has the following attributes:
Fingerprint MD5: FC99580D 0A280EB4 2EB9E72B 941E9BDA
Fingerprint SHA1: 22B10EF0 9A519177 145EA4F6 73667837 3A154C53
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
ipv6 nd secured sec-level minimum 1
interface fastethernet 0/0
ipv6 cga rsakeypair SEND
ipv6 address FE80::260:3EFF:FE11:6770 link-local cga
ipv6 nd secured trustanchor SEND
ipv6 nd secured timestamp delta 300

```

```

exit
ipv6 nd secured full-secure

```

To verify the configuration use the **show running-config** command:

```

host# show running-config

Building configuration...
[snip]
crypto pki trustpoint SEND
  enrollment url http://209.165.200.225
  revocation-check none
!
interface Ethernet1/0
 ip address 209.165.202.129 255.255.255.0
 duplex half
 ipv6 cga rsakeypair SEND
 ipv6 address 2001:100::/64 cga

```

## Configuring a Router to Enable SeND: Example

The following example shows how to configure the router to enable SeND:

```

enable
configure terminal
crypto key generate rsa label SEND modulus 1024
ipv6 cga modifier rsakeypair SEND sec-level 1
crypto pki trustpoint SEND
  subject-name C=FR, ST=PACA, L=Example, O=Cisco, OU=NSSTG, CN=router
  rsakeypair SEND
  revocation-check none
exit
crypto pki authenticate SEND
Certificate has the following attributes:
  Fingerprint MD5: FC99580D 0A280EB4 2EB9E72B 941E9BDA
  Fingerprint SHA1: 22B10EF0 9A519177 145EA4F6 73667837 3A154C53
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
crypto pki enroll SEND
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:

% The subject name in the certificate will include: C=FR, ST=fr, L=example, O=cisco,
OU=nsstg, CN=route r % The subject name in the certificate will include: Router % Include
the router serial number in the subject name? [yes/no]: no % Include an IP address in the
subject name? [no]:

Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate
Authority % The 'show crypto pki certificate SEND verbose' command will show the
fingerprint.

*Feb  5 09:40:37.171: CRYPTO_PKI: Certificate Request Fingerprint MD5:
A6892F9F 23561949 4CE96BB8 CBC85 E64
*Feb  5 09:40:37.175: CRYPTO_PKI: Certificate Request Fingerprint SHA1:
30832A66 E6EB37DF E578911D 383F 96A0 B30152E7
*Feb  5 09:40:39.843: %PKI-6-CERTRET: Certificate received from Certificate Authority

```

```

interface fastethernet 0/0
  ipv6 nd secured sec-level minimum 1
  ipv6 cga rsakeypair SEND
  ipv6 address fe80::link-local cga
  ipv6 nd secured trustanchor SEND
  ipv6 nd secured timestamp delta 300
  exit
ipv6 nd secured full-secure

```

To verify that the certificates are generated, use the **show crypto pki certificates** command:

```
Router# show crypto pki certificates
```

```

Certificate
  Status: Available
  Certificate Serial Number: 0x15
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: Router
    hostname=Router
    c=FR
    st=fr
    l=example
    o=cisco
    ou=nsstg
    cn=router
  Validity Date:
    start date: 09:40:38 UTC Feb 5 2009
    end   date: 09:40:38 UTC Feb 5 2010
  Associated Trustpoints: SEND

```

```

CA Certificate
  Status: Available
  Certificate Serial Number: 0x1
  Certificate Usage: Signature
  Issuer:
    cn=CA
  Subject:
    cn=CA
  Validity Date:
    start date: 10:54:53 UTC Jun 20 2008
    end   date: 10:54:53 UTC Jun 20 2011
  Associated Trustpoints: SEND

```

To verify the configuration, use the **show running-config** command:

```
Router# show running-config
```

```

Building configuration...
[snip]
crypto pki trustpoint SEND
  enrollment url http://209.165.201.1
  subject-name C=FR, ST=fr, L=example, O=cisco, OU=nsstg, CN=router  revocation-check none
rsakeypair SEND !
interface Ethernet1/0
  ip address 209.165.200.225 255.255.255.0
  duplex half
  ipv6 cga rsakeypair SEND
  ipv6 address FE80:: link-local cga
  ipv6 address 2001:100::/64 cga

```

## Configuring a SeND Trustpoint in Router Mode: Example

The following example shows how to configure a SeND trustpoint in router mode:

```
enable
configure terminal
crypto key generate rsa label SEND
  Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 778
% Generating 778 bit RSA keys, keys will be non-exportable...[OK]
ipv6 cga modifier rsakeypair SEND sec-level 1
crypto pki trustpoint trstpt1
  subject-name C=FR, ST=fr, L=example, O=cisco, OU=nsstg, CN=sa14-72b
  rsakeypair SEND
  enrollment terminal
  ip-extension unicast prefix 2001:100:1::/48
exit
crypto pki authenticate trstpt1
crypto pki enroll trstpt1
crypto pki import trstpt1 certificate
interface Ethernet 0/0
  ipv6 nd secured trustpoint trstpt1
```

## Configuring SeND Trust Anchors in the Host Mode: Example

The following example shows how to configure SeND trust anchors on an interface in the host mode:

```
enable
configure terminal
! Configure the location of the CS we trust !
crypto pki trustpoint B1
  enrollment terminal
  crypto pki authenticate anchor1
  exit
! Only Query a certificate signed by the CS at B2 on this interface !
interface Ethernet0/0
  ip address 204.209.1.54 255.255.255.0
  ipv6 cga rsakeypair SEND
  ipv6 address 2001:100::/64 cga
  ipv6 nd secured trustanchor anchor1
```

## Configuring CGA Address Generation on an Interface: Example

The following example shows how to configure CGA address generation on an interface:

```
enable
configure terminal
interface fastEthernet 0/0
  ipv6 cga rsakeypair SEND
  ipv6 address 2001:100::/64 cga
exit
```

# Additional References

The following sections provide references related to the Implementing SeND for IPv6 feature.

## Related Documents

Related Topic	Document Title
Configuring certificate enrollment for a PKI	“ <a href="#">Configuring Certificate Enrollment for a PKI</a> ” module in the <i>Cisco IOS Security Configuration Guide</i>

## Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 3756	<i>IPv6 Neighbor Discovery (ND) Trust Models and Threats</i>
RFC 3779	<i>X.509 Extensions for IP Addresses and AS Identifiers</i>
RFC 3971	<i>Secure Neighbor Discovery (SeND)</i>
RFC 3972	<i>Cryptographically Generated Addresses (CGA)</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Feature Information for Implementing SeND for IPv6

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(15)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the *Start Here: Cisco IOS Software Release Specifies for IPv6 Features* document.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



---

**Note**

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---

**Table 1** Feature Information for Implementing IPv6 Secure Neighbor Discovery

Feature Name	Releases	Feature Information
Secure Neighbor Discovery for Cisco IOS Software	12.4(24)T	<p>The Secure Neighbor Discovery (SeND) protocol is designed to counter the threats of the Neighbor Discovery Protocol. SeND defines a set of neighbor discovery options and two neighbor discovery messages. SeND also defines a new autoconfiguration mechanism to establish address ownership.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">How to Implement SeND for IPv6, page 7.</a></li> </ul> <p>The following commands were introduced:</p> <p><b>ipv6 cga modifier rsakeypair, ipv6 cga modifier rsakeypair (interface), ipv6 nd secured certificate-db, ipv6 nd secured full-secure, ipv6 nd secured full-secure (interface), ipv6 nd secured key-length, ipv6 nd secured sec-level, ipv6 nd secured timestamp, ipv6 nd secured timestamp-db, ipv6 nd secured trustanchor, ipv6 nd secured trustpoint, show ipv6 cga address-db, show ipv6 cga modifier-db, show ipv6 nd secured certificates, show ipv6 nd secured counters interface, show ipv6 nd secured nonce-db, show ipv6 nd secured timestamp-db.</b></p> <p>The following commands were modified:</p> <p><b>auto-enroll, crypto key generate rsa, crypto pki authenticate, crypto pki enroll, crypto pki import, enrollment terminal (ca-trustpoint), enrollment url (ca-trustpoint), fingerprint, ip-extension, ip http server, ipv6 address, ipv6 address link-local, password (ca-trustpoint), revocation-check, rsakeypair, serial-number (ca-trustpoint), subject-name.</b></p>

## Glossary

- **CA**—certification authority.
- **CGA**—cryptographically generated address.
- **CPA**—certificate path answer.
- **CPR**—certificate path response.
- **CPS**—certification path solicitation. The solicitation message used in the addressing process.
- **CRL**—certificate revocation list.
- **CS**—certification server.
- **CSR**—certificate signing request.
- **DAD**—duplicate address detection. A mechanism that ensures two IPv6 nodes on the same link are not using the same address.

- **DER**—distinguished encoding rules. An encoding scheme for data values.
- **nonce**—An unpredictable random or pseudorandom number generated by a node and used once. In SeND, nonces are used to assure that a particular advertisement is linked to the solicitation that triggered it.
- **non-SeND node**—An IPv6 node that does not implement SeND but uses only the Neighbor Discovery protocol without security.
- **NUD**—neighbor unreachability detection. A mechanism used for tracking neighbor reachability.
- **PKI**—public key infrastructure.
- **Router Authorization Certificate**—A public key certificate.
- **RD**—Router discovery allows the hosts to discover what routers exist on the link and what subnet prefixes are available. Router discovery is a part of the Neighbor Discovery protocol.
- **SeND node**—An IPv6 node that implements SeND.
- **trust anchor**—A trust anchor is an entity that the host trusts to authorize routers to act as routers. Hosts are configured with a set of trust anchors to protect router discovery.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

