IPv6 セキュア ネイバー ディスカバリの実装

このマニュアルでは、IPv6 用の Secure Neighbor Discovery（SeND; セキュア ネイバー ディスカバリ）プロトコルの実装について説明します。

SeND 機能は、Neighbor Discovery Protocol（NDP; ネイバー ディスカバリ プロトコル）の脅威に対処する設計になっています。SeND では、一連のネイバー ディスカバリ オプションと 2 つのネイバー ディスカバリ メッセージが定義されています。アドレスの所有者を設定する新しい自動設定メカニズムも定義されています。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「SeND for IPv6 の実装の機能情報」（P.33）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

SeND for IPv6 の実装の前提条件

SeND 機能は、暗号化ライブラリを使用するため、暗号イメージで使用できます。

SeND for IPv6 の実装に関する情報

IPv6 用の SeND プロトコルを設定するには、次の概念を理解する必要があります。

- 「IPv6 ネイバー ディスカバリの信頼モデルと脅威」（P.2）
- 「SeND プロトコル」（P.2）
- 「SeND 配置モデル」（P.3）

IPv6 ネイバー ディスカバリの信頼モデルと脅威

IPv6 ネイバー ディスカバリの信頼モデルは 3 つあります。これらのモデルについて、次に説明します。

- 認証されたすべてのノードは、IP レイヤで正しく動作し、偽りの情報が含まれたネイバー ディスカバリまたは Router Discovery（RD; ルータ ディスカバリ）メッセージを送信することはないと互いを信頼しています。このモデルは、ノードが単一の管理下にあり、非公開グループまたは半公開グループを形成する状況にあることを表します。このモデルの例として、企業イントラネットがあります。
- ネットワーク内の他のノードによって信頼されるルータが正規のルータとなり、ローカル ネットワークと接続された外部ネットワークの間でパケットをルーティングします。このルータは、IP レイヤで正しく動作し、偽りの情報が含まれたネイバー ディスカバリまたは RD メッセージを送信することはないと信頼されています。このモデルは、オペレータによってパブリック ネットワークが運用されていることを表します。クライアントは、オペレータに対して支払いを行うことでオペレータのクレデンシャルを受け取ります。オペレータが IP 転送サービスを提供するとクライアントは信頼しています。クライアントは、互いのことを正しく動作すると信頼していません。他のクライアント ノードは偽りのネイバー ディスカバリおよび RD メッセージを送信する可能性があると見なされます。
- ノードが IP レイヤで相互に直接信頼しないモデル。このモデルは、信頼されたネットワーク オペレータが利用できない場合に適していると考えられます。

同じリンク上のノードは、相互の存在とリンク層アドレスの検出、ルータの検出、およびアクティブ ネイバーへのパスに関する到達可能性情報の保持に NDP を使用します。NDP は、ホストとルータの両方で使用されます。初期の NDP 仕様では、IPsec を使用して NDP メッセージを保護していました。ただし、IPsec の使用に関する詳細な手順はあまりありません。NDP の保護に必要な、手動で設定されたセキュリティ アソシエーションの数が非常に多くなる可能性があるため、このアプローチはほとんどの用途に実用的ではありません。このような脅威を考慮し、排除する必要があります。

SeND プロトコル

SeND プロトコルは、NDP の脅威に対処します。SeND では、一連の新しい ND オプションと 2 つの新しい ND メッセージ（Certification Path Solicitation（CPS; 認証パス請求）と Certification Path Answer（CPA; 認証パス応答））が定義されています。新しい自動設定メカニズムも定義されており、そのメカニズムを新しい ND オプションと組み合せてアドレスの所有者を設定できます。

SeND に定義されている、NDP を保護するためのメカニズムについては、次の各項で説明します。

- 「暗号化生成アドレス」（P.3）

暗号化生成アドレス

Cryptographically Generated Address（CGA; 暗号化生成アドレス）は、公開鍵と補助パラメータの暗号ハッシュから生成された IPv6 アドレスです。これにより、SeND プロトコルで暗号公開鍵を IPv6 アドレスに安全に関連付けることができます。

まず、CGA アドレスを生成するノードで Rivest, Shamir, and Adelman（RSA; Rivest、Shamir、および Adelman）キー ペア（SeND では RSA の公開鍵と秘密鍵のペアを使用）を取得する必要があります。次に、ノードはインターフェイス ID 部分（右端の 64 ビット）を計算し、その結果をプレフィクスに付加して CGA アドレスを形成します。

CGA アドレスの生成は、ワンタイム イベントです。有効な CGA はスプーフィングできず、それに関連付けられた受信 CGA パラメータは再利用されます。これは、メッセージには、アドレスの所有者だけが持っている CGA の生成に使用された公開鍵に一致する秘密鍵で署名する必要があるからです。

シグニチャのライフタイムには制限があるため、ユーザは、CGA アドレス、CGA パラメータ、および CGA シグニチャを含む完全な SeND メッセージを再送できません。

権限委任ディスカバリ

権限委任ディスカバリは、トラスト アンカーを使用したルータの権限の認証に使用します。トラスト アンカーは、ホストが信頼する第三者であり、ルータにはトラスト アンカーへの認証パスがあります。基本的なレベルでは、ルータはトラスト アンカーによって認証されます。複雑な環境では、ルータはトラスト アンカーによって認証されたユーザによって認証されます。ルータ アイデンティティ（またはノードがルータとして機能するための権限）を認証する以外に、認証パスには、ルータがルータ アドバタイズメントでアドバタイズできるプレフィクスに関する情報が含まれます。権限委任ディスカバリを使用すると、ノードはルータをデフォルト ルータとして採用できます。

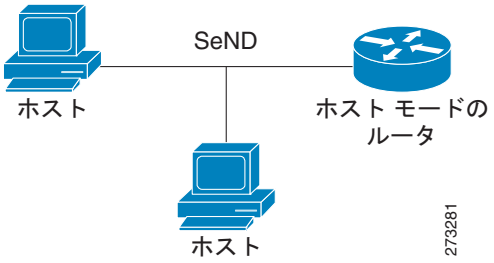
SeND 配置モデル

ここでは、次の SeND 配置モデルについて説明します。

トラスト アンカーのないホスト間配置

ホスト間への SeND の配置は単純です。ホストは、トラスト アンカーを使用して送信元の権限を確立するのではなく、RSA キー ペアをローカルに生成し、CGA アドレスを自動設定して、送信元の権限を検証します。図 1 に、このモデルを示します。

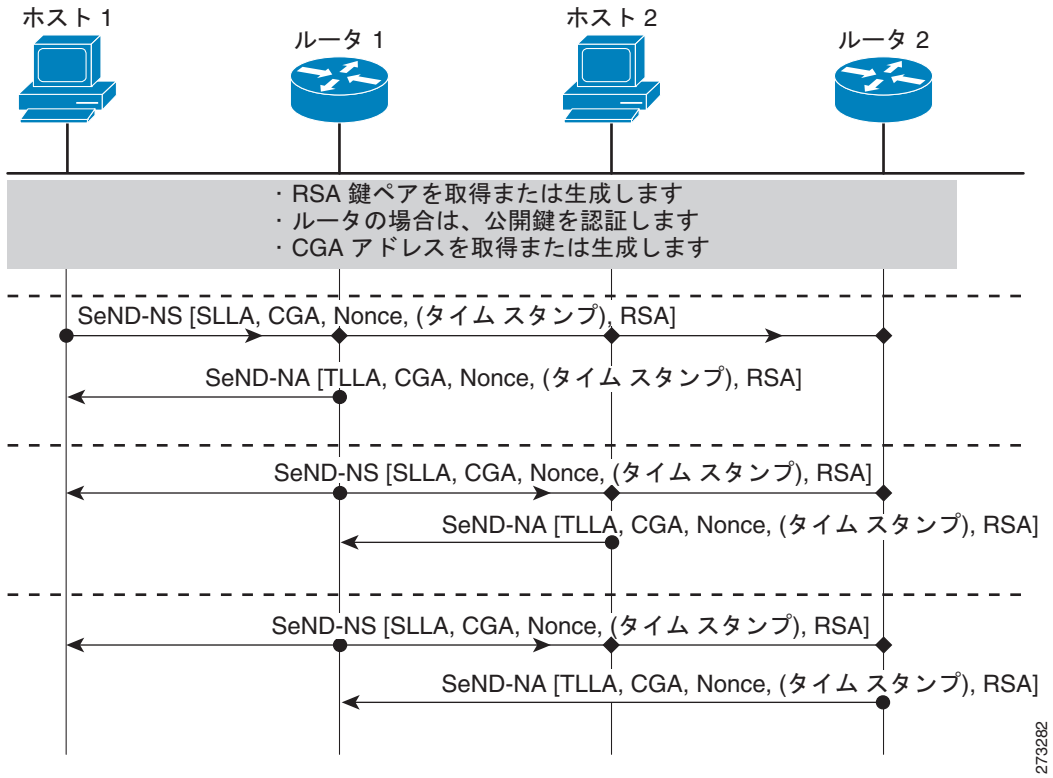
図 1　ホスト間配置モデル



ネイバー請求フロー

ネイバー請求シナリオでは、ホストおよびホスト モードのルータは、ネイバー請求とネイバー アドバタイズメントを交換します。これらのネイバー請求とネイバー アドバタイズメントは、CGA アドレスと CGA オプションで保護され、ナンス、タイムスタンプ、および RSA ネイバー ディスカバリ オプションが含まれます。図 2 に、このシナリオを示します。

図 2　ネイバー請求フロー

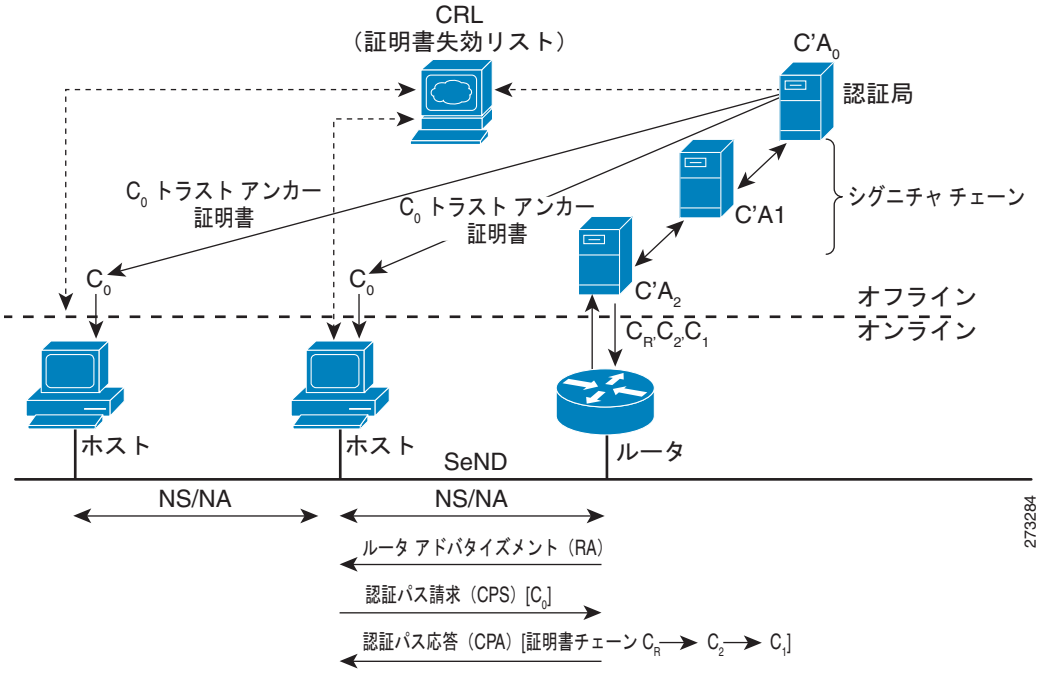


ホストとルータ間の配置モデル

多くの場合、ホストは証明書を取得したりアナウンスしたりできるインフラストラクチャにアクセスできません。このような場合、ホストは CGA を使用して関係を保護し、トラスト アンカーを使用してルータとの関係を保護します。Router Advertisement（RA; ルータ アドバタイズメント）を使用する場

合、トラスト アンカーを使用してルータを認証する必要があります。図 3 に、このシナリオを示します。

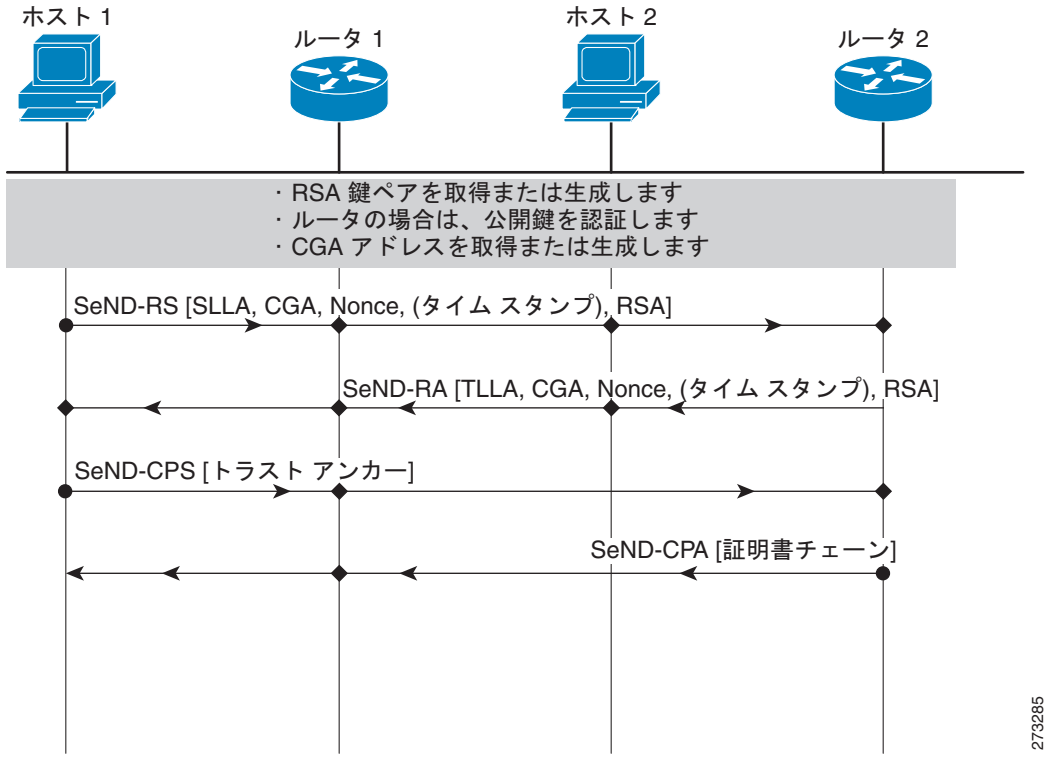
図 3　ホストとルータ間の配置モデル



ルータ アドバタイズメントと認証パスのフロー

図 4 に、認証パス請求の CPS/CPA SeND メッセージを使用して実行される証明書交換を示します。この図では、ルータ R は X.509 証明書を使用して独自の CA（証明書 CR）によって認証されます。CA 自体（CA2）は、独自の CA（証明書 C2）によって認証され、最終的にはホストが信頼する CA（CA0）によって認証されます。証明書 CR には、RFC 3779 に従った IP 拡張が含まれており、ルータ R が RA でアナウンスできるプレフィクス範囲が記述されています。CA2 によって認証されるこのプレフィクス範囲は、CA1 によって認証される CA2 独自の範囲のサブセットです。証明書チェーンの受信時の検証プロセスでは、証明書チェーンおよび入れ子になったプレフィクス範囲の一貫性が検証されます。

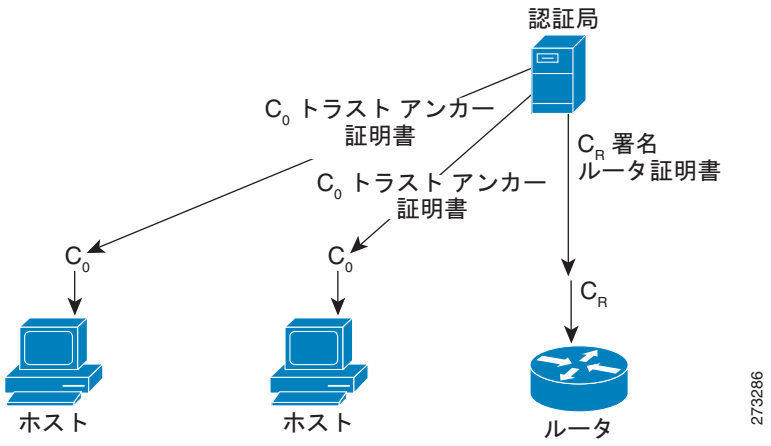
図 4　ルータ アドバタイズメントと認証パスのフロー



単一 CA モデル

図 3 に示す配置モデルは、ホストとルータの両方がシスコの Certification Server（CS; 証明書サーバ）などの単一の CA を信頼する環境で簡略化できます。図 5 に、このモデルを示します。

図 5　単一 CA 配置モデル



SeND for IPv6 の実装方法

ここでは、証明書サーバ、ホスト、およびルータを設定する方法について説明します。

- 「証明書サーバによる SeND のイネーブル化の設定」（P.8）（必須）
- 「ホストによる SeND のイネーブル化の設定」（P.10）（必須）
- 「ルータによる SeND のイネーブル化の設定」（P.12）（必須）

シスコ デバイスで SeND を設定するには、次の概念を理解する必要があります。

- 「証明書サーバ」（P.7）
- 「ホスト」（P.7）
- 「ルータ」（P.7）

証明書サーバ

証明書サーバは、キー ペアの検証および認証後に証明書を許可するために使用されます。SeND の配置では、証明書を許可するためのツールが必須です。Linux 上の Open Secure Sockets Layer（OpenSSL）など、証明書の許可に使用できるツールは多数あります。ただし、IP 拡張を含む証明書の許可をサポートする証明書サーバはごく少数です。Cisco IOS 証明書サーバは、IP 拡張を含む証明書などのあらゆる種類の証明書をサポートします。Cisco IOS 証明書の詳細については、『*Cisco IOS Security Configuration Guide*』の「*Configuring and Managing a Cisco IOS Certificate Server*」の章を参照してください。

ホスト

SeND はホスト モードで使用できます。ホストで使用できる機能は、SeND 機能のサブセットです。CGA は完全に使用可能であり、プレフィクス権限委任は CPS の送信と CPA の受信を行うホスト側でサポートされます。

SeND を実装するには、ホストに次のパラメータを設定します。

- インターフェイス上の CGA アドレスの生成に使用する RSA キー ペア。
- RSA キー ペアを使用して計算される SeND 修飾子。
- SeND インターフェイス上のキー。
- SeND インターフェイス上の CGA。
- コンテンツが最小限の Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）トラストポイント。たとえば、証明書サーバの URL。トラスト アンカーの証明書をホスト上でプロビジョニングする必要があります。

ルータ

SeND はルータ モードで使用できます。**ipv6 unicast-routing** コマンドを使用すると、ノードをルータに設定できます。SeND を実装するには、ルータにホストと同じ要素を設定します。ルータは証明書サーバから独自の証明書を取得する必要があります。証明書サーバから証明書を取得するために、トラストポイントの RSA キーと所有者名が使用されます。証明書を取得してアップロードすると、ルータは証明書サーバに対する証明書要求を生成し、証明書をインストールします。

ホストまたはルータで SeND を設定する前に実行する操作の概要を次に示します。

- ホストに 1 つ以上のトラスト アンカーを設定します。

- ホストに RSA キー ペアを設定するか、RSA キー ペアをローカルに生成する機能を設定します。トラスト アンカーを通じて独自の権限を設定していないホストの場合、これらのキーは CA によって認証されません。
- ルータに RSA キーと対応する証明書チェーンを設定するか、またはチェーンのあるレベルでホストのトラスト アンカーに一致するこれらの証明書チェーンを取得する機能を設定します。

ホストとルータは、起動時に CGA を取得するか、または生成する必要があります。一般的に、ルータは CGA を自動設定して（CGA 操作で使用したキー ペアとともに）永続的なストレージに保存します。少なくとも、SeND インターフェイス上のリンクローカル アドレスを CGA にする必要があります。また、グローバル アドレスを CGA にすることができます。

証明書サーバによる SeND のイネーブル化の設定

SeND パラメータを設定する前に、ホストとルータに RSA キー ペアと対応する証明書チェーンを設定する必要があります。証明書を許可するように証明書サーバを設定するには、次の作業を実行します。証明書サーバを設定したら、証明書サーバの他のパラメータを設定できます。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip http server** **例：** `Router(config)# ip http server`	HTTP サーバを設定します。
ステップ 4	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint CA`	（任意）証明書サーバが使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • X.509 IP 拡張を使用する場合は、このコマンドを使用します。CS トラストポイントを自動的に生成する場合は、ステップ 8 に移動します。
ステップ 5	**ip-extension** [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*} **例：** `Router(ca-trustpoint)# ip-extension prefix 2001:100::/32`	（任意）Cisco IOS CA の Certificate Authority（CA; 認証局）の登録または生成の証明書要求に IP 拡張を含めることを指定します。
ステップ 6	**revocation-check** {[**crl**] [**none**] [**ocsp**]} **例：** `Router(ca-trustpoint)# revocation-check crl`	（任意）1 つ以上の失効チェック方式を設定します。
ステップ 7	**exit** **例：** `Router(ca-trustpoint)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**crypto pki server** *name* **例：** `Router(config)# crypto pki server CA`	PKI サーバを設定し、ルータをサーバ コンフィギュレーション モードにします。
ステップ 9	**grant auto** **例：** `Router(config-server)# grant auto`	（任意）すべての証明書要求を自動的に許可します。
ステップ 10	**cdp-url** *url-name* **例：** `Router(config-server)# cdp-url http://209.165.202.129/CA.crl`	（任意）ホストで Certificate Revocation List（CRL; 証明書失効リスト）を使用する場合は、URL 名を設定します。
ステップ 11	**no shutdown** **例：** `Router(config-server)# no shutdown`	証明書サーバをイネーブルにします。

ホストによる SeND のイネーブル化の設定

SeND はホスト モードで使用できます。ホスト モードで SeND パラメータを設定する前に、まず次のコマンドを使用してホストを設定します。ホストを設定したら、そのホストで SeND パラメータを設定できます。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Host> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Host# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename*:] [**on** *devicename*:] **例：** `Host(config)# crypto key generate rsa label SEND modulus 1024`	RSA キーを設定します。
ステップ 4	**ipv6 cga modifier rsakeypair** *key-label* **sec-level** {**0** | **1**} **例：** `Host(config)# ipv6 cga modifier rsakeypair SEND sec-level 1`	SeND で RSA キーを使用できるようにします（修飾子を生成します）。
ステップ 5	**crypto pki trustpoint** *name* **例：** `Host(config)# crypto pki trustpoint SEND`	ノードのトラストポイントを指定し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	**enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**] **例：** `Host(ca-trustpoint)# enrollment url http://209.165.200.254`	CA の登録パラメータを指定します。
ステップ 7	**revocation-check {[crl] [none] [ocsp]}** **例：** `Host(ca-trustpoint)# revocation-check none`	1 つ以上の失効チェック方式を設定します。
ステップ 8	**exit** **例：** `Host(ca-trustpoint)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**crypto pki authenticate** *name* **例：** `Host(config)# crypto pki authenticate SEND`	CA の証明書を取得して、認証局を認証します。
ステップ 10	**ipv6 nd secured sec-level minimum** *value* **例：** `Host(config)# ipv6 nd secured sec-level minimum 1`	（任意）CGA を設定します。 • セキュリティ レベルやキー サイズなどの追加パラメータを指定できます。 • 例では、ピアによって受け入れられるセキュリティ レベルが設定されています。
ステップ 11	**interface** *type number* **例：** `Host(config)# interface fastethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 12	**ipv6 cga rsakeypair** *key-label* **例：** `Host(config-if)# ipv6 cga rsakeypair SEND`	（任意）インターフェイス上の CGA を設定します。
ステップ 13	**ipv6 address** *ipv6-address/prefix-length* **link-local cga** **例：** `Host(config-if)# ipv6 address FE80::260:3EFF:FE11:6770/23 link-local cga`	インターフェイスの IPv6 リンクローカル アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 14	**ipv6 nd secured trustanchor** *trustanchor-name* **例：** `Host(config-if)# ipv6 nd secured trustanchor SEND`	（任意）証明書の検証に使用するトラスト アンカーを設定します。
ステップ 15	**ipv6 nd secured timestamp** {**delta** *value* | **fuzz** *value*} **例：** `Host(config-if)# ipv6 nd secured timestamp delta 300`	（任意）タイミング パラメータを設定します。
ステップ 16	**exit** **例：** `Host(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 17	**ipv6 nd secured full-secure** **例：** `Host(config)# ipv6 nd secured full-secure`	（任意）全般的な SeND パラメータを設定します。 • 例では、SeND にセキュア モードが設定されています。

ルータによる SeND のイネーブル化の設定

SeND はルータ モードで使用できます。ルータ モードで SeND パラメータを設定する前に、まず次のコマンドを使用してルータを設定します。ルータを設定したら、そのルータで SeND パラメータを設定できます。

手順の概要

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** [**attr** *tag*] [**eq** | **ne** | **co** | **nc**] *string*
7. **rsakeypair** *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 rsakeypair** *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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*] **例：** `Router(config)# crypto key generate rsa label SEND modulus 1024`	RSA キーを設定します。
ステップ 4	**ipv6 cga modifier rsakeypair** *key-label* **sec-level** {**0** | **1**} **例：** `Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1`	SeND で RSA キーを使用できるようにします（修飾子を生成します）。
ステップ 5	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint SEND`	単一階層または複数階層の CA の PKI を設定し、ルータのトラストポイントを指定して、ルータを CA トラストポイント コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 6	**subject-name** [**attr** *tag*][**eq** | **ne** | **co** | **nc**] *string* **例：** `Router(ca-trustpoint)# subject-name C=FR, ST=PACA, L=Example, O=Cisco, OU=NSSTG, CN=router`	ルール エントリを作成します。
ステップ 7	**rsakeypair** *key-label* **例：** `Router(ca-trustpoint)# rsakeypair SEND`	SeND の RSA キー ペアをバインドします。
ステップ 8	**revocation-check** {[**crl**] [**none**] [**ocsp**]} **例：** `Router(ca-trustpoint)# revocation-check none`	1 つ以上の失効チェック方式を設定します。
ステップ 9	**exit** **例：** `host(ca-truspoint)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**crypto pki authenticate** *name* **例：** `host(config)# crypto pki authenticate SEND`	CA の証明書を取得して、認証局を認証します。
ステップ 11	**crypto pki enroll** *name* **例：** `Router(config)# crypto pki enroll SEND`	CA からルータの証明書を取得します。
ステップ 12	**ipv6 nd secured sec-level minimum** *value* **例：** `Router(config)# ipv6 nd secured sec-level minimum 1`	（任意）CGA を設定し、セキュリティ レベルやキー サイズなどの追加パラメータを指定します。 • 例では、SeND がピアから受け入れる最小セキュリティ レベルが設定されています。
ステップ 13	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 14	**ipv6 cga rsakeypair** *key-label* **例：** `Router(config-if)# ipv6 cga rsakeypair SEND`	（任意）インターフェイス上の CGA を設定します。 • 例では、OGA が生成されます。
ステップ 15	**ipv6 address** *ipv6-address/prefix-length* **link-local cga** **例：** `Router(config-if)# ipv6 address fe80::link-local cga`	インターフェイスの IPv6 リンクローカル アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 16	**ipv6 nd secured trustanchor** *trustpoint-name* **例：** `Router(config-if)# ipv6 nd secured trustanchor SEND`	（任意）証明書の検証に使用するトラスト アンカーを設定します。
ステップ 17	**ipv6 nd secured timestamp** {**delta** *value* | **fuzz** *value*} **例：** `Router(config-if)# ipv6 nd secured timestamp delta 300`	（任意）タイミング パラメータを設定します。
ステップ 18	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 19	**ipv6 nd secured full-secure** **例：** `Router(config)# ipv6 nd secured full-secure`	（任意）セキュア モードや認可方式などの全般的な SeND パラメータを設定します。 • 例では、SeND セキュリティ モードをイネーブルにしています。

SeND の実装方法

次の各項の作業では、SeND の実装方法を示します。

- 「RSA キー ペアとそのキー ペアの CGA 修飾子の作成」（P.15）（必須）
- 「PKI の証明書登録の設定」（P.16）（必須）
- 「暗号化生成アドレスの設定」（P.19）（必須）
- 「SeND パラメータの設定」（P.20）（任意）

RSA キー ペアとそのキー ペアの CGA 修飾子の作成

RSA キー ペアとそのキー ペアの CGA 修飾子を作成するには、次の作業を実行します。

手順の概要

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**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename*:] [**on** *devicename*:] **例：** `Router(config)# crypto key generate rsa label SeND`	RSA キー ペアを生成します。
ステップ 4	**ipv6 cga modifier rsakeypair** *key-label* **sec-level** {**0** | **1**} **例：** `Router(config)# ipv6 cga modifier rsakeypair SeND sec-level 1`	指定した RSA キーの CGA 修飾子を生成します。これにより、キーを SeND で使用できるようになります。

PKI の証明書登録の設定

証明書登録は、CA から証明書を取得するプロセスであり、証明書を要求するエンド ホストと CA の間で行われます。PKI に参加する各ピアは、CA に登録する必要があります。

IPv6 では、デバイス証明書を自動的または手動で登録できます。次の作業では、PKI の証明書登録の設定方法を示します。

手順の概要

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**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint trustpoint1`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**subject-name** [*x.500-name*] **例：** `Router(ca-trustpoint)# subject-name name1`	証明書要求の所有者名を指定します。
ステップ 5	**enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**] **例：** `Router(ca-trustpoint)# enrollment url http://name1.example.com`	ルータが証明書要求を送信する CA の URL を指定します。
ステップ 6	**serial-number** [**none**] **例：** `Router(ca-trustpoint)# serial-number`	（任意）証明書要求のルータのシリアル番号を指定します。
ステップ 7	**auto-enroll** [*percent*] [**regenerate**] **例：** `Router(ca-trustpoint)# auto-enroll`	（任意）自動登録をイネーブルにします。これにより、CA から自動的にルータ証明書を要求できます。
ステップ 8	**password** *string* **例：** `Router(ca-trustpoint)# password password1`	（任意）証明書の失効パスワードを指定します。

	コマンドまたはアクション	目的
ステップ 9	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(ca-trustpoint)# rsakeypair SEND`	証明書に関連付けるキー ペアを指定します。
ステップ 10	**fingerprint** *ca-fingerprint* **例：** `Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E`	（任意）認証時に CA 証明書のフィンガープリントと照合するフィンガープリントを指定します。
ステップ 11	**ip-extension** [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*} **例：** `Router(ca-trustpoint)# ip-extension unicast prefix 2001:100:1://48`	IP 拡張（IPv6 プレフィクスまたは範囲）を追加して、ルータがアドバタイズできるプレフィクス リストを確認します。
ステップ 12	**exit** **例：** `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate name1`	CA 証明書を取得し、認証します。 • CA 証明書がコンフィギュレーションにすでにロードされている場合、このコマンドはオプションです。
ステップ 14	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 15	**copy** [**/erase**] [**/verify** | **/noverify**] *source-url destination-url* **例：** `Router# copy system:running-config nvram:startup-config`	（任意）実行コンフィギュレーションを NVRAM スタートアップ コンフィギュレーションにコピーします。
ステップ 16	**show crypto pki certificates** **例：** `Router# show crypto pki certificates`	（任意）証明書、CA の証明書、および RA 証明書に関する情報を表示します。
ステップ 17	**show crypto pki trustpoints** [**status** | *label* [**status**]] **例：** `Router# show crypto pki trustpoints name1`	（任意）ルータに設定されているトラストポイントを表示します。

暗号化生成アドレスの設定

CGA を設定するには、次の作業を実行します。

- 「全般的な CGA パラメータの設定」（P.19）（必須）
- 「インターフェイスにおける CGA アドレス生成の設定」（P.19）（必須）

全般的な CGA パラメータの設定

セキュリティ レベルやキー サイズなどの全般的な CGA パラメータを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd secured sec-level** [**minimum** *value*] **例：** `Router(config)# ipv6 nd secured sec-level minimum 1`	SeND セキュリティ レベルを設定します。
ステップ 4	**ipv6 nd secured key-length** [[**minimum** | **maximum**] *value*] **例：** `Router(config)# ipv6 nd secured key-length minimum 512`	SeND key-length オプションを設定します。

インターフェイスにおける CGA アドレス生成の設定

インターフェイスにおける CGA アドレス生成を設定するには、次の作業を実行します。

手順の概要

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**]}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 cga rsakeypair** *key-label* **例：** `Router(config-if)# ipv6 cga rsakeypair SEND`	指定したインターフェイスで使用する RSA キー ペアを指定します。
ステップ 5	**ipv6 address** {*ipv6-address*/*prefix-length* [**cga**] | *prefix-name sub-bits*/*prefix-length* [**cga**]} **例：** `Router(config-if)# ipv6 address 2001:0DB8:1:1::/64 cga`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。 • **cga** キーワードを指定すると、CGA アドレスが生成されます。 **（注）** **ipv6 address link-local** コマンドを使用して、CGA リンクローカル アドレスを設定する必要があります。

SeND パラメータの設定

SeND を設定するには、次の作業を実行します。

- 「SeND トラストポイントの設定」（P.21）（任意）
- 「インターフェイスの SeND トラスト アンカーの設定」（P.23）（任意）
- 「セキュアなネイバー ディスカバリ メッセージとセキュアでないネイバー ディスカバリ メッセージの共存モードの設定」（P.25）（任意）
- 「SeND パラメータのグローバルな設定」（P.25）（任意）
- 「SeND タイムスタンプの設定」（P.26）（任意）

SeND トラストポイントの設定

ルータ モードで、インターフェイス上の CGA アドレスの生成に使用されたキー ペアを、CA と SeND プロトコルを介してオンデマンドで送信された証明書によって認証する必要があります。1 つの RSA キー ペアおよび関連付けられた証明書があれば SeND は動作できます。ただし、ユーザは異なるラベルで識別される複数のキーを使用する場合があります。SeND と CGA は、キーをラベルで直接参照するか、またはトラストポイントで間接的に参照します。

SeND をトラストポイントにバインドするには、複数の手順が必要になります。まず、キー ペアを生成します。次に、デバイスはトラストポイントでそのキー ペアを参照します。SeND インターフェイスの設定でトラストポイントを指します。複数の手順が必要になる理由は、次の 2 つです。

- 同じキー ペアを複数の SeND インターフェイスで使用できる。
- トラストポイントには、SeND で権限委任の実行に必要な証明書などの追加情報が含まれる。

参照されるトラストポイント用に CA 証明書をアップロードする必要があります。参照されるトラストポイントは、実際にはトラスト アンカーです。

特定のインターフェイスに対して、同じ RSA キーを指す複数のトラストポイントを設定できます。この機能は、ホストごとにトラスト アンカー（つまり、ホストが信頼する CA）が異なる場合に便利です。ルータは、ホストが信頼する CA によって署名された証明書を各ホストに提供できます。

SeND トラストポイントを設定するには、次の作業を実行します。

手順の概要

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*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename*:] [**on** *devicename*:] **例：** `Router(config)# crypto key generate rsa label SEND`	RSA キー ペアを生成します。
ステップ 4	**ipv6 cga modifier rsakeypair** *key-label* **sec-level** {**0** | **1**} **例：** `Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1`	指定した RSA キーの CGA 修飾子を生成します。これにより、キーを SeND で使用できるようになります。
ステップ 5	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint trustpoint1`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	**subject-name** [*x.500-name*] **例：** `Router(ca-trustpoint)# subject-name name1`	証明書要求の所有者名を指定します。
ステップ 7	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(ca-trustpoint)# rsakeypair SEND`	証明書に関連付けるキー ペアを指定します。
ステップ 8	**enrollment terminal** [**pem**] **例：** `Router(ca-trustpoint)# enrollment terminal`	カットアンドペーストによる手動での証明書登録を指定します。
ステップ 9	**ip-extension** [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*} **例：** `Router(ca-trustpoint)# ip-extension unicast prefix 2001:100:1://48`	IP 拡張をルータ証明書要求に追加します。

	コマンドまたはアクション	目的
ステップ 10	**exit** **例：** `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate trustpoint1`	CA の証明書を取得して、認証局を認証します。
ステップ 12	**crypto pki enroll** *name* **例：** `Router(config)# crypto pki enroll trustpoint1`	CA からルータの証明書を取得します。
ステップ 13	**crypto pki import** *name* **certificate** **例：** `Router(config)# crypto pki import trustpoint1 certificate`	証明書を TFTP によって手動でインポートするか、端末でカットアンドペーストによってインポートします。
ステップ 14	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 15	**ipv6 nd secured trustpoint** *trustpoint-name* **例：** `Router(config-if)# ipv6 nd secured trustpoint trustpoint1`	インターフェイスに対して SeND をイネーブルにし、使用するトラストポイントを指定します。

インターフェイスの SeND トラスト アンカーの設定

この作業は、ホスト モードでだけ実行できます。ホストに 1 つ以上のトラスト アンカーを設定する必要があります。SeND がインターフェイス上のトラストポイントにバインドされるとすぐに（「SeND トラストポイントの設定」（P.21）を参照）、このトラストポイントはトラスト アンカーになります。

トラスト アンカーの設定は、次の項目で構成されます。

- 公開鍵のシグニチャ アルゴリズムおよび関連付けられている公開鍵（パラメータが含まれている場合があります）
- 名前
- オプションの公開鍵 ID
- トラスト アンカーが許可されるアドレス範囲のオプション リスト

PKI はすでに設定されているため、トラスト アンカーの設定は、SeND を 1 つまたは複数の PKI トラストポイントにバインドすることによって完了します。PKI は、必要なパラメータ（名前、キーなど）が含まれる、対応する証明書のアップロードに使用されます。

この作業は任意です。この作業を実行すると、証明書の要求時に CPS にリストされるトラスト アンカーを選択できます。トラスト アンカーを設定しない場合は、ホストに設定されているすべての PKI トラストポイントが考慮されます。

インターフェイスのトラスト アンカーを設定するには、次の作業を実行します。

手順の概要

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*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint anchor1`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment terminal** [**pem**] **例：** `Router(ca-trustpoint)# enrollment terminal`	カットアンドペーストによる手動での証明書登録を指定します。
ステップ 5	**exit** **例：** `Router(ca-trustpoint)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate anchor1`	CA の証明書を取得して、認証局を認証します。
ステップ 7	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 8	**ipv6 nd secured trustanchor** *trustanchor-name* **例：** `Router(config-if)# ipv6 nd secured trustanchor anchor1`	インターフェイスのトラスト アンカーを指定し、SeND をトラストポイントにバインドします。

セキュアなネイバー ディスカバリ メッセージとセキュアでないネイバー ディスカバリ メッセージの共存モードの設定

SeND のセキュアなインターフェイスへの移行中、ネットワーク オペレータは、セキュアなネイバー ディスカバリ メッセージを受け入れるノードとセキュアでないネイバー ディスカバリ メッセージを受け入れるノードが共存する環境で特定のインターフェイスを実行する場合があります。同じインターフェイスにおけるセキュアなネイバー ディスカバリ メッセージとセキュアでないネイバー ディスカバリ メッセージの共存モードを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 nd secured trustpoint** *trustpoint-name* **例：** `Router(config-if)# ipv6 nd secured trustpoint trustpoint1`	インターフェイスに対して SeND をイネーブルにし、使用するトラストポイントを指定します。
ステップ 5	**no ipv6 nd secured full-secure** **例：** `Router(config-if)# no ipv6 nd secured full-secure`	同じインターフェイスにおけるセキュアなネイバー ディスカバリ メッセージとセキュアでないネイバー ディスカバリ メッセージの共存モードを指定します。

SeND パラメータのグローバルな設定

SeND パラメータをグローバルに設定するには、次の任意の作業を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd secured key-length** [[**minimum** | **maximum**] *value*] **例：** `Router(config)# ipv6 nd secured key-length minimum 512`	SeND key-length オプションを設定します。
ステップ 4	**ipv6 nd secured sec-level minimum** *value* **例：** `Router(config)# ipv6 nd secured sec-level minimum 2`	ピアから受け入れることができる最小セキュリティ レベル値を設定します。

SeND タイムスタンプの設定

インターフェイスの SeND タイムスタンプを設定するには、次の任意の作業を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 nd secured timestamp** {**delta** *value* | **fuzz** *value*} **例：** `Router(config-if)# ipv6 nd secured timestamp delta 600`	SeND タイムスタンプを設定します。

SeND for IPv6 の実装の設定例

ここでは、次の設定例について説明します。

証明書サーバの設定：例

次に、証明書サーバを設定する例を示します。

```
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
```

（注） IP 拡張のない証明書サーバを設定する必要がある場合は、**ip-extension** コマンドを使用しないでください。

IP 拡張のある証明書サーバを表示するには、**show crypto pki certificates verbose** コマンドを使用します。

```
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
```

ホストによる SeND のイネーブル化の設定：例

次に、SeND をイネーブルにするようにホストを設定する例を示します。

```
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
```

設定を確認するには、**show running-config** コマンドを使用します。

```
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
```

ルータによる SeND のイネーブル化の設定：例

次に、SeND をイネーブルにするようにルータを設定する例を示します。

```
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' commandwill 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
```

証明書が生成されたことを確認するには、**show crypto pki certificates** コマンドを使用します。

```
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
```

設定を確認するには、**show running-config** コマンドを使用します。

```
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
```

ルータ モードでの SeND トラストポイントの設定：例

次に、ルータ モードで SeND トラストポイントを設定する例を示します。

```
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
```

ホスト モードでの SeND トラスト アンカーの設定：例

次に、ホスト モードでインターフェイスの SeND トラスト アンカーを設定する例を示します。

```
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
```

インターフェイスにおける CGA アドレス生成の設定：例

次に、インターフェイスにおける CGA アドレス生成を設定する例を示します。

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

その他の関連資料

ここでは、SeND for IPv6 機能の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
PKI の証明書登録の設定	『*Cisco IOS Security Configuration Guide*』の「Configuring Certificate Enrollment for a PKI」の章

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3756	『*IPv6 Neighbor Discovery (ND) Trust Models and Threats*』
RFC 3779	『*X.509 Extensions for IP Addresses and AS Identifiers*』
RFC 3971	『*Secure Neighbor Discovery (SeND)*』
RFC 3972	『*Cryptographically Generated Addresses (CGA)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする • Product Alert の受信登録 • Field Notice の受信登録 • Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

SeND for IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表に示されているのは、Cisco IOS Release 12.2(15)T 以降のリリースで導入または変更された機能だけです。

ここに記載されていないこのテクノロジーの機能情報については、「*Start Here: Cisco IOS Software Release Specifies for IPv6 Features*」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IPv6 セキュア ネイバー ディスカバリの実装の機能情報

機能名	リリース	機能情報
Cisco IOS ソフトウェアのセキュア ネイバー ディスカバリ	12.4(24)T	Secure Neighbor Discovery（SeND; セキュア ネイバー ディスカバリ）は、ネイバー ディスカバリ プロトコルの脅威に対処する設計になっています。SeND では、一連のネイバー ディスカバリ オプションと 2 つのネイバー ディスカバリ メッセージが定義されています。アドレスの所有者を設定する新しい自動設定メカニズムも定義されています。 この機能に関する詳細については、次の各項を参照してください。 • 「SeND for IPv6 の実装方法」（P.7） 次のコマンドが導入されました。 **ipv6 cga modifier rsakeypair、ipv6 cga modifier rsakeypair（インターフェイス）、ipv6 nd secured certificate-db、ipv6 nd secured full-secure、ipv6 nd secured full-secure（インターフェイス）、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** 次のコマンドが変更されました。 **auto-enroll、crypto key generate rsa、crypto pki authenticate、crypto pki enroll、crypto pki import、enrollment terminal（CA トラストポイント）、enrollment url（CA トラストポイント）、fingerprint、ip-extension、ip http server、ipv6 address、ipv6 address link-local、password（CA トラストポイント）、revocation-check、rsakeypair、serial-number（CA トラストポイント）、subject-name**

用語集

- **CA**：Certification Authority（認証局）
- **CGA**：Cryptographically Generated Address（暗号化生成アドレス）。
- **CPA**：Certificate Path Answer（認証パス応答）。
- **CPR**：Certificate Path Response（証明書パス応答）。
- **CPS**：Certification Path Solicitation（認証パス請求）。アドレッシング プロセスで使用される請求メッセージ。
- **CRL**：Certificate Revocation List（証明書失効リスト）。
- **CS**：Certification Server（証明書サーバ）。

- **CSR**：Certificate Signing Request（証明書署名要求）。
- **DAD**：Duplicate Address Detection（重複アドレス検出）。同じリンク上の 2 つの IPv6 ノードが同じアドレスを使用していないことを確認するメカニズム。
- **DER**：Distinguished Encoding Rule（識別符号化ルール）。データ値の符号化方式。
- **非 SeND ノード**：SeND を実装せず、ネイバー ディスカバリ プロトコルだけをセキュリティなしで使用する IPv6 ノード。
- **NUD**：Neighbor Unreachability Detection（ネイバー到達不能検出）。ネイバー到達可能性の追跡に使用されるメカニズム。
- **PKI**：Public Key Infrastructure（公開鍵インフラストラクチャ）。
- **RD**：Router Discovery（ルータ ディスカバリ）。ホストはリンク上に存在するルータと使用可能なサブネット プレフィクスを検出できます。ルータ ディスカバリは、ネイバー ディスカバリ プロトコルの一部です。
- **SeND ノード**：SeND を実装する IPv6 ノード。
- **トラスト アンカー**：ルータがルータとして機能することを許可するために、ホストが信頼するエンティティ。ホストには、ルータ ディスカバリを保護するために一連のトラスト アンカーが設定されています。
- **ナンス**：ノードによって生成され、一度だけ使用される予測不可能な乱数または疑似乱数。SeND では、ナンスは特定のアドバタイズメントがそれをトリガーした請求にリンクされることを保証するために使用されます。
- **ルータ権限証明書**：公開鍵証明書。