# IPv6 Routing: OSPFv3 Authentication Support with IPsec

In order to ensure that Open Shortest Path First version 3 (OSPFv3) packets are not altered and re-sent to the device, OSPFv3 packets must be authenticated. OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for IPv6 Routing: OSPFv3 Authentication Support with IPsec

Configure the IP Security (IPsec) secure socket application program interface (API) on OSPFv3 in order to enable authentication and encryption.

# Restrictions for IPv6 Routing: OSPFv3 Authentication Support with IPsec

The OSPF for IPv6(OSPFv3) Authentication Support with IPsec feature is not supported on the IP BASE license package. The Advanced Enterprise Services package license must be used.

# Information About IPv6 Routing: OSPFv3 Authentication Support with IPsec

## OSPFv3 Authentication Support with IPsec

In order to ensure that OSPFv3 packets are not altered and re-sent to the device, causing the device to behave in a way not desired by its system administrators, OSPFv3 packets must be authenticated. OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

OSPFv3 requires the use of IPsec to enable authentication. Crypto images are required to use authentication, because only crypto images include the IPsec API needed for use with OSPFv3.

In OSPFv3, authentication fields have been removed from OSPFv3 packet headers. When OSPFv3 runs on IPv6, OSPFv3 requires the IPv6 authentication header (AH) or IPv6 ESP header to ensure integrity, authentication, and confidentiality of routing exchanges. IPv6 AH and ESP extension headers can be used to provide authentication and confidentiality to OSPFv3.

To use the IPsec AH, you must enable the **ipv6 ospf authentication** command. To use the IPsec ESP header, you must enable the **ipv6 ospf encryption** command. The ESP header may be applied alone or in combination with the AH, and when ESP is used, both encryption and authentication are provided. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host.

To configure IPsec, you configure a security policy, which is a combination of the security policy index (SPI) and the key (the key is used to create and validate the hash value). IPsec for OSPFv3 can be configured on an interface or on an OSPFv3 area. For higher security, you should configure a different policy on each interface configured with IPsec. If you configure IPsec for an OSPFv3 area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPFv3, IPsec is invisible to you.

The secure socket API is used by applications to secure traffic. The API needs to allow the application to open, listen, and close secure sockets. The binding between the application and the secure socket layer also allows the secure socket layer to inform the application of changes to the socket, such as connection open and close events. The secure socket API is able to identify the socket; that is, it can identify the local and remote addresses, masks, ports, and protocol that carry the traffic requiring security.

Each interface has a secure socket state, which can be one of the following:

- NULL: Do not create a secure socket for the interface if authentication is configured for the area.

- DOWN: IPsec has been configured for the interface (or the area that contains the interface), but OSPFv3 either has not requested IPsec to create a secure socket for this interface, or there is an error condition.

- GOING UP: OSPFv3 has requested a secure socket from IPsec and is waiting for a CRYPTO_SS_SOCKET_UP message from IPsec.

- UP: OSPFv3 has received a CRYPTO_SS_SOCKET_UP message from IPsec.

- CLOSING: The secure socket for the interface has been closed. A new socket may be opened for the interface, in which case the current secure socket makes the transition to the DOWN state. Otherwise, the interface will become UNCONFIGURED.

- UNCONFIGURED: Authentication is not configured on the interface.

OSPFv3 will not send or accept packets while in the DOWN state.

# How to Configure IPv6 Routing: OSPFv3 Authentication Support with IPsec

## Configuring IPsec on OSPFv3

Once you have configured OSPFv3 and decided on your authentication, you must define the security policy on each of the devices within the group. The security policy consists of the combination of the key and the SPI. To define a security policy, you must define an SPI and a key.

You can configure an authentication or encryption policy either on an interface or for an OSPFv3 area. When you configure for an area, the security policy is applied to all of the interfaces in the area. For higher security, use a different policy on each interface.

You can configure authentication and encryption on virtual links.

## Defining Authentication on an Interface

### Before you begin

Before you configure IPsec on an interface, you must configure OSPFv3 on that interface.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:

    - **ospfv3 authentication** {**ipsec** *spi*} {**md5** | **sha1**} { *key-encryption-type key*} | **null**
    - **ipv6 ospf authentication** {**null** | **ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] [*key*]}

**DETAILED STEPS**

|        | Command or Action | Purpose |
|--------|-------------------|---------|
| Step 1 | **enable**        | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:** Device> enable | • Enter your password if prompted. |
| **Step 2** | **configure terminal** **Example:** Device# configure terminal | Enters global configuration mode. |
| **Step 3** | **interface** *type* *number* **Example:** Device(config)# interface ethernet 0/0 | Specifies an interface type and number, and places the device in interface configuration mode. **Note** For Cisco ASR 901 Series Routers, you should configure the OSPFv3 authentication of the VLAN interface, instead of the physical interface. See the below example: Device(config)# interface VLAN 60 |
| **Step 4** | Do one of the following: • **ospfv3** **authentication** {**ipsec** *spi*} {**md5** \| **sha1**} { *key-encryption-type key*} \| **null** • **ipv6 ospf authentication** {**null** \| **ipsec spi** *spi* *authentication-algorithm* [*key-encryption-type*] [*key*]} **Example:** Device(config-if)# ospfv3 authentication md5 0 275761340947681324733020312097 27 **Example:** Or Device(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef | Specifies the authentication type for an interface. |

## Defining Authentication in an OSPFv3 Area

**SUMMARY STEPS**

1. **enable**
2. **configure** **terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **authentication** **ipsec spi** *spi* *authentication-algorithm* [*key-encryption-type*] *key*

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br><br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ipv6 router ospf** *process-id*<br>**Example:**<br><br>`Device(config)# ipv6 router ospf 1` | Enables OSPFv3 router configuration mode. |
| **Step 4** | **area** *area-id* **authentication ipsec spi** *spi*<br>*authentication-algorithm* [*key-encryption-type*] *key*<br>**Example:**<br><br>`Device(config-rtr)# area 1 authentication ipsec`<br>`spi 678 md5 1234567890ABCDEF1234567890ABCDEF` | Enables authentication in an OSPFv3 area. |

# Configuration Examples for IPv6 Routing: OSPFv3 Authentication Support with IPsec

## Example: Defining Authentication on an Interface

The following example shows how to define authentication on Ethernet interface 0/0:

```
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf authentication null
 ipv6 ospf 1 area 0
```

The following example shows how to define authentication on a VLAN interface of the Cisco ASR 901 Series Router:

```
interface Vlan60
ipv6 ospf encryption ipsec spi 300 esp 3des 4D92199549E0F2EF009B4160F3580E5528A11A45017F3887
 md5 79054025245FB1A26E4BC422AEF54501
```

## Example: Defining Authentication in an OSPFv3 Area

The following example shows how to define authentication on OSPFv3 area 0:

```
ipv6 router ospf 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

# Additional References for IPv6 Routing: OSPFv3 Authentication Support with IPsec

**Related Documents**

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Cisco IOS commands | *Cisco IOS Master Commands List, All Releases* |
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| Cisco IOS IPv6 features | *Cisco IOS IPv6 Feature Mapping* |
| IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec | "*Configuring OSPF* " module in *IP Routing: OSPF Configuration Guide* |

**Standards and RFCs**

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | IPv6 RFCs |

**Technical Assistance**

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for IPv6 Routing: OSPFv3 Authentication Support with IPsec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 1: Feature Information for IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec | | OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets.<br><br>The following commands were introduced or modified: **area authentication (IPv6)**, **ipv6 ospf authentication**, **ipv6 router ospf**, **ospfv3 authentication**. |