OSPFv3 Authentication Trailer

The OSPFv3 Authentication Trailer feature as specified in RFC 7166 provides a mechanism to authenticate Open Shortest Path First version 3 (OSPFv3) protocol packets as an alternative to existing OSPFv3 IPsec authentication.

- Finding Feature Information, on page 1
- Information About OSPFv3 Authentication Trailer, on page 1
- How to Configure OSPFv3 Authentication Trailer, on page 2
- Configuration Examples for OSPFv3 Authentication Trailer, on page 4
- Additional References for OSPFv3 Authentication Trailer, on page 6
- Feature Information for OSPFv3 Authentication Trailer, on page 6

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.

Information About OSPFv3 Authentication Trailer

Overview of OSPFv3 Authentication Trailer

Prior to the OSPFv3 Authentication Trailer, OSPFv3 IPsec as defined in RFC 4552 was the only mechanism for authenticating protocol packets. The OSPFv3 Authentication Trailer feature defines an alternative mechanism to authenticate OSPFv3 protocol packets that additionally provides a packet replay protection via sequence number and does not have any platform dependencies.

To perform non-IPsec cryptographic authentication, OSPFv3 devices append a special data block, that is, Authentication Trailer, to the end of the OSPFv3 packets. The length of the Authentication Trailer is not included in the length of the OSPFv3 packet but is included in the IPv6 payload length. The Link-Local Signaling (LLS) block is established by the L-bit setting in the “OSPFv3 Options” field in OSPFv3 hello and
database description packets. If present, the LLS data block is included along with the OSPFv3 packet in the
cryptographic authentication computation.

A new Authentication Trailer (AT)-bit is introduced into the OSPFv3 Options field. OSPFv3 devices must
set the AT-bit in OSPFv3 Hello and Database Description packets to indicate that all the packets on this link
will include an Authentication Trailer. For OSPFv3 Hello and Database Description packets, the AT-bit
indicates the AT is present. For other OSPFv3 packet types, the OSPFv3 AT-bit setting from the OSPFv3
Hello/Database Description setting is preserved in the OSPFv3 neighbor data structure. OSPFv3 packet types
that do not include an OSPFv3 Options field will use the setting from the neighbor data structure to determine
whether or not the AT is expected. The AT-bit must be set in all OSPFv3 Hello and Database Description
packets that contain an Authentication Trailer.

To configure the Authentication Trailer, OSPFv3 utilizes existing Cisco IOS key chain command. For outgoing
OSPFv3 packets, the following rules are used to select the key from the key chain:

- Select the key that is the last to expire.
- If two keys have the same stop time, select the one with the highest key ID.

The security association (SA) ID maps to the authentication algorithm and the secret key, which is used to
generate and verify the message digest. If the authentication is configured but the last valid key is expired,
then the packets are sent using the key. A syslog message is also generated. If no valid key is available then
the packet is sent without the authentication trailer. When packets are received, the key ID is used to look up
the data for that key. If the key ID is not found in the key chain or if the SA is not valid, the packet is dropped.
Otherwise, the packet is verified using the algorithm and the key that is configured for the key ID. Key chains
support rollover using key lifetimes. A new key can be added to a key chain with the send start time set in
the future. This setting allows the new key to be configured on all devices before the keys are actually used.

The hello packets have higher priority than any other OSPFv3 packets and therefore can get re-ordered on
the outgoing interface. This reordering can create problems with sequence number verification on neighboring
devices. To prevent sequence mismatch, OSPFv3 verifies the sequence number separately for each packet
type.

See RFC 7166 for more details on the authentication procedure.

How to Configure OSPFv3 Authentication Trailer

Configuring OSPFv3 Authentication Trailer

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ospfv3 [pid] [ipv4 | ipv6] authentication {key-chain chain-name | null}
5. router ospfv3 [process-id]
6. address-family ipv6 unicast vrf vrf-name
7. area area-id authentication {key-chain chain-name | null}
8. area area-id virtual-link router-id authentication key-chain chain-name
9. area area-id sham-link source-address destination-address authentication key-chain chain-name
10. authentication mode {deployment | normal}
11. end  
12. show ospfv3 interface  
13. show ospfv3 neighbor [detail]  
14. debug ospfv3 vrf authentication

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable`  
**Example:** Device> enable | Enables privileged EXEC mode.  
- 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 GigabitEthernet 2/0 | Specifies the interface type and number. |
| Step 4 | `ospfv3 [pid] [ipv4 | ipv6] authentication {key-chain chain-name | null}`  
**Example:** Device(config-if)# ospfv3 1 ipv4 authentication key-chain ospf-1 | Specifies the authentication type for an OSPFv3 instance. |
| Step 5 | `router ospfv3 [process-id]`  
**Example:** Device(config-if)# router ospfv3 1 | Enters OSPFv3 router configuration mode. |
| Step 6 | `address-family ipv6 unicast vrf vrf-name`  
**Example:** Device(config-router)# address-family ipv6 unicast vrf vrf1 | Configures the IPv6 address family in the OSPFv3 process and enters IPv6 address family configuration mode. |
| Step 7 | `area area-id authentication {key-chain chain-name | null}`  
**Example:** Device(config-router-af)# area 1 authentication key-chain ospf-chain-1 | Configures the authentication trailer on all interfaces in the OSPFv3 area. |
| Step 8 | `area area-id virtual-link router-id authentication key-chain chain-name`  
**Example:** Device(config-router-af)# area 1 virtual-link 1.1.1.1 authentication key-chain ospf-chain-1 | Configures the authentication for virtual links. |
### Configuration Examples for OSPFv3 Authentication Trailer

#### Example: Configuring OSPFv3 Authentication Trailer

```
interface GigabitEthernet 0/0
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 9** | area area-id sham-link source-address destination-address authentication key-chain chain-name  
Example:  
Device(config-router-af)# area 1 sham-link 1.1.1.1 1.1.1.0 authentication key-chain ospf-chain-1 | Configures the authentication for sham links. |
| **Step 10** | authentication mode {deployment | normal}  
Example:  
Device(config-router-af)# authentication mode deployment | Specifies the type of authentication used for the OSPFv3 instance. The deployment keyword provides adjacency between configured and unconfigured authentication devices. In deployment mode, a router processes packets as following:  
- The ospf checksum is calculated for the outgoing packets even if the authentication trailer is configured.  
- However, for the incoming packets the packets without authentication trailer or the wrong authentication hash packets get dropped.  
In this mode, the show ospfv3 neighbor detail command shows the last packet authentication status which can be used to verify the authentication trailer method. |
| **Step 11** | end  
Example:  
Device(config-router-af)# end | Exits IPv6 address family configuration mode and returns to privileged EXEC mode. |
| **Step 12** | show ospfv3 interface  
Example:  
Device# show ospfv3 | (Optional) Displays OSPFv3-related interface information. |
| **Step 13** | show ospfv3 neighbor [detail]  
Example:  
Device# show ospfv3 neighbor detail | (Optional) Displays OSPFv3 neighbor information on a per-interface basis. |
| **Step 14** | debug ospfv3 vrf authentication  
Example:  
Device# debug ospfv3 vrf authentication | (Optional) Displays debugging information for OSPFv3. |
**Example: Verifying OSPFv3 Authentication Trailer**

The following examples show the output of the `show ospfv3` commands.

```
Device# show ospfv3
OSPFv3 1 address-family ipv6
    Router ID 1.1.1.1
    --
    RFC1583 compatibility enabled
    Authentication configured with deployment key lifetime
    Active Key-chains:
        Key chain mama: Send key 1, Algorithm HMAC-SHA-256, Number of interfaces 1
        Area BACKBONE(0)

Device# show ospfv3 neighbor detail
OSPFv3 1 address-family ipv6 (router-id 2.2.2.2)
    Neighbor 1.1.1.1
        In the area 0 via interface GigabitEthernet0/0
        Neighbor: interface-id 2, link-local address FE80::A8BB:CCFF:FE01:2D00
        Neighbor priority is 1, State is FULL, 6 state changes
        DR is 2.2.2.2 BDR is 1.1.1.1
        Options is 0x0004413 in Hello (V6-Bit, E-Bit, R-Bit, AT-Bit)
        Options is 0x0004413 in DBD (V6-Bit, E-Bit, R-Bit, AT-Bit)
        Dead timer due in 00:00:33
        Neighbor is up for 00:05:07
        Last packet authentication succeed
        Index 1/1/1, retransmission queue length 0, number of retransmission 0
        First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
        Last retransmission scan length is 0, maximum is 0
        Last retransmission scan time is 0 msec, maximum is 0 msec

Device# show ospfv3 interface
GigabitEthernet0/0 is up, line protocol is up
    --
    Cryptographic authentication enabled
        Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain ospf-keys
        Last retransmission scan time is 0 msec, maximum is 0 msec
```
Additional References for OSPFv3 Authentication Trailer

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Configuring OSPF features</td>
<td>IP Routing: OSPF Configuration Guide</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC for Supporting Authentication Trailer for OSPFv3</td>
<td>RFC 6506</td>
</tr>
<tr>
<td>RFC for Authentication/Confidentiality for OSPFv3</td>
<td>RFC 4552</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
</table>
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.  
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.  
Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.                                                                                                                   | http://www.cisco.com/support|

Feature Information for OSPFv3 Authentication Trailer

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.
The OSPFv3 Authentication Trailer feature as specified in RFC 6506 provides a mechanism to authenticate OSPFv3 protocol packets as an alternative to existing OSPFv3 IPsec authentication.

The following commands were introduced or modified: `ospfv3 authentication key-chain`, `authentication mode`, `debug ospfv3 vrf authentication`.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 Authentication Trailer</td>
<td></td>
<td>The OSPFv3 Authentication Trailer feature as specified in RFC 6506 provides a mechanism to authenticate OSPFv3 protocol packets as an alternative to existing OSPFv3 IPsec authentication. The following commands were introduced or modified: <code>ospfv3 authentication key-chain</code>, <code>authentication mode</code>, <code>debug ospfv3 vrf authentication</code>.</td>
</tr>
</tbody>
</table>