BFD Single-Hop Authentication

The BFD Single-Hop Authentication feature enables authentication for single-hop Bidirectional Forwarding Detection (BFD) sessions between two directly connected devices. This feature supports Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) authentication types.

This module explains the BFD Single-Hop Authentication feature.

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 BFD Single-Hop Authentication

You must configure keys and key chains on both connected devices that are involved in a BFD session. You must configure the algorithm and the key chain on both devices in such a way that the configurations match.

Restrictions for BFD Single-Hop Authentication

- If key chains are removed from the established BFD single-hop sessions or no active keys are present in the key chain, the BFD template and the map entry are invalidated. Such invalidation is considered as a map entry deletion.
- Meticulous keyed MD5 authentication and meticulous keyed SHA-1 are not supported in In-Service Software Upgrade (ISSU) because checkpointing of sequence numbers does not occur in all packets.
- Meticulous MD5 and meticulous SHA-1 authentication types are not preserved after Route Processor (RP) failures in Stateful Switchover (SSO) mode. The sessions could flap causing link instability of the registered protocols.
- Only timers with values greater than or equal to 50 milliseconds are supported.
- The authentication type negotiation and key exchange between two BFD peers does not occur.
- When there is a missing key chain or when keys are not configured in a key chain, the BFD template and its associated map entries are invalidated, and the BFD session is not created.
- You can apply Bidirectional Forwarding Detection (BFD) single-hop Authentication in a BFD-template configuration only. You cannot apply BFD single-hop authentication in legacy configurations.

Information About BFD Single-Hop Authentication

Benefits of BFD Single-Hop Authentication

Using the Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) authentication methods defined in RFC 5880, the BFD Single Hop Authentication feature provides security against attacks on data links between a pair of directly connected devices involved in a BFD session. This feature is applied on data links between a BFD source-destination pair that communicates through IPv4 and IPv6 protocols across a single IP hop that is associated with an incoming interface. The communication may occur through physical media, virtual circuits, and tunnels.

Role of BFD Single-Hop Authentication in Preventing Denial of Service Attacks

To prevent denial of service (DoS) attacks, a BFD single-hop session validates the sequence number of a packet on receiving the packet. Detect multiplier is the number of missing BFD hello messages from another BFD device before the local device detects a fault in the forwarding path. The detect multiplier is used to determine the detect timer. The following are the ranges of valid sequence numbers that are accepted by the BFD Single-Hop Authentication feature:

- For nonmeticulous keyed types: Last received sequence number to (last received sequence number + 3 * detect multiplier)
- For meticulous keyed types: Last received sequence number + 1) to (last received sequence number + 3 * detect multiplier)

Note For BFD, (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.

How to Configure BFD Single-Hop Authentication

Configuring Key Chains

Perform this task on one of the two devices that are involved in a BFD session, and repeat the steps on the other device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *chain-name*
4. **key** *key-id*
5. **key-string** *text*
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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	**key chain** *chain-name* **Example:** `Device(config)# key chain chain1`	Defines an authentication key chain needed to enable authentication for routing protocols and enters key-chain configuration mode.
Step 4	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Defines an authentication key on the key chain and enters keychain-key configuration mode.
Step 5	**key-string** *text* **Example:**	Defines an authentication string for a key.

	Command or Action	Purpose
	`Device(config-keychain-key)# key-string key1`	
Step 6	**end** **Example:** `Device(config-keychain-key)# end`	Exits keychain-key configuration mode and returns to privileged EXEC mode.

Configuring a BFD Template with Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bfd-template single-hop** *template-name*
4. **interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value*
5. **authentication** *authentication-type* **keychain** *keychain-name*
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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	**bfd-template single-hop** *template-name* **Example:** `Device(config)# bfd-template single-hop template1`	Creates a BFD template and enters BFD configuration mode.
Step 4	**interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value* **Example:** `Device(config-bfd)# interval min-tx 120 min-rx 100 multiplier 3`	Configures transmit and receive intervals between BFD packets and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.
Step 5	**authentication** *authentication-type* **keychain** *keychain-name* **Example:**	Configures authentication in a BFD template for single-hop sessions.

	Command or Action	Purpose
	`Device(config-bfd)# authentication sha-1 keychain keychain1`	
Step 6	**end** **Example:** `Device(config-bfd)# end`	Exits BFD configuration mode and returns to privileged EXEC mode.

Configuring a Single-Hop Template on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd template** *template-name*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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 0/0/1`	Enters interface configuration mode.
Step 4	**bfd template** *template-name* **Example:** `Device(config-if)# bfd template bfdtemplate`	Binds a single-hop BFD template to an interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying BFD Single-Hop Authentication

SUMMARY STEPS

1. **show bfd drops**
2. **show bfd neighbor**

DETAILED STEPS

Procedure

Step 1 **show bfd drops**

Example:

```
Device> show bfd drops
```

This command displays the number of dropped packets in BFD.

Step 2 **show bfd neighbor**

Example:

```
Device> show bfd neighbor
```

This command displays a line-by-line listing of existing BFD adjacencies.

Configuration Examples for BFD Single-Hop Authentication

Example: Configuring Key Chains

```
Device> enable
Device# configure terminal
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# end
```

Example: Configuring a BFD Template with Authentication

```
Device> enable
Device# configure terminal
Device(config)# bfd-template single-hop template1
Device(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
Device(bfd-config)# authentication sha-1 keychain keychain1
Device(bfd-config)# end
```

Example: Configuring a Single-Hop Template on an Interface

```
Device> enable
Device# configure terminal
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# end
```

Example: Verifying BFD Single-Hop Authentication

Sample Output for the show bfd neighbor command

```
Device> show bfd neighbor

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.168.0.2                            1/12          Up        Up        Et0/0
Session state is UP and using echo function with 300 ms interval.
Session Host: Software
OurAddr: 192.168.0.1
Handle: 12
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(62244)
Rx Count: 62284, Rx Interval (ms) min/max/avg: 1/2436/878 last: 239 ms ago
Tx Count: 62247, Tx Interval (ms) min/max/avg: 1/1545/880 last: 246 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub CEF
Template: my-template
Authentication(Type/Keychain): sha-1/my-chain
Uptime: 00:22:06
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 12             - Your Discr.: 1
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 300000
```

Sample Output for the show bfd drops command.

```
Device> show  bfd drops

BFD Drop Statistics
                       IPV4    IPV6    IPV4-M  IPV6-M  MPLS_PW MPLS_TP_LSP
Invalid TTL            0       0       0       0       0       0
BFD Not Configured     0       0       0       0       0       0
No BFD Adjacency       0       0       0       0       0       0
Invalid Header Bits    0       0       0       0       0       0
Invalid Discriminator  0       0       0       0       0       0
Session AdminDown      0       0       0       0       0       0
Authen invalid BFD ver 0       0       0       0       0       0
Authen invalid len     0       0       0       0       0       0
```

```
Authen invalid seq      0        0       0       0       0       0
Authen failed           0        0       0       0       0       0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
IP Routing: Protocol-Independent Commands	*Cisco IOS IP Routing Protocol-Independent Command Reference*

Standards and RFCs

Standard/RFC	Title
RFC 5880	*Bidirectional Forwarding Detection*

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 BFD Single-Hop Authentication

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 BFD Single Hop Authentication

Feature Name	Releases	Feature Information
BFD Single-Hop Authentication	15.2(4)S	The BFD Single-Hop Authentication feature enables authentication for single hop BFD sessions between directly connected devices. This feature supports Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1) authentication types. The following commands were introduced or modified: **authentication (BFD)**, **bfd template**, **bfd-template**, **show bfd drops** and **show bfd neighbors**.