

HSRP MD5 Authentication

- Finding Feature Information, on page 1
- Information About HSRP MD5 Authentication, on page 1
- How to Configure HSRP MD5 Authentication, on page 2
- Configuration Examples for HSRP MD5 Authentication, on page 7
- Additional References, on page 9
- Feature Information for HSRP MD5 Authentication, on page 10

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 http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About HSRP MD5 Authentication

HSRP Text Authentication

HSRP ignores unauthenticated HSRP protocol messages. The default authentication type is text authentication.

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device

HSRP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packets.
- Text authentication strings differ on the device and in the incoming packet.

HSRP MD5 Authentication

Before the introduction of HSRP MD5 authentication, HSRP authenticated protocol packets with a simple plain text string. HSRP MD5 authentication is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This functionality provides added security and protects against the threat from HSRP-spoofing software.

MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each HSRP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and if the hash within the incoming packet does not match the generated hash, the packet is ignored.

The key for the MD5 hash can be either given directly in the configuration using a key string or supplied indirectly through a key chain.

HSRP has two authentication schemes:

- Plain text authentication
- MD5 authentication

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device.

HSRP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packets.
- MD5 digests differ on the device and in the incoming packet.
- Text authentication strings differ on the device and in the incoming packet.

How to Configure HSRP MD5 Authentication

Configuring HSRP MD5 Authentication Using a Key Chain

Perform this task to configure HSRP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. HSRP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**

8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **standby** [*group-number*] **priority** *priority*
11. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
12. **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*
13. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
14. Repeat Steps 1 through 12 on each device that will communicate.
15. **end**
16. **show standby**

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** *name-of-chain* **Example:** `Device(config)# key chain hsrp1`	Enables authentication for routing protocols, identifies a group of authentication keys, and enters key-chain configuration mode.
Step 4	**key** *key-id* **Example:** `Device(config-keychain)# key 100`	Identifies an authentication key on a key chain and enters key-chain key configuration mode. • The value for the*key-id* argument must be a number.
Step 5	**key-string** *string* **Example:** `Device(config-keychain-key)# key-string mno172`	Specifies the authentication string for a key. • The value for the *string* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral
Step 6	**exit** **Example:** `Device(config-keychain-key)# exit`	Returns to key-chain configuration mode.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-keychain)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 9	**ip address** *ip-address mask* [**secondary**] **Example:** `Device(config-if)# ip address 10.21.8.32 255.255.255.0`	Specifies a primary or secondary IP address for an interface.
Step 10	**standby** [*group-number*] **priority** *priority* **Example:** `Device(config-if)# standby 1 priority 110`	Configures HSRP priority.
Step 11	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] **Example:** `Device(config-if)# standby 1 preempt`	Configures HSRP preemption.
Step 12	**standby** [*group-number*] **authentication md5 key-chain** *key-chain-name* **Example:** `Device(config-if)# standby 1 authentication md5 key-chain hsrp1`	Configures an authentication MD5 key chain for HSRP MD5 authentication. • The key chain name must match the name specified in Step 3.
Step 13	**standby** [*group-number*] **ip** [*ip-address* [*secondary*]] **Example:** `Device(config-if)# standby 1 ip 10.21.8.12`	Activates HSRP.
Step 14	Repeat Steps 1 through 12 on each device that will communicate.	—
Step 15	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 16	**show standby**	(Optional) Displays HSRP information.

	Command or Action	Purpose
	Example: `Device# show standby`	• Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Troubleshooting HSRP MD5 Authentication

Perform this task if HSRP MD5 authentication is not operating correctly.

SUMMARY STEPS

1. **enable**
2. **debug standby errors**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug standby errors** **Example:** `Device# debug standby errors`	Displays error messages related to HSRP. • Error messages will be displayed for each packet that fails to authenticate, so use this command with care.

Examples

In the following example, Device A has MD5 text string authentication configured, but Device B has the default text authentication:

```
Device# debug standby errors

A:Jun 16 12:14:50.337:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 confgd
 but no tlv
B:Jun 16 12:16:34.287:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, Text auth
 failed
```

In the following example, both Device A and Device B have different MD5 authentication strings:

```
Device# debug standby errors

A:Jun 16 12:19:26.335:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 auth
failed
```

```
B:Jun 16 12:18:46.280:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, MD5 auth
failed
```

Configuring HSRP Text Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

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 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Device(config-if)# ip address 10.0.0.1 255.255.255.0`	Specifies a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 5	**standby** [*group-number*] **priority** *priority* **Example:** `Device(config-if)# standby 1 priority 110`	Configures HSRP priority.
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] **Example:** `Device(config-if)# standby 1 preempt`	Configures HSRP preemption.
Step 7	**standby** [*group-number*] **authentication text** *string* **Example:** `Device(config-if)# standby 1 authentication text authentication1`	Configures an authentication string for HSRP text authentication. • The default string is cisco.
Step 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Device(config-if)# standby 1 ip 10.0.0.3`	Activates HSRP.
Step 9	Repeat Steps 1 through 8 on each device that will communicate.	--
Step 10	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 11	**show standby** **Example:** `Device# show standby`	(Optional) Displays HSRP information. • Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Configuration Examples for HSRP MD5 Authentication

Example: Configuring HSRP MD5 Authentication Using Key Strings

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP MD5 Authentication Using Key Chains

In the following example, HSRP queries the key chain "hsrp1" to obtain the current live key and key ID for the specified key chain:

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP MD5 Authentication Using Key Strings and Key Chains

The key ID for key-string authentication is always zero. If a key chain is configured with a key ID of zero, then the following configuration will work:

Device 1

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 0
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

Device 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP Text Authentication

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication text company2
Device(config-if)# standby 1 ip 10.21.0.10
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS First Hop redundancy Protocols Command Reference*
HSRP for IPv6	"HSRP for IPv6" module
Troubleshooting HSRP	Hot Standby Router Protocol: Frequently Asked Questions

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 792	*Internet Control Message Protocol*
RFC 1828	*IP Authentication Using Keyed MD5*
RFC 2281	*Cisco Hot Standby Router Protocol*

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 HSRP MD5 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 https://cfnng.cisco.com/. An account on Cisco.com is not required.