



HSRP MD5 Authentication

Prior to the introduction of the HSRP MD5 Authentication feature, the Hot Standby Router Protocol (HSRP) authenticated protocol packets with a simple plain text string. The HSRP MD5 Authentication feature is an enhancement to generate an Message Digest 5 (MD5) digest for the HSRP portion of the multicast HSRP protocol packet. This feature provides added security and protects against the threat from HSRP-spoofing software.

Feature History for the HSRP MD5 Authentication Feature

Release	Modification
12.3(2)T	This feature was introduced.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for HSRP MD5 Authentication, page 2](#)
- [Information About HSRP MD5 Authentication, page 2](#)
- [How to Configure HSRP MD5 Authentication, page 3](#)
- [Configuration Examples for HSRP MD5 Authentication, page 8](#)
- [Additional References, page 9](#)
- [Command Reference, page 11](#)
- [Glossary](#)



Restrictions for HSRP MD5 Authentication

Text authentication cannot be combined with MD5 authentication for an HSRP group at any one time. When MD5 authentication is configured, the text authentication field in HSRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

Information About HSRP MD5 Authentication

Before you configure HSRP MD5 authentication, you should understand the following concepts:

- [How HSRP MD5 Authentication Works, page 2](#)
- [Benefits of HSRP MD5 Authentication, page 2](#)

How HSRP MD5 Authentication Works

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

The key for the MD5 hash can either be 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, Router A has a priority of 120 and is the active router. If a host sends spoof HSRP hello packets with a priority of 130, then Router A stops being the active router. If Router A has authentication configured such that the spoof HSRP hello packets are ignored, Router A will remain the active router.

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

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

Benefits of HSRP MD5 Authentication

- Protects against HSRP-spoofing software
- Uses the industry-standard MD5 algorithm for improved reliability and security

How to Configure HSRP MD5 Authentication

The following sections describe configuration tasks for HSRP MD5 authentication. The task you perform depends on whether you want to use a simple MD5 key string or MD5 key chains for authentication.

- [Configuring HSRP MD5 Authentication Using a Key String, page 3](#)
- [Configuring HSRP MD5 Authentication Using a Key Chain, page 5](#)
- [Troubleshooting HSRP MD5 Authentication, page 7](#)

Configuring HSRP MD5 Authentication Using a Key String

This task describes how to configure HSRP MD5 authentication using a key string.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **standby** [*group-number*] **priority** *priority*
7. **standby** [*group-number*] **preempt**
8. **standby** [*group-number*] **authentication md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **end**
11. **show standby**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface Ethernet0/1	Configures an interface type and enters interface configuration mode.

	Command	Purpose
Step 4	<code>ip address ip-address mask [secondary]</code> Example: Router(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	<code>standby [group-number] ip [ip-address [secondary]]</code> Example: Router(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.
Step 6	<code>standby [group-number] priority priority</code> Example: Router(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 7	<code>standby [group-number] preempt</code> Example: Router(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 8	<code>standby [group-number] authentication md5 key-string [0 7] key [timeout seconds]</code> Example: Router(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30	Configures an authentication string for HSRP MD5 authentication. <ul style="list-style-type: none"> • The <i>key</i> argument can be up to 64 characters in length and it is recommended that at least 16 characters be used. • No prefix to the <i>key</i> argument or specifying 0 means the key will be unencrypted. • Specifying 7 means the key will be encrypted. The key-string authentication key will automatically be encrypted if the service password-encryption global configuration command is enabled. • The timeout value is the period of time that the old key string will be accepted to allow configuration of all routers in a group with a new key.
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	—
Step 10	<code>end</code> Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 11	<code>show standby</code> Example: Router# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none"> • Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Troubleshooting Tips

If you are changing a key string in a group of routers, change the active router last to prevent any HSRP state change. The active router should have its key string changed no later than one holdtime period, specified by the **standby timers** interface configuration command, after the non-active routers. This procedure ensures that the non-active routers do not time out the active router.

Configuring HSRP MD5 Authentication Using a Key Chain

This task describes how 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 key chain process 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. **interface** *type number*
8. **ip address** *ip-address mask* [**secondary**]
9. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
10. **standby** [*group-number*] **priority** *priority*
11. **standby** [*group-number*] **preempt**
12. **standby** [*group-number*] **authentication md5 key-chain** *name-of-chain*
13. Repeat steps 1 through 12 on each router that will communicate.
14. **end**
15. **show standby**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command	Purpose
Step 3	key chain <i>name-of-chain</i> Example: Router(config)# key chain hsrp1	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Router(config-keychain)# key 100	Identifies an authentication key on a key chain. <ul style="list-style-type: none"> The <i>key-id</i> must be a number.
Step 5	key-string <i>string</i> Example: Router(config-keychain-key)# key-string mno172	Specifies the authentication string for a key. <ul style="list-style-type: none"> The <i>string</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	exit Example: Router(config-keychain-key)# exit	Returns to global configuration mode.
Step 7	interface <i>type number</i> Example: Router(config)# interface Ethernet0/1	Configures an interface type and enters interface configuration mode.
Step 8	ip address <i>ip-address mask [secondary]</i> Example: Router(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 9	standby [<i>group-number</i>] ip [<i>ip-address [secondary]</i>] Example: Router(config-if)# standby 1 ip 10.21.8.12	Activates HSRP.
Step 10	standby [<i>group-number</i>] priority <i>priority</i> Example: Router(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 11	standby [<i>group-number</i>] preempt Example: Router(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 12	standby [<i>group-number</i>] authentication md5 key-chain <i>key-chain-name</i> Example: Router(config-if)# standby 1 authentication md5 key-chain hsrp1	Configures an authentication MD5 key chain for HSRP MD5 authentication. <ul style="list-style-type: none"> The key chain name must match the name specified in Step 3.
Step 13	Repeat Steps 1 through 12 on each router that will communicate.	—

	Command	Purpose
Step 14	<code>end</code> Example: <code>Router(config-if)# end</code>	Returns to privileged EXEC mode.
Step 15	<code>show standby</code> Example: <code>Router# show standby</code>	(Optional) Displays HSRP information. <ul style="list-style-type: none"> 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

- `enable`
- `debug standby errors`

DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>debug standby errors</code> Example: <code>Router# debug standby errors</code>	Displays error messages related to HSRP. <ul style="list-style-type: none"> Error messages will be displayed for each packet that fails to authenticate so use this command with care. See the “Examples” section for an example of the type of error messages displayed when two routers are not authenticating.

Examples

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

```
Router# 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 Router A and Router B have different MD5 authentication strings:

```
Router# 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
```

Configuration Examples for HSRP MD5 Authentication

This section provides the following configuration examples:

- [HSRP MD5 Authentication Using Key Strings: Example, page 8](#)
- [HSRP MD5 Authentication Using Key Chains: Example, page 8](#)
- [HSRP MD5 Authentication Using Key Strings and Key Chains: Example, page 8](#)

HSRP MD5 Authentication Using Key Strings: Example

The following example configures HSRP MD5 authentication using a key string:

```
!
interface Ethernet0/1
 standby 1 ip 10.21.0.10
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 54321098452103ab timeout 30
```

HSRP MD5 Authentication Using Key Chains: Example

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

```
key chain hsrp1
 key 1
  key-string 54321098452103ab

interface Ethernet0/1
 standby 1 ip 10.21.0.10
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-chain hsrp1
```

HSRP MD5 Authentication Using Key Strings and Key Chains: Example

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:

Router 1

```
key chain hsrp1
 key 0
  key-string 54321098452103ab

interface Ethernet0/1
 standby 1 ip 10.21.0.10
```

```
standby 1 authentication md5 key-chain hsrp1
```

Router 2

```
interface Ethernet0/1
standby 1 ip 10.21.0.10
standby 1 authentication md5 key-string 54321098452103ab
```

Additional References

The following sections provide information related to HSRP MD5 authentication.

Related Documents

Related Topic	Document Title
HSRP: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> , Release 12.3
Key chains and key management: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> , Release 12.3
HSRP configuration tasks; key chain and key management configuration tasks	<i>Cisco IOS IP Configuration Guide</i>

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
No new MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1828	<i>IP Authentication Using Keyed MD5</i>

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

- [show standby](#)
- [standby authentication](#)

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [*type number* [*group*]] [**active** | **init** | **listen** | **standby**] [**brief**]

Syntax Description	
<i>type number</i>	(Optional) Interface type and number for which output is displayed.
<i>group</i>	(Optional) Group number on the interface for which output is displayed.
active	(Optional) Displays HSRP groups in the active state.
init	(Optional) Displays HSRP groups in the initial state.
listen	(Optional) Displays HSRP groups in the listen or learn state.
standby	(Optional) Displays HSRP groups in the standby or speak state.
brief	(Optional) A single line of output summarizes each standby group.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(3)T	The following keywords were added: <ul style="list-style-type: none"> • active • init • listen • standby
	12.2(8)T	The output for the command was made clearer and easier to understand.
	12.3(2)T	The output was enhanced to display information about Message Digest 5 (MD5) authentication.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines	
	To specify a group, you must specify an interface type and number.

Examples	
	The following is sample output from the show standby command:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
```

```

Active virtual MAC address is 0004.4d82.7981
  Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
  Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is local
Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
Priority 95 (configured 120)
  Tracking 2 objects, 0 up
    Down Interface Ethernet0/2, pri 15
    Down Interface Ethernet0/3
IP redundancy name is "HSRP1", advertisement interval is 34 sec

```

The following is sample output from the **show standby** command with an interface and the **brief** and **init** keywords specified:

```
Router# show standby ethernet0/1 1 init brief
```

Interface	Grp	Prio	P	State	Active addr	Standby addr	Group addr
Et0	0	120		Init	10.0.0.1	unknown	10.0.0.12

The following is sample output from the **show standby** command when HSRP MD5 authentication is configured:

```
Router# show standby
```

```

Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string "f33r45", timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Et0/1-1" (default)

```

[Table 1](#) describes the significant fields shown in the displays.

Table 1 *show standby Field Descriptions*

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface.
State is	State of local router; can be one of the following: <ul style="list-style-type: none"> • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • Learn—Router is neither in the active nor standby state, nor does it have enough information to attempt to claim the active or standby roles. • Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active addr and Standby addr fields will show “unknown.” The state is listed as disabled in the fields when the standby ip command has not been specified.
Virtual IP address is, secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as “duplicate.” A duplicate address indicates that the router has failed to defend its Address Resolution Protocol (ARP) cache entry.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Local virtual MAC address	Virtual MAC address that would be used if this router became the active router. The origin of this address (displayed in parentheses) can be “default,” “bia,” (burned-in address) or “configd” (configured).
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the command. The holdtime is the time (in seconds) before other routers declare the active or standby router to be down, based on the standby timers command. All routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
Next hello sent in ...	Time in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Authentication...	Authentication type configured based on the standby authentication command.
key string	Key string used for authentication. Key chains are displayed if configured.
timeout	Duration (in seconds) that HSRP will accept message digests based on both the old and new keys.
Preemption enabled, sync delay	Indicates whether preemption is enabled. If enabled, the minimum delay is the time a higher-priority nonactive router will wait before preempting the lower-priority active router. The sync delay is the maximum time (in seconds) a group will wait to synchronize with the IP redundancy clients.

Table 1 *show standby Field Descriptions (continued)*

Field	Description
Active router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the current active Hot Standby router.
Standby router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the “standby” router (the router that is next in line to be the Hot Standby router).
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Tracking	List of interfaces that are being tracked and their corresponding states. Based on the standby track command.
IP redundancy name is	Name of IP redundancy service. Default name is hsrp-Et0/1-1.

Related Commands

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby mac-address	Specifies the virtual MAC address for the virtual router.
standby mac-refresh	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
standby timers	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bia	Configures HSRP to use the BIA of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

standby authentication

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **standby authentication** command in interface configuration mode. To delete an authentication string, use the **no** form of this command.

```
standby [group-number] authentication { text string | md5 { key-string [0 | 7] key
[timeout seconds] | key-chain name-of-chain }
```

```
no standby [group-number] authentication { text string | md5 { key-string [0 | 7] key
[timeout seconds] | key-chain name-of-chain }
```

Syntax Description		
<i>group-number</i>	(Optional) Group number on the interface to which this authentication string applies.	
text <i>string</i>	Authentication string. It can be up to eight characters long. The default string is cisco.	
md5	Message Digest 5 (MD5) authentication.	
key-string <i>key</i>	Specifies the secret key for MD5 authentication. The key can contain up to 64 characters. We recommend using at least 16 characters.	
0	(Optional) Unencrypted key. If no prefix is specified, the text also is unencrypted.	
7	(Optional) Encrypted key.	
timeout <i>seconds</i>	(Optional) Duration in seconds that HSRP will accept message digests based on both the old and new keys.	
key-chain <i>name-of-chain</i>	Identifies a group of authentication keys.	

Defaults The default group number is 0. The default string is cisco.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.1	The text keyword was added.
	12.3(2)T	The md5 keyword and associated parameters were added.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines The authentication string is sent unencrypted in all HSRP messages when using the **standby authentication text** *string* option. The same authentication string must be configured on all routers and access servers on a cable to ensure interoperability. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

If password encryption is configured with the **service password-encryption** command, the software saves the key string as encrypted text.

The **timeout seconds** is the duration that the HSRP group will accept message digests based on both the old and new keys. This allows time for configuration of all routers in a group with the new key. HSRP route flapping can be minimized by changing the keys on all the routers, provided that the active router is changed last. The active router should have its key string changed no later than one holdtime period, specified by the **standby timers** interface configuration command, after the non-active routers. This procedure ensures that the non-active routers do not time out the active router.

Examples

The following example configures “company1” as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
interface ethernet 0
 standby 1 authentication text company1
```

The following example configures MD5 authentication using a key string named “345890”:

```
!
interface Ethernet0/1
 standby 1 ip 10.21.0.12
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 345890 timeout 30
```

The following example configures MD5 authentication using a key chain. HSRP queries the key chain “hsrp1” to obtain the current live key and key ID for the specified key chain:

```
key chain hsrp1
 key 1
 key-string 543210

interface Ethernet0/1
 standby 1 ip 10.21.0.10
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-chain hsrp1
```

Related Commands

Command	Description
service password-encryption	Encrypts passwords.
standby timers	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.

Glossary

encryption—Encryption is the translation of data into a secret code. Encryption is a way to achieve data security. Encryption prevents the password or key from being easily readable in the configuration file.

MD5—Message Digest 5. An algorithm that is used to create digital signatures. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest. When using a one-way hash function, you can compare a calculated message digest against the received message digest to verify that the message hasn't been tampered with. This comparison is called a *hashcheck*.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)