



Enhancing Security in an IS-IS Network

First Published: November 30, 2007

Last Updated: May 5, 2008

This module describes processes that you can follow to enhance network security when you use Intermediate System-to-Intermediate System (IS-IS) in your network. You can set passwords, prevent unauthorized routers from forming adjacencies with routers in your IS-IS network, and use the IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication feature.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Enhancing Security in an IS-IS Network](#)” section on [page 17](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

- [Prerequisites for Enhancing Security in an IS-IS Network, page 2](#)
- [Information About Enhancing Security in an IS-IS Network, page 2](#)
- [How to Enhance Security in an IS-IS Network, page 2](#)
- [Configuration Examples for Enhancing Security in an IS-IS Network, page 14](#)
- [Additional References, page 15](#)
- [Feature Information for Enhancing Security in an IS-IS Network, page 17](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007–2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for Enhancing Security in an IS-IS Network

- Before performing the tasks in this module, you should be familiar with the concepts described in the [“Integrated IS-IS Routing Protocol Overview”](#) and [“Configuring a Basic IS-IS Network”](#) modules.
- It is assumed you already have IS-IS running on your network.

Information About Enhancing Security in an IS-IS Network

Before you configure the features in this module, you should understand the following concept:

[Importance of Preventing Unauthorized Information from Entering an IS-IS Network, page 2](#)

Importance of Preventing Unauthorized Information from Entering an IS-IS Network

It is recommended that you configure the security features described in this module in order to prevent unauthorized routing messages from being placed into the network routing domain. You can set an authentication password for each interface, as well as set an area password for each IS-IS area to prevent unauthorized routers from injecting false routing information into the link-state database, or you can configure a type of IS-IS authentication—either IS-IS HMAC-MD5 or enhanced clear text authentication.

How to Enhance Security in an IS-IS Network

This module describes the following processes that can enhance your network security when you use IS-IS on your network:

- [Setting an Authentication Password for each Interface, page 2](#)
- [Setting an Area Password for each IS-IS Area, page 3](#)
- [Configuring IS-IS Authentication, page 6](#)

Setting an Authentication Password for each Interface

Entering the **isis password** command enables you to prevent unauthorized routers from forming adjacencies with this router and thus protects the network from intruders.

Restrictions

The password is exchanged as plain text and thus provides only limited security.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **isis password** *password* [**level-1** | **level-2**]
5. Repeat Step 4 for each interface password that you want to set.
6. **end**
7. **show ip interface** [*type number*] [**brief**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables 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.
Step 3	interface <i>type number</i> Example: Router(config)# interface ethernet 0	Enters interface configuration mode.
Step 4	isis password <i>password</i> [level-1 level-2] Example: Router(config-if)# isis password sjpass level-1	Configures the authentication password for an interface. <ul style="list-style-type: none"> • Different passwords can be assigned for different routing levels using the level-1 and level-2 keywords. • Specifying the level-1 or level-2 keyword disables the password only for Level 1 or Level 2 routing, respectively.
Step 5	Repeat Step 4 for each interface password that you want to set.	—
Step 6	end Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 7	show ip interface [<i>type number</i>] [brief] Example: Router# show ip interface serial 1	Displays the usability status of interfaces configured for IP.

Setting an Area Password for each IS-IS Area

This section contains the following tasks:

[Setting a Password at Level 1, page 4](#)

[Setting a Password at Level 2, page 5](#)

Setting a Password at Level 1

Perform this task to set an area password for each IS-IS area in your network. Using the **area-password** command on all routers in an area will prevent unauthorized routers from injecting false routing information into the link-state database.

This password is inserted in Level 1 protocol data unit (PDU) link-state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Restrictions

This password is exchanged as plain text, and, thus, this feature provides only limited security.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **area-password** *password*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables 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.
Step 3	router isis [<i>area-tag</i>] Example: Router(config)# router isis salesarea	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	area-password <i>password</i> Example: Router(config-router)# area-password companyz	Configures the IS-IS area authentication password.
Step 5	end Example: Router(config-router)# end	Returns to privileged EXEC mode.

Setting a Password at Level 2

Perform this task to set a Level 2 area password for each IS-IS area in your network. Using the **domain-password** command on all routers in an area will prevent unauthorized routers from injecting false routing information into the link-state database.

This password is inserted in Level 2 PDU link-state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs). If you specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, the IS-IS routing protocol will insert the password into sequence number PDUs (SNPs).

Restrictions

This password is exchanged as plain text, and, thus, this feature provides only limited security.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **domain-password** *password* [**authenticate snp** { **validate** | **send-only** }]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables 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.
Step 3	router isis [<i>area-tag</i>] Example: Router(config)# router isis salesarea	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. <ul style="list-style-type: none"> • Enters router configuration mode.

	Command or Action	Purpose
Step 4	<pre>domain-password password [authenticate snp {validate send-only}]</pre> <p>Example: Router(config-router)# domain-password company2</p>	<p>Configures the IS-IS routing domain authentication password.</p> <p>Note If you do not specify the authenticate snp keyword along with either the validate or send-only keyword, the IS-IS routing protocol does not insert the password into SNPs.</p>
Step 5	<pre>end</pre> <p>Example: Router(config-router)# end</p>	<p>Returns to privileged EXEC mode.</p>

Configuring IS-IS Authentication

The following sections describe configuration tasks for IS-IS authentication. Two types of authentication are supported: IS-IS HMAC-MD5 and clear text. The task you perform depends on whether you are introducing authentication or migrating from an existing authentication scheme.

Before you can configure authentication, you must make the following decisions:

- Whether to configure authentication for the IS-IS instance and/or for individual IS-IS interfaces (both tasks are included in this section).
- At what level(s) authentication is to be used.
- What type of authentication (IS-IS HMAC-MD5 or clear text) is to be used.

This section contains the following procedures:

- [Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time, page 7](#)
- [Migrating to a New Authentication Type, page 11](#)
- [Configuring Authentication on a New Router Being Added to a Network That Already Has Authentication Configured, page 13](#)

Before you configure IS-IS HMAC-MD5 authentication or clear text authentication, you should understand the following concepts:

- [IS-IS Authentication Functionality, page 6](#)
- [Benefits of IS-IS Clear Text Authentication, page 7](#)
- [Benefits of IS-IS HMAC-MD5 Authentication, page 7](#)

IS-IS Authentication Functionality

New style IS-IS authentication (IS-IS HMAC-MD5 and clear text) provides a number of advantages over the old style password configuration commands that were described in the previous sections, “[Setting an Authentication Password for each Interface](#)” section on page 2 and “[Setting an Area Password for each IS-IS Area](#)” section on page 3.

- Passwords are encrypted when the software configuration is displayed.
- Passwords are easier to manage and change.
- Passwords can be rolled over to new passwords without disrupting network operations.

- Non-disruptive authentication transitions are supported by allowing configuration which allowed the router to accept PDUs without authentication or with stale authentication information, yet send PDUs with current authentication. Such transitions are useful when you are migrating from no authentication to some type of authentication, when you are changing authentication type, and when you are changing keys.

IS-IS has five PDU types: link state PDU (LSP), LAN Hello, Point-to-Point Hello, complete sequence number PDU (CSNP), and partial sequence number PDU (PSNP). IS-IS HMAC-MD5 authentication or clear text password authentication can be applied to all five PDU types. The authentication can be enabled on different IS-IS levels independently. The interface-related PDUs (LAN Hello, Point-to-Point Hello, CSNP, and PSNP) can be enabled with authentication on different interfaces, with different levels and different passwords.

Either authentication mode or old password mode may be configured on a given scope (IS-IS instance or interface) and level—but not both. However, different modes may be configured for different modes that can be configured for different scopes or levels. If mixed modes are intended, different keys should be used for different modes in order not to compromise the encrypted password in the PDUs.

Benefits of IS-IS Clear Text Authentication

IS-IS clear text (plain text) authentication provides the same functionality as is provided by using the **area-password** or **domain-password** command. However, use of clear text authentication takes advantage of the more flexible key management capabilities described above.

Benefits of IS-IS HMAC-MD5 Authentication

- IS-IS now supports MD5 authentication, which is more secure than clear text authentication. IS-IS HMAC-MD5 authentication adds an HMAC-MD5 digest to each IS-IS protocol data unit (PDU). HMAC is a mechanism for message authentication codes (MACs) using cryptographic hash functions. The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain.
- MD5 authentication or clear text authentication can be enabled on Level 1 or Level 2 independently.
- Passwords can be rolled over to new passwords without disrupting routing messages.
- For the purpose of network transition, you can configure the networking device to *accept* PDUs without authentication or with wrong authentication information, yet *send* PDUs with authentication. Such transition might be because you are migrating from no authentication to some type of authentication, you are changing authentication type, or you are changing keys.

Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time

This section contains the following tasks:

- [Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance, page 7](#)
- [Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface, page 10](#)

Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance

To achieve a smooth transition to authenticating IS-IS PDUs, perform the following steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

In order to use HMAC-MD5 or clear text authentication with encrypted keys, the Integrated IS-IS routing protocol must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **exit**
8. **router isis** [*area-tag*]
9. **authentication send-only** [**level-1** | **level-2**]
10. Repeat Steps 1 through 9 on each router that will communicate.
11. **authentication mode** {**md5** | **text**} [**level-1** | **level-2**]
12. **authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
13. Repeat Steps 11 and 12 on each router that will communicate.
14. **no authentication send-only**
15. Repeat Step 14 on each router that will communicate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables 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.
Step 3	key chain <i>name-of-chain</i> Example: Router(config)# key chain remote3754	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> argument must be a number.

	Command or Action	Purpose
Step 5	<p>key-string <i>text</i></p> <p>Example: Router(config-keychain-key)# key-string mno172</p>	<p>Specifies the authentication string for a key.</p> <ul style="list-style-type: none"> The <i>text</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	<p>exit</p> <p>Example: Router(config-keychain-key)# exit</p>	<p>Returns to keychain configuration mode.</p>
Step 7	<p>exit</p> <p>Example: Router(config-keychain)# exit</p>	<p>Returns to global configuration mode.</p>
Step 8	<p>router isis [<i>area-tag</i>]</p> <p>Example: Router(config)# router isis 1</p>	<p>Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required.</p> <ul style="list-style-type: none"> Enters router configuration mode.
Step 9	<p>authentication send-only [<i>level-1</i> <i>level-2</i>]</p> <p>Example: Router(config-router)# authentication send-only</p>	<p>Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS PDUs being sent (not received).</p>
Step 10	<p>Repeat Steps 1 through 9 on each router that will communicate.</p>	<p>Use the same key string on each router.</p>
Step 11	<p>authentication mode {<i>md5</i> <i>text</i>} [<i>level-1</i> <i>level-2</i>]</p> <p>Example: Router(config-router)# authentication mode md5</p>	<p>Specifies the type of authentication used in IS-IS PDUs for the IS-IS instance.</p> <ul style="list-style-type: none"> Specify md5 for MD5 authentication. Specify text for clear text authentication.
Step 12	<p>authentication key-chain <i>name-of-chain</i> [<i>level-1</i> <i>level-2</i>]</p> <p>Example: Router(config-router)# authentication key-chain remote3754</p>	<p>Enables MD5 authentication for the IS-IS instance.</p>
Step 13	<p>Repeat Steps 11 and 12 on each router that will communicate.</p>	<p>—</p>
Step 14	<p>no authentication send-only</p> <p>Example: Router(config-router)# no authentication send-only</p>	<p>Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS PDUs being sent and received.</p> <ul style="list-style-type: none"> In Step 9 you enable authentication to be performed only for IS-IS PDUs that are being sent. In Step 14 you enter the no authentication send-only command so that the authentication is now performed on PDUs sent and received.
Step 15	<p>Repeat Step 14 on each router that will communicate.</p>	<p>—</p>

Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface

To achieve a smooth transition to authenticating IS-IS PDUs, perform the following steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **isis authentication send-only** [**level-1** | **level-2**]
10. Repeat Steps 1 through 9 on each router that will communicate.
11. **isis authentication mode** { **md5** | **text** } [**level-1** | **level-2**]
12. **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
13. Repeat Steps 11 and 12 on each router that will communicate.
14. **no isis authentication send-only**
15. Repeat Step 14 on each router that will communicate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables 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.
Step 3	key chain <i>name-of-chain</i> Example: Router(config)# key chain multistate87723	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Router(config-keychain)# key 201	Identifies an authentication key on a key chain. <ul style="list-style-type: none"> • The <i>key-id</i> argument must be a number.

	Command or Action	Purpose
Step 5	<code>key-string text</code> Example: Router(config-keychain-key)# key-string idaho	Specifies the authentication string for a key. <ul style="list-style-type: none"> The <i>text</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	<code>exit</code> Example: Router(config-keychain-key)# exit	Returns to keychain configuration mode.
Step 7	<code>exit</code> Example: Router(config-keychain)# exit	Returns to global configuration mode.
Step 8	<code>interface type number</code> Example: Router(config)# interface ethernet 0	Configures an interface.
Step 9	<code>isis authentication send-only [level-1 level-2]</code> Example: Router(config-if)# isis authentication send-only	Specifies that authentication is performed only on PDUs being sent (not received) on a specified IS-IS interface.
Step 10	Repeat Steps 1 through 9 on each router that will communicate.	Use the same key string on each router.
Step 11	<code>isis authentication mode {md5 text} [level-1 level-2]</code> Example: Router(config-if)# isis authentication mode md5	Specifies the type of authentication used for an IS-IS interface. <ul style="list-style-type: none"> Specify md5 for MD5 authentication. Specify text for clear text authentication.
Step 12	<code>isis authentication key-chain name-of-chain [level-1 level-2]</code> Example: Router(config-if)# isis authentication key-chain multistate87723	Enables MD5 authentication for an IS-IS interface. <ul style="list-style-type: none"> For information about key chains and key management see the “Related Documents” section on page 15.
Step 13	Repeat Steps 11 and 12 on each router that will communicate.	—
Step 14	<code>no isis authentication send-only</code> Example: Router(config-if)# no isis authentication send-only	Specifies that authentication is performed on PDUs being sent and received on a specified IS-IS interface.
Step 15	Repeat Step 14 on each router that will communicate.	—

Migrating to a New Authentication Type

Before you migrate from using one type of security authentication to another, all routers must be loaded with the new image that supports the new authentication type. The routers will continue to use the original authentication method until all routers have been loaded with the new image that supports the new authentication method, and all routers have been configured to use the new authentication method.

Once all routers are loaded with the required image, you must follow the configuration steps for the desired new authentication method as described in the previous [“Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance”](#) section on page 7. You also must decide whether to configure authentication for the IS-IS area or for individual IS-IS interfaces. Both tasks are included in the referenced section.

**Note**

To achieve a smooth transition from one authentication method to another, allowing for continuous authentication of IS-IS PDUs, perform the task steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

Before you migrate from your original authentication method to a new method, you should be familiar with the information in the following sections:

- [Migration from Old Clear Text Authentication to HMAC-MD5 Authentication, page 12](#)
- [Migration from Old Clear Text Authentication to the New Clear Text Authentication, page 12](#)

Migration from Old Clear Text Authentication to HMAC-MD5 Authentication

When you configure MD5 authentication, the **area-password** and **domain-password** command settings will be overridden automatically with the new authentication commands. When you configure MD5 authentication, the **isis password** command setting will be overridden automatically with the new authentication commands.

Migration from Old Clear Text Authentication to the New Clear Text Authentication

The benefits of migrating from the old method of clear text authentication to the new method of clear text authentication are as follows:

- Passwords are easier to change and maintain.
- Passwords can be encrypted when the system configuration is being displayed (if you use key management).

To migrate from your original authentication method to a new method, perform the following steps.

SUMMARY STEPS

1. Load all routers with the image required to support the new, desired authentication method.
2. Configure the new authentication mode on both the interface and the IS-IS area by following the appropriate tasks in the [“Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time”](#) section on page 7.

DETAILED STEPS

-
- Step 1** Load all routers with the image required to support the new, desired authentication method.
- Step 2** Configure the new authentication mode on both the interface and the IS-IS area by following the appropriate tasks in the [“Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time”](#) section on page 7.
-

Configuring Authentication on a New Router Being Added to a Network That Already Has Authentication Configured

Once your network is running authentication, you will need to configure authentication for any router that is later added to the network. Perform the following steps to configure authentication on the new router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **isis authentication mode** { *md5* | *text* } [*level-1* | *level-2*]
10. **isis authentication key-chain** *name-of-chain* [*level-1* | *level-2*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables 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.
Step 3	key chain <i>name-of-chain</i> Example: Router(config)# key chain multistate87723	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Router(config-keychain)# key 201	Identifies an authentication key on a key chain. <ul style="list-style-type: none"> • The <i>key-id</i> argument must be a number.
Step 5	key-string <i>text</i> Example: Router(config-keychain-key)# key-string idaho	Specifies the authentication string for a key. <ul style="list-style-type: none"> • The <i>text</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.

	Command or Action	Purpose
Step 6	exit Example: Router(config-keychain-key)# exit	Returns to keychain configuration mode.
Step 7	exit Example: Router(config-keychain)# exit	Returns to global configuration mode.
Step 8	interface <i>type number</i> Example: Router(config)# interface ethernet 0	Configures an interface.
Step 9	isis authentication mode { md5 text } [level-1 level-2] Example: Router(config-if)# isis authentication mode md5	Specifies the type of authentication used for an IS-IS interface. <ul style="list-style-type: none"> Specify md5 for MD5 authentication. Specify text for clear text authentication.
Step 10	isis authentication key-chain <i>name-of-chain</i> [level-1 level-2] Example: Router(config-if)# isis authentication key-chain multistate87723	Enables MD5 authentication for an IS-IS interface. <ul style="list-style-type: none"> For information about key chains and key management see the “Related Documents” section on page 15.

Configuration Examples for Enhancing Security in an IS-IS Network

This section provides the following configuration examples:

- [Configuring IS-IS HMAC-MD5 Authentication: Example, page 14](#)
- [Configuring IS-IS Clear Text Authentication: Example, page 15](#)

Configuring IS-IS HMAC-MD5 Authentication: Example

The following example configures a key chain and key for IS-IS HMAC-MD5 authentication for Ethernet interface 3 (on Hello PDUs) and for the IS-IS instance (on LSP, CSNP, and PSNP PDUs).

```
!
key chain cisco
  key 100
  key-string tasman-drive
!
interface Ethernet3
  ip address 10.1.1.1 255.255.255.252
  ip router isis real_secure_network
  isis authentication mode md5 level-1
  isis authentication key-chain cisco level-1
```

```

!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain cisco level-1
!

```

Configuring IS-IS Clear Text Authentication: Example

The following example configures a key chain and key for IS-IS clear text authentication for Ethernet interface 3 (on Hello PDUs) and for the IS-IS instance (on LSP, CSNP, and PSNP PDUs).

```

!
key chain cisco
 key 100
 key-string tasman-drive
!
interface Ethernet3
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication mode text level-1
 isis authentication key-chain cisco level-1
!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode text level-1
 authentication key-chain cisco level-1
!

```

Additional References

The following sections provide references related to configuring IS-IS to enhance network security.

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	Cisco IOS IP Routing Protocols Command Reference
Key chains and key management	<ul style="list-style-type: none"> IP Routing Protocol-Independent Commands chapters in the Cisco IOS IP Routing Protocols Command Reference “Configuring IP Routing Protocol-Independent Features” chapter in the Cisco IOS IP Routing Protocols Configuration Guide
Roadmap of IS-IS features	“ Integrated IS-IS Features Roadmap ” module
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	“ Integrated IS-IS Routing Protocol Overview ” module

Standards

Standard	Title
None	—

RFCs

RFC	Title
RFC 1321	<i>The MD5 Message-Digest Algorithm</i>
RFC 2104	<i>HMAC: Keyed-Hashing for Message Authentication</i>
RFC 3567	IS-IS Cryptographic Authentication

Technical Assistance

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

Feature Information for Enhancing Security in an IS-IS Network

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(13)T, 12.0(21)S, 12.2(11)S, or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Integrated IS-IS Features Roadmap](#)” module.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Enhancing Security in an IS-IS Network

Feature Name	Releases	Feature Information
IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication	12.0(21)ST 12.0(22)S 12.2(11)S 12.2(13)T 12.2(14)S	<p>The IS-IS HMAC-MD5 authentication feature adds an HMAC-MD5 digest to each Intermediate System-to-Intermediate System (IS-IS) protocol data unit (PDU). The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain. IS-IS clear text (plain text) authentication is enhanced so that passwords are encrypted when the software configuration is displayed and passwords are easier to manage and change.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Configuring IS-IS Authentication, page 6

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.

