



IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication

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 message 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.

Feature Specifications for the IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication Feature

Feature History

Release	Modification
12.0(21)ST	This feature was introduced.
12.2(11)S	This feature was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This feature was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

Supported Platforms

Cisco 7200 series, Cisco 7400 series, Cisco 7500 series, Cisco 10000 series, Cisco 10720 Internet router, Cisco 12000 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

Contents

- [Prerequisites for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication, page 2](#)
- [Information About IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication, page 2](#)
- [How to Configure IS-IS HMAC-MD5 Authentication or Enhanced Clear Text Authentication, page 3](#)
- [Configuration Examples for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication, page 16](#)
- [Additional References, page 17](#)
- [Command Reference, page 19](#)

Prerequisites for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication

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

Information About IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication

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

- [IS-IS HMAC-MD5 Authentication, page 3](#)
- [Benefits of IS-IS HMAC-MD5 Authentication, page 3](#)
- [Benefits of IS-IS Clear Text Authentication, page 3](#)

IS-IS HMAC-MD5 Authentication

The IS-IS HMAC-MD5 authentication feature adds an HMAC-MD5 digest to each IS-IS 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.

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

The HMAC-MD5 mode cannot be mixed with the clear text mode on the same authentication scope (LSP or interface). However, administrators can use one mode for LSP and another mode for some interfaces, for example. 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 HMAC-MD5 Authentication

- IS-IS now supports MD5 authentication, which is more secure than clear text authentication.
- 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.

Benefits of IS-IS Clear Text Authentication

IS-IS clear text (plain text) authentication was formerly configured only by using the **area-password** or **domain-password** command. Clear text authentication can now be configured using new commands that cause passwords to be encrypted when the software configuration is displayed and make passwords easier to manage and change.

How to Configure IS-IS HMAC-MD5 Authentication or Enhanced Clear Text Authentication

The following sections describe configuration tasks for IS-IS authentication. The task you perform depends on whether you are introducing authentication or migrating from an existing authentication scheme.

- [Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time](#) (optional)
- [Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication](#) (optional)
- [Migrating from Old Clear Text Authentication to the New Clear Text Authentication](#) (optional)

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

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

- Whether to configure authentication for the IS-IS instance or for individual IS-IS interfaces (both tasks are included in this section)
- Whether to configure HMAC-MD5 authentication or clear text authentication (this decision is made with the **authentication mode** command if you are configuring an IS-IS instance, or with the **isis authentication mode** command if you are configuring an IS-IS interface)

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

To achieve a smooth transition to authenticating IS-IS packets, 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. **router isis** *area-tag*
8. **authentication send-only** [**level-1** | **level-2**]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **authentication mode** {**md5** | **text** } [**level-1** | **level-2**]
11. **authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no authentication send-only**
14. Repeat Step 13 on each router that will communicate.

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	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. The <i>key-id</i> must be a number.
Step 5	key-string <i>text</i> Example: Router(config-keychain-key)# key-string mno172	Specifies the authentication string for a key. The <i>text</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	router isis <i>area-tag</i> Example: Router(config)# router isis 1	Enables the IS-IS routing protocol and specifies an IS-IS process.
Step 8	authentication send-only [level-1 level-2] Example: Router(config-router)# authentication send-only	Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS packets being sent (not received).
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	Use the same key-string on each router.
Step 10	authentication mode { md5 text } [level-1 level-2] Example: Router(config-router)# authentication mode md5	Specifies the type of authentication used in IS-IS packets for the IS-IS instance. - Specify md5 for MD5 authentication. - Specify text for clear text authentication.

	Command	Purpose
Step 11	authentication key-chain <i>name-of-chain</i> [level-1 level-2] Example: Router(config-router)# authentication key-chain remote3754	Enables MD5 authentication for the IS-IS instance.
Step 12	Repeat Steps 10 and 11 on each router that will communicate.	—
Step 13	no authentication send-only Example: Router(config-router)# no authentication send-only	Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS packets being sent and received.
Step 14	Repeat Step 13 on each router that will communicate.	—

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

To achieve a smooth transition to authenticating IS-IS packets, 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. **interface *type number***
8. **isis authentication send-only [level-1 | level-2]**
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **isis authentication mode {md5 | text } [level-1 | level-2]**
11. **isis authentication key-chain *name-of-chain* [level-1 | level-2]**
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no isis authentication send-only**
14. Repeat Step 13 on each router that will communicate.

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	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. The <i>key-id</i> 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. The <i>text</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 ethernet 0	Configures an interface.
Step 8	isis authentication send-only [level-1 level-2] Example: Router(config-if)# isis authentication send-only	Specifies that MD5 authentication is performed only on packets being sent (not received) on a specified IS-IS interface.
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	Use the same key-string on each router.
Step 10	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.

	Command	Purpose
Step 11	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. Refer to the key management feature, which is referenced in the “Related Documents” section.
Step 12	Repeat Steps 10 and 11 on each router that will communicate.	—
Step 13	Router(config-if)# no isis authentication send-only Example: Router(config-if)# no isis authentication send-only	Specifies that MD5 authentication is performed on packets being sent and received on a specified IS-IS interface.
Step 14	Repeat Step 13 on each router that will communicate.	—

Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication

When you are migrating from the old clear text authentication to HMAC-MD5 authentication, after you load the first router with an image that includes this feature, the router will continue to use the old clear text authentication with other routers on the network.



Note

If you want HMAC-MD5 authentication, all routers in the authentication scope must have the new image before HMAC-MD5 can be configured. The scope can be either a Level 1 or Level 2 domain.

Before you can configure authentication, you must decide whether to configure authentication for the IS-IS instance or for individual IS-IS interfaces (both tasks are in this section).

Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication for the IS-IS Instance

To achieve a smooth transition to authenticating IS-IS packets, 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.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **router isis** *area-tag*
8. **authentication send-only** [**level-1** | **level-2**]

9. Repeat Steps 1 through 8 on each router that will communicate.
10. **authentication mode md5** [level-1 | level-2]
11. **authentication key-chain** *name-of-chain* [level-1 | level-2]
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no authentication send-only**
14. Repeat Step 13 on each router that will communicate.

	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	key chain <i>name-of-chain</i> Example: Router(config)# key chain dinosaur	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Router(config-keychain)# key 301	Identifies an authentication key on a key chain. The <i>key-id</i> must be a number.
Step 5	key-string <i>text</i> Example: Router(config-keychain-key)# key-string pterodactyl	Specifies the authentication string for a key. The <i>text</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	router isis <i>area-tag</i> Example: Router(config)# router isis 1	Enables the IS-IS routing protocol and specifies an IS-IS process.
Step 8	authentication send-only [level-1 level-2] Example: Router(config-router)# authentication send-only	Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS packets being sent (not received).
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	Use the same key-string on each router.

	Command	Purpose
Step 10	authentication mode md5 [<i>level-1</i> <i>level-2</i>] Example: Router(config-router)# authentication mode md5	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
Step 11	authentication key-chain <i>name-of-chain</i> [<i>level-1</i> <i>level-2</i>] Example: Router(config-router)# authentication key-chain remote3754	Enables MD5 authentication for the IS-IS instance.
Step 12	Repeat Steps 10 and 11 on each router that will communicate.	—
Step 13	no authentication send-only Example: Router(config-router)# no authentication send-only	Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS packets being sent and received.
Step 14	Repeat Step13 on each router that will communicate.	—

Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication for an IS-IS Interface

Prerequisites

Before you can migrate from the old method of clear text authentication to HMAC-MD5 authentication at the interface level, you must upgrade all the routers associated with the media of the interfaces to the new image containing the HMAC-MD5 feature.

To achieve a smooth transition to authenticating IS-IS packets, it is important to perform the 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.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **interface** *type number*
8. **isis authentication send-only** [*level-1* | *level-2*]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **isis authentication mode md5** [*level-1* | *level-2*]
11. **isis authentication key-chain** *name-of-chain* [*level-1* | *level-2*]

12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no isis authentication send-only**
14. Repeat Step 13 on each router that will communicate.

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	key chain <i>name-of-chain</i> Example: Router(config)# key chain dinosaur	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Router(config-keychain)# key 301	Identifies an authentication key on a key chain. The <i>key-id</i> must be a number.
Step 5	key-string <i>text</i> Example: Router(config-keychain-key)# key-string pterodactyl	Specifies the authentication string for a key. The <i>text</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 ethernet 0	Configures an interface.
Step 8	isis authentication send-only [level-1 level-2] Example: Router(config-if)# isis authentication send-only	Specifies that MD5 authentication is performed only on packets being sent (not received) on a specified IS-IS interface.
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	Use the same key-string on each router.
Step 10	isis authentication mode md5 [level-1 level-2] Example: Router(config-if)# isis authentication mode md5	Specifies the type of authentication used for an IS-IS interface.

	Command	Purpose
Step 11	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. Refer to the key management feature, which is referenced in the “Related Documents” section.
Step 12	Repeat Steps 10 and 11 on each router that will communicate.	—
Step 13	Router(config-if)# no isis authentication send-only Example: Router(config-if)# no isis authentication send-only	Specifies that MD5 authentication is performed on packets being sent and received on a specified IS-IS interface.
Step 14	Repeat Step 13 on each router that will communicate.	—

Migrating 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).

Before you can configure authentication, you must decide whether to configure authentication for the IS-IS instance or for individual IS-IS interfaces (both tasks are in this section).

Migrating from Old Clear Text Authentication to the New Clear Text Authentication for the IS-IS Instance

To achieve a smooth transition to authenticating LSPs, 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. **router isis** *area-tag*
8. **authentication send-only** [**level-1** | **level-2**]
9. Repeat Steps 1 through 8 on each router that will communicate.

10. **authentication mode text** [level-1 | level-2]
11. **authentication key-chain** *name-of-chain* [level-1 | level-2]
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no authentication send-only**
14. Repeat Step 13 on each router that will communicate.

	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	key chain <i>name-of-chain</i> Example: Router(config)# key chain dinosaur	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Router(config-keychain)# key 301	Identifies an authentication key on a key chain. • The <i>key-id</i> must be a number.
Step 5	key-string <i>text</i> Example: Router(config-keychain-key)# key-string pterodactyl	Specifies the authentication string for a key. • The <i>text</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	router isis <i>area-tag</i> Example: Router(config)# router isis 1	Enables the IS-IS routing protocol and specifies an IS-IS process.
Step 8	authentication send-only [level-1 level-2] Example: Router(config-router)# authentication send-only	Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS packets being sent (not received).
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	Use the same key-string on each router.
Step 10	authentication mode text [level-1 level-2] Example: Router(config-router)# authentication mode text	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.

	Command	Purpose
Step 11	authentication key-chain <i>name-of-chain</i> [level-1 level-2] Example: Router(config-router)# authentication key-chain remote3754	Enables MD5 authentication for the IS-IS instance.
Step 12	Repeat Steps 10 and 11 on each router that will communicate.	—
Step 13	no authentication send-only Example: Router(config-router)# no authentication send-only	Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS packets being sent and received.  Note Do not perform this step if some of the routers sharing the media on the interface do not run the new image. In software releases prior to those on which this feature runs, authentication is not applied to SNP packets. If the router runs the new image without the authentication send-only command configured and with the new clear text password scheme, it will fail to authenticate the SNP packets from the router with old images.
Step 14	Repeat Step 13 on each router that will communicate.	—

Migrating from Old Clear Text Authentication to the New Clear Text Authentication for an IS-IS Interface

This section describes how to configure authentication on interface-related PDUs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **interface** *type number*
8. **isis authentication send-only** [**level-1** | **level-2**]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **isis authentication mode text** [**level-1** | **level-2**]
11. **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
12. Repeat Steps 10 and 11 on each router that will communicate.

13. Load the new image on all the other routers that share the media that the interface uses.
14. **no isis authentication send-only**
15. Repeat Step 14 on each interface.

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	key chain <i>name-of-chain</i> Example: Router(config)# key chain dinosaur	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Router(config-keychain)# key 301	Identifies an authentication key on a key chain. The <i>key-id</i> must be a number.
Step 5	key-string <i>text</i> Example: Router(config-keychain-key)# key-string pterodactyl	Specifies the authentication string for a key. The <i>text</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 ethernet 0	Configures an interface.
Step 8	isis authentication send-only [level-1 level-2] Example: Router(config-if)# isis authentication send-only	Specifies that MD5 authentication is performed only on packets being sent (not received) on a specified IS-IS interface.
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	Use the same key-string on each router.
Step 10	isis authentication mode text [level-1 level-2] Example: Router(config-if)# isis authentication mode text	Specifies the type of authentication used for an IS-IS interface.

	Command	Purpose
Step 11	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. Refer to the key management feature, which is referenced in the “Related Documents” section.
Step 12	Repeat Steps 10 and 11 on each router that will communicate.	—
Step 13	Load the new image on all the other routers that share the media that the interface uses.	—
Step 14	Router(config-if)# no isis authentication send-only Example: Router(config-if)# no isis authentication send-only	Specifies that MD5 authentication is performed on packets being sent and received on a specified IS-IS interface.
Step 15	Repeat Step 14 on each interface.	—

Configuration Examples for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication

This section provides the following configuration examples:

- [Configuring IS-IS HMAC-MD5 Authentication Example, page 16](#)
- [Configuring IS-IS Clear Text Authentication Example, page 17](#)

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 packets) and for the IS-IS instance (on LSP, CSNP, and PSNP packets):

```

!
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 packets) and for the IS-IS instance (on LSP, CSNP, and PSNP packets):

```
!
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

For additional information related to IS-IS HMAC-MD5 authentication and clear text authentication, refer to the following references:

- [Related Documents, page 17](#)
- [MIBs, page 18](#)
- [RFCs, page 18](#)
- [Technical Assistance, page 18](#)

Related Documents

Related Topic	Document Title
Key chains and key management	• “IP Routing Protocol-Independent Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i>, Release 12.2 • “Configuring IP Routing Protocol-Independent Features” chapter in the <i>Cisco IOS IP Configuration Guide</i>, Release 12.2
IS-IS routing protocol	• “Integrated IS-IS Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i>, Release 12.2 • “Configuring Integrated IS-IS” chapter in the <i>Cisco IOS IP Configuration Guide</i>, Release 12.2

MIBs

MIBs ¹	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
draft-ietf-isis-hmac-03.txt	<i>IS-IS Cryptographic Authentication</i>
RFC 1321	<i>The MD5 Message-Digest Algorithm</i>
RFC 2104	<i>HMAC: Keyed-Hashing for Message Authentication</i>

1. Not all supported RFCs are listed.

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 the following new commands related to IS-IS HMAC-MD5 authentication. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [authentication key-chain](#)
- [authentication mode](#)
- [authentication send-only](#)
- [debug isis authentication](#)
- [isis authentication key-chain](#)
- [isis authentication mode](#)
- [isis authentication send-only](#)

This section also documents the following revised commands related to clear text authentication. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [area-password](#)
- [domain-password](#)

area-password

To configure the IS-IS area authentication password, use the **area-password** command in router configuration mode. To disable the password, use the **no** form of this command.

area-password *password* [**authenticate snp** { **validate** | **send-only** }]

no area-password [*password*]

Syntax Description

<i>password</i>	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into sequence number PDUs (SNPs).
validate	(Optional) Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	(Optional) Causes the system only to insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Defaults

No area password is defined, and area password authentication is disabled.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The authenticate snp , validate , and send-only keywords were added.

Usage Guidelines

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 exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 1 (station router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an area authentication password and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
router isis
 area-password track authenticate snp validate
```

Related Commands

Command	Description
domain-password	Configures the IS-IS routing domain authentication password.
isis password	Configures the authentication password for an interface.

authentication key-chain

To enable authentication for Intermediate System-to-Intermediate System (IS-IS), use the **authentication key-chain** command in router configuration mode. To disable such authentication, use the **no** form of this command.

authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Syntax Description

<i>name-of-chain</i>	Enables authentication and specifies the group of keys that are valid.
level-1	(Optional) Enables authentication for Level 1 packets only.
level-2	(Optional) Enables authentication for Level 2 packets only.

Defaults

No key chain authentication is provided for IS-IS packets at the router level.

Command Modes

Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.

Usage Guidelines

If no key chain is configured with the **key chain** command, no key chain authentication is performed.

Key chain authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the **authentication mode** command.

Only one authentication key chain is applied to IS-IS at one time. That is, if you configure a second **authentication key-chain** command, the first is overridden.

If neither the **level-1** nor **level-2** keyword is configured, the chain applies to both levels.

You can specify authentication for an individual IS-IS interface by using the **isis authentication key-chain** command.

Examples

The following example configures IS-IS to accept and send any key belonging to the key chain named site1:

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain site1 level-1
```

Related Commands

Command	Description
authentication mode	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
isis authentication key-chain	Enables authentication for an IS-IS interface.
key chain	Enables authentication for routing protocols.

authentication mode

To specify the type of authentication used in IS-IS packets for the IS-IS instance, use the **authentication mode** command in router configuration mode. To restore clear text authentication, use the **no** form of this command.

authentication mode {md5 | text} [level-1 | level-2]

no authentication mode

Syntax Description

md5	Message Digest 5 (MD5) authentication.
text	Clear text authentication.
level-1	(Optional) Enables the specified authentication for Level 1 packets only.
level-2	(Optional) Enables the specified authentication for Level 2 packets only.

Defaults

No authentication is provided for IS-IS packets at the router level by use of this command, although clear text (plain text) authentication could be configured by other means, such as the **area-password** command or the **domain-password** command.

Command Modes

Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.

Usage Guidelines

If neither the **level-1** nor **level-2** keyword is configured, the mode applies to both levels.

You can specify the type of authentication and the level to which it applies for a single IS-IS interface, rather than per IS-IS instance, by using the **isis authentication mode** command.

If you had clear text authentication configured by using the **area-password** or **domain-password** command, the **authentication mode** command overrides both of those commands.

If you configure the **authentication mode** command and subsequently try to configure the **area-password** or **domain-password** command, you will not be allowed to do so. If you truly want to configure clear text authentication using the **area-password** or **domain-password** command, you must use the **no authentication mode** command first.

Examples

The following example configures for the IS-IS instance that MD5 authentication is performed on Level 1 packets:

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain cities level-1
```

Related Commands

Command	Description
area-password	Configures the IS-IS area authentication password.
authentication key-chain	Enables authentication for IS-IS packets and specifies the set of keys that can be used on an interface.
domain-password	Configures the IS-IS routing domain authentication password.
isis authentication mode	Specifies the type of authentication used for an ISIS interface.
key chain	Enables authentication for routing protocols.

authentication send-only

To specify for the IS-IS instance that authentication is performed only on IS-IS packets being sent (not received), use the **authentication send-only** command in router configuration mode. To configure for the IS-IS instance that if authentication is configured at the router level, such authentication be performed on packets being sent and received, use the **no** form of this command.

authentication send-only [**level-1** | **level-2**]

no authentication send-only

Syntax Description	level-1	(Optional) Authentication is performed only on Level 1 packets that are being sent (not received).
	level-2	(Optional) Authentication is performed only on Level 2 packets that are being sent (not received).

Defaults	If authentication is configured at the router level, it applies to IS-IS packets being sent and received.
-----------------	---

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(21)ST	This command was introduced.

Usage Guidelines

Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then specify the **no authentication send-only** command to disable the send-only feature.

If neither the **level-1** nor **level-2** keyword is configured, the send-only feature applies to both levels.

This command could apply to clear text authentication or MD5 authentication. The mode is determined by the **authentication mode** command.

Examples

The following example configures IS-IS Level 1 packets to use clear text authentication on packets being sent (not received):

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication send-only level-1
 authentication mode text level-1
 authentication key-chain cities level-1
```

Related Commands

Command	Description
authentication key-chain	Enables authentication for IS-IS packets and specifies the set of keys that can be used on an interface.
authentication mode	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
key chain	Enables authentication for routing protocols.

debug isis authentication

To enable debugging of IS-IS authentication, use the **debug isis authentication** command in privileged EXEC mode. To disable such debug output, use the **no** form of this command.

debug isis authentication information

no debug isis authentication information

Syntax Description

information	Required keyword that specifies IS-IS authentication information.
--------------------	---

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.

Examples

The following example displays output from the **debug isis authentication** command with the **information** keyword:

```
Router# debug isis authentication information
```

```
3d03h:ISIS-AuthInfo:No auth TLV found in received packet
3d03h:ISIS-AuthInfo:No auth TLV found in received packet
```

The sample output indicates that the router has been running for 3 days and 3 hours. Debug output is about IS-IS authentication information. The local router is configured for authentication, but it received a packet that does not contain authentication data; the remote router does not have authentication configured.

domain-password

To configure the IS-IS routing domain authentication password, use the **domain-password** command in router configuration mode. To disable a password, use the **no** form of this command.

domain-password *password* [**authenticate snp** {**validate** | **send-only**}]

no domain-password [*password*]

Syntax Description	<i>password</i>	Password you assign.
	authenticate snp	(Optional) Causes the system to insert the password into SNP protocol data units (PDUs).
	validate	(Optional) Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
	send-only	(Optional) Causes the system only to insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Defaults	No domain password is specified and no authentication is enabled for exchange of Level 2 routing information.
-----------------	---

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(21)ST	The authenticate snp , validate , and send-only keywords were added.

Usage Guidelines	This password is exchanged as plain text and thus this feature provides only limited security. This password is inserted in Level 2 (area router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs). If you do not specify the authenticate snp keyword along with either the validate or send-only keyword, then the IS-IS routing protocol does not insert the password into SNPs.
-------------------------	---

Examples	The following example assigns an authentication password to the routing domain and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:
-----------------	---

```
router isis
 domain-password users2j45 authenticate snp validate
```

Related Commands	Command	Description
	area-password	Configures the IS-IS area authentication password.
	isis password	Configures the authentication password for an interface.

isis authentication key-chain

To enable authentication for an IS-IS interface, use the **isis authentication key-chain** command in interface configuration mode. To disable such authentication, use the **no** form of this command.

isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Syntax Description

<i>name-of-chain</i>	Enables authentication and specifies the group of keys that are valid.
level-1	(Optional) Enables authentication for Level 1 packets only.
level-2	(Optional) Enables authentication for Level 2 packets only.

Defaults

No key chain authentication is configured for a specific IS-IS interface, although it might be configured at the IS-IS instance level.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.

Usage Guidelines

If no key chain is configured with the **key chain** command, no key chain authentication is performed. Only one authentication key chain is applied to an IS-IS interface at one time. That is, if you configure a second **isis authentication key-chain** command, the first is overridden.

If neither the **level-1** nor **level-2** keyword is configured, the chain applies to both levels.

You can specify authentication for an entire instance of IS-IS instead of at the interface level by using the **authentication key-chain** command.

Examples

The following example configures Ethernet interface 0 to accept and send any key belonging to the key chain named trees:

```
interface Ethernet0
 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 trees level-1
```

Related Commands

Command	Description
authentication key-chain	Enables authentication for IS-IS at the instance level.
key chain	Enables authentication for routing protocols.

isis authentication mode

To specify the type of authentication used for an IS-IS interface, use the **isis authentication mode** command in interface configuration mode. To restore clear text authentication, use the **no** form of this command.

isis authentication mode { **md5** | **text** } [**level-1** | **level-2**]

no isis authentication mode

Syntax Description

md5	Message Digest 5 (MD5) authentication.
text	Clear text authentication.
level-1	(Optional) Enables the specified authentication on the interface for Level 1 packets only.
level-2	(Optional) Enables the specified authentication on the interface for Level 2 packets only.

Defaults

No authentication is provided for IS-IS packets on an interface level, although authentication could be provided at the IS-IS instance level by several means.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.

Usage Guidelines

If neither the **level-1** nor **level-2** keyword is configured, the mode applies to both levels.

If you had clear text authentication configured by using the **area-password** or **domain-password** command, the **authentication mode** command overrides both of those commands.

If you configure the **isis authentication mode** command and subsequently try to configure the **area-password** or **domain-password** command, you will not be allowed to do so. If you truly want to configure clear text authentication using the **area-password** or **domain-password** command, you must use the **no isis authentication mode** command first.

You can specify the type of authentication and the level to which it applies for the entire IS-IS instance, rather than per interface, by using the **authentication mode** command.

Examples

The following example configures IS-IS Level 2 packets to use MD5 authentication on Ethernet interface 0:

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
```

```
isis authentication mode md5 level-2
isis authentication key-chain cisco level-2
```

Related Commands

Command	Description
area-password	Configures the IS-IS area authentication password.
authentication mode	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
domain-password	Configures the IS-IS routing domain authentication password.
key chain	Enables authentication for routing protocols.

isis authentication send-only

To specify that authentication is performed only on packets being sent (not received) on a specified IS-IS interface, use the **isis authentication send-only** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis authentication send-only [**level-1** | **level-2**]

no isis authentication send-only

Syntax Description	level-1	(Optional) Authentication is performed only on Level 1 packets that are being sent (not received).
	level-2	(Optional) Authentication is performed only on Level 2 packets that are being sent (not received).

Defaults If MD5 authentication is configured at the interface level, it applies to IS-IS packets being sent and received over all interfaces.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(21)ST	This command was introduced.

Usage Guidelines Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then specify the **no isis authentication send-only** command to disable the send-only feature.

If neither the **level-1** nor **level-2** keyword is configured, the send-only feature applies to both levels.

Examples The following example configures IS-IS Level-1 packets to use MD5 authentication on packets being sent (not received) on Ethernet interface 0:

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication send-only level-1
 isis authentication mode md5 level-1
 isis authentication key-chain cisco level-1
```

Related Commands

Command	Description
isis authentication key-chain	Enables authentication for IS-IS packets and specifies the set of keys that can be used on an interface.
isis authentication mode	Specifies the type of authentication used in IS-IS packets for the interface.
key chain	Enables authentication for routing protocols.

isis authentication send-only