# Enhancing Security in an IS-IS Network

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

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

## Prerequisites for 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

## 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 devices 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.

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.

### 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" and "Setting a Password at Level 1".

- 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.

## 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.

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, on page 8. 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.

### 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).

### ISIS Authentication Changes

ISIS supports both plain text and cryptographic authentication. However, only one authentication scheme can be configured at a time:

- Configure plain text authentication using the **area-password** command.
- Configure cryptographic authentication using the **authentication key-chain** command for MD5, SHA, or other authentication schemes.

The following behavioral change was introduced that impacts the ISIS authentication configuration method.

Starting with Release 16.10.1, the **authentication key-chain** command can be used to enable cryptographic authentication. Therefore, plain text authentication cannot be configured using the **area-password** command if the **authentication key-chain** command is already configured.

After Release 16.10.1, you are no longer required to issue the **authentication mode** command. Enter the **authentication key-chain** command to configure cryptography. This command cannot co-exist with the plain-text **area-password** command. As a result of the new behavior, you will see the following error message when you attempt to configure authentication in combination with the **authentication key-chain** command:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#router isis abc
Device(config-router)#authentication key-chain isis-key
Device(config-router)#area-password text-pw
%Please configure password using authentication command
Device(config-router)
```

Since the new software does not allow configuration of the **authentication key-chain** command to coexist with the **area-password** command, the behavior change will cause a service interruption when a device is upgraded. This command will be automatically deleted from the new configuration.

# How to Enhance Security in an IS-IS Network

## Setting an Authentication Password for each Interface

**Note** 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**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface gigabitethernet 0/0/0` | Enters interface configuration mode. |
| **Step 4** | **isis password** *password* [**level-1**| **level-2**]<br>**Example:**<br>`Device(config-if)# isis password sjpass level-1` | Configures the authentication password for an interface.<br>• Different passwords can be assigned for different routing levels using the **level-1** and **level-2** keywords.<br>• 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**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show ip interface** [*type number*] [**brief**]<br>**Example:**<br>`Device# show ip interface gigabitethernet 0/0/0` | Displays the usability status of interfaces configured for IP. |

# Setting a Password at Level 1

**Note** 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**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router isis** [**area-** *tag*]<br>**Example:**<br>`Device(config)# router isis salesarea` | Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required.<br>• Enters router configuration mode. |
| **Step 4** | **area-password** *password*<br>**Example:**<br>`Device(config-router)# area-password companyz` | Configures the IS-IS area authentication password.<br>• Using the **area-password** command on all devices in an area will prevent unauthorized devices from injecting false routing information into the link-state database.<br>• 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). |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-router)# end` | Returns to privileged EXEC mode. |

# Setting a Password at Level 2

**Note** 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**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router isis** [*area-tag*]<br>**Example:**<br>`Device(config)# router isis salesarea` | Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required.<br>• Enters router configuration mode. |
| **Step 4** | **domain-password** *password* [**authenticate snp** {**validate** \| **send-only**}]<br>**Example:**<br>`Device(config-router)# domain-password company2` | Configures the IS-IS routing domain authentication password.<br>**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.<br>**Note** Using the **domain-password** command on all devices in an area will prevent unauthorized devices from injecting false routing information into the link-state database.<br>**Note** 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). |
| **Step 5** | **end**<br>**Example:** | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-router)# end` | |

# Configuring IS-IS Authentication

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

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

#### Before you begin

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

#### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **key chain** *name-of-chain*<br>**Example:**<br>`Device(config)# key chain remote3754` | Enables authentication for routing protocols and identifies a group of authentication keys. |
| **Step 4** | **key** *key-id*<br>**Example:**<br>`Device(config-keychain)# key 100` | Identifies an authentication key on a key chain.<br>• The *key-id* argument must be a number. |
| **Step 5** | **key-string** *text*<br>**Example:**<br>`Device(config-keychain-key)# key-string mno172` | Specifies the authentication string for a key.<br>• The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-keychain-key)# exit` | Returns to keychain configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-keychain)# exit` | Returns to global configuration mode. |
| **Step 8** | **router isis** [**area-** *tag*]<br>**Example:**<br>`Device(config)# router isis 1` | Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required.<br>• Enters router configuration mode. |
| **Step 9** | **authentication send-only** [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-router)# authentication send-only` | Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS PDUs being sent (not received). |
| **Step 10** | Repeat Steps 1 through 9 on each device that will communicate. | Use the same key string on each device. |
| **Step 11** | **authentication key-chain** *name-of-chain* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-router)# authentication key-chain remote3754` | Enables MD5 authentication for the IS-IS instance. |
| **Step 12** | Repeat Steps 11 and 12 on each router that will communicate. | -- |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **no authentication send-only**<br>**Example:**<br>`Device(config-router)# no authentication send-only` | Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS PDUs being sent and received.<br>• 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 14** | Repeat Step 14 on each device that will communicate. | -- |

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

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

#### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **key chain** *name-of-chain*<br>**Example:** | Enables authentication for routing protocols and identifies a group of authentication keys. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# key chain multistate87723` | |
| **Step 4** | **key** *key-id*<br>**Example:**<br>`Device(config-keychain)# key 201` | Identifies an authentication key on a key chain.<br>• The *key-id* argument must be a number. |
| **Step 5** | **key-string** *text*<br>**Example:**<br>`Device(config-keychain-key)# key-string idaho` | Specifies the authentication string for a key.<br>• The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-keychain-key)# exit` | Returns to keychain configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-keychain)# exit` | Returns to global configuration mode. |
| **Step 8** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface gigabitethernet 0/0/0` | Configures an interface. |
| **Step 9** | **isis authentication send-only** [**level-1** \| **level-2**]<br>**Example:**<br>`Device(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 device that will communicate. | Use the same key string on each device. |
| **Step 11** | **isis authentication key-chain** *name-of-chain* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)# isis authentication key-chain multistate87723` | Enables MD5 authentication for an IS-IS interface. |
| **Step 12** | Repeat Steps 11 and 12 on each router that will communicate. | -- |
| **Step 13** | **no isis authentication send-only**<br>**Example:** | Specifies that authentication is performed on PDUs being sent and received on a specified IS-IS interface. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-if)# no isis authentication send-only` | |
| **Step 14** | Repeat Step 14 on each device that will communicate. | -- |

## Migrating to a New Authentication Type

### SUMMARY STEPS

1. Load all devices 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, on page 8.

### DETAILED STEPS

**Step 1** Load all devices 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, on page 8.

## Configuring Authentication on a New Router Being Added to a Network That Already Has Authentication 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. **interface** *type number*
9. **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **key chain** *name-of-chain*<br>**Example:**<br>`Device(config)# key chain multistate87723` | Enables authentication for routing protocols and identifies a group of authentication keys. |
| **Step 4** | **key** *key-id*<br>**Example:**<br>`Device(config-keychain)# key 201` | Identifies an authentication key on a key chain.<br>• The *key-id* argument must be a number. |
| **Step 5** | **key-string** *text*<br>**Example:**<br>`Device(config-keychain-key)# key-string idaho` | Specifies the authentication string for a key.<br>• The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-keychain-key)# exit` | Returns to keychain configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-keychain)# exit` | Returns to global configuration mode. |
| **Step 8** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface gigabitethernet 0/0/0` | Configures an interface. |
| **Step 9** | **isis authentication key-chain** *name-of-chain* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)# isis authentication key-chain multistate87723` | Enables MD5 authentication for an IS-IS interface. |

# Configuration Examples for Enhancing Security in an IS-IS Network

## Example Configuring IS-IS HMAC-MD5 Authentication

The following example configures a key chain and key for IS-IS HMAC-MD5 authentication for GigabitEthernet interface 3/0/0 (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 GigabitEthernet3/0/0
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication key-chain cisco level-1
!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication key-chain cisco level-1
!
```

## Example Configuring IS-IS Clear Text Authentication

The following example configures a key chain and key for IS-IS clear text authentication for GigabitEthernet interface 3/0/0 (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 GigabitEthernet3/0/0
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication key-chain cisco level-1
!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication key-chain cisco level-1
!
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Cisco IOS commands | *Cisco IOS Master Commands List, All Releases* |
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| Cisco IOS IPv6 features | *Cisco IOS IPv6 Feature Mapping* |
| IPv6 Routing: IS-IS Multitopology Support for IPv6 | " *Reducing Link Failure and Topology Change Notification Times in IS-IS Networks* " module |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | *IPv6 RFCs* |

### MIBs

| MIB | MIBs Link |
|---|---|
| | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Enhancing Security in an IS-IS Network

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

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

| Feature Name | Releases | Feature Information |
|---|---|---|
| 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 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.<br><br>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |