A

Contents

1 Configuring Keys

1.1 Introduction

1.1.1 Overview

Keys are a kind of parameters that are used in algorithms for conversion from plaintext to ciphertext or from ciphertext to plaintext.

To allow packet authentication in a routing protocol to support plaintext authentication and ciphertext authentication, you must use keys.

Note

- Now, keys are used only for RIP and ISIS packet authentication.
- In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

The key chain provides a tool for the authentication mechanism in a routing protocol.

1. Key Chain

A key chain contains the TCP authentication configuration, authentication algorithm ID, and multiple different keys. Each key has the following attributes:

- Key ID: Identifies a key. In the current key chain, each key corresponds to one ID.
- Authentication string: Specifies a set of key characters used for verifying the consistency of authentication strings in a routing protocol.
- Lifetime: Specifies the lifetime of the current key for sending or receiving packets. Different authentication keys can be used in different periods.
- Authentication algorithm: It is used by keys to authenticate routing protocols.

1.2 Configuring a Key Chain

1.2.1 Overview

This section defines a key chain to be used by a routing protocol.

1.2.2 Restrictions and Guidelines

A key chain can take effect only after it is associated with a routing protocol.

1.2.3 Configuration Tasks

The key configuration includes the following tasks:

(1) Creating a Key Chain

(2) Configuring a Key ID

(3) Configuring a Key String

(4) (Optional) Configuring the Send-Lifetime

(5) (Optional) Configuring the Accept-Lifetime

1.2.4 Creating a Key Chain

1. Overview

In the global configuration mode, you can run the **key chain** *key-chain-name* command to define a key chain and enter the key chain configuration mode.

2. Restrictions and Guidelines

- This configuration is mandatory if a key chain needs to be used.
- If there is no special requirement, you should perform this configuration on all routers that need to authenticate routing protocols.
- To make a key chain take effect, you must configure at least one key.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a key chain, and enter the key chain configuration mode.

key chain *key-chain-name*

No key chain is configured by default.

1.2.5 Configuring a Key ID

1. Overview

In the key chain configuration mode, you can run the **key** *key-id* command to define a key and enter the key chain key configuration mode.

2. Restrictions and Guidelines

- This configuration is mandatory if a key chain needs to be used.

- If there is no special requirement, you should perform this configuration on all devices that need to authenticate routing protocols.
- After the key is configured, it must meet two conditions before it takes effect: (1) the key-string is configured; (2) the key is in the lifetime (send-lifetime and accept-lifetime). If the lifetime is not configured, the key is considered effective permanently once the key-string is configured. Two effective states are defined: effective on the sending end and effective on the receiving end. The two states correspond to send-lifetime and accept-lifetime respectively.
- If there is no special demand, you can configure a key by incrementing the key-id to avoid the authentication state oscillation caused by the possible changes of effective keys. If multiple effective keys exist, each routing protocol uses the key with the smallest key-id.
- In the TCP enhanced authentication scenario, the key-id ranges from 0 to 63.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Create a key ID, and enter the key configuration mode of the key chain.

key *key-id*

No key is configured by default.

1.2.6 Configuring a Key String

1. Overview

In the key configuration mode of the key chain, you can specify a key string in plaintext or cyphertext. To ensure security, you are advised to use cyphertext. If you run the **service password-encryption** command to enable the encryption service, you can forcibly convert a plaintext key string into a ciphertext string.

2. Restrictions and Guidelines

- This configuration is mandatory if a key chain needs to be used.
- If there is no special requirement, you should perform this configuration on all routers that need to authenticate routing protocols.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Enter the key configuration mode of the key chain.

key *key-id*

(5) Configure a key string.

key-string [**0** | **7**] *string-text*

No key string is configured by default.

1.2.7 Configuring the Send-Lifetime

1. Overview

This section defines the lifetime of a key in the sending direction.

2. Restrictions and Guidelines

If the send-lifetime is not configured, the key chain is always effective.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Enter the key configuration mode of the key chain.

key *key-id*

(5) Configure the send-lifetime.

send-lifetime *start-time* { **infinite** | *end-time* | **duration** *duration-time* }

By default, the send-lifetime of a key chain is disabled.

1.2.8 Configuring the Accept-Lifetime

1. Overview

This section defines the lifetime of a key in the receiving direction.

2. Restrictions and Guidelines

If the accept-lifetime is not configured, the key chain is always effective.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Enter the key configuration mode of the key chain.

key *key-id*

(5) Configure the accept-lifetime.

accept-lifetime *start-time* { **infinite** | *end-time* | **duration** *duration-time* }

By default, the accept-lifetime of a key chain is disabled.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Key Monitoring

Command	Purpose
show key chain [*key-chain-name*]	Displays the configurations of a key chain.

1.4 Configuration Examples

1.4.1 Configuring a Key Chain and Using the Key Chain in RIP Packet Authentication

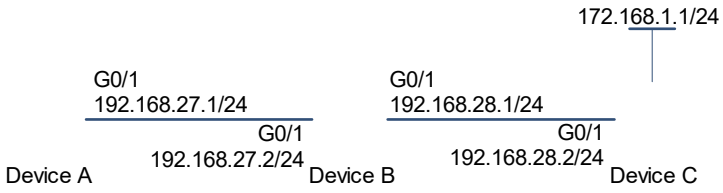
1. Requirements

Device A and Device B are interconnected using the RIP routing protocol. To improve security, you can configure the MD5 encryption algorithm between Device A and Device B to encrypt RIP packets.

Device B accesses 172.168.1.1/24 via the static route.

2. Topology

Figure 1-1 Topology for key authentication



3. Notes

- Configure keys on all routers.
- Configure RIP on all routers.
- Enable RIP authentication on all routers.

4. Procedure

(1) Configure the IP addresses of interfaces.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitEthernet 0/1
Device A(config-if)# ip address 192.168.27.1 255.255.255.0
Device A(config-if)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.27.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure keys and lifetime of each key.

Configure Device A.

```
Device A# configure terminal
Device A(config)# key chain ripchain
Device A(config-keychain)# key 1
Device A(config-keychain-key)# key-string Hello
Device A(config-keychain-key)# accept-lifetime 16:30:00 Oct 1 2013 duration
43200
Device A(config-keychain-key)# send-lifetime 16:30:00 Oct 1 2013 duration 43200
```

```
Device A(config-keychain-key)# exit
Device A(config-keychain)# key 2
Device A(config-keychain-key)# key-string World
Device A(config-keychain-key)# accept-lifetime 04:00:00 Oct 2 2013 infinite
Device A(config-keychain-key)# send-lifetime 04:00:00 Oct 2 2013 infinite
Device A(config-keychain-key)# exit
```

Configure Device B.

```
Device B# configure terminal
Device B(config)# key chain ripchain
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string Hello
Device B(config-keychain-key)# accept-lifetime 16:30:00 Oct 1 2013 duration
43200
Device B(config-keychain-key)# send-lifetime 16:30:00 Oct 1 2013 duration 43200
Device B(config-keychain-key)# exit
Device B(config-keychain)# key 2
Device B(config-keychain-key)# key-string World
Device B(config-keychain-key)# accept-lifetime 04:00:00 Oct 2 2013 infinite
Device B(config-keychain-key)# send-lifetime 04:00:00 Oct 2 2013 infinite
Device B(config-keychain-key)# exit
```

(3) Configure the basic RIP.

Configure Device A.

```
Device A(config)# router rip
Device A(config-router)# version 2
Device A(config-router)# network 192.168.27.0
Device A(config-router)# exit
```

Configure Device B.

```
Device B(config)# router rip
Device B(config-router)# version 2
Device B(config-router)# network 192.168.27.0
Device B(config-router)# redistribute static
Device B(config-router)# exit
```

(4) Set the interface authentication mode to MD5, and specify the authentication key chain.

Configure Device A.

```
Device A(config)# interface gigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain
ripchain
Device A(config-if)# ip rip authentication mode md5
```

Configure Device B.

```
Device B(config)# interface gigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.27.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain
ripchain
Device B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5
```

5. Verification

Check whether Device A can receive routes from Device B.

```
Device A# show ip route rip
R     172.168.0.0/16 [120/1] via 192.168.27.2, 00:05:16, GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file

```
!
key chain ripchain
 key 1
  key-string Hello
  accept-lifetime 16:30:00 Oct 1 2013 duration 43200
  send-lifetime 16:30:00 Oct 1 2013 duration 43200
 key 2
  key-string World
  accept-lifetime 04:00:00 Oct 2 2013 infinite
  send-lifetime 04:00:00 Oct 2 2013 infinite
!
interface gigabitEthernet 0/1
 ip address 192.168.27.1 255.255.255.0
 ip rip authentication key-chain ripchain
 ip rip authentication mode md5
!
router rip
 version 2
 network 192.168.27.0
!
```

- Device B configuration file

```
!
key chain ripchain
 key 1
  key-string Hello
  accept-lifetime 16:30:00 Oct 1 2013 duration 43200
  send-lifetime 16:30:00 Oct 1 2013 duration 43200
```

```
key 2
  key-string World
  accept-lifetime 04:00:00 Oct 2 2013 infinite
  send-lifetime 04:00:00 Oct 2 2013 infinite
!
interface gigabitEthernet 0/1
 ip address 192.168.27.2 255.255.255.0
 ip rip authentication key-chain ripchain
 ip rip authentication mode md5
!
router rip
 version 2
 network 192.168.27.0
 redistribute static
!
```

7. Common Errors

- A key is not correctly associated with a routing protocol, resulting in authentication failures.
- The keys configured on multiple routers are inconsistent, resulting in authentication failures.