Key Management

bintec-Dm 792-I

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1 Introduction

1.1 Introduction

Key management is a method of controlling authentication keys used by routing protocols.

Not all protocols that use authentication have to manage their keys in this way.

The keys must be configured prior to configuring authentication in the protocol.

The key system is simple. It consists of groups of keys known as *key-chains*. Each *key-chain* contains one or more keys. Each key has a unique identifier within the *key-chain*. The keys have a lifetime, which by default is infinite, and can be configured by the network manager. A key is valid until its lifetime has expired.

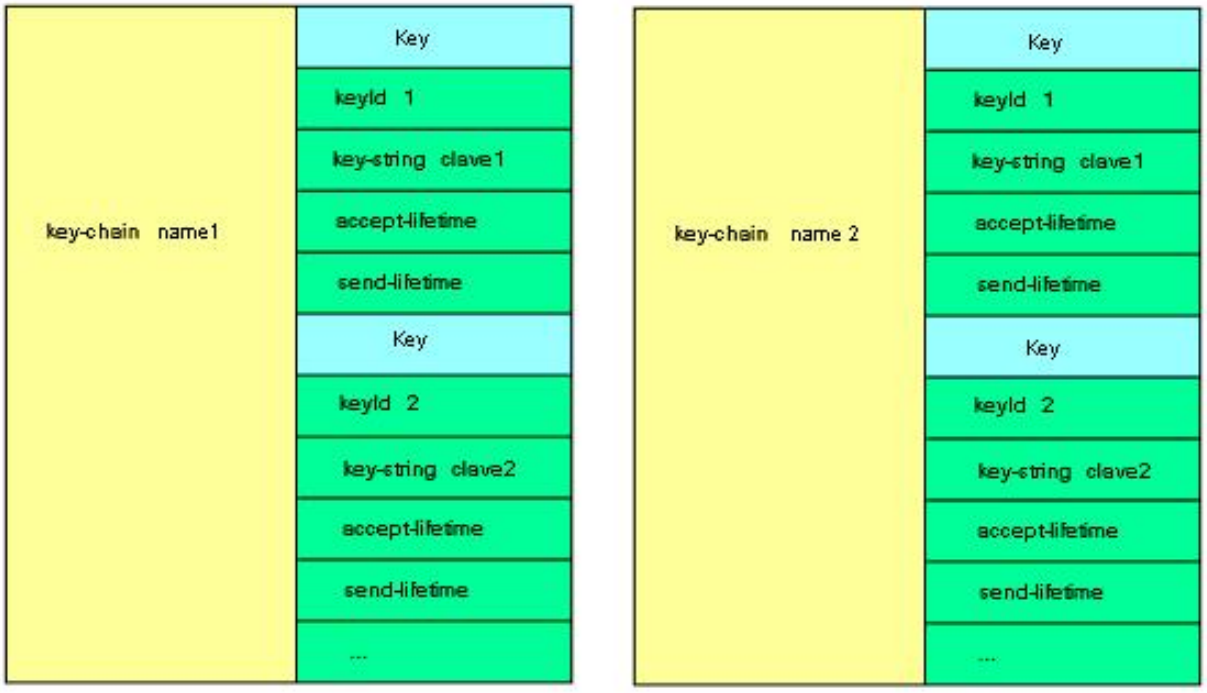
A *key-chain* can have more than one valid key at the same time, but the first valid key with the lowest identifier number is used (activated).

If an active key expires, the next valid key will be used. The keys must be configured to have overlapping lifetimes, i.e., before an active key expires, another must be valid.

Chapter 2 Configuration

2.1 Introduction

Each *key-chain* has two parameters: its name and an array of keys. Each key has the following parameters: identifier, the key itself, the send lifetime and the accept lifetime.



2.2 Accessing the configuration

The creation, modification or elimination *key-chain* operations are executed from a specific menu where you can also view the groups of keys created.

Key Management is organized as a FEATURE in the router's configuration structure. To view the router's configuration functionalities, you must enter the **feature** command followed by a question mark (?).

Example:

```
Config>feature ?
  access-lists              Access generic access lists configuration
                            environment
  afs                       Advanced stateful firewall and routing
  bandwidth-reservation     Bandwidth-Reservation configuration environment
  control-access            Control-access configuration environment
  dns                       DNS configuration environment
  dns-updater               DNS Updater configuration environment
  frame-relay-switch        Frame Relay Switch configuration environment
  ip-discovery              TIDP configuration environment
  istud                     IPSEC Tunnel Server Discovery configuration
                            environment
  key-chain                 Key chain management
  ldap                      LDAP configuration environment
  mac-filtering             Mac-filtering configuration environment
  netflow                   Netflow client configuration
  nsla                      Network Service Level Advisor configuration
  nsm                       Network Service Monitor configuration environment
  ntp                       NTP configuration environment
  prefix-lists              Access generic prefix lists configuration
                            environment
  radius                    RADIUS protocol configuration environment
  route-map                 Route-map configuration environment
```

```
  scada-forwarder          SCADA Forwarder configuration environment
  sniffer                  Sniffer configuration environment
  ssh                      Secure Shell configuration environment
  stun                     Stun facility configuration environment
  syslog                   Syslog configuration environment
  tftp                     TFTP configuration environment
  tips                     Intrusion prevention system
  tms                      TMS configuration environment
  vlan                     IEEE 802.1Q switch configuration environment
  vrf                      VRF configuration environment
  wrr-backup-wan           WRR configuration environment
  wrs-backup-wan           WRS configuration environment
Config>
```

To access the Key Management configuration menu, enter the word **feature** followed by **key-chain** in the configuration root menu (PROCESS 4).

Example:

```
Config> feature key-chain

-- Key Chain user configuration --
Key-chain Config>
```

This gives you access to the Key Management functionality in the configuration main menu. This menu allows you to create, delete and view the groups of keys.

2.3 Main Configuration Menu

The following commands are found in the Key Management main menu:

Command	Function
? (HELP)	Lists the available commands or their options.
Key-chain	Configures a key-chain.
NO	Negates a command or sets its default value.
EXIT	Returns to the general configuration prompt.

2.3.1 ? (HELP)

This command is used to list the valid commands at the current prompt level. You can also use this command after a specific command to list its options.

Syntax:

```
Key-chain Config >?
```

Example:

```
Key-chain Config>?
  key-chain    Key-chain management
  no           Negate a command or set its defaults
  exit
Key-chain Config>
```

2.3.2 KEY-CHAIN

Through this command you can access a submenu that allows you to configure the key-chain parameters.

The name for the group of keys can be up to 16 characters long.

Syntax:

```
Key-chain Config>key-chain ?
  <1..16 chars>    Key-chain name
```

Example:

```
Key-chain Config>key-chain prueba
```

```
Key-chain [prueba] Config>
```

2.3.3 NO

This command is used to disable functions or to set some parameters to their default values.

Syntax:

```
Key-chain Config>no ?
  key-chain    Key-chain management
```

2.3.3.1 NO KEY-CHAIN

Deletes a key-chain and all its content.

Syntax:

```
Key-chain Config>no key-chain <name of key-chain>
```

Example:

```
Key-chain Config>no key-chain prueba
Key-chain Config>
```

2.3.4 EXIT

Exits the Key Management feature configuration menu and returns to the general configuration prompt.

Syntax:

```
Key-chain Config>exit
```

Example:

```
Key-chain Config>exit
Config>
```

2.4 Key Configuration Submenu

You access this menu when editing or creating a new group of keys or *key-chain.*

At the prompt in the new submenu, indicate the group of keys where you want to include the key that will be created.

Example:

```
Key-chain Config>key-chain prueba

Key-chain [prueba] Config>
```

The Key Configuration submenu includes the following subcommands:

Command	Function
? (HELP)	Lists the available commands or their options.
Key	Configures a key.
NO	Negates a command or sets its default value.
EXIT	Returns to the Key Management main menu prompt.

2.4.1 ? (HELP)

This command is used to list the valid commands at the current prompt level. You can also use this command after a specific command to list its options.

Syntax:

```
Key-chain [xxx] Config>?
```

Example:

```
Key-chain [prueba] Config>?
  key     Configure a key
  no      Negate a command or set its defaults
  exit
Key-chain [prueba] Config>
```

2.4.2 KEY

Allows you to modify and create a key within a *key-chain*. This command must be entered followed by an identifier which is the number that identifies the key. The identifier is unique; therefore, if you enter an already existing identifier, the existing entry is changed.

Syntax:

```
Key-chain [xxx] Config>key <id> {<key-string> | <accept-lifetime> | <send-lifetime>}
```

The configuration options for a key are as follows:

```
Key-chain [xxx] Config>key <id> ?
  accept-lifetime    Set accept lifetime of key
  default            Set a command to its defaults
  key-string         Set key string
  send-lifetime      Set send lifetime of key
```

2.4.2.1 KEY <id> ACCEPT-LIFETIME

This command allows you to specify the time period (start and end times and dates) during which a key can be received.

Syntax:

```
Key-chain [xxx] Config>key <id> accept-lifetime <start> <end>
```

Example:

```
Key-chain [prueba] Config>key 1 accept-lifetime 10:30:00 7 aug 2009 infinite
Key-chain [prueba] Config>
```

The key expiration time and date can be defined in one of three ways:

Example:

```
Key-chain [prueba] Config>key 1 accept-lifetime 10:30:00 7 aug 2009 ?
  <0..2147483647>         Set key lifetime duration
  <00:00:00..23:59:00>    Time to stop
  infinite                Never expires
```

Options:

- Enter the validity period in seconds.
- Enter a time and a date, as in the start time and date.
- *Infinite* option: where the key is always valid from the moment it's activated.

2.4.2.2 KEY <id> DEFAULT

The default option sets the default values for the key: *accept-lifetime* and *send-lifetime*.

Syntax:

```
Key-chain [xxx] Config>key <id> default { <key-string> | <accept-lifetime> | <send-lifetime> }
```

Example:

```
Key-chain [prueba] Config>key 1 default ?
  accept-lifetime    Set accept lifetime of key
  key-string         Set key string
  send-lifetime      Set send lifetime of key
```

The following values are established:

- *key-string*: empty.
- *accept-lifetime*: infinite.

- *send-lifetime*: infinite.

2.4.2.3 KEY <id> KEY-STRING

Allows you to enter, in text form, the key that will be used for authentication.

Syntax:

```
Key-chain [xxx] Config>key <id> key-string <key>
```

Example:

```
Key-chain [prueba] Config>key 1 key-string prueba
Key-chain [prueba] Config>
```

The moment you configure a key, the *accept-lifetime* and *send-lifetime* values take their default values.

2.4.2.4 KEY <id> SEND-LIFETIME

Allows you to specify the time period (start and end times and dates) during which a key is valid to be sent.

Syntax:

```
Key-chain [xxx] Config>key <id> send-lifetime <start> <end>
```

Example:

```
Key-chain [prueba] Config>key 1 send-lifetime 10:30:00 7 aug 2009 infinite
Key-chain [prueba] Config>
```

The key expiration time and date can be defined in one of three ways:

Example:

```
Key-chain [prueba] Config>key 1 send-lifetime 10:30:00 7 aug 2009 ?
  <0..2147483647>         Set key lifetime duration
  <00:00:00..23:59:00>    Time to stop
  infinite                Never expires
```

Options:

- Enter the validity period in seconds.
- Enter a time and a date, as in the start time and date.
- *Infinite* option: where the key is always valid from the moment it's activated.

2.4.3 NO

This command is used to disable functions or to set some parameters to their default values.

Syntax:

```
Key-chain [xxx] Config>no ?
  key    Configure a key
```

2.4.3.1 NO KEY

Removes an entry from the array of keys in the *key-chain*.

Syntax:

```
Key-chain [xxx] Config>no key <id>
```

Example:

```
Key-chain [prueba] Config>no key 1
Key-chain [prueba] Config>
```

2.4.4 EXIT

Exits the key configuration menu and returns to the main Key Management menu prompt.

Syntax:

```
Key-chain [xxx] Config>exit
```

Example:

```
Key-chain [prueba] Config>exit
Key-chain Config>
```