K Commands

key

To create a key or to enter the configuration mode for an existing key, use the **key** command. To remove the key, use the **no** form of this command.

key *key-ID*

no key *key-ID*

Syntax Description

key-ID	ID of the key to be configured. This ID must be a whole number between 0 and 65535. **Note** The MACsec key identifier must range from 1 to 32 octet, and the maximum size is 64 characters.

Command Default

None

Command Modes

Keychain configuration (config-keychain)

MACsec keychain configuration (config-macseckeychain)

Command History

Release	Modification
8.2(1)	This command was modified. Support for the MACsec keychain configuration mode was added.
4.0(1)	This command was introduced.

Usage Guidelines

- A new key contains no key strings.
- This command does not require a license.
- To use this command in MACsec keychain configuration mode, you should enable the MKA feature first.

Examples

This example shows how to enter the key configuration mode for key 13 in the glbp-keys keychain:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)#
```

This example shows how to enter the MACsec key configuration mode for key 01 in the k1 MACsec keychain:

```
switch# configure terminal
switch(config)# key chain k1 macsec
switch(config-macseckeychain)# key 01
switch(config-macseckeychain-macseckey)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
feature mka	Enables the MKA feature.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
key-string	Configures the shared secret (text) for a specific key.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
send-lifetime	Configures a send lifetime for a key.
show key chain	Displays keychain configuration.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key chain

To create a keychain or to configure an existing keychain, use the **key chain** command. To unconfigure the keychain, use the **no** form of this command.

key chain *keychain-name* **[macsec]**

no key chain *keychain-name* **[macsec]**

Syntax Description

key chain *keychain-name*	Specifies the name of the keychain. The maximum size is 63 alphanumeric characters. It is case sensitive.
macsec	(Optional) Configures the MACsec keychain.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
8.2(1)	This command was modified. The **macsec** keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

- This command creates a keychain if it does not already exist. A new keychain contains no keys. Note that removing a keychain also removes the keys that are a part of this keychain. Before you remove a keychain, ensure that no feature is using it. If a feature is configured to use a keychain that you remove, that feature is likely to fail to communicate with other devices.
- This command does not require a license.
- To configure a MACsec keychain, you should enable the MKA feature first.

Examples

This example shows how to configure a keychain named glbp-keys:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)#
```

This example shows how to configure a MACsec key chain named k1:

```
switch# configure terminal
switch(config)# key chain k1 macsec
switch(config-macseckeychain)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
feature mka	Enables the MKA feature.
key	Configures a key.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
key-string	Configures a key string.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
send-lifetime	Configures a send lifetime for a key.
show key chain	Displays the keychain configuration.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key config-key

To configure the master key for type-6 encryption, use the **key config-key** command. To delete the master key and stop type-6 encryption, use the **no** form of this command.

key config-key ascii *new-master-key*

no key config-key ascii

Syntax Description

ascii	Specifies the ASCII format.
new-master-key	The master key. The master key can be a minimum of 16 to a maximum of 32 alphanumeric characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the master key for type-6 encryption:

```
switch# key config-key ascii

New Master Key:
Retype Master Key:
```

This example shows how to delete the master key and stop type-6 encryption:

```
switch# no key config-key ascii

Warning deletion of master-key will stop further type-6 encryption.
Do you want to proceed (y/n)[n]: [n] y
switch#
```

Related Commands

Command	Description
feature password encryption aes	Enables the AES password encryption features.
show encryption service stat	Displays the status of the encryption service.

key-octet-string

To configure the text for a MACsec key, use the **key-octet-string** command. To remove the text, use the **no** form of this command.

key-octet-string [**0** | **7**] *key-octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**}

no key-octet-string [**0** | **7**] *key-octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**}

Syntax Description

0	(Optional) Specifies the type of encryption to use. The *key-octet-string* argument that you enter is unencrypted text.
7	(Optional) Specifies the type of encryption to use. The *key-octet-string* argument that you enter is encrypted. The encryption method is a Cisco-proprietary method. This option is useful when you are entering a text string based on the encrypted output of the **show key chain** command that you run on another Cisco NX-OS device.
key-octet-string	Text of the key octet string. The text is alphanumeric, case sensitive, and can have up to 64 characters. **Note** The text can have up to 130 characters for encryption type 7.
cryptographic-algorithm	Specifies the Cipher-based Message Authentication Code (CMAC) algorithm for authentication.
AES_128_CMAC	Configures the 128-bit AES encryption algorithm.
AES_256_CMAC	Configures the 256-bit AES encryption algorithm.

Command Default

The key octet string is not encrypted.

Command Modes

MACsec key configuration (config-macseckeychain-macseckey)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

The key octet string is a shared secret. The device stores key strings in a secure format. You can obtain encrypted key strings by using the **show key chain** command on another Cisco NX-OS device. This command does not require a license. To use this command, you must enable the MKA feature.

Examples

This example shows how to set a key octet string:

```
switch# configure terminal
switch(config)# key chain k1 macsec
switch(config-macseckeychain)# key 03
switch(config-macseckeychain-macseckey)# key-octet-string 0123456789aabbcc0123456789aabbcc
 cryptographic-algorithm AES_128_CMAC
switch(config-macseckeychain-macseckey)#
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key-server-priority

To configure the preference for a device to serve as the key server for MACsec Key Agreement (MKA) encryption, use the **key-server-priority** command. To reset the default preference, use the **no** form of this command.

key-server-priority *value*

no key-server-priority *value*

Syntax Description

value	Priority for a device to become the key server. The lower the value, the higher the preference. The range is from 0 to 255.

Command Default

16

Command Modes

MACsec policy configuration (config-macsec-policy)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, enable the MKA feature.

Examples

This example shows how to set the key server priority:

```
switch# configure terminal
switch(config)# macsec policy p1
switch(config-macsec-policy)# key-server-priority 9
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec keychain policy	Configures the MACsec keychain policy.

Command	Description
macsec policy	Configures the MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key-string

To configure the text for a key, use the **key-string** command. To remove the text, use the **no** form of this command.

key-string [*encryption-type*] *text-string*

no key-string *text-string*

Syntax Description

encryption-type	(Optional) Type of encryption to use. The *encryption-type* argument can be one of the following values: • 0—The text-string argument that you enter is unencrypted text. This is the default. • 7—The text-string argument that you enter is encrypted. The encryption method is a Cisco proprietary method. This option is useful when you are entering a text string based on the encrypted output of a **show key chain** command that you ran on another Cisco NX-OS device.
text-string	Text of the key string, up to 63 case-sensitive, alphanumeric characters. The value of the first 2 digits of a type 7 key string configured by using the **key-string 7** *text-string* command has to be between 0 and 15. For example, you can configure 07372b557e2c1a as the key string value in which case the sum value of the first 2 digits will be 7. But, you cannot configure 85782916342021 as the key string value because the value of the first 2 digits will be 85. We recommend unconfiguring any type 7 key strings that do not adhere to this value or to configure a type 0 string.

Command Default

None

Command Modes

Key configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The key-string text is a shared secret. The device stores key strings in a secure format.

You can obtain encrypted key strings by using the **show key chain** command on another Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enter an encrypted shared secret for key 13:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# key-string 7 071a33595c1d0c1702170203163e3e21213c20361a021f11
switch(config-keychain-key)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key	Configures a key.
key chain	Configures a keychain.
send-lifetime	Configures a send lifetime for a key.
show key chain	Shows keychain configuration.