About This Document

Intended Audience

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Interface Numbering Conventions

Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

Security Conventions

- Password setting
  - When configuring a password, the cipher text is recommended. To ensure device security, change the password periodically.
  - When you configure a password in plain text that starts and ends with %^%#.....%^%# (the password can be decrypted by the device), the password is displayed in the same manner as the configured one in the configuration file. Do not use this setting. After the system master key is set using the **set master-key** command, do not start and end the key with **%@%#** because the string starting and ending with **%@%#** is considered as a valid cipher-text key.
  - When you configure a password in cipher text, different features cannot use the same cipher-text password. For example, the cipher-text password set for the AAA feature cannot be used for other features.

- After the system software is downgraded and the switch restarts with the configuration of the higher version, AAA, VTY, serial interface login, and SNMP user passwords become invalid. As a result, users fail to log in to the switch using the passwords and the switch is disconnected from the network management system.

  To address this problem, take the following measures:

  i. If no password is configured for the console port, log in to the device through the console port, and reconfigure AAA and password for users such as VTY and SNMP users. For security purposes, the console port password is recommended.

  ii. If a password is configured for login through the console port, the password becomes invalid after the downgrade and you cannot log in to the switch through the console port. In this case, contact Huawei technical support engineers for assistance.

- Encryption algorithm

  Currently, the device uses the following encryption algorithms: DES, 3DES, AES, DSA, RSA, DH, ECDH, HMAC, SHA1, SHA2, PBKDF2, scrypt, and MD5. The encryption algorithm depends on the applicable scenario. Use the recommended encryption algorithm; otherwise, security defense requirements may be not met.

  - For the symmetrical encryption algorithm, use AES with the key of 256 bits or more.
  - When you need to use an asymmetric cryptography, RSA (3072-bit or longer key) is recommended. In addition, use different key pairs for encryption and signature.
  - For the digital signature, RSA (3072-bit or longer key) or DSA (2048-bit or longer key) is recommended.
  - For key negotiation, DH (2048-bit or longer key) or ECDH (256-bit or longer key) is recommended.
  - For the hash algorithm, use SHA with the key of 256 bits or more.
  - For the HMAC algorithm, use HMAC-SHA2.
  - DES, 3DES, RSA and AES are reversible encryption algorithm. If protocols are used for interconnection, the locally stored password must be reversible.
  - SHA1, SHA2, and MD5 are irreversible encryption algorithm. When configuring a password for local administrator, it is recommended that you use the SHA2 irreversible encryption algorithm.
  - To prevent brute force cracking of the user password, the iteration algorithm is added to the password on the basis of salts. The iteration algorithm uses PBKDF2 or scrypt key export algorithm.
  - The ECB mode has a poor capability of defending against plaintext playback attacks, so ECB is not recommended for password encryption.
  - In SSH2.0, the symmetric cryptography using the CBC mode may undergo the plaintext-recovery attack to cause a data leak. Therefore, the CBC mode is not recommended for SSH2.0.

- Data

  Some data (such as MAC or IP addresses of terminals) may be obtained or used during operation or fault location of your purchased products, services,

features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect data.

- The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this manual are mentioned only to describe the product's function of communication error or failure detection, and do not involve collection or processing of any personal information or communication data of users.

Declaration

- This manual is only a reference for you to configure your devices. The contents in the manual, such as command line syntax, and command outputs, are based on the device conditions in the lab. The manual provides instructions for general scenarios, but do not cover all usage scenarios of all product models. The contents in the manual may be different from your actual device situations due to the differences in software versions, models, and configuration files. The manual will not list every possible difference. You should configure your devices according to actual situations.
- The specifications provided in this manual are tested in lab environment (for example, the tested device has been configured with a certain type of cards or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values with multiple functions enabled on the device.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.

Mapping Between Product Software and Related Products

For details about the mapping between product software and related products, see **CloudEngine Switches Software Versions**. Select the correct matching version. Otherwise, functions may be unavailable.

 Copyright © Huawei Technologies Co., Ltd.