About This Document

Intended Audience

This document is intended for network engineers responsible for switch configuration and management. You should be familiar with basic Ethernet knowledge and have extensive experience in network deployment and management.

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
  - To ensure device security, use ciphertext when configuring a password and change the password periodically.
  - The switch considers all passwords starting and ending with %^%#, %#%#, %@%@ or @%@% as ciphertext and attempts to decrypt them. If you configure a plaintext password that starts and ends with %^%#, %#%#, %@%@ or @%@%, the switch decrypts it and records it into the configuration file (plaintext passwords are not recorded for the sake of security). Therefore, do not set a password starting and ending with %^%#, %#%#, %@%@ or @%@%.
  - When you configure passwords in ciphertext, different features must use different ciphertext passwords. For example, the ciphertext password set for the AAA feature cannot be used for other features.

- Encryption algorithms

  The switch currently supports the 3DES, AES, RSA, SHA1, SHA2, and MD5. 3DES, RSA, and AES are reversible, whereas SHA1, SHA2, and MD5 are irreversible. Using the encryption algorithms DES, 3DES, RSA (RSA-1024 or lower), MD5 (in digital signature scenarios and password encryption), or SHA1 (in digital signature scenarios) is a security risk. If protocols allow, use more secure encryption algorithms, such as AES, RSA (RSA-2048 or higher), SHA2, or HMAC-SHA2.

  An irreversible encryption algorithm must be used for the administrator password. SHA2 is recommended for this purpose.

- Personal data

  Some personal 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 personal data.

- Mirroring

  The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this document 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.

- Reliability design declaration

  Network planning and site design must comply with reliability design principles and provide device- and solution-level protection. Device-level protection includes planning principles of dual-network and inter-board dual-link to avoid single point or single link of failure. Solution-level protection refers to a fast convergence mechanism, such as FRR and VRRP. If solution-level protection is used, ensure that the primary and backup paths do not share links or transmission devices. Otherwise, solution-level protection may fail to take effect.

Disclaimer

- This document is designed as a reference for you to configure your devices. Its contents, including web pages, command line input and output, are based on laboratory conditions. It provides instructions for general scenarios, but does not cover all use cases of all product models. The examples given may differ from your use case due to differences in software versions, models, and configuration files. When configuring your device, alter the configuration depending on your use case.
- The specifications provided in this document are tested in a lab environment (for example, a certain type of cards have been installed on the tested device or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values due to factors such as differences in hardware configurations and carried services.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.