前言

读者对象

本文档适用于负责配置和管理交换机的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其他不可预知的结果。 “须知”不涉及人身伤害。
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。

格式	意义
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

接口编号约定

本手册中出现的接口编号仅作示例，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。

安全约定

- 密码配置约定
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置明文模式的密码时，请不要以“%^%#.....%^%#”、“%#%#.....%#%#”、“%@%@.....%@%@”或者“@%@%.....@%@%”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文。
  - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
- 加密算法约定

  目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。
- 个人数据约定

  您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。
- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用，不涉及采集、处理任何个人数据或任何用户通信内容。
- 可靠性设计声明

  对于网络规划和站点设计，必须严格遵守可靠性设计原则，具备设备级和方案级保护。设备级保护包括双网双平面，双机、跨板双链路的规划原则，避免出现单

点，单链路故障。方案级指FRR、VRRP等快速收敛保护机制。在应用方案级保护时，应避免保护方案的主备路径经过相同链路或者传输，以免方案级保护不生效。

特别声明

- 本文档仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。文档提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成文档中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本文档不再针对前述情况造成的差异一一说明。
- 本文档中提供的最大值是设备在实验室特定场景（例如，被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与文档中提供的数据不一致。
- 出于特性介绍及配置示例的需要，本文档可能会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。

