V7交换机使用configuration encrypt进行配置加密使用的加密算法是什么?

加密引擎 彭旭 2022-01-15 发表

问题描述

V7交换机使用configuration encrypt进行配置加密使用的加密算法是什么?

解决方法

configuration encrypt命令用来开启配置文件加密功能

private-key：使用私钥进行加密。所有运行Comware V7平台软件的设备拥有相同的私钥。

public-key：使用公钥进行加密。所有运行Comware V7平台软件的设备拥有相同的公钥。

实现原理为明文配置经3des-cbc加密为密文配置，上面提及的公钥和私钥并不是密码学上特指的非对称加解密使用的公钥和私钥的概念（公钥加密、私钥解密），对于密码模块，公钥和私钥就是两把独立的key，都是用来做3des-cbc加解密的。