

交换机密码策略实现的解决办法

产品特性 H3C模拟器 韦家宁 2020-02-18 发表

组网及说明

不涉及

本案例采用H3C HCL模拟器的S5820来配置设备的密码策略

问题描述

随着网络安全的发展，对于网络设备密码的安全性有了更加严格要求。因此需要在网络设备通过密码策略来保障设备的安全。

过程分析

- 1、如果需要针对交换机管理的所有用户登陆密码做限制，需要在全局配置密码策略。
- 2、如果仅针对交换机的某个用户做密码策略的限制，需要在具体的用户视图下配置密码策略。

解决方法

- 1、针对全部的登陆用户做限制，需要在全局配置密码策略：

```
[H3C]password-control enable //开启密码策略
[H3C]password-control aging enable //开启密码有效期的策略
[H3C]password-control aging 90 //配置密码有效的时间为90天
[H3C]password-control length enable //开启密码长度的限制
[H3C]password-control length 16 //配置密码长度最小为16位
[H3C]password-control login-attempt 10 exceed lock-time 10 //配置密码可尝试的失败次数为10次，10次失败以后被锁定10分钟后方可继续尝试
```

- 2、针对某个用户做限制，需要在具体用户视图下做配置：

```
[H3C]password-control enable //开启密码策略
[H3C]local-user admin //创建admin用户
[H3C-luser-manage-admin]password-control aging 90 //配置admin用户密码有效期为90天
[H3C-luser-manage-admin]password-control length 8 //配置admin用户密码长度最小为8位
[H3C-luser-manage-admin]password-control login-attempt 10 exceed lock-time 5 //配置admin用户的密码可尝试的失败次数为10次，10次失败以后被锁5分钟后方可继续尝试
```

注意：

- 1、假设用户内和全局都配置了密码策略，则该用户内的密码策略生效
- 2、假设用户内没有配置密码策略且全局开启了密码策略，则生效的是全局的密码策略