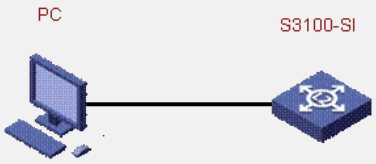
S3100-SI使用不同版本做SSH登录时存在差异的经验案例

董亮 2007-08-01 发表

S3100-SI使用不同版本做SSH登录时存在差异的经验案例

一、 组网：



PC通过SSH方式登陆到S3100-SI交换机上。

二、 问题描述：

S3100-SI使用R0011P02版本及其之前的版本配合secureCRT做SSH登录时,采用password方式，可以正常登录；当使用R2102P01版本及其以后的版本配合secureCRT做SSH登录时,采用password方式，必须更改相应配置之后才能正常登录。

三、 过程分析：

由于使用版本R2102P01时，交换机跟secureCRT终端协商的过程中采用的加密方式可能是RSA的也可能是DSA，如果交换机上没有生成对应的密钥对，则无法正常登录。而R0011P02之前的版本紧紧支持RSA方式，因此不必要创建DSA密钥对，也不可能协商成DSA方式，而在R2102P以后的版本同时支持了DSA方式。所以在使用SSH登陆时必须保证在交换机上同时生成RSA和DSA的密钥对,才能正常登录。

四、 解决方法：

无论是S3100-SI的那些版本都必须配置下面的通用配置：

1．设置用户接口上的认证模式为AAA认证。

[H3C] user-interface vty 0 4

[H3C-ui-vty0-4] authentication-mode scheme

2．设置用户接口上支持SSH协议

[H3C-ui-vty0-4] protocol inbound ssh

3．指定用户client001的登录协议为SSH，认证方式为password，认证密码为abc

[H3C] local-user client001

[H3C-luser-client001] password simple abc

[H3C-luser-client001] service-type ssh level 3

[H3C-luser-client001] quit

[H3C] ssh user client001 authentication-type password

在完成上述通用配置的基础之上，还必须根据不同的版本选择创建不同的密钥对：

配置一（适用于R0011P02之前的版本）：

1．生成本地RSA密钥

<H3C>system-view

[H3C] rsa local-key-pair create

配置二（适用于R2102之后的版本）：

1．生成本地RSA密钥

[H3C] public-key local create rsa

2．生成本地DSA密钥

[H3C] public-key local create dsa