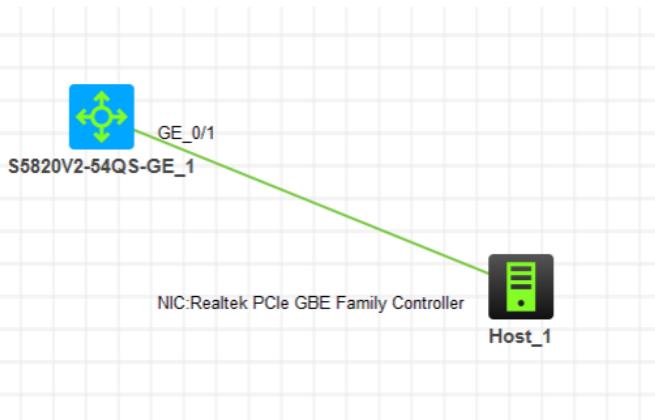


H3C 5820交换机用户分权解决办法

SSH 对象组 蒙面人-乙 2019-12-01 发表

组网及说明

随着网络安全问题的趋势日益严峻，设备访问权限越来越重要，根据用户分权的需求，不同的登陆用户要分配不同的账号。



配置步骤

- 1、配置基础网络，确保终端能PING通交换机
- 2、创建管理员账号，赋予最高权限，并只能通过SSH登录
- 3、创建访客账号，赋予1级权限，无法对设备进行配置，仅赋予查看等普通权限，并只能通过SSH登录

配置关键点

1、基础网络配置：

```
<H3C>sys  
System View: return to User View with Ctrl+Z.  
[H3C]vlan 10  
[H3C-vlan10]quit  
[H3C]int vlan 10  
[H3C-Vlan-interface10]ip address 192.168.124.254 24  
[H3C-Vlan-interface10]quit  
[H3C]int gi 1/0/1  
[H3C-GigabitEthernet1/0/1]port link-type access  
[H3C-GigabitEthernet1/0/1]port access vlan 10  
[H3C-GigabitEthernet1/0/1]quit
```

2、创建管理员账号，并赋予最高权限，仅允许SSH登录

```
[H3C]local-user admin  
New local user added.  
[H3C-luser-manage-admin]password simple admin  
[H3C-luser-manage-admin]service-type ssh  
[H3C-luser-manage-admin]authorization-attribute user-role network-admin  
[H3C-luser-manage-admin]quit
```

3、创建访客账号，赋予1级权限，仅允许SSH登录

```
[H3C]local-user user  
New local user added.  
[H3C-luser-manage-user]password simple 123456  
[H3C-luser-manage-user]service-type ssh  
[H3C-luser-manage-user]authorization-attribute user-role level-1  
[H3C-luser-manage-user]quit
```

4、开启SSH功能

```
[H3C]ssh server enable
```

5、在VTY调用本地用户登录

```
[H3C]line vty 0 4  
[H3C-line-vty0-4]authentication-mode scheme  
[H3C-line-vty0-4]protocol inbound ssh  
[H3C-line-vty0-4]quit
```

6、设置电脑IP，并PING通交换机

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator.USER-20190510MA>ipconfig

Windows IP 配置

以太网适配器 本地连接:

连接特定的 DNS 后缀 . . . . . : fe80::5545:6be3:e25f:35fa%12
本地链接 IPv6 地址 . . . . . : fe80::5545:6be3:e25f:35fa%12
IPv4 地址 . . . . . : 192.168.124.7
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 192.168.124.1
```

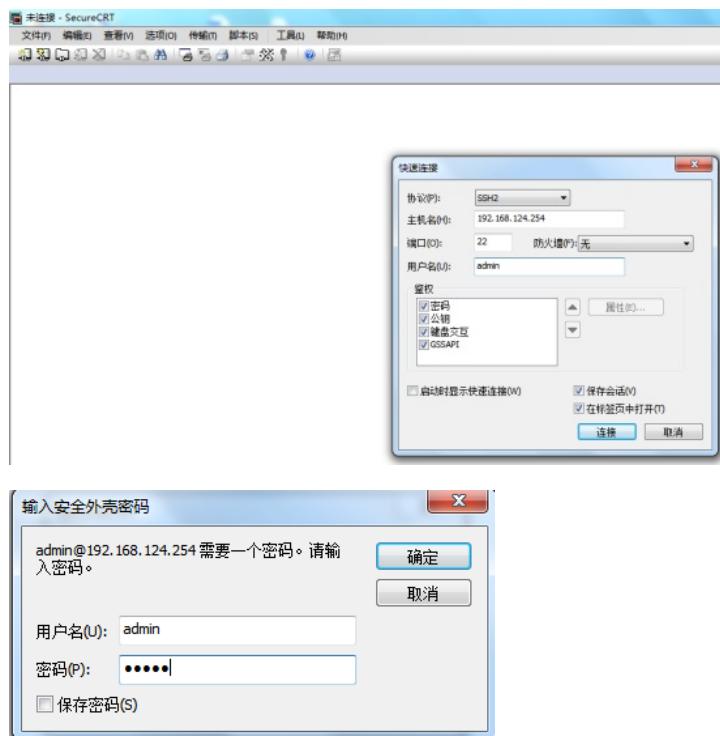
```
C:\Users\Administrator.USER-20190510MA> ping 192.168.124.254

正在 Ping 192.168.124.254 具有 32 字节的数据:
来自 192.168.124.254 的回复: 字节=32 时间<1ms TTL=255

192.168.124.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 <0% 丢失>,
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator.USER-20190510MA>
```

7、使用管理员登录账号，且能进行配置

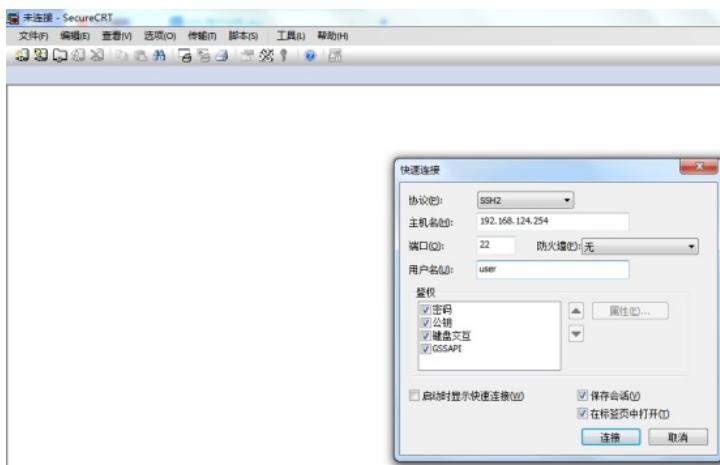


```
192.168.124.254 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(I) 帮助(H)
192.168.124.254

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved. *
* without the owner's prior written consent. *
* no decompiling or reverse-engineering shall be allowed. *
*****
```

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]
```

8、使用访客账号登录交换机，无法对交换机进行配置



```
192.168.124.254 (4) - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(U) 帮助(H)

192.168.124.254 (4)

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved. *
* without the owner's prior written consent,                         *
* no decompiling or reverse-engineering shall be allowed.          *
*****  
  
<H3C>sys
System view: return to User view with Ctrl+Z.
[H3C]?
System view commands:
  access-list Alias for 'acl'
  display  Display current system information
  end      Alias for 'return'
  erase    Alias for 'delete'
  exit     Alias for 'quit'
  hostname Alias for 'sysname'
  local-user Configure a local user
  logging  Alias for 'info-center'
  no       Alias for 'undo'
  ping     Ping function
  probe    Probe Module
  quit    Exit from current command view
  return   Exit to User view
  show    Alias for 'display'
  tracert Tracert function
  write   Alias for 'save'  
  
[H3C]vlan 10
Permission denied.
[H3C]
```

附件下载: H3C用户分权.doc