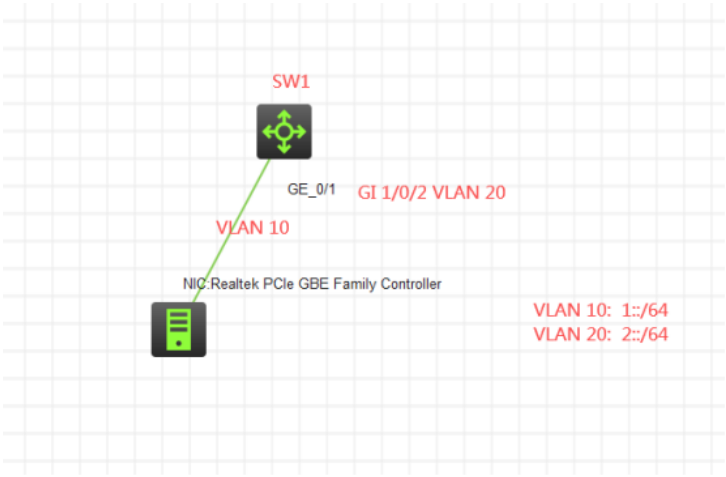
使用IPV6 ACL对telnet登陆进行限定

IPv6 ACL VLAN Telnet H3C模拟器 **韦家宁** 2020-02-27 发表

组网及说明



组网说明:
本案例采用H3C HCL模拟器的S5820交换机来使用IPV6 ACL对telnet进行登录的限定。要求仅允许VLAN 10的IPV6地址能对SW1交换机进行telnet远程登陆管理。

特别说明:
由于模拟器的局限性，因此首先使用物理机通过VLAN10来进行SSH登录测试，其次在将物理机切换到VLAN20来进行telnet登录测试。

配置步骤

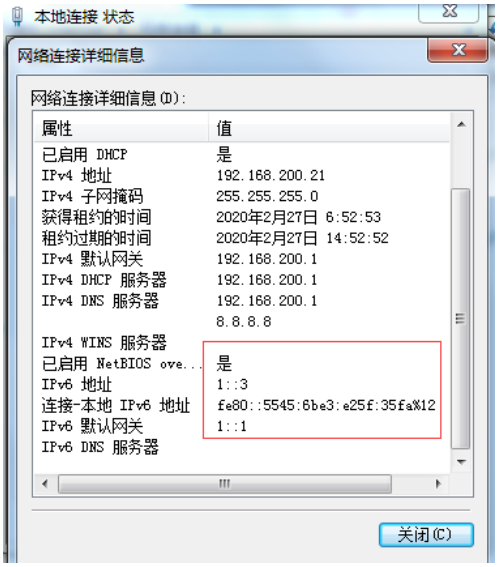
1、按照网络拓扑图正确划分VLAN并配置IP地址
2、SW1开启telnet服务，并创建相应账户及赋予权限。
3、SW1创建IPV6 ACL，并应用到telnet

配置关键点

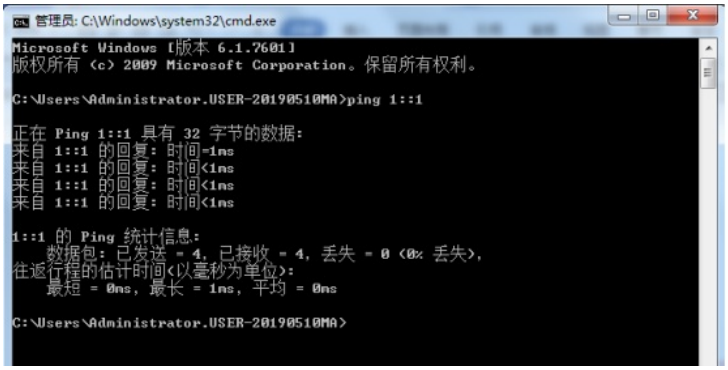
```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SW1
[SW1]vlan 10
[SW1-vlan10]quit
[SW1]vlan 20
[SW1-vlan20]quit
[SW1]int vlan 10
[SW1-Vlan-interface10]ipv6 address 1::1 64
[SW1-Vlan-interface10]quit
[SW1]int vlan 20
[SW1-Vlan-interface20]ipv6 address 2::1 64
[SW1-Vlan-interface20]quit
[SW1]int gi 1/0/2
[SW1-GigabitEthernet1/0/2]port link-type access
[SW1-GigabitEthernet1/0/2]port access vlan 20
[SW1-GigabitEthernet1/0/2]quit
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-type access
[SW1-GigabitEthernet1/0/1]port access vlan 10
[SW1-GigabitEthernet1/0/1]quit
[SW1]acl ipv6 basic 2000
[SW1-acl-ipv6-basic-2000]rule 0 permit source 1:: 64
[SW1-acl-ipv6-basic-2000]rule 1 deny source any
[SW1]local-user ninglihua
New local user added.
[SW1-luser-manage-ninglihua]password simple ninglihua
[SW1-luser-manage-ninglihua]service-type ssh telnet http https
```

[SW1-luser-manage-ninglihua]authorization-attribute user-role network-admin
[SW1-luser-manage-ninglihua]quit
[SW1]line vty 0 4
[SW1-line-vty0-4]authentication-mode scheme
[SW1-line-vty0-4]protocol inbound all
[SW1-line-vty0-4]quit
[SW1]telnet server enable
[SW1]telnet server ipv6 acl ipv6 2000

测试：
物理机填写IP地址：

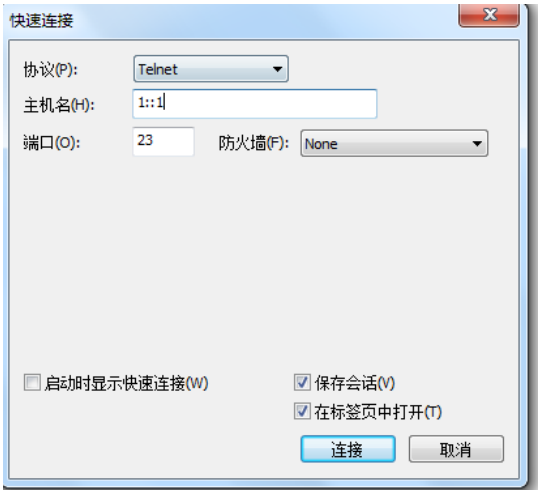


物理机能PING通SW1：

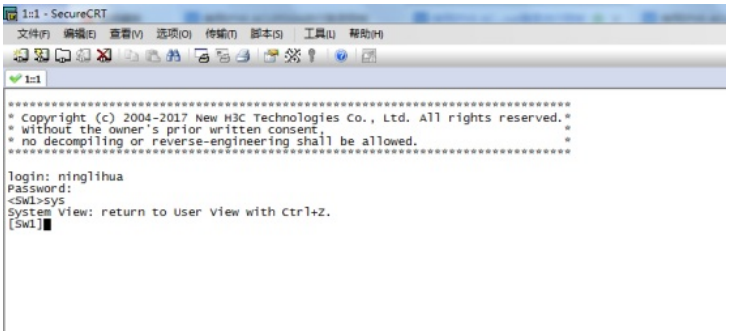


打开CRT：

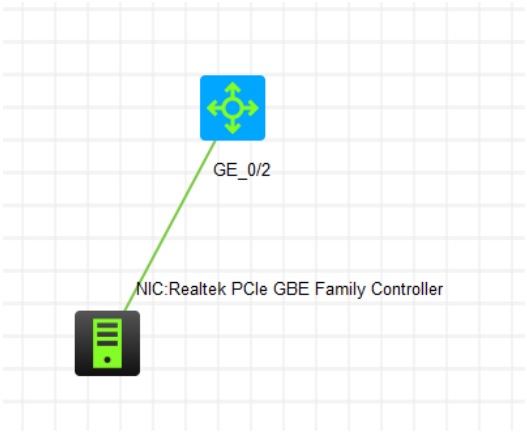
输入要登陆SW1的IPV6地址，点击连接：



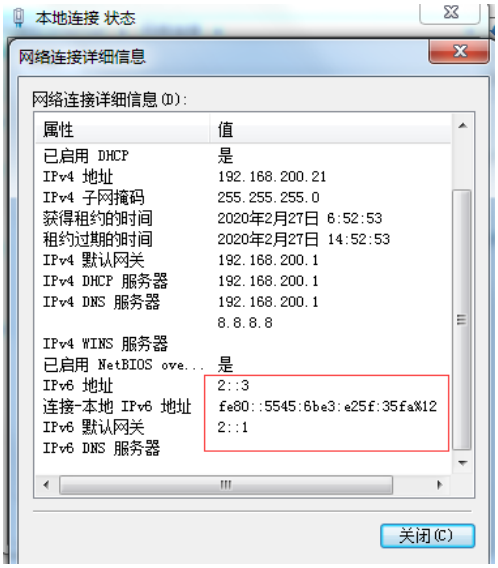
输入用户名、密码，回车，登陆成功：



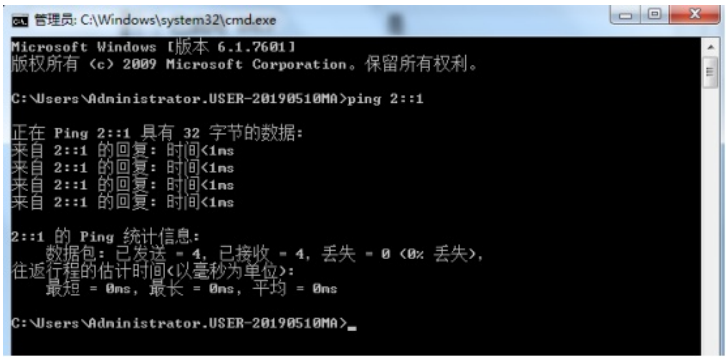
将物理机接到SW1的GI 1/0/2端口，GI 1/0/2端口所属VLAN20：



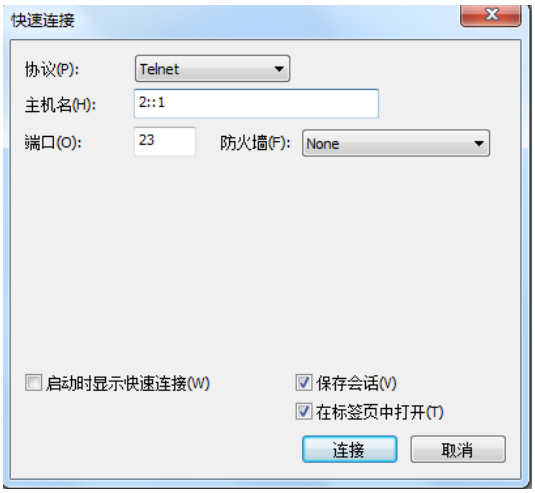
物理机修改IP地址：



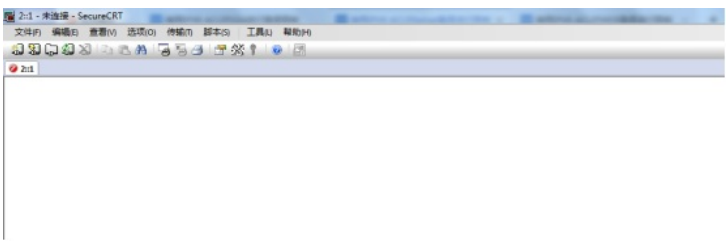
物理机能PING通SW1：



继续打开CRT，输入要SSH登陆SW1的IPV6地址，和用户名，点击连接：



使用VLAN 20的地址telnet登陆SW1失败：



在SW1可看到拒绝登陆的提示：

查看IPV6 ACL的匹配记录：

```
[SW1]dis acl ipv6 all
Basic IPv6 ACL 2000, 2 rules,
ACL's step is 5
 rule 0 permit source 1::/64
 rule 1 deny (7 times matched)

[SW1]
```

至此，使用IPV6 ACL对telnet登录进行限定的典型组网配置案例已完成！