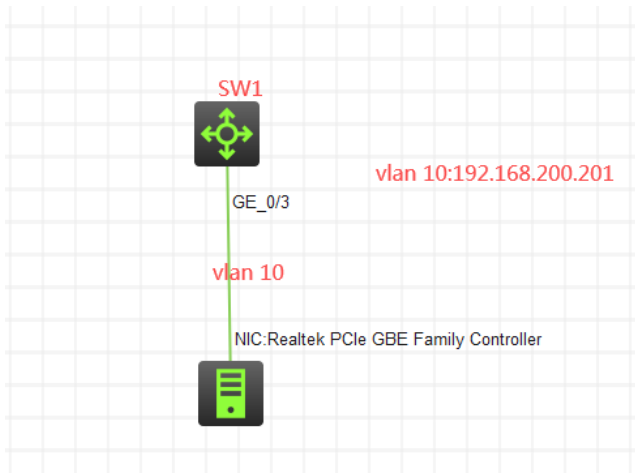


知 使用ACL对telnet登陆交换机限制典型组网配置案例

VLAN ACL Telnet H3C模拟器 韦家宁 2020-02-26 发表

组网及说明



组网说明:

本案例采用H3C HCL模拟器来实现telnet远程登陆管理，并通过ACL对telnet进行限定。

配置步骤

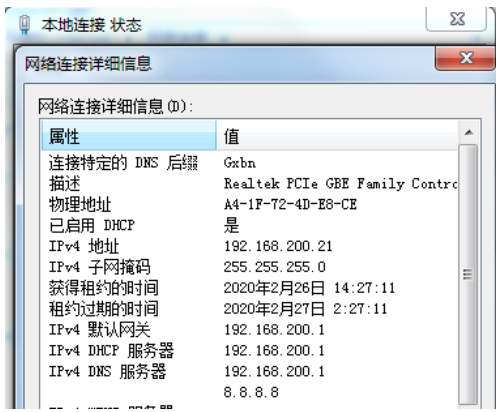
- 1、按照网络拓扑图正确配置IP地址及划分VLAN
- 2、SW1开启telnet功能，并创建相应账户及赋予权限
- 3、SW1配置ACL，仅允许192.168.200.21登陆，并绑定到telnet，对telnet登陆进行限定

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]int vlan 10
[SW1-Vlan-interface10]ip address 192.168.200.201 24
[SW1-Vlan-interface10]quit
[SW1]int gi 1/0/3
[SW1-GigabitEthernet1/0/3]port link-type access
[SW1-GigabitEthernet1/0/3]port access vlan 10
[SW1-GigabitEthernet1/0/3]quit
[SW1]local-user weijianing
New local user added.
[SW1-luser-manage-weijianing]password simple weijianing
[SW1-luser-manage-weijianing]service-type telnet
[SW1-luser-manage-weijianing]authorization-attribute user-role network-admin
[SW1-luser-manage-weijianing]quit
[SW1]telnet server enable
[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]acl basic 2000
[SW1-acl-ipv4-basic-2000]rule 0 permit source 192.168.200.21 0
[SW1-acl-ipv4-basic-2000]quit
[SW1]telnet server acl 2000
```

测试:

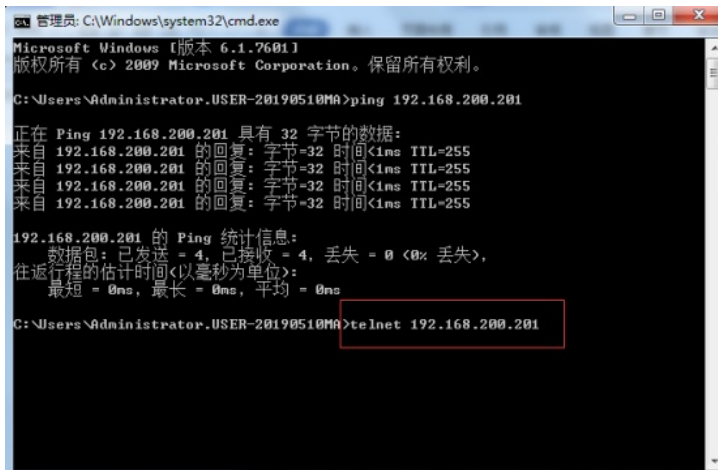
物理机填写IP地址:



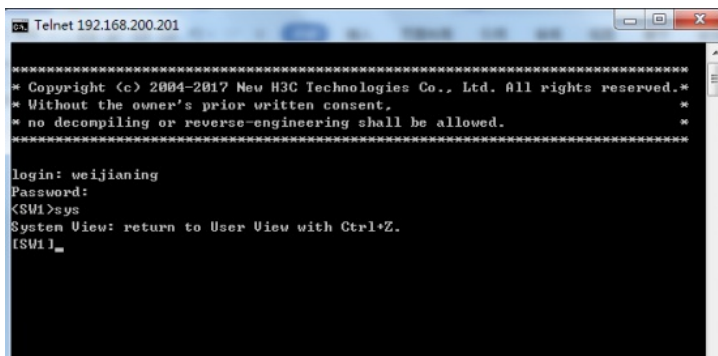
物理机能PING通SW1:



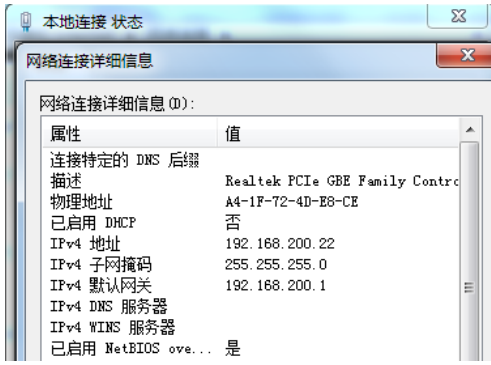
使用telnet 192.168.200.201命令, 登陆交换机:



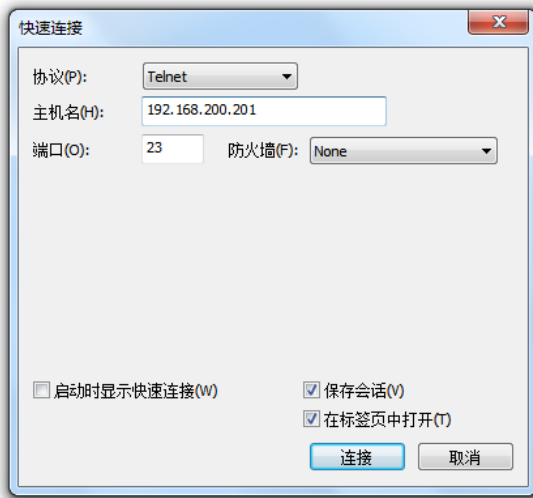
输入用户名、密码, 回车, 登陆成功:



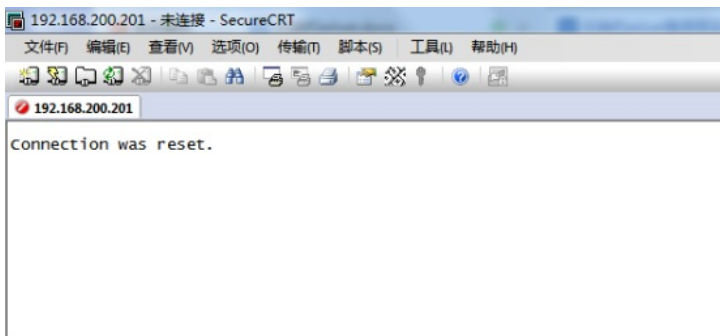
修改物理机的IP地址为: 192.168.200.22



使用CRT:



无法登陆上:



交换机有拒绝登陆的提示:

```
hcl_ywpm9
SS820V2-5443-GE_1
[SW1-luser-manage-weijianing]authorization-attribute user-role network-admin
[SW1-luser-manage-weijianing]quit
[SW1]telnet server enable
[SW1]line
[SW1]line vt
[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]acl basic 2000
[SW1-acl-ipv4-basic-2000]rule 0 permit source 192.168.200.21 0
[SW1-acl-ipv4-basic-2000]quit
[SW1]tel
[SW1]telnet ser
[SW1]telnet server a
[SW1]telnet server acl 2000
[SW1]Feb 26 21:37:48:910 2020 SW1 SHELL/5/SHELL_LOGIN: weijianing logged in from 192.168.200.21.
Feb 26 21:39:45:444 2020 SW1 SHELL/5/SHELL_LOGOUT: weijianing logged out from 192.168.200.21.
Feb 26 21:41:16:150 2020 SW1 TELNETD/5/TELNETD_ACL_DENY: The Telnet Connection 192.168.200.22 request was denied according to ACL rules.
Feb 26 21:42:14:014 2020 SW1 TELNETD/5/TELNETD_ACL_DENY: The Telnet Connection 192.168.200.22 request was denied according to ACL rules.
```

查看ACL的匹配情况:

```
[SW1]dis acl all
Basic IPv4 ACL 2000, 1 rule,
ACL's step is 5
rule 0 permit source 192.168.200.21 0 (2 times matched)
[SW1]
```

至此，telnet登陆限制已完成!