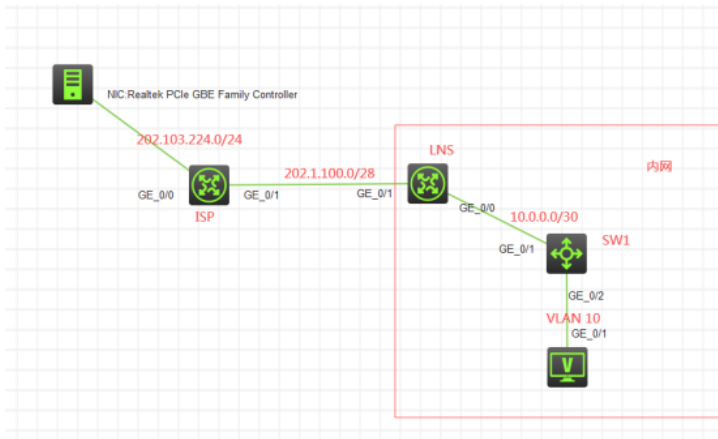


组网及说明



组网说明:

本案例采用H3C HCL模拟器来实现客户LAC模式的组网实验。内网和外网在网络拓扑图已有明确的标识。由于模拟器及本物理机的局限性，因此采用S5820交换机开启WEB功能来模拟成为WEB服务器。LNS模拟成为L2TP的LNS，物理机通过拨号的方式接入内网。

特别说明:

本实验仅仅是测试L2TP VPN (客户LAC模式) 的实现效果，不作为真实组网的案例。

配置步骤

- 1、按照网络拓扑图正确配置IP地址
- 2、SW1开启WEB功能，并创建相应账户及赋予权限
- 3、SW1配置默认路由指向到LNS
- 4、LNS配置NAT地址转换，在配置L2TP前，外网终端无法访问内网的SW1
- 5、LNS配置L2TP，外网终端通过设置拨号，拨号进入内网访问内网的SW1的WEB服务

配置关键点

- 1、第一阶段配置 (基础网络调试，配置L2TP前) :

SW1:

```
<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 192.168.10.1 24
[SW1-Vlan-interface10]quit
[SW1]int gi 1/0/2
[SW1-GigabitEthernet1/0/2]port link-type access
[SW1-GigabitEthernet1/0/2]port access vlan 10
[SW1-GigabitEthernet1/0/2]quit
[SW1]ip http enable
[SW1]ip https enable
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-mode route
[SW1-GigabitEthernet1/0/1]ip address 10.0.0.1 30
[SW1-GigabitEthernet1/0/1]des <connect to LNS>
[SW1-GigabitEthernet1/0/1]quit
[SW1]ip route-static 0.0.0.0 0.0.0.0 10.0.0.2
[SW1]local-user admin
New local user added.
[SW1-luser-manage-admin]password simple admin
[SW1-luser-manage-admin]service-type http https
[SW1-luser-manage-admin]authorization-attribute user-role network-admin
[SW1-luser-manage-admin]quit
[SW1]
```

LNS:

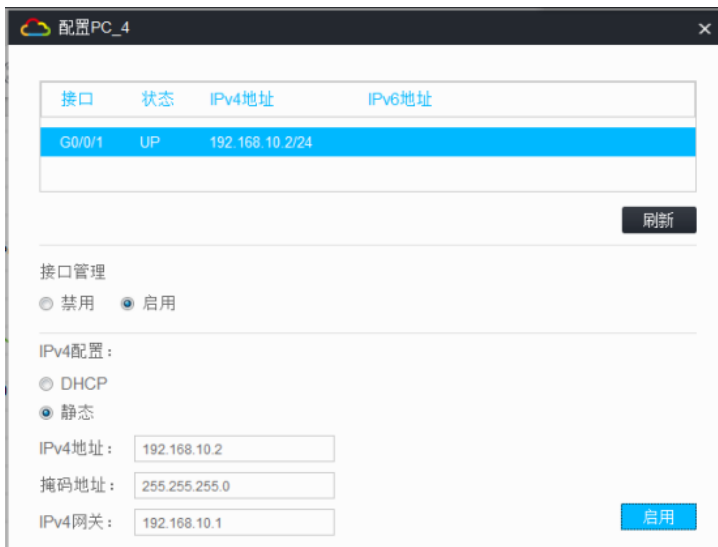
```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname LNS
[LNS]int gi 0/0
[LNS-GigabitEthernet0/0]des <connect to SW1>
[LNS-GigabitEthernet0/0]ip address 10.0.0.2 30
[LNS-GigabitEthernet0/0]quit
[LNS]ip route-static 192.168.10.0 255.255.255.0 10.0.0.1
[LNS]acl basic 2000
[LNS-acl-ipv4-basic-2000]rule 0 permit source any
[LNS-acl-ipv4-basic-2000]quit
[LNS]int gi 0/1
[LNS-GigabitEthernet0/1]ip address 202.1.100.2 28
[LNS-GigabitEthernet0/1]nat outbound 2000
[LNS-GigabitEthernet0/1]quit
[LNS]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
```

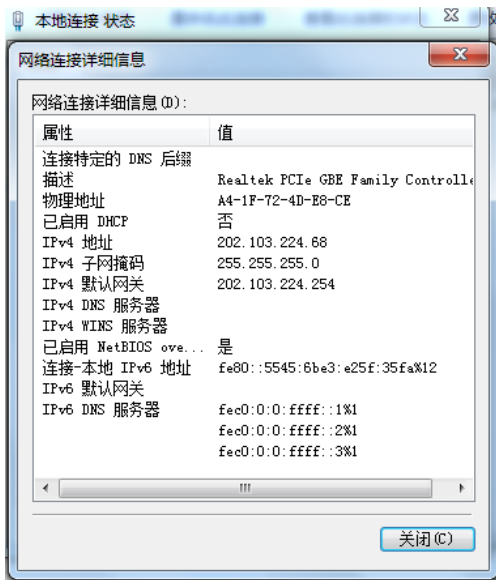
ISP:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/1
[ISP-GigabitEthernet0/1]des <connect to LNS>
[ISP-GigabitEthernet0/1]ip address 202.1.100.1 28
[ISP-GigabitEthernet0/1]quit
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]ip address 202.103.224.254 24
[ISP-GigabitEthernet0/0]quit
[ISP]ip route-static 202.1.100.0 255.255.255.240 202.1.100.2
[ISP]
```

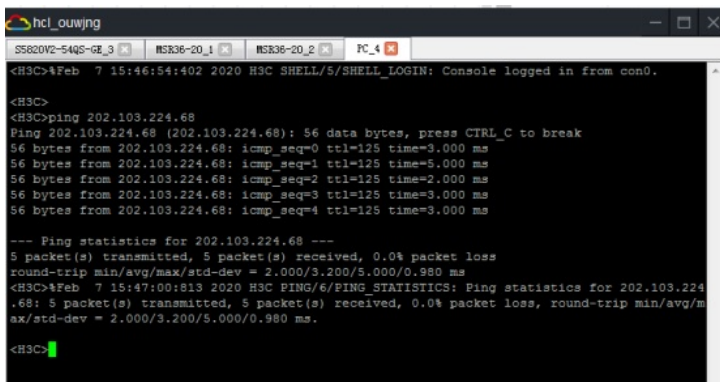
第一阶段测试:

所有终端都设置IP地址:

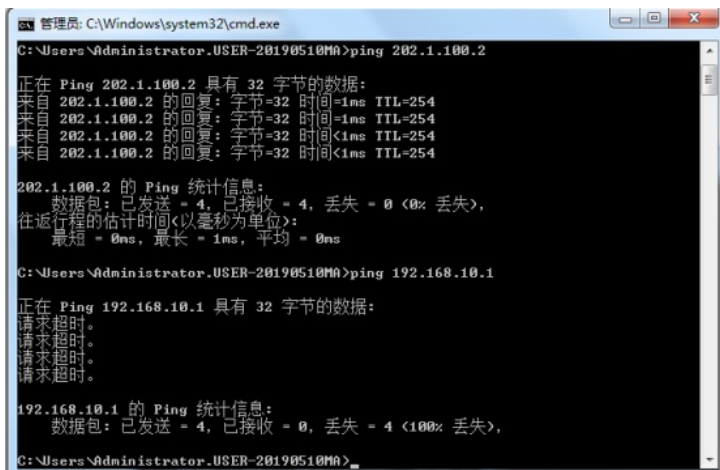




内网PC能PING外网终端:



外网终端仅能PING通到LNS的外网口IP, 无法PING通到内网:



2、第二阶段配置 (L2TP关键配置点) :

[LNS]local weijianing class network //创建用户名、密码, 并赋予PPP认证的方式
New local user added.

[LNS-luser-network-weijianing]password simple weijianing

[LNS-luser-network-weijianing]service-type ppp

[LNS-luser-network-weijianing]quit

[LNS]domain name system //配置域, 验证方式为本地PPP

[LNS-isp-system]authentication ppp local

[LNS-isp-system]quit

[LNS]ip pool weijianing 192.168.0.2 192.168.0.100 //创建地址池, 用于VPN拨号用户的IP地址分配

```
[LNS]jint Virtual-Template 1 //创建虚拟模板1
[LNS-Virtual-Template1]ip address 192.168.0.1 255.255.255.0 //配置模板的IP地址
[LNS-Virtual-Template1]ppp authentication-mode chap domain system //PPP认证方式为CHAP，并调用system的domain域
[LNS-Virtual-Template1]remote address pool weijianing //调用地址池
[LNS-Virtual-Template1]quit

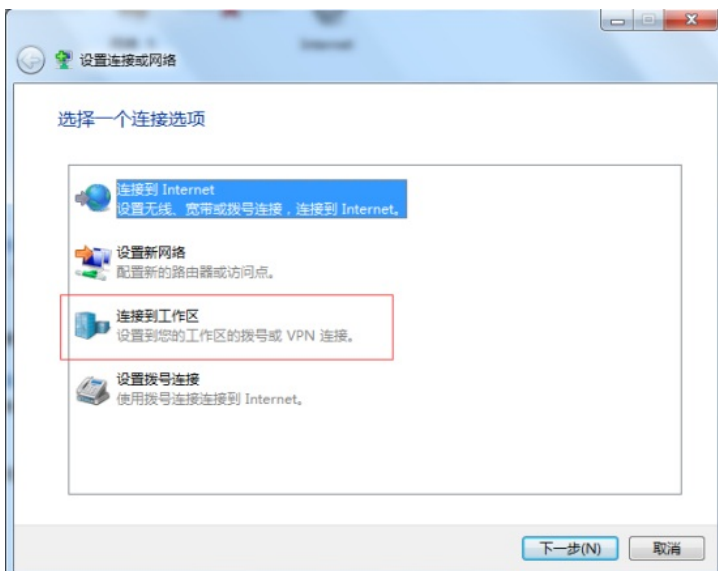
[LNS]l2tp enable //开启L2TP
[LNS]l2tp-group 1 mode lns //创建L2TP组1，模式为LNS
[LNS-l2tp1]tunnel name LNS //配置隧道名称为LNS
[LNS-l2tp1]allow l2tp virtual-template 1 //调用虚拟模板1到L2TP组
[LNS-l2tp1]undo tunnel authentication //关闭隧道功能
[LNS-l2tp1]quit
[LNS]domain default enable system
```

第二阶段测试：

本物理机是windows 7 32的操作系统，因此需要提前设置VPN拨号。
打开网络和共享中心，点击“设置新的连接或网络”：



选择“连接到工作区”后，点击“下一步”：



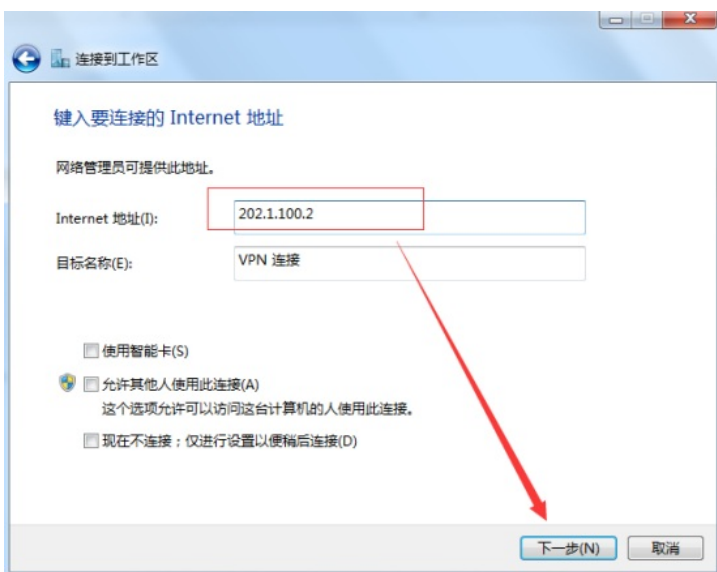
选择“使用我的Internet连接 (VPN) ”



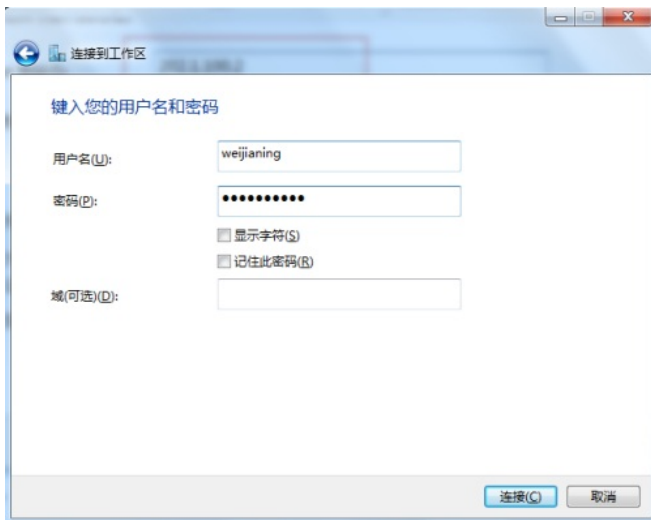
选择“我稍后决定”，点击“下一步”：



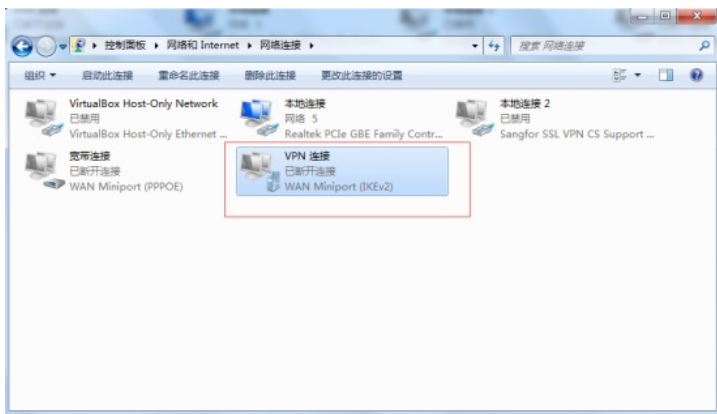
输入internet地址后，点击“下一步”



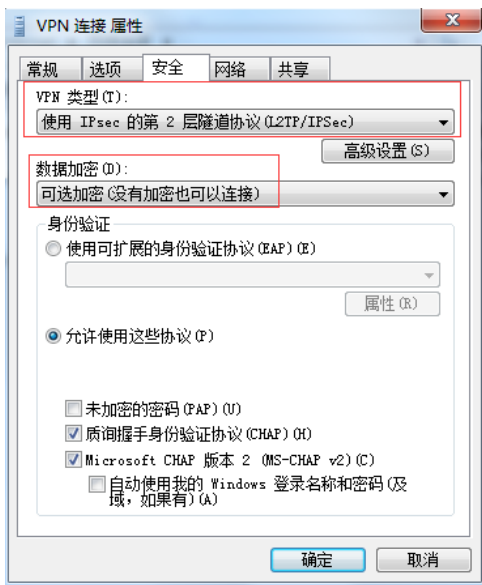
输入用户名，密码，点击“连接”：



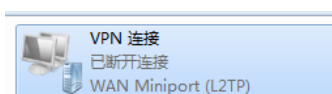
右键，选择“属性”：



选择“安全”，设置VPN类型，在设置“数据加密”，如下图所示：



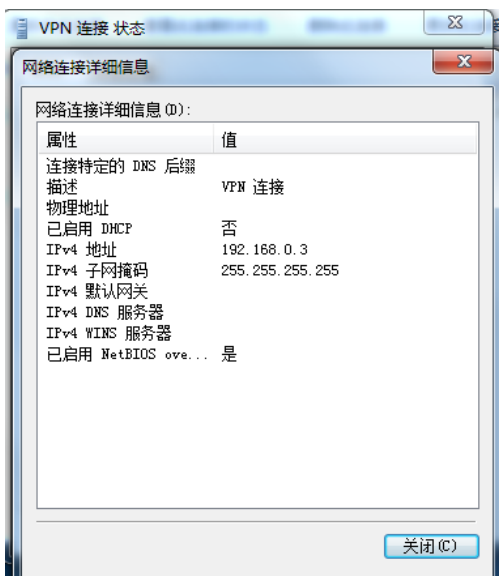
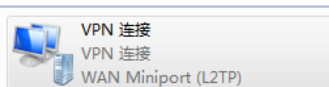
打开之前创建的“VPN”连接



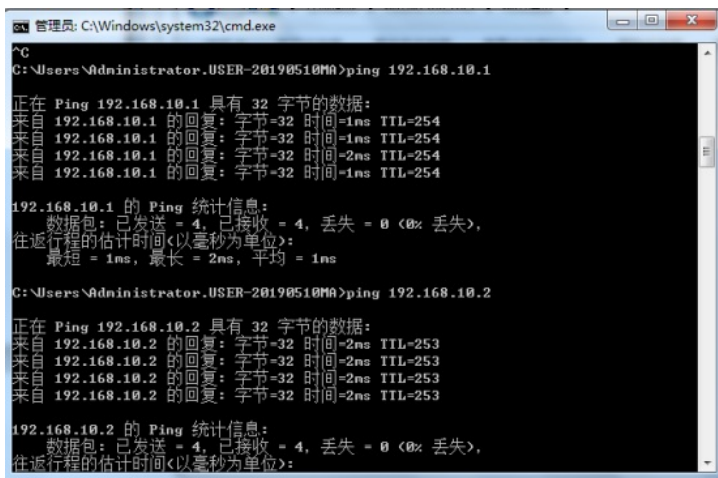
输入用户名、密码，点击连接：



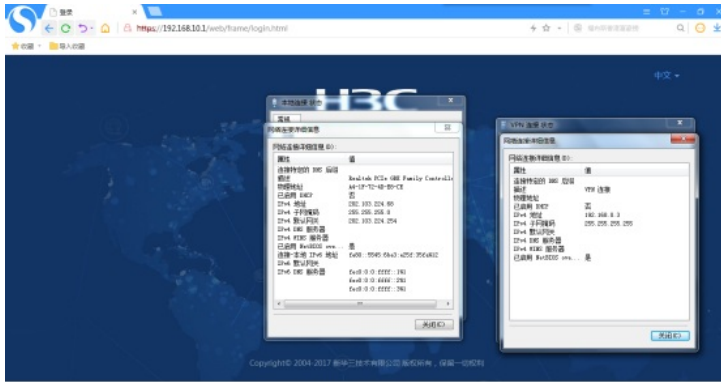
VPN已连接上，并查看VPN信息：



此时，外网终端已能ping通内网：



同时，也可以打开内网的WEB服务



在LNS上查看VPN的信息:

```
<LNS>dis l2tp session
LocalSID   RemoteSID   LocalTID   State
23994      1            41037     Established
<LNS>
```

```
<LNS>dis l2tp tunnel
LocalTID RemoteTID State Sessions RemoteAddress RemotePort RemoteName
41037 2 Established 1 202.103.224.68 1701 wgw2195.h3c.huawei-3co.m.com
<LNS>
```

至此，L2TP VPN典型组网配置实验（客户LAC模式）已完成！