

编号	
密级	

工程测试指导文档

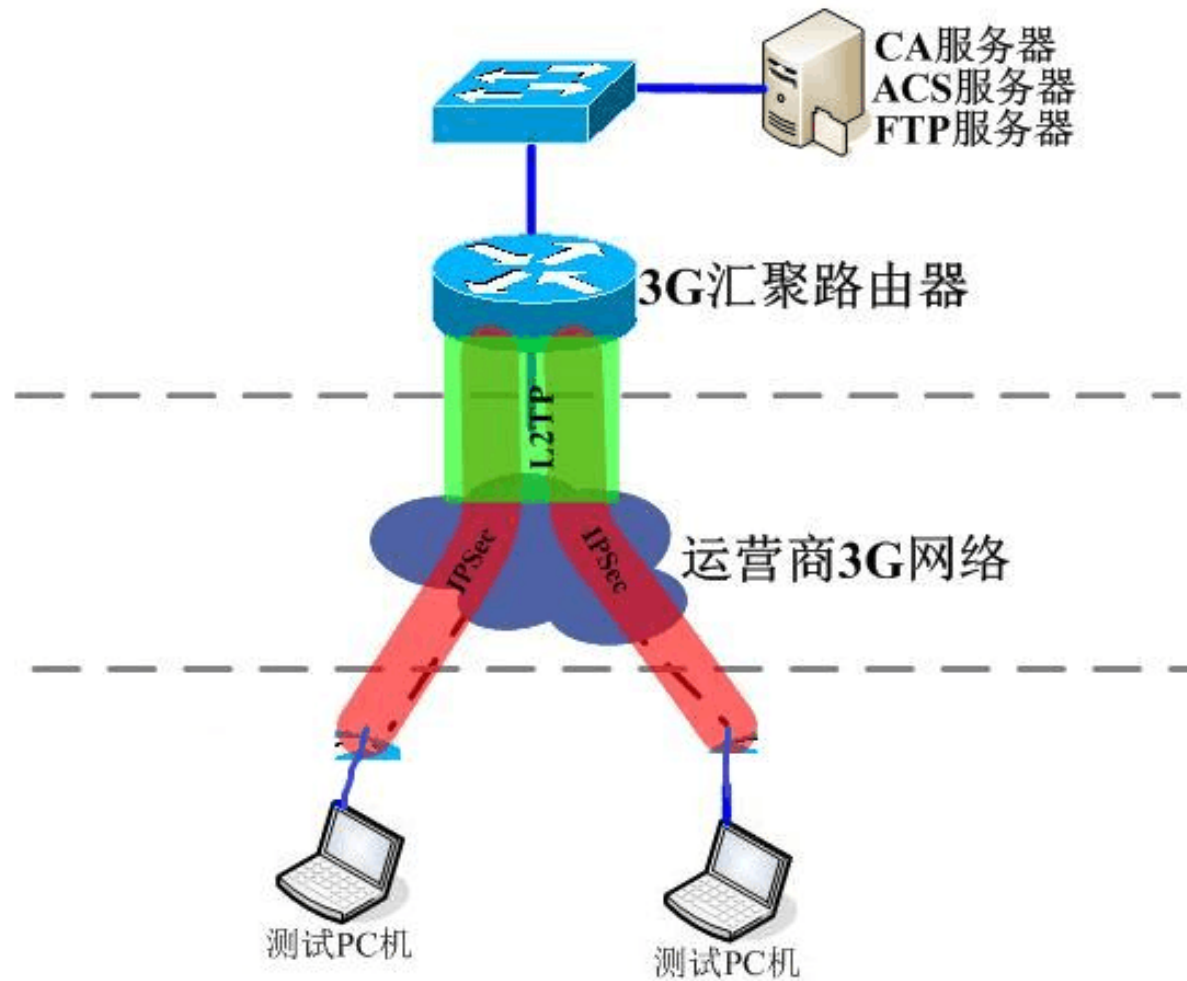
# 关于黑龙江建行 E-动终端测试问题解 决方案

北京金科润天信息技术有限公司

2011 年 9 月



## 1、拓扑如下



## 2、简要说明

3G 路由器（为 vpdn LNS 端）跟运营商建立 l2tp隧道，并设置相应 vpdn 设置，详细看配置



（配置如下：[LNS配置.txt](#)）；ACS 上配置相应用户（如：用户：[3g1@ccb.vpdn.hl](#)密码：123456）并为客户端下发 ip 地址，下面客户端用 3G 上网卡带着用户：[3g1@ccb.vpdn.hl](#)密码：123456 进行 vpdn 拨号。

## 3、客户需求

根据行里需求，要求实现多客户端同时拨同一账号，即在 ACS 上建立一个账号密码，并且分配一个 ip pool 实现在 ACS 上认证的同时，再给客户端分配动态 ip 地址。

## 4、前期测试结果

建立一个用户(账号: [3g1@ccb.vpdn.h1](#) 密码: 123456), 并分配固定 ip: 20.20.10.,1 拨号成功

建立一个用户(账号: [3g1@ccb.vpdn.h1](#) 密码: 123456), 并分配一个地址池: 20.20.10.0/24 拨号失败, acs上的 log信息提示认证失败

## 5、解决方案

### 5.1、测试内容

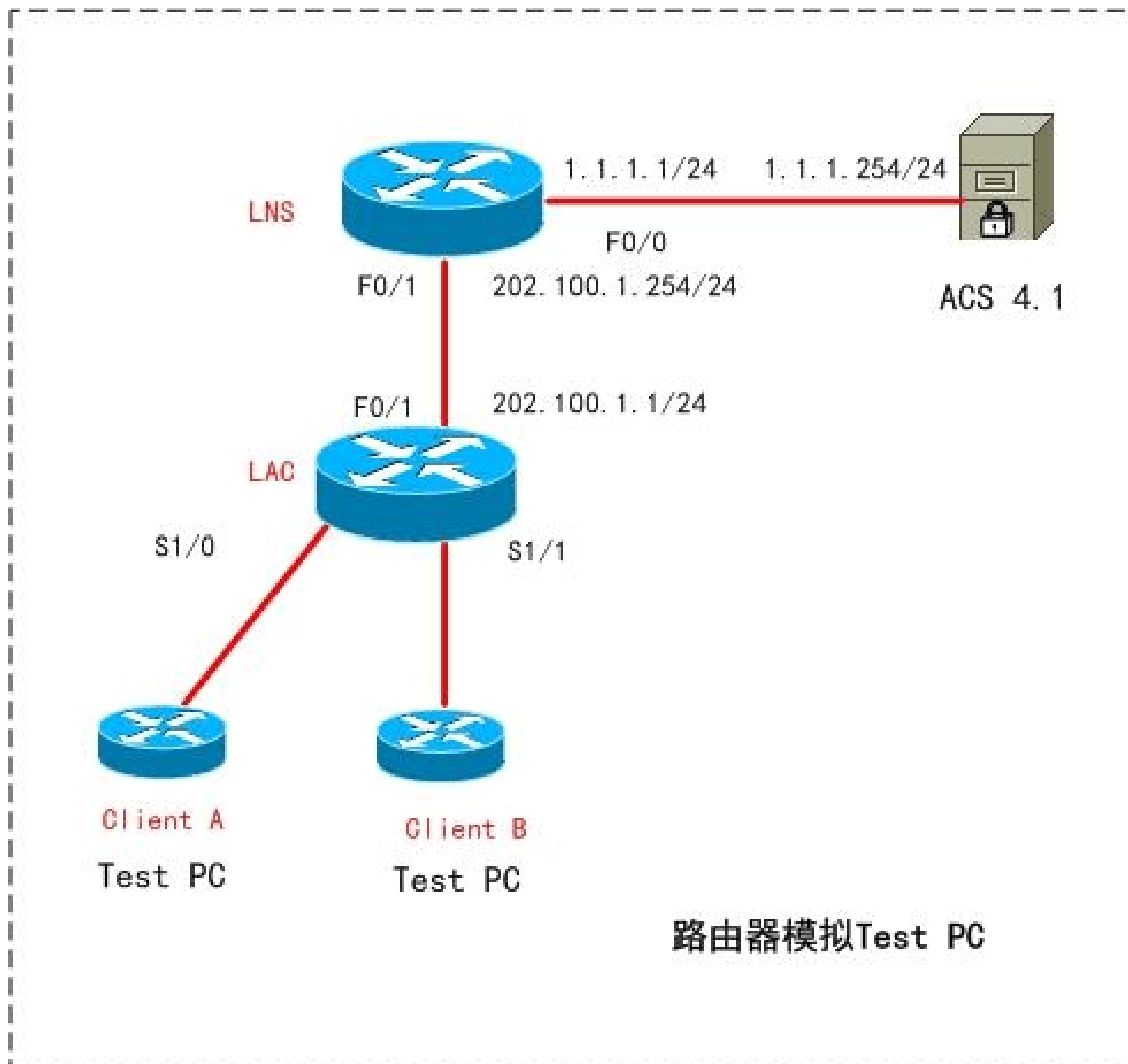
测试 VPDN(L2TP) 与 ACS4.1 联动向多客户端推送 IP 地址可行性(多客户端使用同一用户名、密码)

### 5.2、测试步骤

(1) 将 IP Pool与认证服务器配置在路由器上, 验证 VPDN 及 IP POOL 状态。

(2) 将 IP POOL 与认证服务功能迁移至 ACS 服务器上, 验证状态、可行性。

### 5.3、模拟实验拓扑图



#### 5.4、第一阶段配置

将 IP Pool 与认证服务器配置在路由器上，验证 VPDN 及 IP pool 状态

##### LNS

```

!
hostname lns
!
vpdn enable
!
vpdn-group lns
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname lac
 local name lns
 no l2tp tunnel authentication

```

```
l2tp tunnel receive-window 1024
!
username ccb@ccb.com password 0 ccb123
archive
log config
hidekeys
!
interface FastEthernet0/0
description Connect_to_ACS4.1
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
description Connect_to_LAC_F0/1
ip address 202.100.1.254 255.255.255.0
duplex auto
speed auto
!
interface Virtual-Template1
ip address 11.1.1.254 255.255.255.0
peer default ip address pool ccb
ppp authentication chap
!
ip local pool ccb 11.1.1.1 11.1.1.253
```

## LAC

```
!
hostname lac
!
vpdn enable
vpdn search-order domain
!
vpdn-group lac
request-dialin
protocol l2tp
domain ccb
domain ccb.com
initiate-to ip 202.100.1.254
local name lac
no l2tp tunnel authentication
l2tp tunnel receive-window 1024
!
```

```
interface FastEthernet0/1
 ip address 202.100.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 encapsulation ppp
 serial restart-delay 0
 ppp authentication chap
!
interface Serial1/1
 no ip address
 encapsulation ppp
 serial restart-delay 0
 ppp authentication chap
!
```

## ClientA

```
!
hostname ClientA
!
interface Serial1/0
 ip address negotiated
 encapsulation ppp
 serial restart-delay 0
 ppp chap hostname ccb@ccb.com
 ppp chap password 0 ccb123
!
ip route 0.0.0.0 0.0.0.0 11.1.1.254
!
```

## ClientB

```
!
hostname ClientB
!
interface Serial1/1
 ip address negotiated
 encapsulation ppp
 serial restart-delay 0
 ppp chap hostname ccb@ccb.com
 ppp chap password 0 ccb123
```

```
!  
ip route 0.0.0.0 0.0.0.0 11.1.1.254
```

验证 VPDN 状态及向客户端 ClientA ClientB推送地址状况

```
lns#show vpdn tunnel
```

```
L2TP Tunnel Information Total tunnels 1 sessions 2
```

LocTunID	RemTunID	Remote Name	State	Remote Address	Sessn Count	L2TP VPDN Group	Class/Group
25915	57078	lac	est	202.100.1.1	2	lns	

```
lns#show vpdn session
```

```
L2TP Session Information Total tunnels 1 sessions 2
```

LocID	RemID	TunID	Username, Intf/ Vcid, Circuit	State	Last Chg	Uniq ID
31	31	25915	ccb@ccb.com, Vi2.1	est	00:53:05	30
32	32	25915	ccb@ccb.com, Vi2.2	est	00:47:35	31

```
lac#show vpdn tunnel
```

```
L2TP Tunnel Information Total tunnels 1 sessions 2
```

LocTunID	RemTunID	Remote Name	State	Remote Address	Sessn Count	L2TP VPDN Group	Class/Group
57078	25915	lns	est	202.100.1.254	2	lac	

```
lac#show vpdn session
```

```
L2TP Session Information Total tunnels 1 sessions 2
```

LocID	RemID	TunID	Username, Intf/ Vcid, Circuit	State	Last Chg	Uniq ID
-------	-------	-------	----------------------------------	-------	----------	---------



```
31          31          57078          ccb@ccb.com, Se1/0  est   00:53:37 424
32          32          57078          ccb@ccb.com, Se1/1  est   00:48:07 546
```

## ClientA#show interfaces serial 1/0

```
Serial1/0 is up, line protocol is up
  Hardware is M4T
  Internet address 1.1.1.1/32
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Listen: CDPCP
  Open: IPCP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  CRC checking enabled
  Last input 00:55:48, output 00:00:09, output hang never
  Last clearing of "show interface" counters 01:55:28
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations 0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5468 packets input, 104734 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    4469 packets output, 76636 bytes, 0 underruns
    0 output errors, 0 collisions, 948 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    948 carrier transitions
  DCD=up   DSR=up   DTR=up   RTS=up   CTS=up
```

## ClientB#show interfaces serial 1/1

```
Serial1/1 is up, line protocol is up
  Hardware is M4T
  Internet address 1.1.1.2/32
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation PPP, LCP Open
Listen: CDPCP
Open: IPCP, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
CRC checking enabled
Last input 00:50:51, output 00:00:06, output hang never
Last clearing of "show interface" counters 01:54:53
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/1/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  3750 packets input, 72497 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  3280 packets output, 54931 bytes, 0 underruns
  0 output errors, 0 collisions, 625 interface resets
  74 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
  625 carrier transitions DCD=up   DSR=up   DTR=up   RTS=up   CTS=up
```

## 5.5、将 VPDN 认证及推送 IP 功能迁移至 ACS 步骤

### 1) LNS 与 ACS 服务器可达性

```
lns#ping 1.1.1.254
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 1.1.1.254, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/22/40 ms
```

```
lns#
```

### 1) 在 LNS 上添加 3A 认证服务器,并设置 VPDN 认证模式为 3a 服务器,不使用本地认证

#### LNS

```
aaa new-model
```

```
radius-server host 1.1.1.254 auth-port 1645 acct-port 1646 key ccb
```

!

aaa authentication login group radius 此命令主要用于测试 3A 服务器

aaa authentication ppp group radius 此命令用于 ppp 3A 认证

aaa authorization network group radius 此命令主要用于 PPP 授权以使用 3A 服务器推送 IP 地址

aaa authorization auth-proxy default group radius 此命令主要用于代理认证可不添加

!

```
interface Virtual-Template1
```

```
ip address 11.1.1.254 255.255.255.0
```

```
peer match aaa-pools 此处使用 3A 服务器上的地址池
```

```
no peer default ip address
```

```
ppp authentication chap 此处表示指定 PPP 认证为 3A list
```

```
ppp authorization vdn 此处表示指定 PPP 制授权为 3A list
```

```
end
```

## 配置 3A 服务器

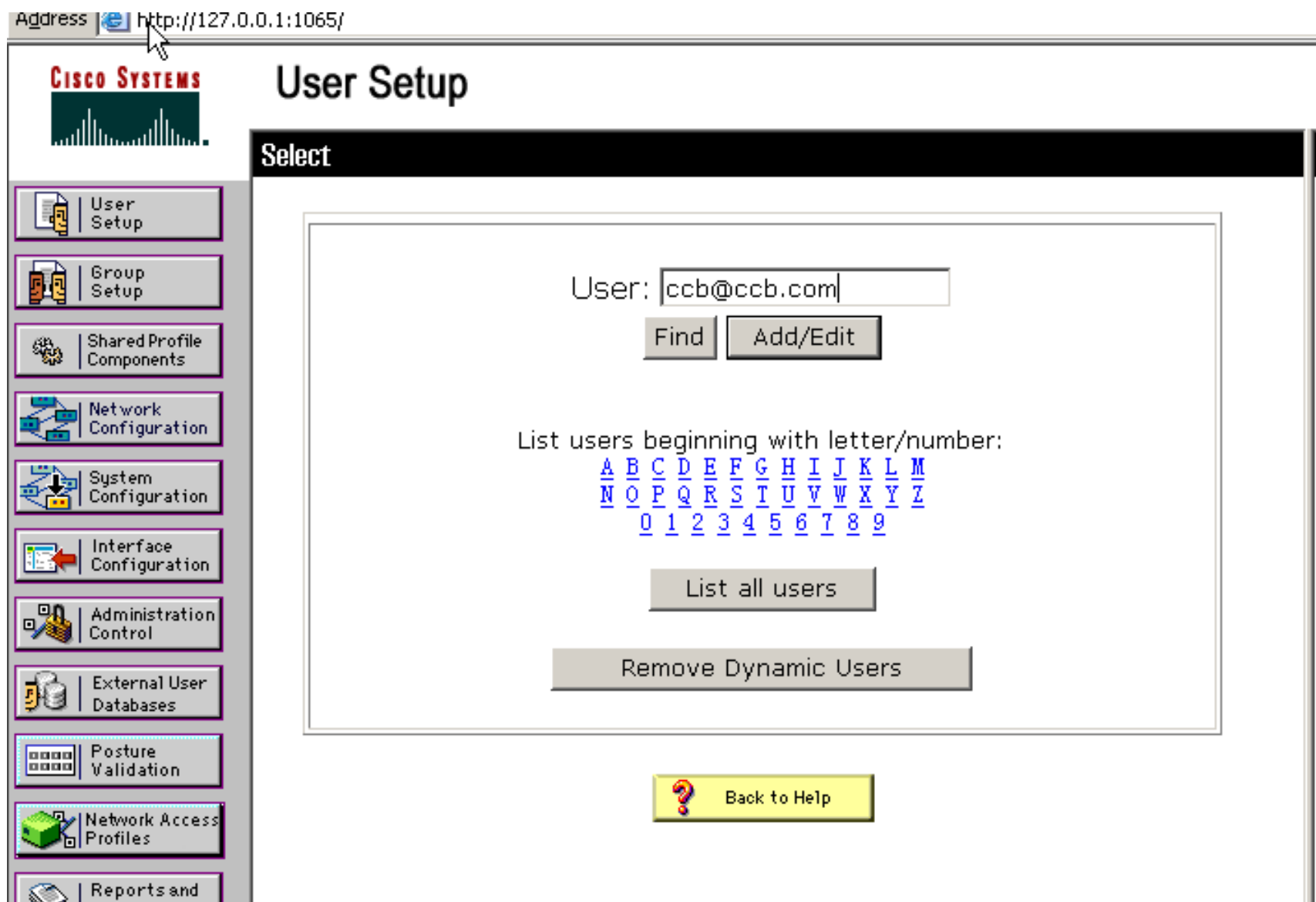
### 1. 在 ACS 上添加 3A Client

点击 Network Configuration 按钮 --> 点击 AAA Clients 列表下 Add Entry 按钮如下图所示：  
设备名称 lns IP 地址 1.1.1.1 即 路由器 lns 的 f0/0 接口地址。此图已添加完成。

The screenshot shows the Cisco ACS Network Configuration interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, and Network Access. The main area is titled 'Select' and contains two tables. The first table, 'AAA Clients', has columns for AAA Client Hostname, AAA Client IP Address, and Authenticate Using. It shows one entry with Hostname 'lns', IP Address '1.1.1.1', and Authenticate Using 'RADIUS (IETF)'. Below the table are 'Add Entry' and 'Search' buttons. The second table, 'AAA Servers', has columns for AAA Server Name, AAA Server IP Address, and AAA Server Type. It shows one entry with Server Name 'dzq-0y7totizud2', IP Address '1.1.1.254', and Server Type 'CiscoSecure ACS'. Below this table are also 'Add Entry' and 'Search' buttons.


### 2. 在 ACS 上用户名密码

点击 菜单栏 User Setup 按钮，--> 在右侧列表框中输入要添加的用户名（[此处 ccb@ccb.com](#) 仅为示例），--> 然后点击 add/edi 按钮进行添加，进入用户设置界面。



3. 对添加的用户名设置密码

进入此界面后在 User setup框下设置密码 password 及确认密码 Confirm Password,注意此处密码不可太短。




# User Setup

Edit

**User: ccb@ccb.com (New User)**


Account Disabled

**Supplementary User Info** 


Real Name

Description

---

**User Setup** 

Password Authentication:



CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

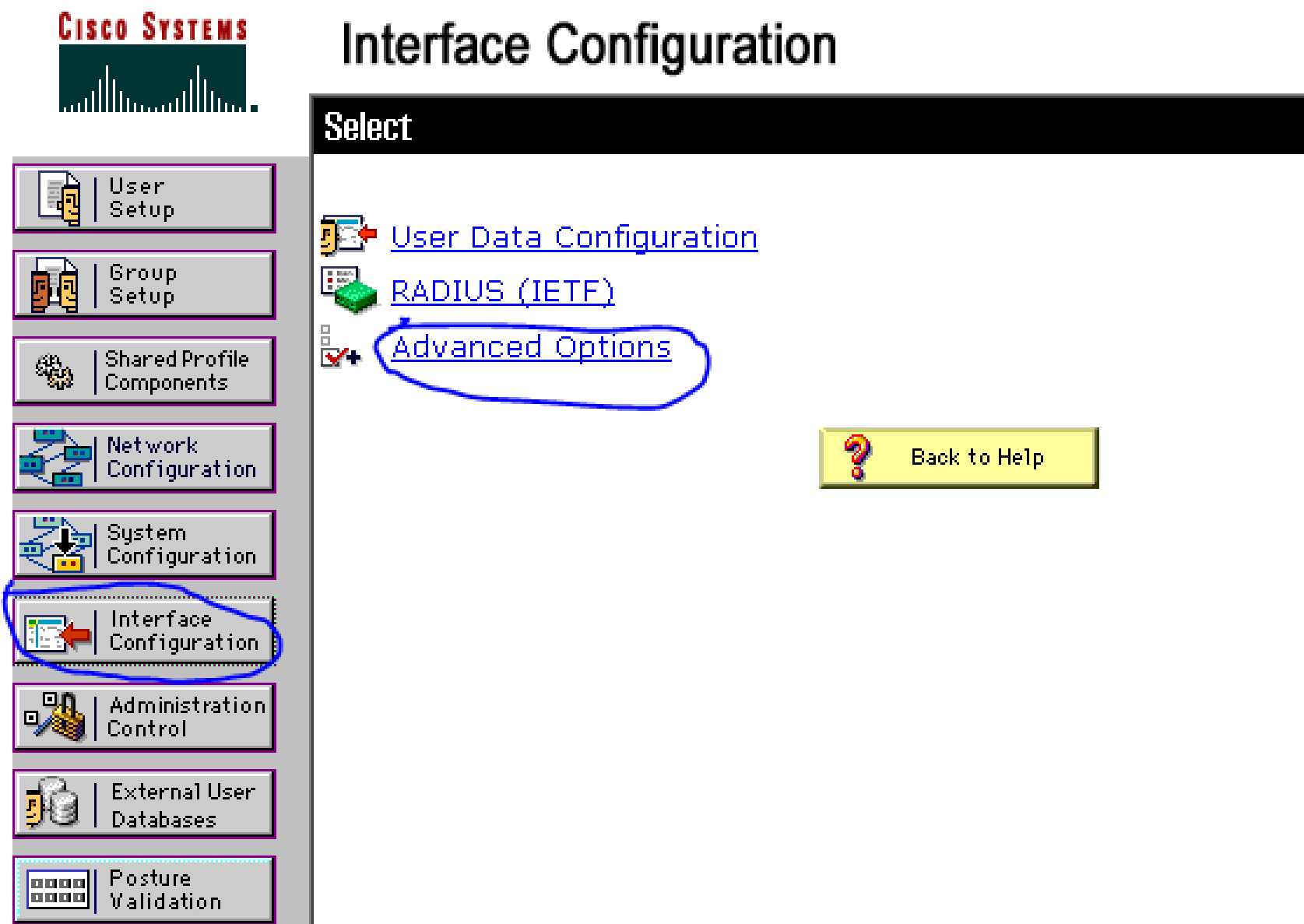
Confirm Password

- 用户名密码添加完成后在路由器 1ns 上进行测试如下：  

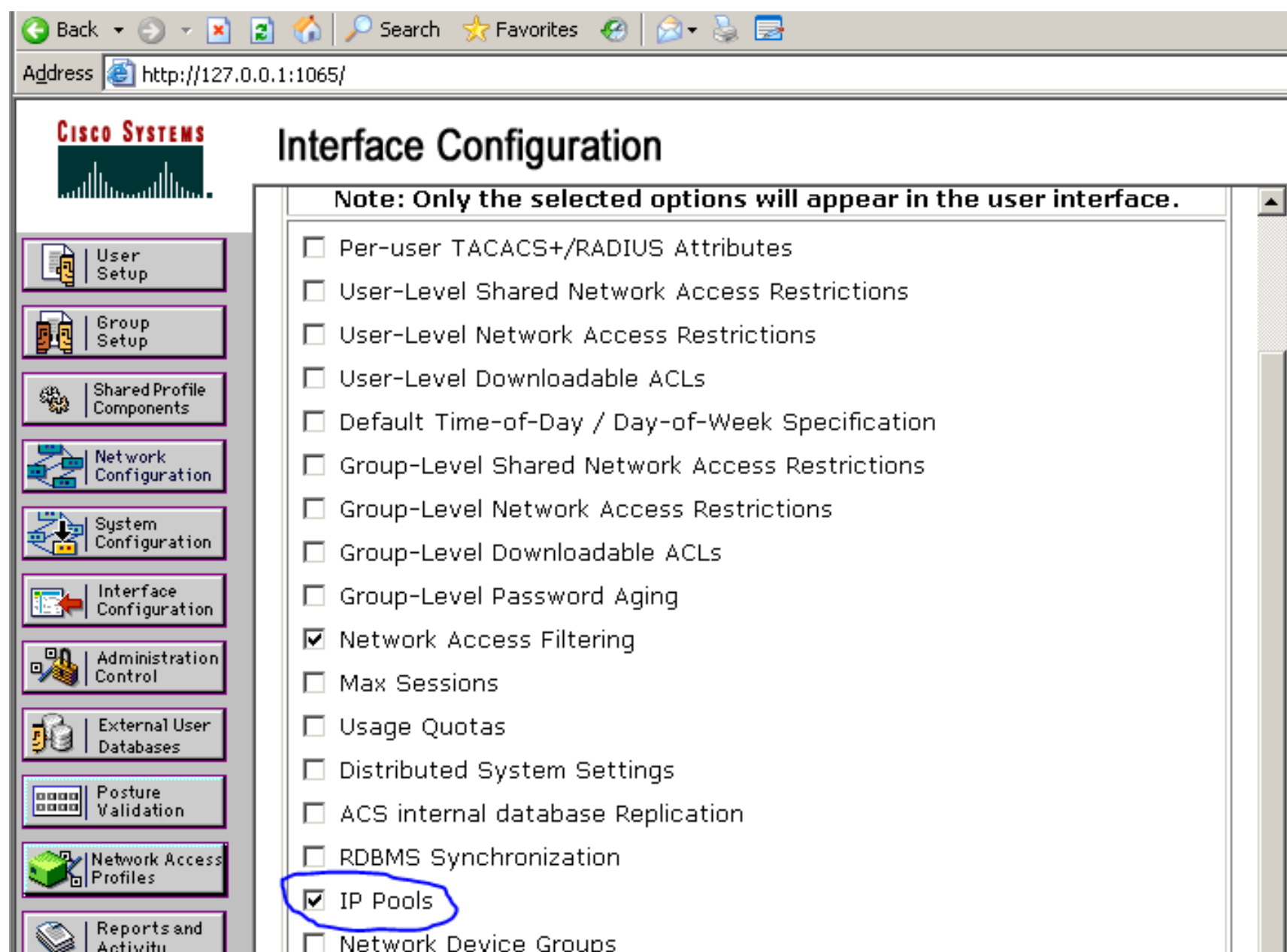
```
1ns#test aaa group radius ccb@ccb.com ccb123 ne
1ns#test aaa group radius ccb@ccb.com ccb123 new-code
User successfully authenticated
```

上一行中红色部分表示测试成功，路由器和 3A 服务器通讯正常，基本设置正常

- 在 ACS 服务器上添加 IP 地址池



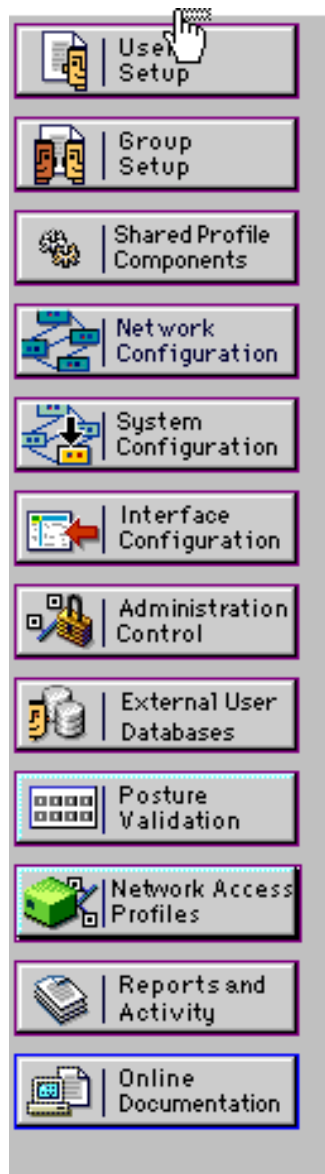
点击菜单栏目中 interface Configuration 按钮 ----> 再点击右侧 advanced options 选项 出现如下界面:




选中 IP pool 选项然后应用。

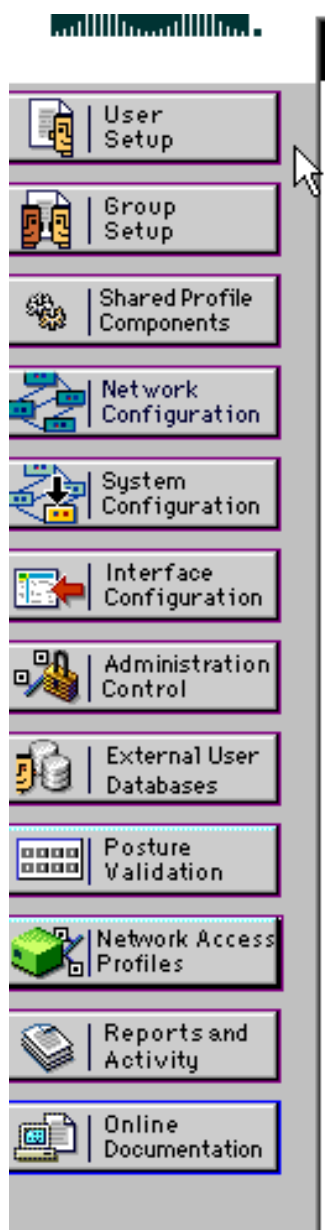


再回到菜单栏中点击 system Configuration 按钮--> 点击右侧 ip pool server 选项可进入 IP POOL 设置




AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
<a href="#">vpdn</a>	11.1.1.100	11.1.1.253	0%


 Back to Help



Edit

vpdn 	
Name	<input type="text" value="vpdn"/>
Start Address	<input type="text" value="11.1.1.100"/>
End Address	<input type="text" value="11.1.1.253"/>
In Use	0
Available	154

Submit Delete Reset Cancel

 Back to Help

6. 将 IP 地址池与用户关联

回到用户设置中，找到 Client ip address assignment 项，选中 assigned form aaa pool 项目，并将地址池名 vpdn 选中添加到右侧表框中，然后应用即可。



以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/005342312142012011>