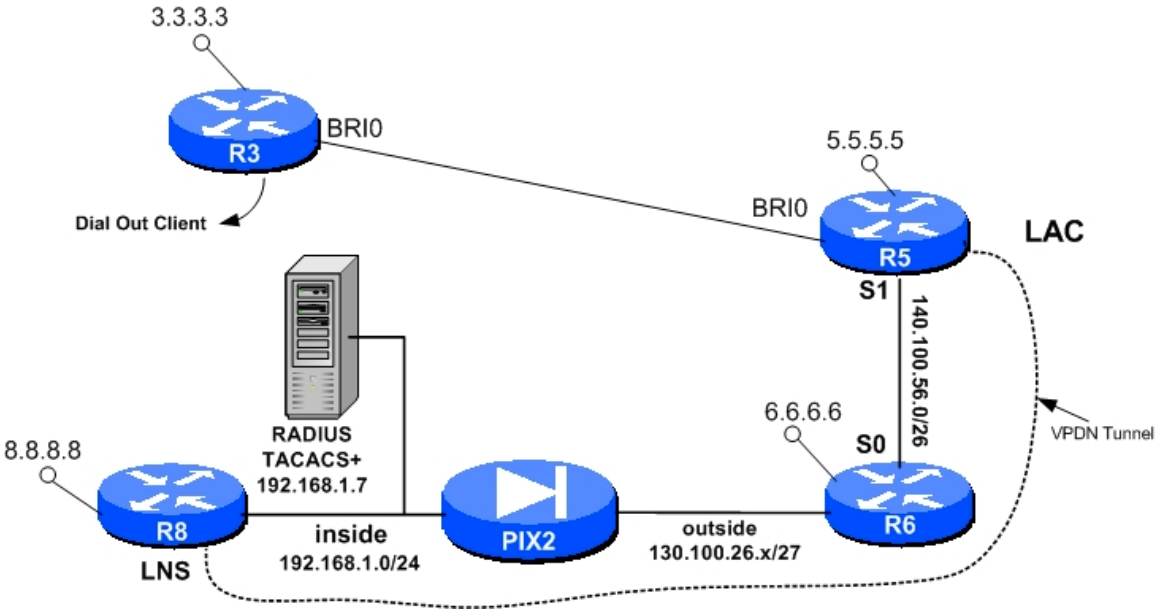


Figure 1 Section 9: Configuring TACACS+ Authentication and Authorization for VPDN

```
hostname R3
!
interface BRI0/0
no ip address
encapsulation ppp
dialer pool-member 1
isdn switch-type basic-ni
isdn spid1 26278037230101
isdn spid2 26278037240101
ppp authentication chap
!
interface Dialer0
ip address negotiated
encapsulation ppp
no ip route-cache
no ip mroute-cache
dialer pool 1
dialer remote-name ccie4460@cisco.com
dialer string 5551212
dialer-group 1
no cdp enable
ppp authentication chap callin
ppp chap hostname ccie4460@cisco.com
ppp chap password cisco
!
dialer-list 1 protocol ip permit
!
 ip route 0.0.0.0 0.0.0.0 Dialer 0
```

LAC/NAS Configuration with a TACACS+

```
R5

aaa new-model
aaa authentication ppp default group tacacs+
aaa authorization network default group tacacs+
!
vpdn enable
vpdn search-order domain
interface BRI0/0
no ip address
encapsulation ppp
dialer pool-member 1
isdn switch-type basic-ni
isdn spid1 26293867870101
isdn spid2 26293867880101
ppp authentication chap
!
interface Dialer0
ip unnumbered serial 0
encapsulation ppp
no ip route-cache
no ip mroute-cache
dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap
!
dialer-list 1 protocol ip permit
!
tacacs-server host 130.100.26.7 key cisco6727
```

LNS/Home-Gateway Configuration for AAA with the TACACS+ Server

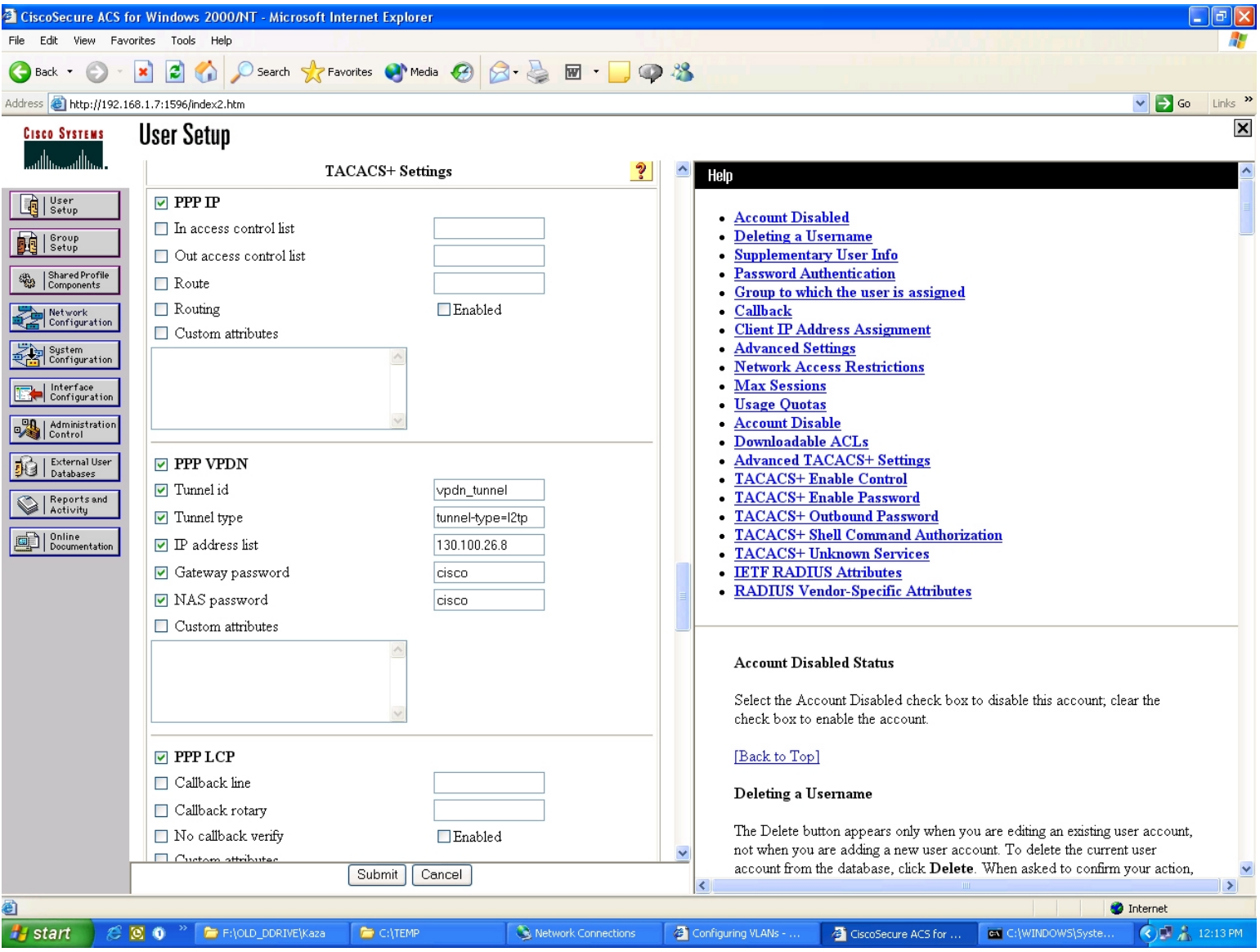
```
R8

aaa new-model
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
!
vpdn enable
vpdn-group 1
!
 accept-dialin
  protocol any
  virtual-template 1
  terminate-from hostname R5
 local name R8
 lcp renegotiation always
 l2tp tunnel password 0 cisco
!
interface Virtual-Template1
 ip unnumbered Loopback100
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 peer default ip address pool HOME
```

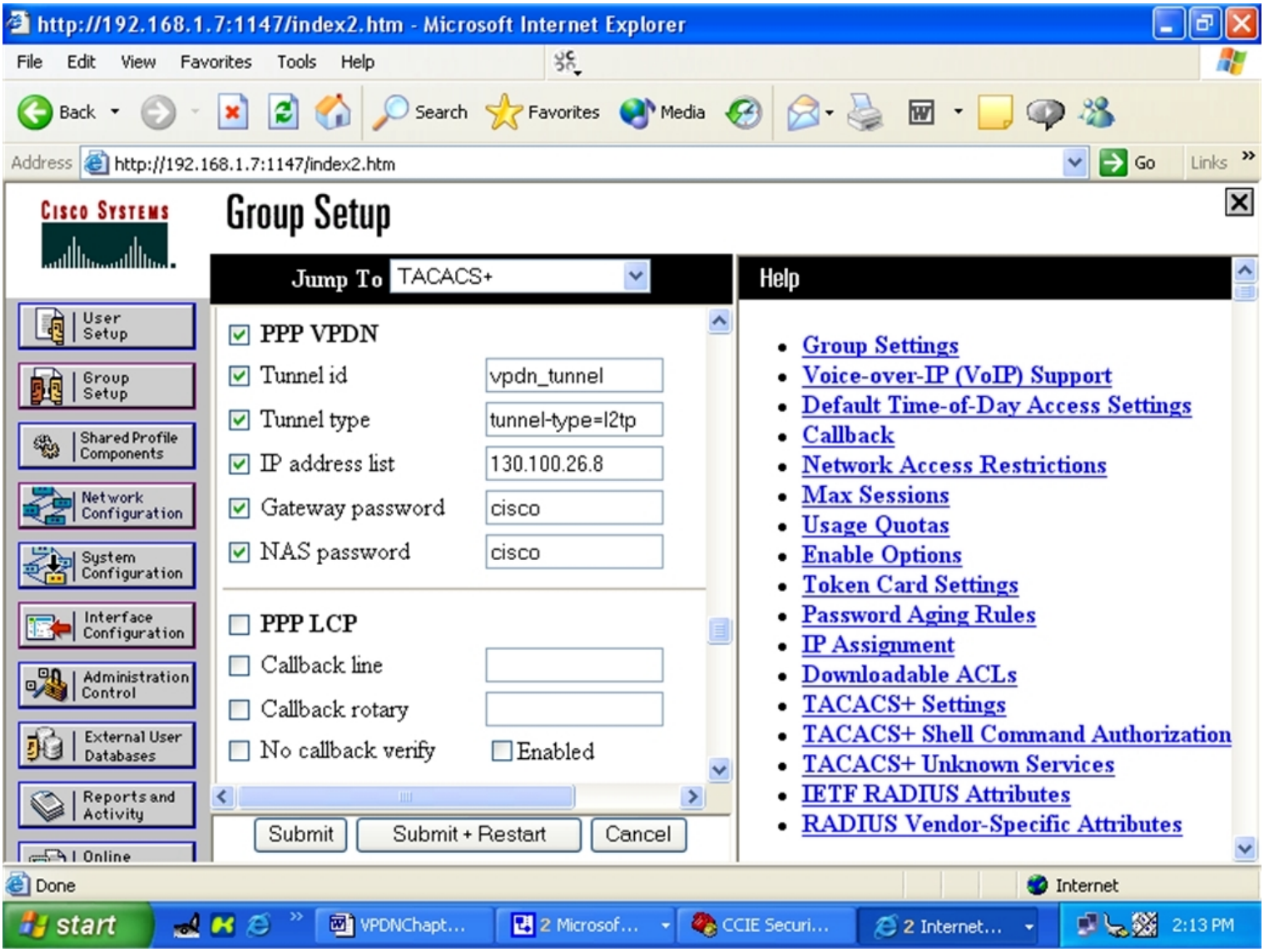
```
 ppp authentication chap
!
interface Loopback100
 ip address 192.168.100.1 255.255.255.0
!
ip local pool HOME 192.168.100.10 192.168.100.20
!
tacacs-server host 192.168.1.7 key cisco6727
```

PIX2

```
ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0
static (inside,outside) 130.100.26.7 192.168.1.7 netmask
255.255.255.255 0 0
static (inside,outside) 130.100.26.8 192.168.1.1 netmask
255.255.255.255 0 0
access-list outside_access_in permit udp any host
130.100.26.8 eq 1701
access-list outside_access_in permit tcp any host
130.100.26.7 eq tacacs
access-group outside_access_in in interface outside
```

Configuring cisco.com User on the TACACS+ Server


CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.7:1596/index2.htm
Go Links
Cisco Systems
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
TACACS+ Settings
PPP IP
In access control list
Out access control list
Route
Routing
Enabled
Custom attributes
PPP VPDN
Tunnel id
vpdn_tunnel
Tunnel type
tunnel-type=l2tp
IP address list
130.100.26.8
Gateway password
cisco
NAS password
cisco
Custom attributes
PPP LCP
Callback line
Callback rotary
No callback verify
Enabled
Submit
Cancel
Help
Account Disabled
Deleting a Username
Supplementary User Info
Password Authentication
Group to which the user is assigned
Callback
Client IP Address Assignment
Advanced Settings
Network Access Restrictions
Max Sessions
Usage Quotas
Account Disable
Downloadable ACLs
Advanced TACACS+ Settings
TACACS+ Enable Control
TACACS+ Enable Password
TACACS+ Outbound Password
TACACS+ Shell Command Authorization
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Account Disabled Status
Select the Account Disabled check box to disable this account; clear the check box to enable the account.
[Back to Top]
Deleting a Username
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action,
Internet
start
F:\OLD_DDRIVE\Kaza
C:\TEMP
Network Connections
Configuring VLANs - ...
CiscoSecure ACS for ...
C:\WINDOWS\Syste...
12:13 PM


http://192.168.1.7:1147/index2.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.7:1147/index2.htm
Go Links
Cisco Systems
Group Setup
Jump To TACACS+
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online
PPP VPDN
Tunnel id vpdn_tunnel
Tunnel type tunnel-type=l2tp
IP address list 130.100.26.8
Gateway password cisco
NAS password cisco
PPP LCP
Callback line
Callback rotary
No callback verify Enabled
Submit Submit + Restart Cancel
Help
Group Settings
Voice-over-IP (VoIP) Support
Default Time-of-Day Access Settings
Callback
Network Access Restrictions
Max Sessions
Usage Quotas
Enable Options
Token Card Settings
Password Aging Rules
IP Assignment
Downloadable ACLs
TACACS+ Settings
TACACS+ Shell Command Authorization
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Done
Internet
start
VPDNChapt...
2 Microsof...
CCIE Securi...
2 Internet...
2:13 PM