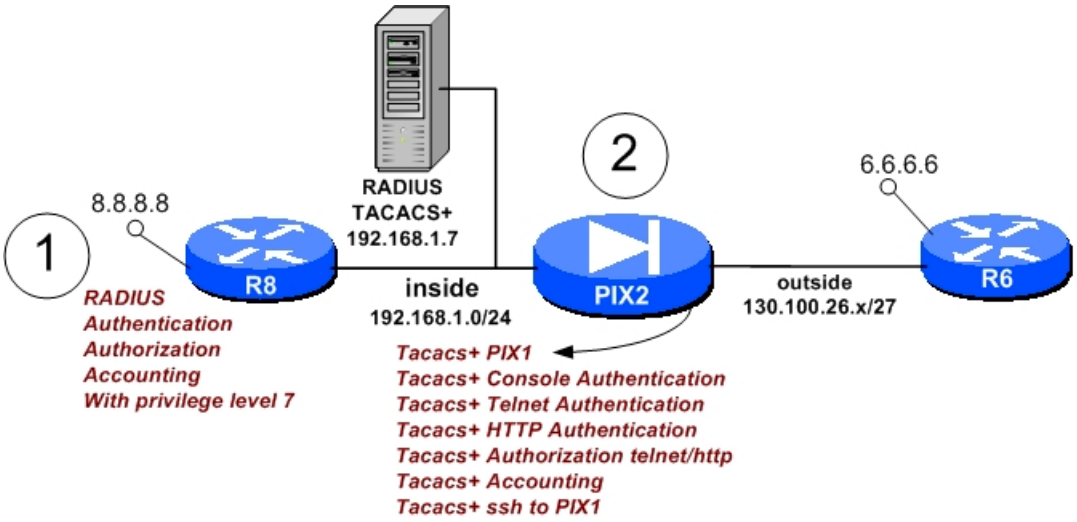
For this lab section, refer to Figure 26-5 on page 922 of the book.

```
PIX2(config)# sho config
: Saved
: Written by enable_15 at 00:29:11.836 UTC Fri Jan 1 1993
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 DMZ2 security10
nameif ethernet3 DMZ security15
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX2
domain-name cisco.com
names
name 130.100.26.6 R6


access-list inside_authentication_TACACS+ permit tcp any any eq
        telnet
access-list inside_authentication_TACACS+ permit tcp any any eq www
access-list inside_authorization_TACACS+ permit tcp any any eq
        telnet
access-list inside_authorization_TACACS+ permit tcp any any eq www
access-list inside_accounting_TACACS+ permit tcp any any eq telnet
access-list inside_accounting_TACACS+ permit tcp any any eq www


interface ethernet0 10full
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 10baset

mtu outside 1500
mtu inside 1500

ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0

global (outside) 10 interface

nat (inside) 10 0.0.0.0 0.0.0.0 0 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


route outside 0.0.0.0 0.0.0.0 R6 1
route inside 8.8.8.0 255.255.255.0 192.168.1.1 1


aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ (inside) host 192.168.1.7 cisco6727 timeout 5
aaa-server RADIUS protocol radius
```

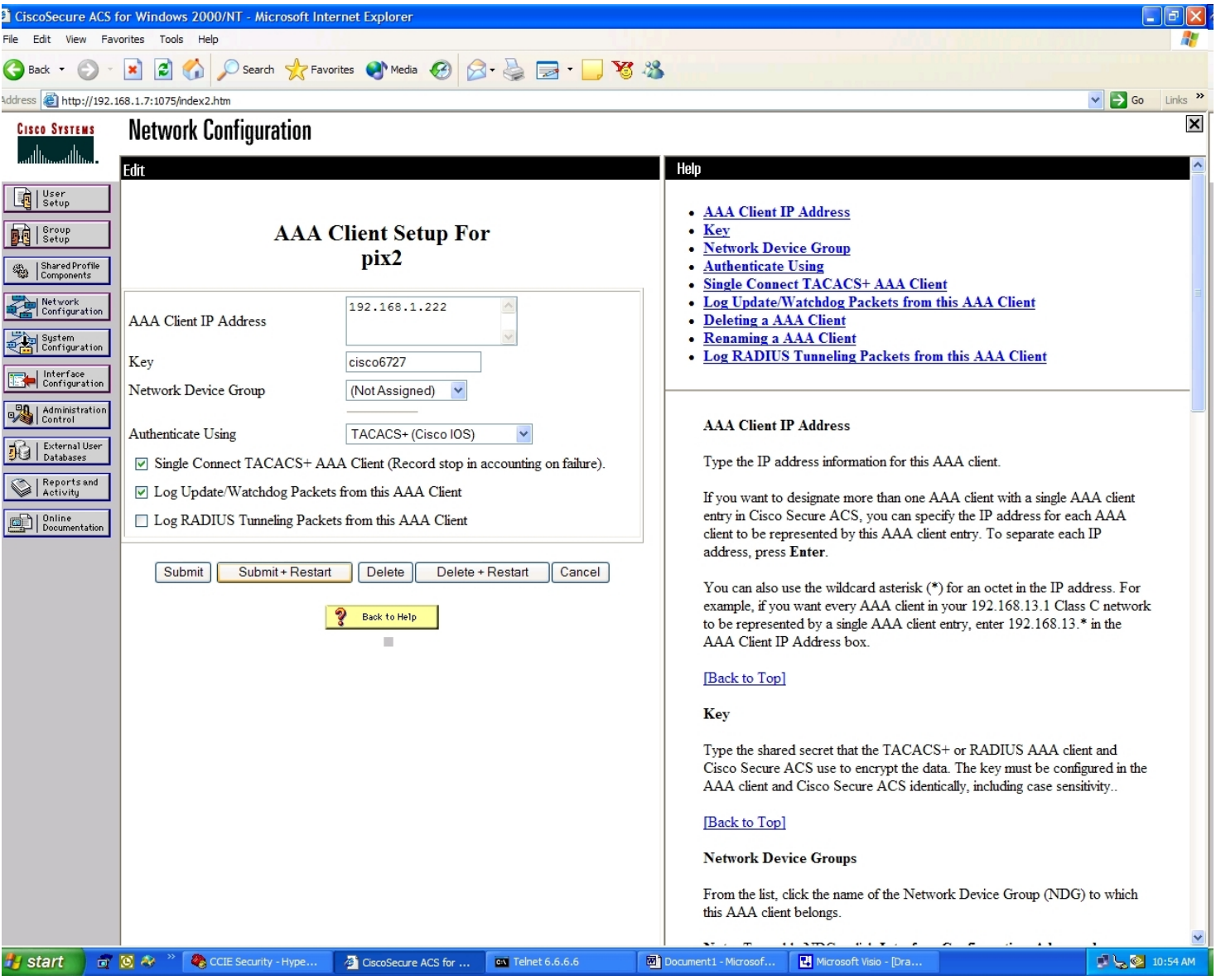
```
aaa-server LOCAL protocol local

aaa authentication match inside_authentication_TACACS+ inside
        TACACS+
aaa authentication telnet console TACACS+
aaa authentication ssh console TACACS+

aaa authorization match inside_authorization_TACACS+ inside TACACS+
aaa accounting match inside_accounting_TACACS+ inside TACACS+

auth-prompt prompt Authentication Login please

auth-prompt accept Welcome to CCIE Lab
auth-prompt reject You enter wrong login: Check ACS Server
telnet 192.168.1.0 255.255.255.0 inside
```

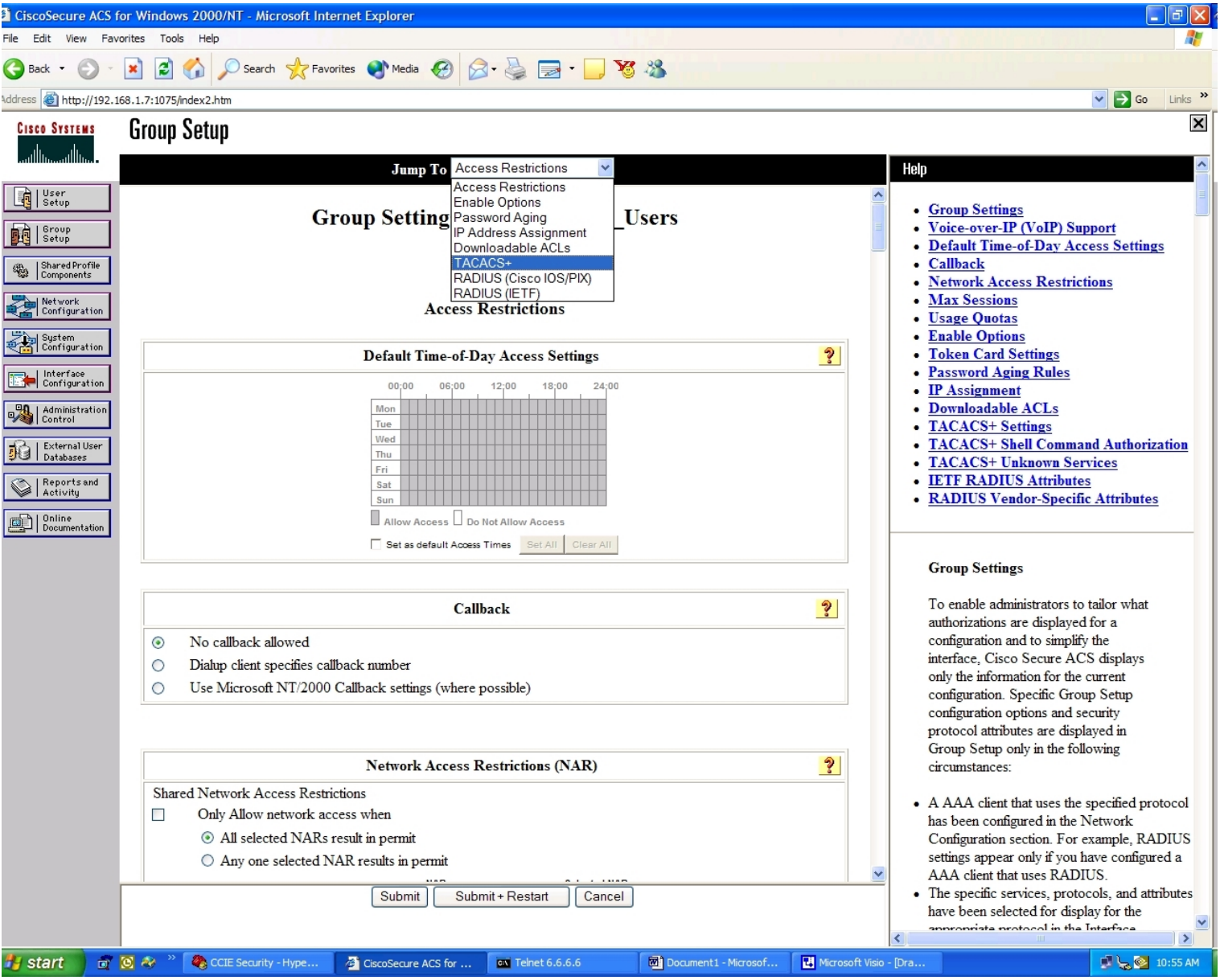


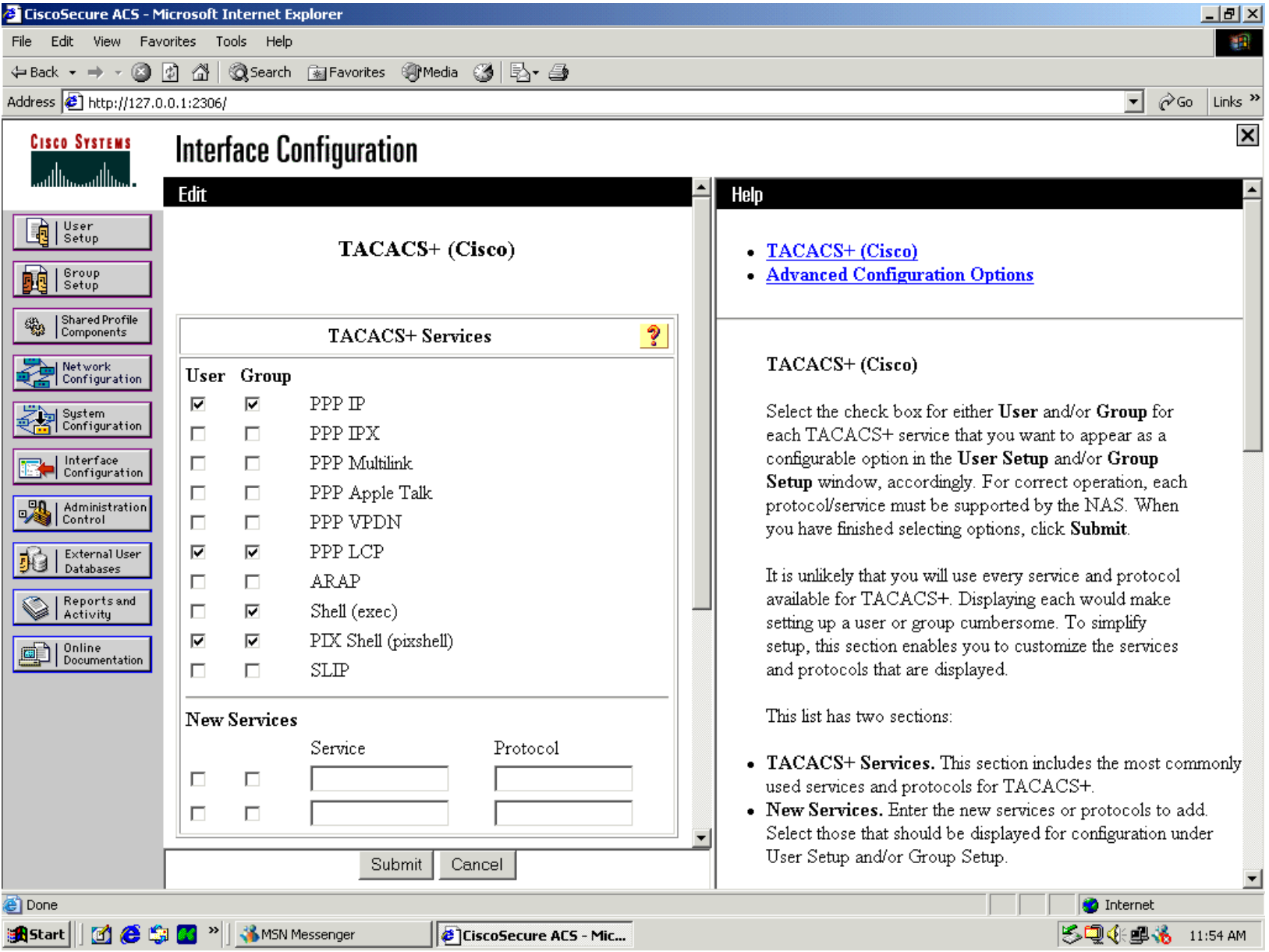

```
PIX2(config)# sho ca my rsa
% Key pair was generated at: 17:14:26 UTC Jun 26 2002
Key name: PIX2.cisco.com
 Usage: General Purpose Key
 Key Data:
  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081
89028181 00d7f87b
  15f565ac 9899dad2 a51d5cd8 a10b367d a79f52fe eaee425d
790b02c3 1f7b8231
  5385eb6f 0771c4aa f1b2975b 3b4455c2 f4b33d7c baf4a5f9
0c6687fc 83c4d7d4
  5d1fdbac dfae4858 09d9081c cc2eb27c 0690bd90 ed3892d1
d0e2543c 079a68c9
  9a8ea939 b98b4418 4d561d69 dd69fecb 7e434234 7fc6160b
5d8398b8 f3020301 0001
PIX2(config)#

hostname PIX2
domain-name cisco.com
aaa authentication ssh console TACACS+
ssh 192.168.1.100 255.255.255.255 inside
ssh 192.168.1.1 255.255.255.255 inside
ssh timeout 5
```

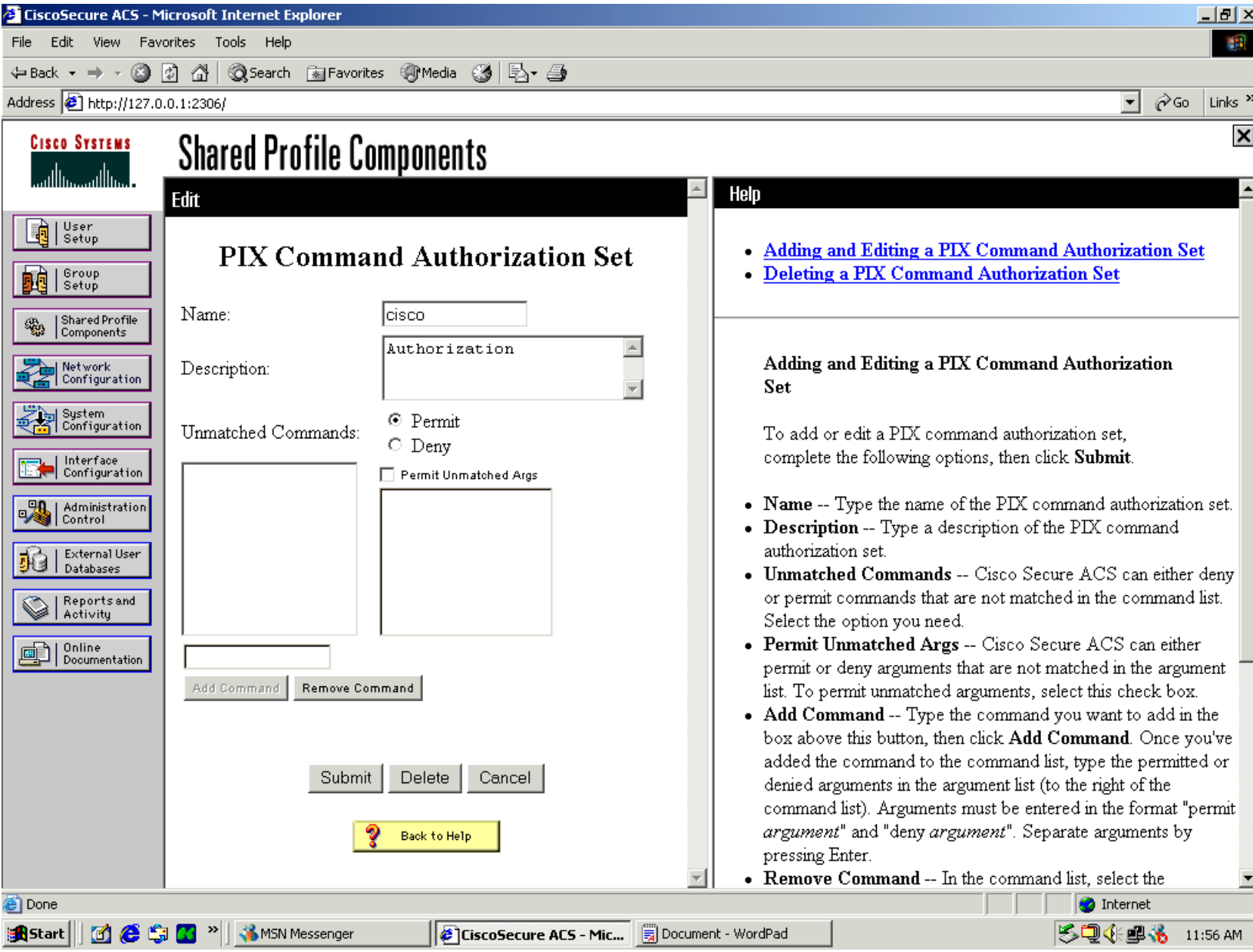
Test AAA from Client to R6

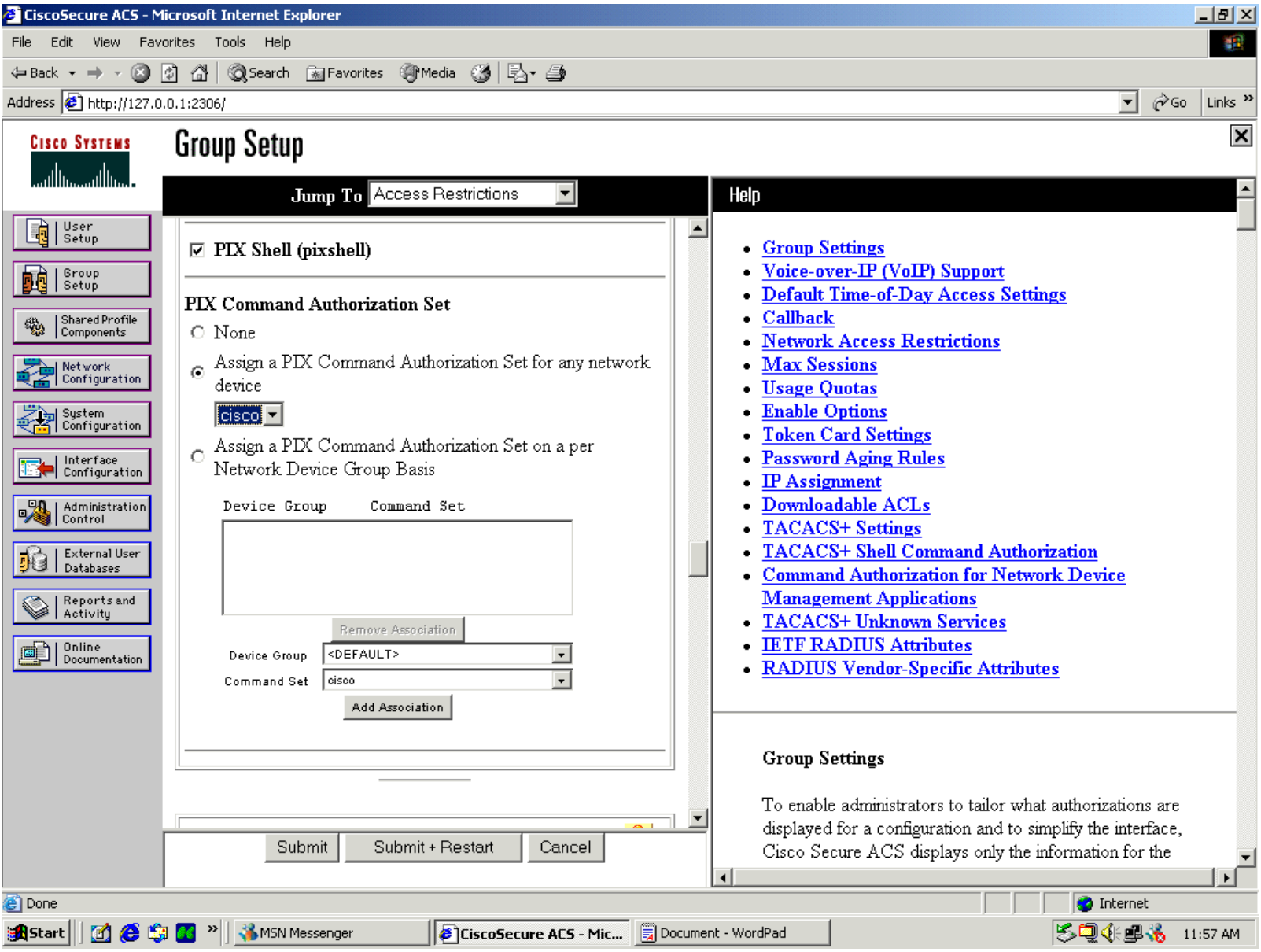
```
Authentication Login please
Username: user2
Password:
Welcome to CCIE Lab
User Access Verification
Username: r8
Password:
```


CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.7:1075/index2.htm
Go Links
Cisco Systems
Network Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Edit
AAA Client Setup For pix2
AAA Client IP Address
192.168.1.222
Key
cisco6727
Network Device Group
(Not Assigned)
Authenticate Using
TACACS+ (Cisco IOS)
Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
Log Update/Watchdog Packets from this AAA Client
Log RADIUS Tunneling Packets from this AAA Client
Submit
Submit + Restart
Delete
Delete + Restart
Cancel
Back to Help
Help
AAA Client IP Address
Key
Network Device Group
Authenticate Using
Single Connect TACACS+ AAA Client
Log Update/Watchdog Packets from this AAA Client
Deleting a AAA Client
Renaming a AAA Client
Log RADIUS Tunneling Packets from this AAA Client
AAA Client IP Address
Type the IP address information for this AAA client.
If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.
You can also use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.
[Back to Top]
Key
Type the shared secret that the TACACS+ or RADIUS AAA client and Cisco Secure ACS use to encrypt the data. The key must be configured in the AAA client and Cisco Secure ACS identically, including case sensitivity..
[Back to Top]
Network Device Groups
From the list, click the name of the Network Device Group (NDG) to which this AAA client belongs.
start
CCIE Security - Hype...
CiscoSecure ACS for ...
Telnet 6.6.6.6
Document1 - Microsof...
Microsoft Visio - [Dra...
10:54 AM


CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.7:1075/index2.htm
Go Links
Cisco Systems
Group Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Jump To Access Restrictions
Access Restrictions
Enable Options
Password Aging
IP Address Assignment
Downloadable ACLs
TACACS+
RADIUS (Cisco IOS/PIX)
RADIUS (IETF)
Group Setting _Users
Access Restrictions
Default Time-of-Day Access Settings
00:00 06:00 12:00 18:00 24:00
Mon Tue Wed Thu Fri Sat Sun
Allow Access Do Not Allow Access
Set as default Access Times Set All Clear All
Callback
No callback allowed
Dialup client specifies callback number
Use Microsoft NT/2000 Callback settings (where possible)
Network Access Restrictions (NAR)
Shared Network Access Restrictions
Only Allow network access when
All selected NARs result in permit
Any one selected NAR results in permit
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
Group Settings
To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:
A AAA client that uses the specified protocol has been configured in the Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA client that uses RADIUS.
The specific services, protocols, and attributes have been selected for display for the
start
CCIE Security - Hype...
CiscoSecure ACS for ...
Telnet 6.6.6.6
Document1 - Microsof...
Microsoft Visio - [Dra...
10:55 AM


CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://127.0.0.1:2306/
Go Links
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Edit
TACACS+ (Cisco)
TACACS+ Services
User Group
PPP IP
PPP IPX
PPP Multilink
PPP Apple Talk
PPP VPDN
PPP LCP
ARAP
Shell (exec)
PIX Shell (pixshell)
SLIP
New Services
Service
Protocol
Submit
Cancel
Help
TACACS+ (Cisco)
Advanced Configuration Options
TACACS+ (Cisco)
Select the check box for either User and/or Group for each TACACS+ service that you want to appear as a configurable option in the User Setup and/or Group Setup window, accordingly. For correct operation, each protocol/service must be supported by the NAS. When you have finished selecting options, click Submit.
It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, this section enables you to customize the services and protocols that are displayed.
This list has two sections:
TACACS+ Services. This section includes the most commonly used services and protocols for TACACS+.
New Services. Enter the new services or protocols to add. Select those that should be displayed for configuration under User Setup and/or Group Setup.
Done
Internet
Start
MSN Messenger
CiscoSecure ACS - Mic...
11:54 AM


CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://127.0.0.1:2306/
Go Links
Cisco Systems
Shared Profile Components
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Edit
PIX Command Authorization Set
Name:
cisco
Description:
Authorization
Unmatched Commands:
Permit
Deny
Permit Unmatched Args
Add Command
Remove Command
Submit
Delete
Cancel
Back to Help
Help
Adding and Editing a PIX Command Authorization Set
Deleting a PIX Command Authorization Set
Adding and Editing a PIX Command Authorization Set
To add or edit a PIX command authorization set, complete the following options, then click Submit.
Name -- Type the name of the PIX command authorization set.
Description -- Type a description of the PIX command authorization set.
Unmatched Commands -- Cisco Secure ACS can either deny or permit commands that are not matched in the command list. Select the option you need.
Permit Unmatched Args -- Cisco Secure ACS can either permit or deny arguments that are not matched in the argument list. To permit unmatched arguments, select this check box.
Add Command -- Type the command you want to add in the box above this button, then click Add Command. Once you've added the command to the command list, type the permitted or denied arguments in the argument list (to the right of the command list). Arguments must be entered in the format "permit argument" and "deny argument". Separate arguments by pressing Enter.
Remove Command -- In the command list, select the
Done
Internet
Start
MSN Messenger
CiscoSecure ACS - Mic...
Document - WordPad
11:56 AM



Prior to adding PIX command authorization, CSNT 3.0 must be patched. Registered users can download the patch from the Software Center. You can also view additional information about this issue by accessing Cisco Bug ID CSCdw78255 (registered customers only).