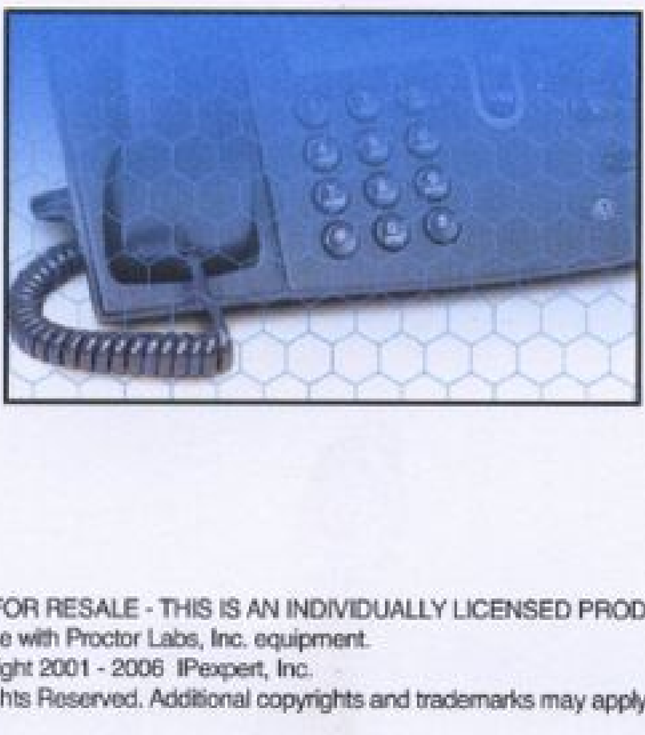
Dual Voice IE GUARANTEE

"When will you be an IPexpert?"

IPexpert's CCIE® Voice Proctor Guide (Version 4.0)

A companion to IPexpert's CCIE™ Voice Preparation Workbook



ipexpert™

powered by PROCTOR LABS

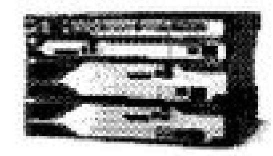
For technical support peer groups, subscribe for free to

CertificationTalk
http://www.certificationtalk.com

ONLINE study list
http://www.onlinestudylist.com

IPexpert's CCIE Voice Proctor Guide (Version 4.0)

(To be used in conjunction with IPexpert's Ultimate Preparation Workbook for the Cisco® CCIE™ Voice Laboratory Exam, Version 4.0)



Before We Begin

This guide was created to provide you with not only a hand-holding walk-through, but also to provide you with a "Proctor Like" experience. Used in conjunction with our CCIE Voice Lab Preparation Workbook (Version 4.0), you're guaranteed a real self-paced learning experienced like no other!

Technical Support

CertificationTalk *(http://www.CertificationTalk.com)*

ONLINE study list *(http://www.OnlineStudyList.com)*

IPexpert is proud to lead the industry with multiple support options at your disposal free of charge. Our online forums (www.CertificationTalk.com) have attracted a membership of nearly 20,000 of your peers from around the world! At www.OnlineStudyList.com, you may subscribe to multiple "SPAM-free" email lists. Also, if you are an IPexpert Elite Member and need support for your IPexpert products, simply open a support ticket at www.IPexpert.com and it will be addressed promptly. In fact, IPexpert *guarantees* a response within one business day.

About The Authors

IPexpert employs only the best and brightest CCIE developers and instructors in the industry. Our celebrated team of diverse experts holds multiple CCIE certifications gained from substantial and highly relevant real-world experience. These key attributes give IPexpert the leading edge for delivering the most effective training possible.

Wayne A. Lawson II
CCIE #5244 (R&S), CCNA, CCDA, Nortel NCSE, MCP, MCSE (NT 4.0), MCSE +I, CNA, CNE (4.0), CNX Ethernet, Cisco Wireless LAN Design Specialist, Cisco IP Telephony Design Specialist
Founder & President – IPexpert, Inc.
With 15 years of networking, sales and marketing experience, Mr. Lawson possesses the technical competency, leadership and visionary talent possessed only by the most successful entrepreneurs around the globe. Wayne has served as a highly effective contributing member of five major organizations, including the United States Marine Corps (USMC), International Network Services (INS), Cisco Systems, Vertical Networks and IPexpert, Inc. He has been published on the topics of "Building Cisco Remote Access Networks" (ISBN: 1-928993-13-X) and "Configuring

Cisco AVVID" (ISBN: 1-928994-14-8), and has written for various technical and entrepreneurial magazines. Mr. Lawson founded IPexpert in 2001 and continues to revolutionize the way engineers prepare for the coveted CCIE Lab certification. Wayne's unique visionary approach to cutting-edge technologies and enterprise network solutions, coupled with a fanatical dedication to customer satisfaction, propel the engine of success at IPexpert. With a talent for revolutionizing products, services and solutions, and a drive to achieve perfection, his leadership and business ethics have molded IPexpert into the clear leader in CCIE Lab training. In addition to acting as the President and Senior Director of IPexpert, Inc., Wayne is also preparing for his CCIE Voice Lab exam.

Scott Morris
Quad CCIE #4713 (R&S, ISP-Dial, Security and Service Provider), CCDP, CCSP, Cisco Cable Communications Specialist, Cisco IP Telephony Support Specialist, Cisco IP Telephony Design Specialist, CCNA (WAN Switching), MCSE (NT 4.0), Juniper Networks JNCIP and JCNIS, RiverStone Networks RCNP, NSA/CNSS INFOSEC Professional, TIA Convergence Technology Professional (CTP), and CISSP #37445.
Senior Technical Instructor and Developer – IPexpert, Inc.
Boasting more than 18 years of technical training and consulting experience and a wealth of technical certifications, Scott Morris has proven himself among the elite in the technical training industry. Scott is one of the few people in the world currently holding four separate CCIE certifications, and he is actively preparing for his fifth – the CCIE Voice. Scott has an outstanding track record of success in editing, writing and reviewing training books for Cisco Press, Wylie, Sybex, Que Publishing and McGraw-Hill, and teaching CCIE lab preparation materials. He has served as a contributing author for works including Cisco Press' Managing Cisco Network Security book (ISBN: 1578701031) - Chapters on the PIX Firewall; and Cisco Press' CCIE Practical Studies, Vol. 2 (ISBN: 1587050722) - Chapter on Multicast. Scott has also written various articles for Packet Magazine and TCP Mag.

Vik Malhi
CCIE #13890 Voice, CCVP, Cisco IP Telephony Support Specialist, Cisco IP Telephony Operations Specialist, Cisco IP Telephony Design Specialist and Cisco Wireless LAN Design Specialist.
Sr. Voice Technical Instructor and Developer – IPexpert, Inc.
With nearly 10 years of IP Telephony training and consulting experience and a wealth of technical certifications, Vik Malhi has proven that he? one of the top Cisco voice instructors and consultants in the world! Vik was the first engineer to install CM 3.0 in Europe, Has over 6 years of AVVID consulting and implementation experience and has taught CCIE Voice Lab classes for the past several months. Vik has joined IPexpert's accredited team of experts and will be in charge of updating, supporting and teaching IPexpert's CCIE Voice-related products, services and classes.

Mark Snow
CCIE #14073 Voice, CCVP, CCNP, CCDP, CSE, CQS-CIPCCES, CQS-CIPTDS, CQS-CIPTOS, CQS-CIPTSS, MCSE.
Sr. Voice Technical Instructor and Developer – IPexpert, Inc.
From the age of 5 in his father's (patented inventor) laboratory, Mark passion for technology has never stopped growing. With over 10 years working professionally in the IT industry and over 5 years spent consulting internationally with a focus on large-scale, Cisco IP Telephony, Mark brings a wealth of knowledge to the training arena. Mark holds a CCIE in Voice, as well as many other Cisco and Microsoft certifications. Mark plans to begin working on his next CCIE in Security. Mark is responsible for IPexpert's CCIE Voice training, self-paced product development and support.

Feedback

Do you have a suggestion or other feedback regarding this book or other IPexpert products? At IPexpert, we look to you – our valued clients – for the real world, frontline evaluation that we believe is necessary to improve continually. Please send an email with your thoughts to feedback@ipexpert.com or call 1.866.225.8064 (international callers dial +1.810.326.1444).

In addition, when you pass the CCIE™ Lab exam, we want to hear about it! Email your CCIE™ number to success@ipexpert.com and let us know how IPexpert helped you succeed. We would like to send you a gift of thanks and congratulations.

Additional CCIE™ Preparation Material

IPexpert, Inc. is committed to developing the most effective Cisco CCIE™ R&S, Security, Service Provider, and Voice Lab certification preparation tools available. Our team of certified networking professionals develops the most up-to-date and comprehensive materials for networking certification, including self-paced workbooks, online Cisco hardware rental, classroom training, online (distance learning) instructor-led training, audio products, and video training materials. Unlike other certification-training providers, we employ the most experienced and accomplished team of experts to create, maintain, and constantly update our products. At IPexpert, we are focused on making your CCIE™ Lab preparation more effective.

IPexpert features a variety of CCIE™ training materials to suit your needs and learning preferences. Please review the catalog that has been incorporated into this book for additional products that are available to you!

A message from the Author(s):

The scenarios covered in this workbook were developed by Voice CCIEs to help you prepare for the Cisco CCIE Voice laboratory. It is strongly recommended that you use other reading materials in addition to this workbook.

Training is not the CCIE Voice workbook objective. The intent of these labs is to test your knowledge and ability of implementing Cisco Enterprise Voice Solutions.

Time management is very important, if you get stuck on a lab scenario be sure to write it down. Formulate a Checklist for skipped sections and then return to those sections once you have gone through the entire lab. Be sure to revisit the questions that you do not understand.

For more information on the CCIE Voice lab, please visit
http://www.cisco.com/warp/public/625/ccie/voice/lab_exam.html

Helpful Hints

- Keep It Simple, try to avoid any extra work (example: adding descriptions)
- Always try to use "Cisco Best Practices" http://www.cisco.com/go/srnd
- Save your router configurations (write memory)
- Restart the CallManager service periodically.

IPEXPERT END-USER LICENSE AGREEMENT

END USER LICENSE FOR ONE (1) PERSON ONLY

IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, DO NOT OPEN OR USE THE TRAINING MATERIALS.

This is a legally binding agreement between you and IPEXPERT, the "Licensor," from whom you have licensed the IPEXPERT training materials (the "Training Materials"). By using the Training Materials, you agree to be bound by the terms of this License, except to the extent these terms have been modified by a written agreement (the "Governing Agreement") signed by you (or the party that has licensed the Training Materials for your use) and an executive officer of Licensor. If you do not agree to the License terms, the Licensor is unwilling to license the Training Materials to you. In this event, you may not use the Training Materials, and you should promptly contact the Licensor for return instructions.

The Training Materials shall be used by only **ONE (1) INDIVIDUAL** who shall be the sole individual authorized to use the Training Materials throughout the term of this License.

Copyright and Proprietary Rights

The Training Materials are the property of IPEXPERT, Inc. ("IPEXPERT") and are protected by United States and International copyright laws. All copyright, trademark, and other proprietary rights in the Training Materials and in the Training Materials, text, graphics, design elements, audio, and all other materials originated by IPEXPERT at its site, in its workbooks, scenarios and courses (the "IPEXPERT Information") are reserved to IPEXPERT.

The Training Materials cannot be used by or transferred to any other person. You may not rent, lease, loan, barter, sell or time-share the Training Materials or accompanying documentation. You may not reverse engineer, decompile, or disassemble the Training Materials. You may not modify, or create derivative works based upon the Training Materials in whole or in part. You may not reproduce, store, upload, post, transmit, download or distribute in any form or by any means, electronic, mechanical, recording or otherwise any part of the Training Materials and IPEXPERT Information other than printing out or downloading portions of the text and images for your own personal, non-commercial use without the prior written permission of IPEXPERT.

You shall observe copyright and other restrictions imposed by IPEXPERT. You may not use the Training Materials or IPEXPERT Information in any manner that infringes the rights of any person or entity.

Exclusions of Warranties

THE TRAINING MATERIALS AND DOCUMENTATION ARE PROVIDED "AS IS." LICENSOR HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE LIMITATION OF INCIDENTAL DAMAGES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. This agreement gives you specific legal rights, and you may have other rights that vary from state to state.

Choice of Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of the State of Michigan, without reference to any conflict of law principles. You agree that any litigation or other proceeding between you and Licensor in connection with the Training Materials shall be brought in the Michigan state or courts located in Port Huron, Michigan, and you consent to the jurisdiction of such courts to decide the matter. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this License. If any provision of this Agreement is held invalid, the remainder of this License shall continue in full force and effect.

Limitation of Claims and Liability

ANY ACTION ON ANY CLAIM AGAINST IPEXPERT MUST BE BROUGHT BY THE USER WITHIN ONE (1) YEAR FOLLOWING THE DATE THE CLAIM FIRST ACCRUED, OR SHALL BE DEEMED WAIVED. IN NO EVENT WILL THE LICENSOR'S LIABILITY UNDER, ARISING OUT OF, OR RELATING TO THIS AGREEMENT EXCEED THE AMOUNT PAID TO LICENSOR FOR THE TRAINING MATERIALS. LICENSOR SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, REGARDLESS OF WHETHER LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WITHOUT LIMITING THE FOREGOING, LICENSOR WILL NOT BE LIABLE FOR LOST PROFITS, LOSS OF DATA, OR COSTS OF COVER.

Entire Agreement

This is the entire agreement between the parties and may not be modified except in writing signed by both parties.

U.S. Government - Restricted Rights

The Training Materials and accompanying documentation are "commercial computer Training Materials" and "commercial computer Training Materials documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction release, performance, display, or disclosure of the Training Materials and accompanying documentation by the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

IF YOU DO NOT AGREE WITH THE ABOVE TERMS AND CONDITIONS, DO NOT OPEN OR USE THE TRAINING MATERIALS AND CONTACT LICENSOR FOR INSTRUCTIONS ON RETURN OF THE TRAINING MATERIALS.

IPexpert's CCIE Voice Proctor Guide (Version 4.0)

Table of Contents

NOTE:

You are encouraged to take advantage of the knowledge and support from your peers around the globe. Join www.CertificationTalk.com to participate in online forums along with nearly 20,000 other members! Subscribe to one or more email lists at www.OnlineStudyList.com to stay informed and involved with others who are working to achieve the same goals. CertificationTalk and OnlineStudyList memberships are available to you at no charge!

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 1: Basic Campus Design

Estimated Time to Complete: 2 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 1 Basic Campus Design

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab

The devices which are plugged into the actual switches in the POD are there to test that the Infrastructure and QoS Section are configured correctly. The devices will auto-answer after 5 seconds and you should be able to hear a recorded message. To test dial plan we recommend you bring up Cisco IP Communicator and multiple instances of IP Blue. The PSTN phone is a 7960 attached to the Catalyst 6000.

Section 1 Configuration Tasks

Task 1.1

Ensure that the link between the HQ/BR1/BR2 routers and appropriate switches are configured as DOT1Q trunks. Give the voice sub-interface the appropriate ip address from Table 2. Check connectivity between all sites and Call Manager/Unity.

NOTE:

- All Layer 2 and Layer 3 routing and switching should be pre-configured but the candidate should be aware of how to troubleshoot. For this reason we shall cover these topics without going into too much detail - remember, there is another exam for R&S.
- Although the Native or Data Vlan is not being used, we are assuming a PC is connected into the switched port of the phone and that the Native Vlan IS operational.

➔ **On the HQ router verify that the LAN interface is configured correctly. There should not be any IP addresses defined on the main interface. Two sub-interfaces should be created with the encapsulation type set to 802.1Q. The VLAN identifier should be configured on each sub-interface and an IP address should be assigned to the Voice Sub-interface. Use Table 1 for VLAN Identifiers and Table 2 for IP Addresses.**

```
P5-HQ-RTR#sh run | begin FastEthernet
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 150 native
!
interface FastEthernet0/0.2
 encapsulation dot1Q 250
 ip address 10.5.200.3 255.255.255.0
```

➔ **Check that the Frame Relay PVCs have been created.**

```
P2-HQ-RTR#sh run | beg Serial0/1/0
interface Serial0/1/0:0
 no ip address
 encapsulation frame-relay IETF
 frame-relay lmi-type ansi
!
interface Serial0/1/0:0.1 point-to-point
 ip address 162.6.101.1 255.255.255.0
 ip ospf mtu-ignore
 frame-relay interface-dlci 201
!
interface Serial0/1/0:0.2 point-to-point
 ip address 162.6.102.1 255.255.255.0
 ip ospf mtu-ignore
 frame-relay interface-dlci 202
```

➔ **Ensure that none of the appropriate interfaces are shutdown.**

```
P2-HQ-RTR#sh ip int bri
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual up                    up
FastEthernet0/0.110    unassigned      YES unset  deleted               down
FastEthernet0/0.160    unassigned      YES unset  up                    up
FastEthernet0/0.210    unassigned      YES manual deleted               down
FastEthernet0/0.260    10.6.200.3      YES manual up                    up
FastEthernet0/1        unassigned      YES NVRAM  administratively down down
Serial0/1/0:0          unassigned      YES unset  up                    up
Serial0/1/0:0.1        162.6.101.1     YES manual up                    up
Serial0/1/0:0.2        162.6.102.1     YES manual up                    up
Loopback0              172.6.100.1     YES NVRAM  up                    up
P2-HQ-RTR#
```

➔ **Verify that OSPF has loaded successfully and has established neighbor adjacency with other routers.**

```
P2-HQ-RTR#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.6.200.2        1   FULL/DROTHER    00:00:33    10.6.200.2      FastEthernet0/0.260
209.124.41.3      1   FULL/DR         00:00:39    10.6.200.9      FastEthernet0/0.260
172.6.102.1       0   FULL/  -        00:00:32    162.6.102.2     Serial0/1/0:0.2
172.6.101.1       0   FULL/  -        00:00:34    162.6.101.2     Serial0/1/0:0.1
P2-HQ-RTR#
```

➔ **On the 6500 switch force the port to which the HQ-RTR is connected to become a trunk and set the encapsulation type to 802.1Q. Use the port names on the 6500 to find out which port to configure.**

```
Console> (enable) sh port 2
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
...
2/20 P1-HQ-RTR             notconnect     210     full    100 10/100BaseTX
2/21 P2-HQ-RTR             connected      trunk   a-full  a-100 10/100BaseTX
2/22 P3-HQ-RTR             notconnect     130     auto    auto 10/100BaseTX
2/23 P4-HQ-RTR             notconnect     140     auto    auto 10/100BaseTX
2/24 P5-HQ-RTR             connected      150     a-full  a-100 10/100BaseTX
2/25 P6-HQ-RTR             notconnect     220     auto    auto 10/100BaseTX

Console> (enable) set trunk 2/24 on dot1q

Console> (enable) sh port 2/24
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
2/24 P5-HQ-RTR           connected trunk   a-full   a-100 10/100BaseTX
```

➔ **On the BR2 router perform the same procedure followed on the HQ-RTR to enable 802.1Q tunneling. Check that the interfaces are administratively "up" and that OSPF has loaded. The Frame-Relay configuration is given below.**

```
P5-BR2-RTR#sh run | b Serial
interface Serial0/1/0
 no ip address
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay lmi-type ansi
!
interface Serial0/1/0.1 point-to-point
 ip address 162.5.102.2 255.255.255.0
 frame-relay interface-dlci 102
```

➔ **Check that you can ping the HQ-RTR.**

```
P5-BR2-RTR#ping 10.5.200.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.200.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/12 ms
```

➔ **On the BR2 switch find out which port the BR2 router is connected by checking for Cisco Neighbors. On the uplink enable 802.1Q tunneling and force the port to become a trunk. You will a message indicating that the port has been reset.**

```
Switch#sh cdp neig
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID          Local Intrfce   HoldtmeCapability   Platform      Port ID
P5-BR2-RTR         Fas 0/1         175      R S I      Cisco 2811    Fas 0/0
SEP0011BBD259A5    Fas 0/24        129      H          Cisco IP      PPort 1
SEP0011BB9A0EFF    Fas 0/23        136      H          Cisco IP      PPort 1

Switch(config)#int f0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
1w3d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to downch
1w3d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

➔ **The BR1 router contains an integrated Etherswitch module so there is no 802.1Q trunk to configure. Instead ensure the VLAN Identifers exist in the VLAN database, create a VLAN interface and assign the ip address defined in Table 2.**

```
P5-BR1-RTR#vlan database
P5-BR1-RTR(vlan)#sh current
 VLAN ISL Id: 1
   Name: default
   Media Type: Ethernet
   VLAN 802.10 Id: 100001
   State: Operational
   MTU: 1500
   Translational Bridged VLAN: 1002
   Translational Bridged VLAN: 1003

 VLAN ISL Id: 150
   Name: data
   Media Type: Ethernet
   VLAN 802.10 Id: 100150
   State: Operational
   MTU: 1500

 VLAN ISL Id: 250
   Name: voice
   Media Type: Ethernet
   VLAN 802.10 Id: 100250
   State: Operational
   MTU: 1500

P5-BR1-RTR(config)#int vlan 250
P5-BR1-RTR(config-if)#ip addr 10.5.201.1 255.255.255.0
P5-BR1-RTR(config-if)#no shutdown
```


➔ **Ensure that the Serial interface is pre-configured.**

```
P5-BR1-RTR# sh run | begin Serial0/1/0
interface Serial0/1/0
 no ip address
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay lmi-type ansi
!
interface Serial0/1/0.1 point-to-point
 ip address 162.5.101.2 255.255.255.0
 ip ospf mtu-ignore
 frame-relay interface-dlci 101
```

➔ **Check all interface are UP and that OSPF has been loaded successfully.**

```
P5-BR1-RTR#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES TFTP   administratively down down
GigabitEthernet0/1     unassigned      YES TFTP   administratively down down
Serial0/1/0            unassigned      YES TFTP   up                    up
Serial0/1/0.1          162.5.101.2     YES TFTP   up                    up
<....snip....>
Vlan1                  unassigned      YES TFTP   administratively down down
Vlan250                10.5.201.1      YES TFTP   up                    down
Loopback0              172.5.101.1     YES TFTP   up                    up
```

NOTE:

- The VLAN interface will show as Line Protocol "Down" until you configure VLAN 250 on one of the FastEthernet ports and that port becomes active.

➔ **A good idea now is to ping the HQ-RTR to verify connectivity.**

```
P5-BR1-RTR#ping 10.5.200.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.200.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms
```

Task 1.2

Configure Voice and Data VLAN for all IP Phones including ATA and VG248. VLAN IDs are defined in Table 1. Use Table 3 for 6500 port assignment. For BR1 and BR2 port allocation you are required to find out port allocation by your own methods.

➔ **Check 6500 port allocation using Table 3 of the WB. Also the Port Names on the switch should be accurate. Be careful to configure only those ports assigned to your POD since this is a shared switch. Notice that the voice VLAN is known as the auxiliary VLAN on the CatOS.**

```
Console> (enable) set port enable 2/15
Console> (enable) set vlan 150 2/14
VLAN  Mod/Ports
---- -----------------------
150  2/13-14
Console> (enable) set port auxiliaryvlan 2/14 250
AuxiliaryVlan Status  Mod/Ports
------------- -------- -------------------------------------------------------
250         active  2/14
```

➔ **Verify the port has accepted the configuration changes.**

```
Console> (enable) sh port 2/14
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name             Status    Vlan     Duplex Speed    Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 2/14 POD15 HQ PHONE     connected 150      a-full     a-100 10/100BaseTX

Port  AuxiliaryVlan AuxVlan-Status
----- ------------- --------------
 2/14 250         active
```

➔ **On both the BR1 and BR2 switches verify which ports have Cisco Phones connected by checking CDP Neighbors. Before you see any neighbors ensure that all switched ports are administratively up.**

```
P5-BR1-RTR(config)#interface range f1/0 - 15
P5-BR1-RTR(config-if-range)#no shutdown
P5-BR1-RTR(config-if-range)#do sh cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
               S - Switch, H - Host, I - IGMP, r - Repeater

Device ID       Local Intrfce   Holdtme   Capability  Platform  Port ID
SEP0011BBD25868 Fas 1/0          179         H       IP Phone 7Port 1
SEP0011BBD25F29 Fas 1/8          140         H       IP Phone 7Port 1
```

➔ **Configure the Voice and Native VLAN on each port the phone is connected. To reduce the size of the configuration (on issuing the "show running-config" command) we suggest you only configure those ports which are active. You have to configure the port as a trunk, set the encapsulation type as 802.1Q, set the VLAN to be used for voice and set the native VLAN used for sending and receiving untagged traffic.**

```
P5-BR1-RTR(config-if)#int f1/0
P5-BR1-RTR(config-if)#switchport trunk encapsulation dot1q
P5-BR1-RTR(config-if)#switchport voice vlan 250
P5-BR1-RTR(config-if)#switchport trunk native vlan 150
P5-BR1-RTR(config-if)#switchport mode trunk
```

➔ **After we complete the above configuration we should see the following message informing us that the Line Protocol on Interface Vlan 250 has change to "up" and that the port in question has become a DOT1Q trunk.**

```
*Aug 30 14:00:52.147: %DTP-5-TRUNKPORTON: Port Fa1/0 has become dot1q trunk
*Aug 30 14:00:52.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan250,
changed state to up
```

➔ **On the BR2-3550 you can either use the method shown above to specify Voice Vlan or use the alternative method shown below.**

```
Switch(config-if-range)#int range f0/23 - 24
Switch(config-if-range)#switch access vlan 150
Switch(config-if-range)#switchport voice vlan 250
```

Task 1.3

Configure all phone ports such that they bypass the spanning-tree listening and learning states.

NOTE:

- It is more efficient to configure this task while configuring Task 1.2 – this goes to show that there is a benefit from reading the entire lab beforehand.

➔ **On both the BR1 and BR2 switches, put the port in the spanning tree forwarding state.**

```
Switch(config)#int range f0/23 - 24
Switch(config-if-range)#spanning-tree portfast
```

➔ **On the CatOS the syntax is slightly different.**

Console> (enable) set spantree portfast 2/14 enable

Warning: Connecting Layer 2 devices to a fast start port can cause temporary spanning tree loops. Use with caution.

Spantree port 2/14 fast start enabled.

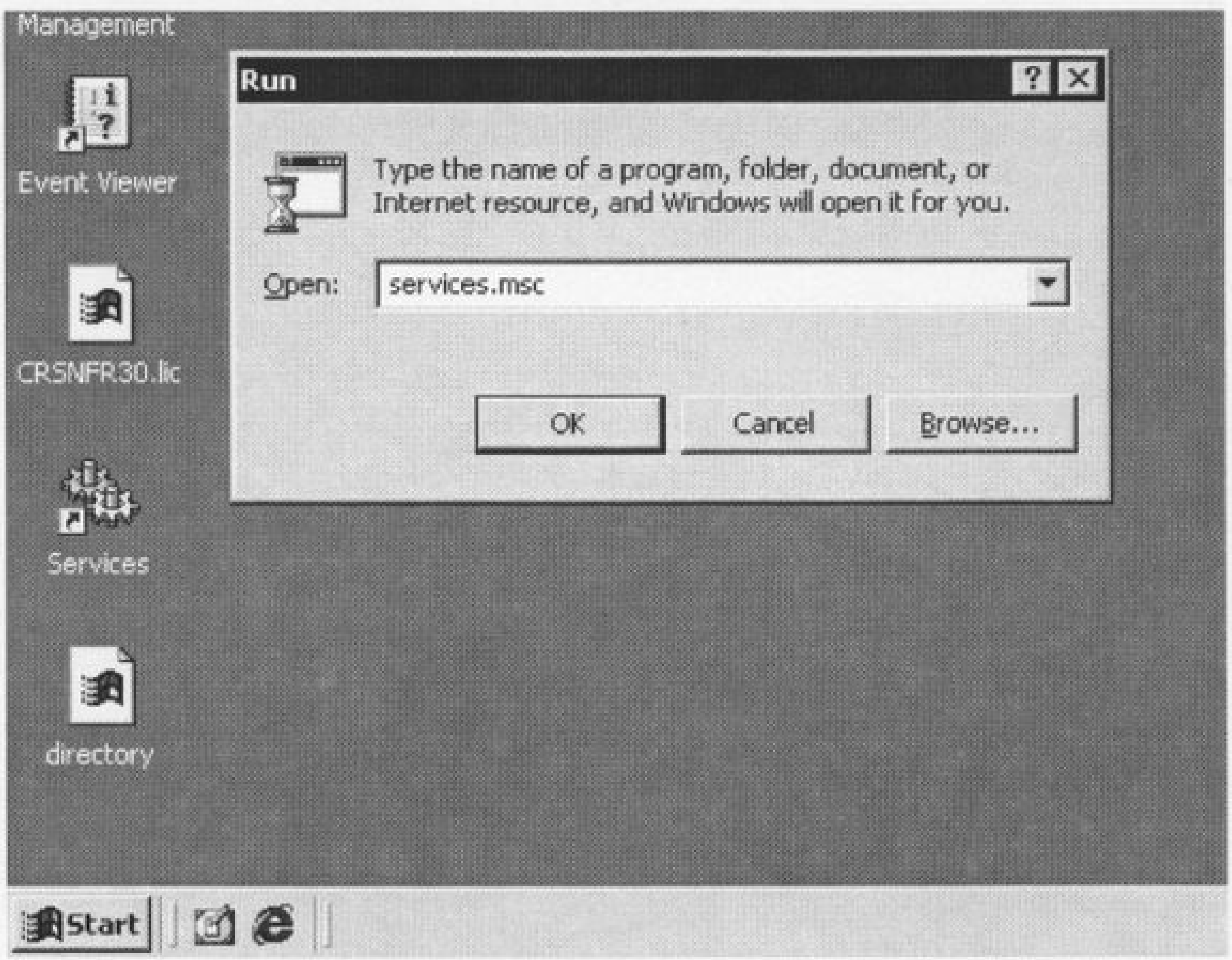
Task 1.4

Configure Microsoft DHCP Server on the Call Manager server. HQ and Branch 1 phones should get IP Address and other relevant information from the Call Manager Server. Use Table 2 for subnet information—only xx.xx.xx.120 – xx.xx.xx.129 from the voice subnet should be assigned from the server.

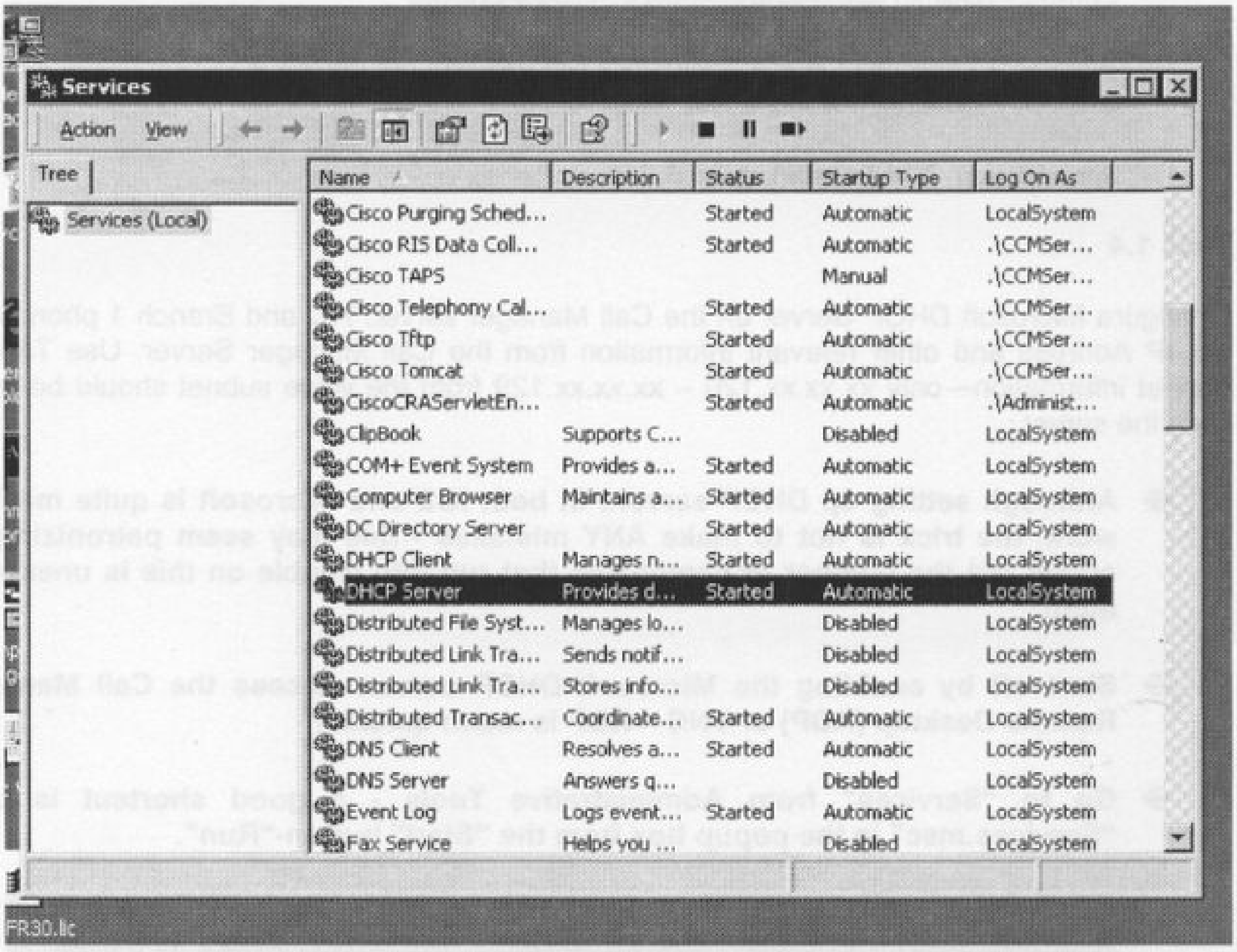
➔ **Although setting up DHCP servers in both IOS and Microsoft is quite mechanical work, the trick is not to make ANY mistakes - this may seem patronizing at the outset but the number of candidates that run into trouble on this is unexpectedly high!**

➔ **Start off by enabling the Microsoft DHCP server. Access the Call Manager via Remote Desktop (RDP) or VNC – RDP is much quicker!**

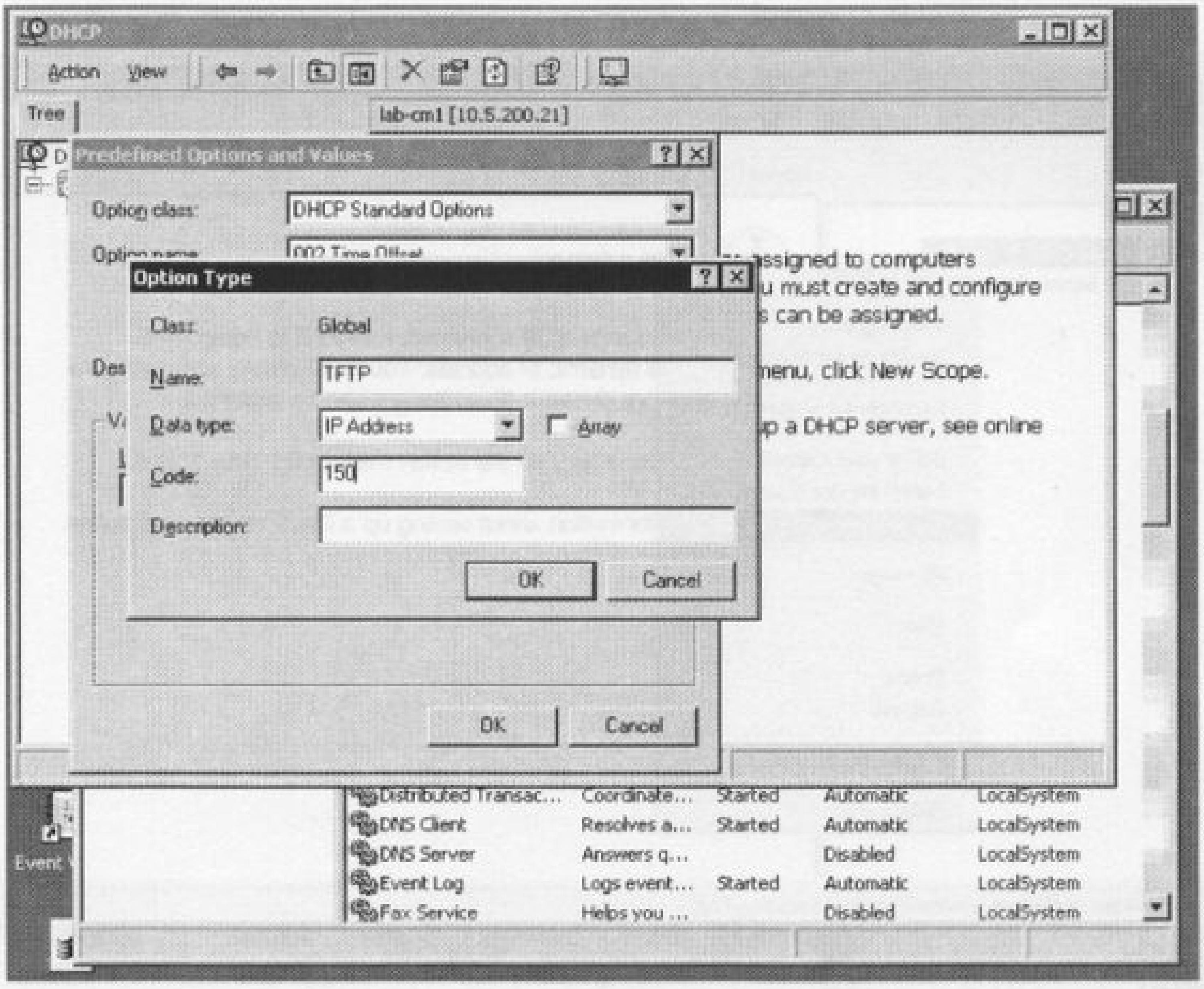
➔ **Go to "Services" from Administrative Tools - a good shortcut is to type "Services.msc" in the popup box from the "Start" button-"Run".**



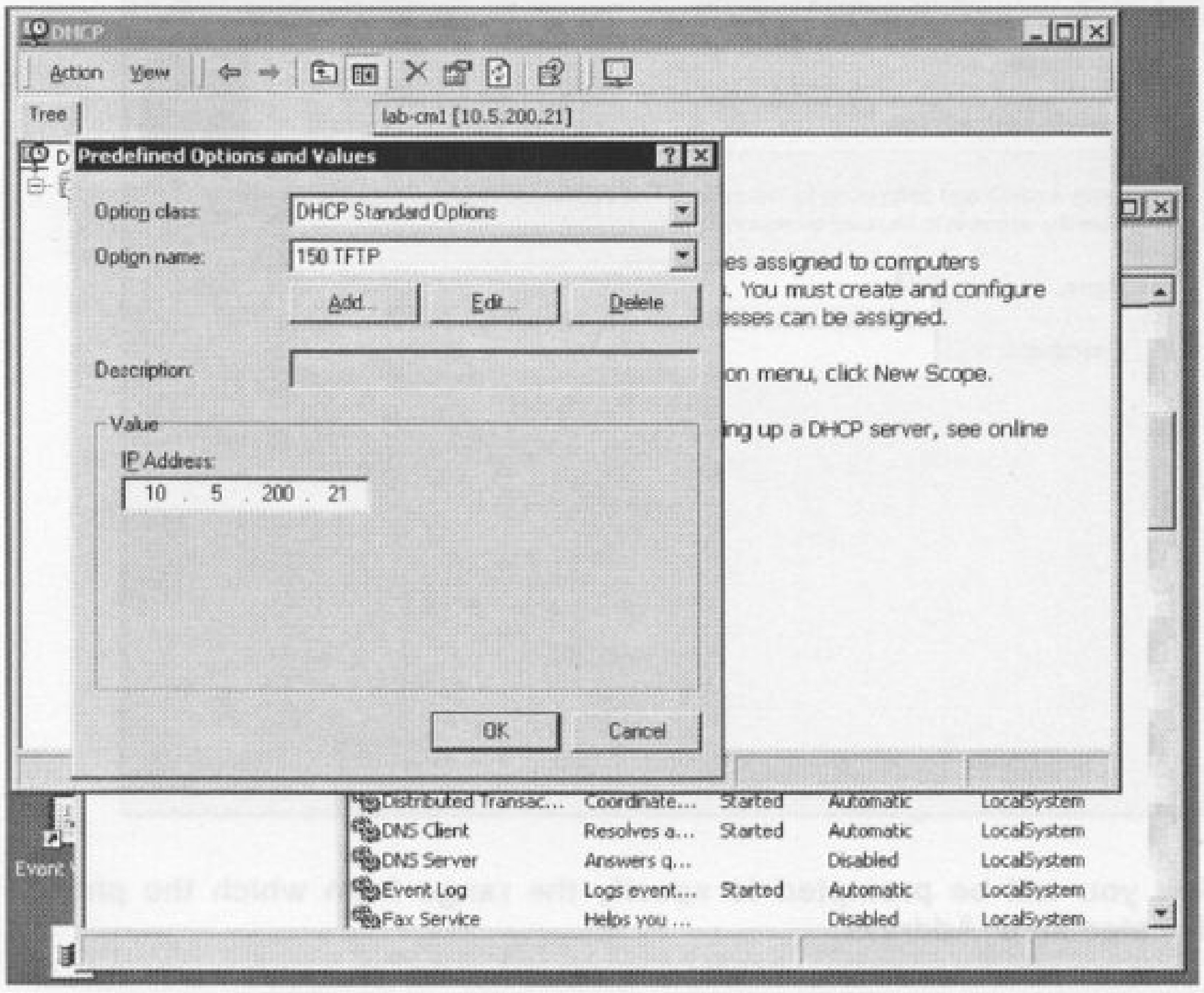
➔ **Ensure that the DHCP server is set to start "Automatic" after a reboot and has been started.**



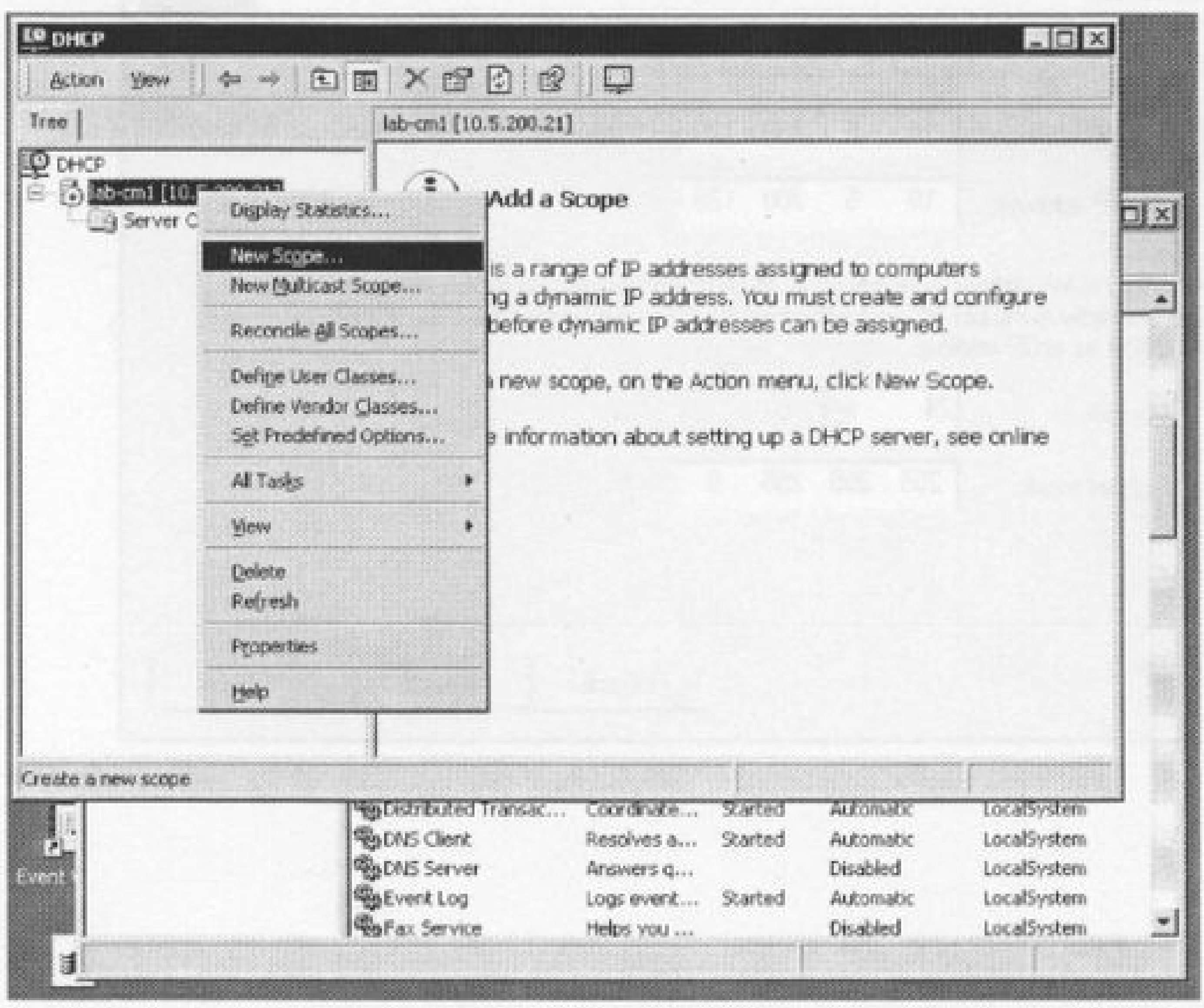
➔ **Give the new option a name (doesn't matter what you call it but "TFTP" makes logical sense). The code that Cisco TFTP uses is '150' and you must configure as an IP Address.**



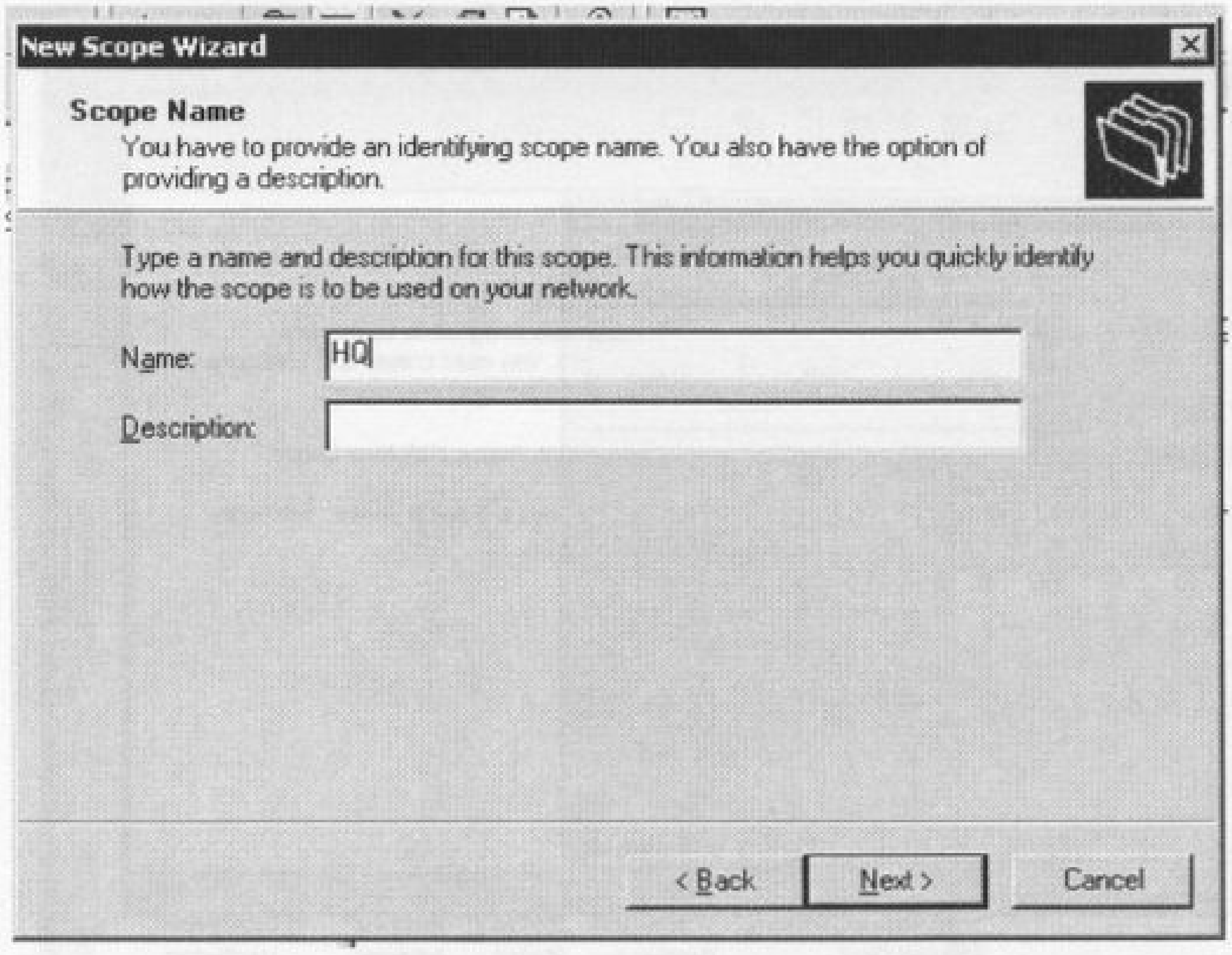
➔ **Define the IP Address of the TFTP Server - in this case the Publisher Call Manager is running the TFTP service.**



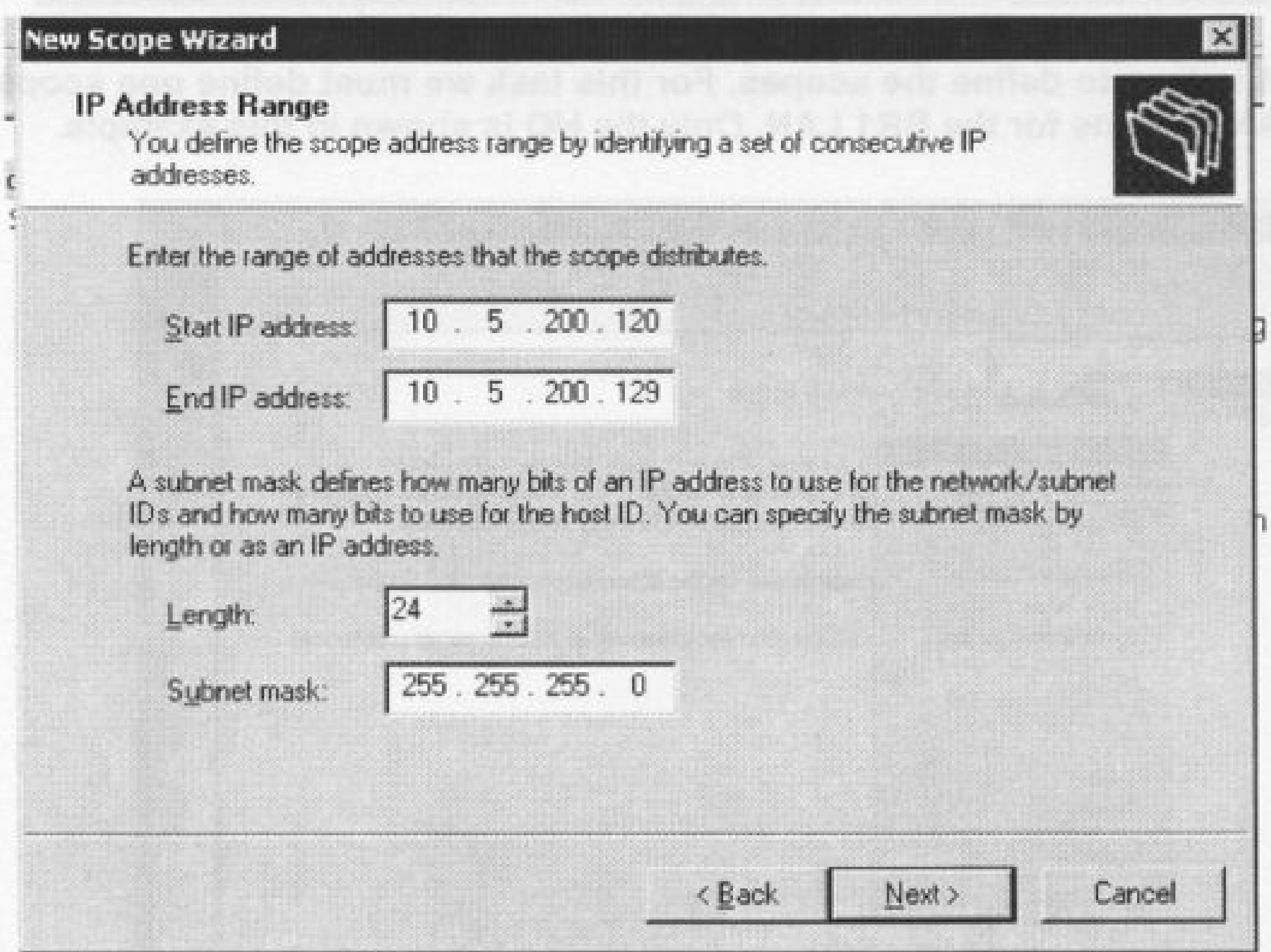
➔ **Now it is time to define the scopes. For this task we must define one scope for the HQ LAN and one for the BR1 LAN. Only the HQ is shown in this example.**



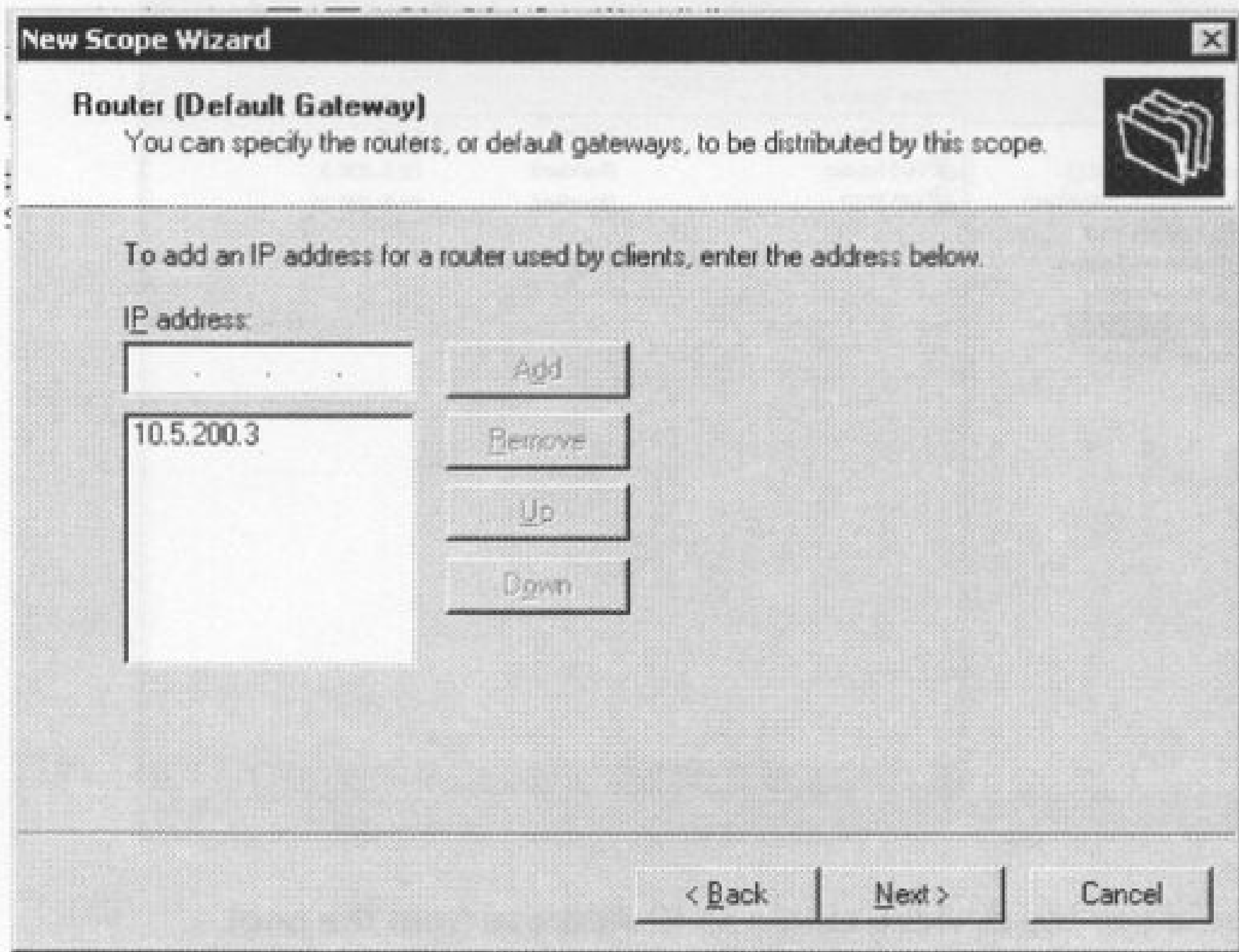
➔ **Give the scope a descriptive name.**



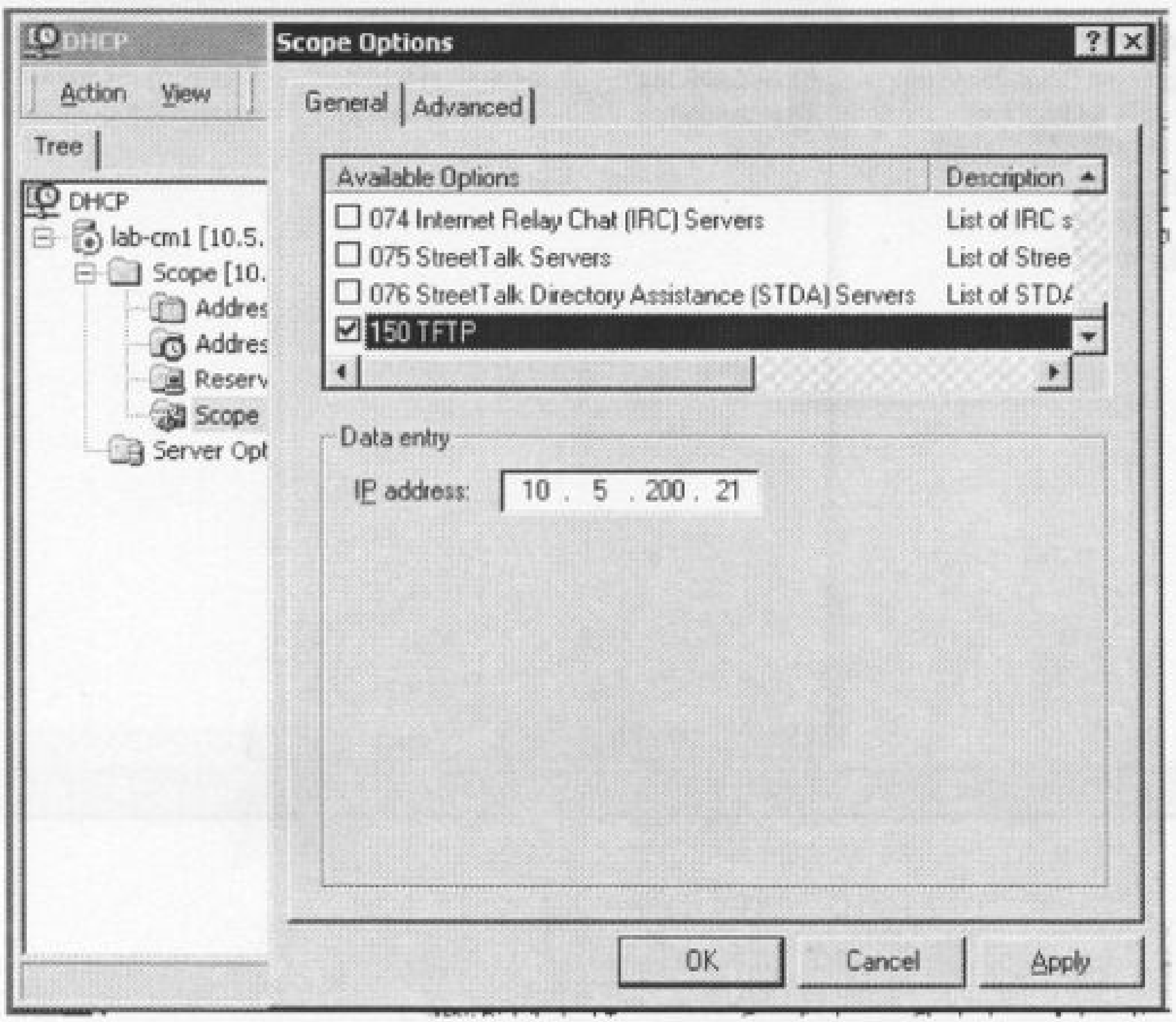
➔ **Now you will be prompted to specify the range from which the phones will be allocated an IP Address.**



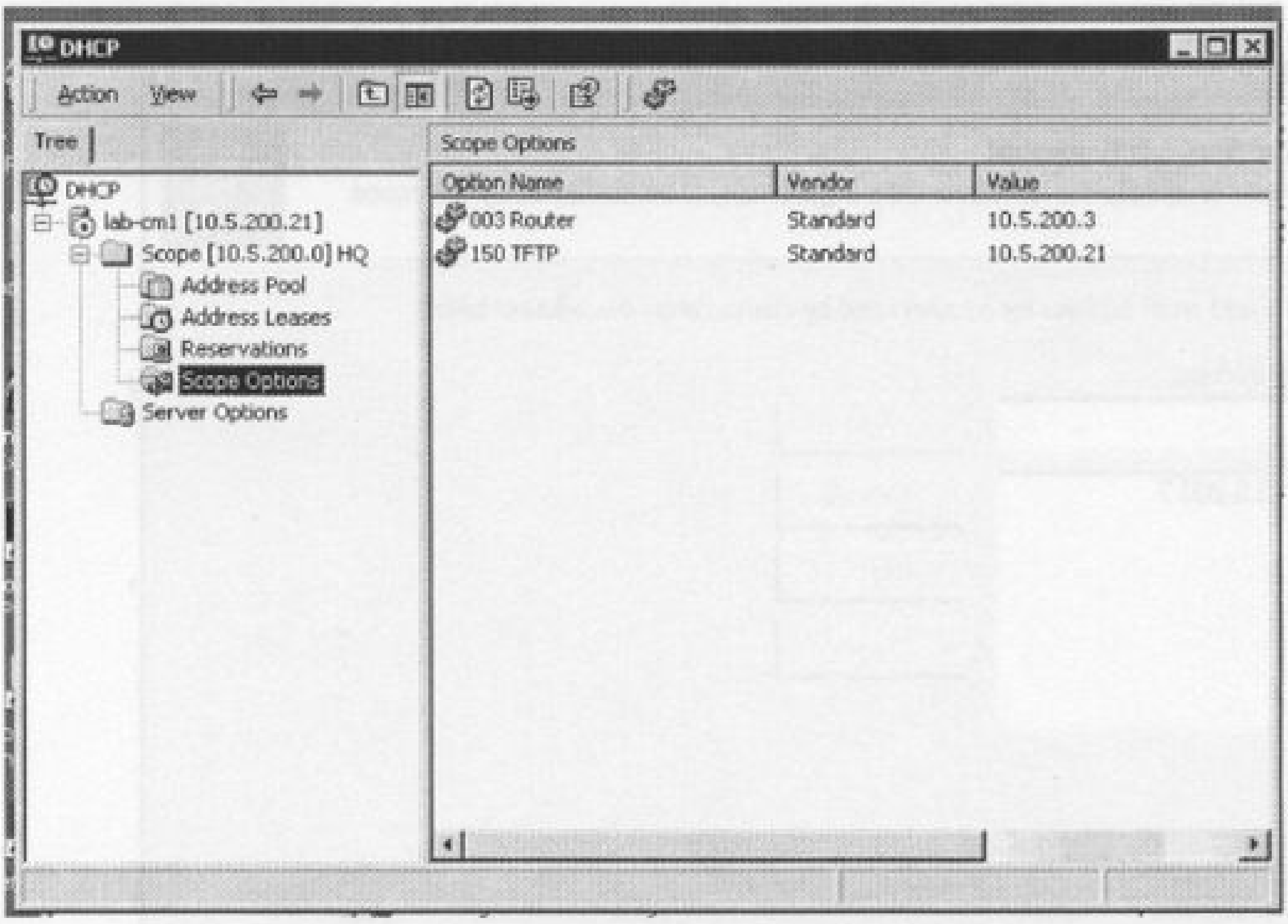
➔ **Other than default gateway and TFTP, no other options require any input to achieve this task - so you don't need to bother to exclude any IP Addresses or define a DNS/WINS server.**



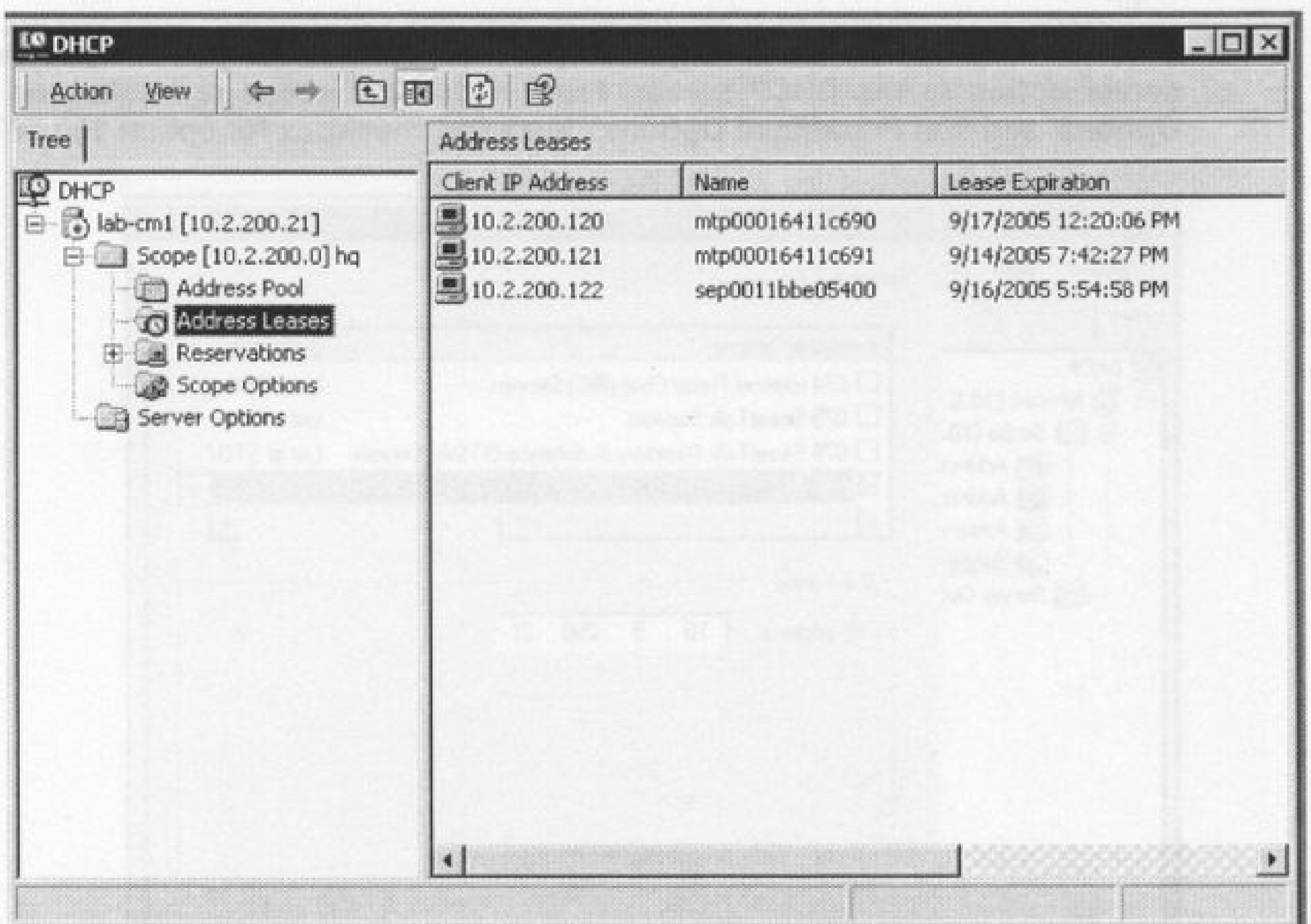
➔ **You have to complete the configuration of the scope before you can add the TFTP server option to the DHCP server. From within the scope right click on 'Scope Options' and 'Set Predefined Options'. Mark the checkbox for option 150 TFTP.**



➔ **Verify that the two required options have been set correctly before doing the same for the BR1 scope.**



➔ **You should see the devices obtain an IP Address from the pool.**



Task 1.5

Configure IOS DHCP on the Branch 2 router – only Branch 2 phones should get IP address and relevant information from this DHCP server. Use Table 2 for subnet information – only xx.xx.xx.120 – xx.xx.xx.129 should be assigned from the server.

➔ **At this stage it is worth checking to see if the Branch 2 router (or any router acting as a DHCP server) is acting as a Call Manager Express (CME). This is important to know beforehand because it will affect the IP Address you specify for option 150 (TFTP Server). In this case, you will see by looking at the last question in this lab that the BR2 router is indeed a CME. Ensure that the TFTP ip address defined in the DHCP server is the same as the source address of the CME.**

```
P5-BR2-RTR(config)#ip dhcp excluded-address 10.5.202.1 10.5.202.119
P5-BR2-RTR(config)#ip dhcp excluded-address 10.5.202.130 10.5.202.254
P5-BR2-RTR(config)#ip dhcp pool BR2
P5-BR2-RTR(dhcp-config)#network 10.5.202.0 255.255.255.0
P5-BR2-RTR(dhcp-config)#default-router 10.5.202.1
P5-BR2-RTR(dhcp-config)#option 150 ip 10.5.202.1
```

➔ **Verify the phones have successfully been allocated an IP Address. You may have to power cycle the handsets - remember that the Catalyst is offering inline power so simply resetting the ports to which the phones are connected will suffice (in the real lab the phones will be in front of you so you can enter "**#**" on the keypad which initiates a power cycle.**

```
Switch#sh power inline

Interface Admin  Oper   Power     Device      Class
                        (Watts)
---------- ----- ---------- ------- ------------------- ----------
Fa0/1     auto  off     0.0  n/a           n/a
Fa0/2     auto  off     0.0  n/a           n/a
<.......snip......>
Fa0/23    auto  on      6.3  Cisco IP Phone 7940  n/a
Fa0/24    auto  on      6.3  Cisco IP Phone 7940  n/a
```

➔ **After resetting the phone ports check the DHCP server to see if it has indeed allocated the correct IP Addresses to the phones.**

```
P5-BR2-RTR#sh ip dhcp bind
Bindings from all pools not associated with VRF:
IP address      Client-ID/        Lease expiration        Type
10.5.202.120    0100.11bb.d259.a5   Sep 01 2005 03:58 PM   Automatic
10.5.202.121    0100.11bb.9a0e.ff   Sep 01 2005 03:56 PM   Automatic
```

Task 1.6

Set the hardware clock on the HQ router (use EST as the time zone which is 5 hours behind GMT). Configure the HQ-RTR to become an authoritative time source which distributes the time via NTP. Configure the BR1 and BR2 routers to synchronize their clock with HQ-RTR.

➔ **Normally Cisco routers use an external time source to get its time - for this task we need to make the HQ-RTR the NTP master clock to which peers synchronize. Note that the software clock on the HQ-RTR must have been set before the NTP Master command is issued otherwise the "ntp master" command will have no effect. If no stratum is defined then the default of 8 is used.**

```
P5-HQ-RTR#sh clock
*22:30:01.856 UTC Wed Aug 31 2005
P5-HQ-RTR(config)#ntp master
```

➔ **For the Branch routers we will configure them to synchronize with the HQ-RTR. Set the time zone before defining the IP Address of the NTP Server. It is optional for this task whether you observe daylight savings.**

```
P5-BR1-RTR(config)#clock timezone est -5
P5-BR1-RTR(config)#clock summer-time EDT recurring
*Aug 31 22:39:31.855: %SYS-6-CLOCKUPDATE: System clock has been updated from
22:39:31 UTC Wed Aug 31 2005 to 17:39:31 est Wed Aug 31 2005, configured from console by
console.time

P5-BR1-RTR(config)#ntp server 10.5.200.3
```

➔ **For verification that the Branch routers have indeed synchronized with the Master, we are looking for the following output.**

```
P5-BR1-RTR#sh ntp status
Clock is synchronized, stratum 9, reference is 10.5.200.3
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is C6C0B066.5432BC11 (17:40:38.328 est Wed Aug 31 2005)
clock offset is 0.0420 msec, root delay is 10.12 msec
root dispersion is 1875.11 msec, peer dispersion is 1875.05 msec
```

➔ **While it is not part of the question, it is worth covering the commands to synchronize the CatOS using NTP.**

```
Console> (enable) set ntp timezone EST -5
Timezone set to 'EST', offset from UTC is -5 hours
Console> (enable) set summertime enable EDT
Summertime is enabled and set to 'EDT'
 Start : Sun Apr 3 2005, 02:00:00
 End   : Sun Oct 30 2005, 02:00:00
 Offset: 60 minutes
 Recurring: yes, starting at 02:00am of first Sunday of April and ending on 02:00am of last
Sunday of October.
Console> (enable) set ntp server 10.5.200.3
NTP server 10.5.200.3 added
Console> (enable) set ntp client enable
```

```
NTP Client mode enabled
Console> (enable) sh ntp

Current time: Thu Sep 1 2005, 08:21:41 EDT
Timezone: 'EST', offset from UTC is -5 hours
Summertime: 'EDT', enabled
  Start : Sun Apr 3 2005, 02:00:00
  End   : Sun Oct 30 2005, 02:00:00
  Offset: 60 minutes
Last NTP update:
Broadcast client mode: disabled
Broadcast delay: 3000 microseconds
Client mode: enabled
Authentication: disabled

NTP-Server                        Server Key
----------------------------------------  ----------
10.5.200.3                         -
```

Task 1.7

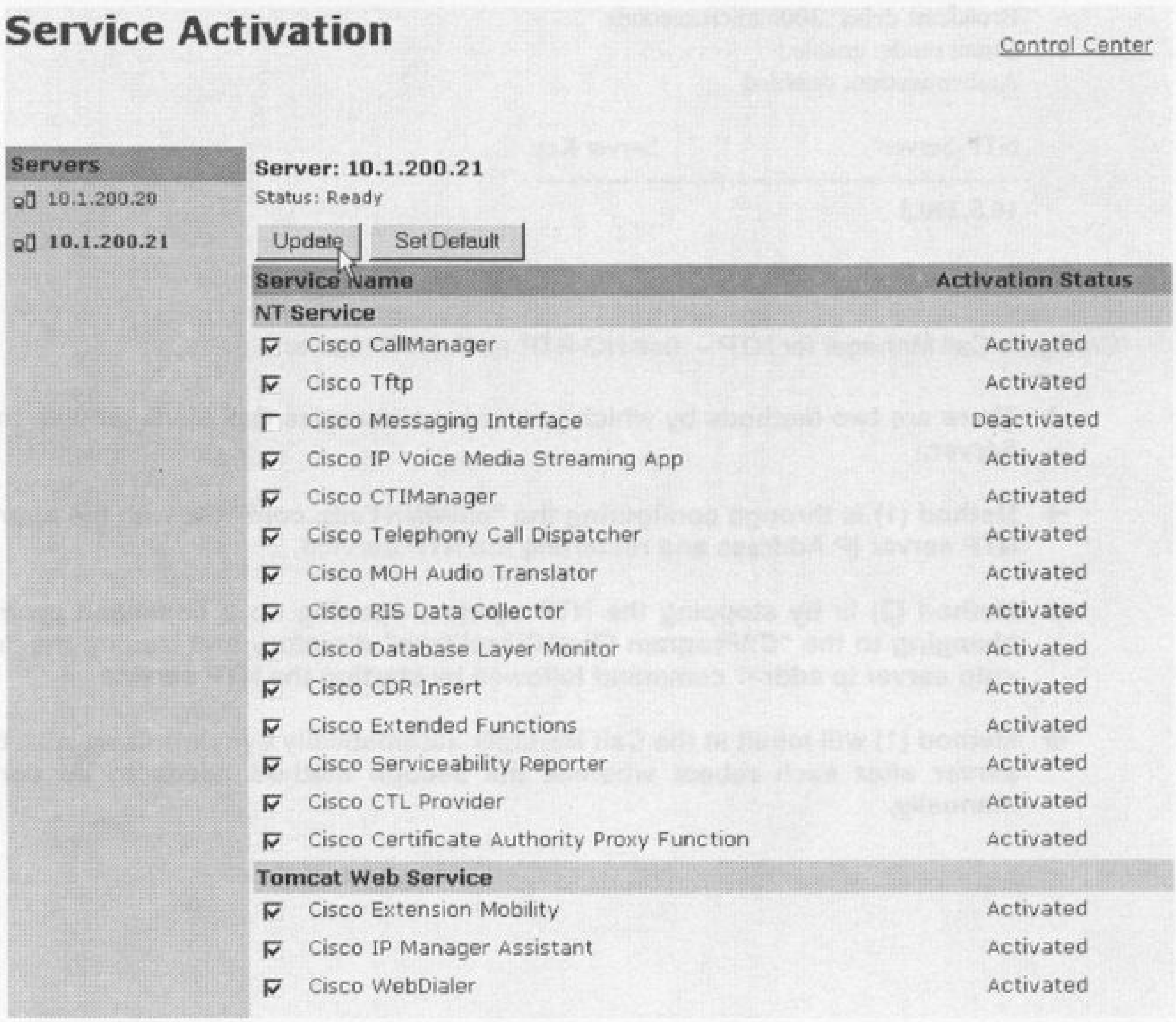
Configure Call Manager for NTP – use HQ-RTR as the NTP server.

- ➔ **There are two methods by which you can synchronize Call Manager with the Time Server.**
- ➔ **Method (1) is through configuring the "c:\WINNT\ntp.conf" file with the appropriate NTP server IP Address and restarting the NTP service.**
- ➔ **Method (2) is by stopping the NTP service, opening up a command prompt and changing to the "C:\Program Files\Cisco\Xntp" directory and issuing the "ntpdate <ntp server ip addr>" command followed by starting the NTP service.**
- ➔ **Method (1) will result in the Call Manager automatically synchronizing with the NTP server after each reboot whereas the second method needs to be performed manually.**

Task 1.8

Register HQ and BR1 phones to Call Manager based on Tables 5 and 6.

➔ **Don't forget to start the relevant Services from Service Activation in Call Manager Serviceability. While not all of them are required to register the phones, there is no harm activating all the likely services that are going to be used in a typical Call Manager environment. Cisco Messaging Interface will never be required based on the current blueprint since this is required for SMDI and you are not going to be asked to configure a legacy voicemail system.**



➔ **One difference between the Proctor Labs setup and the actual Lab environment is that a Subscriber Call Manager exists in the real thing. However as stated, you should practice configuring your CallManager and Gateways as if one did exist.**

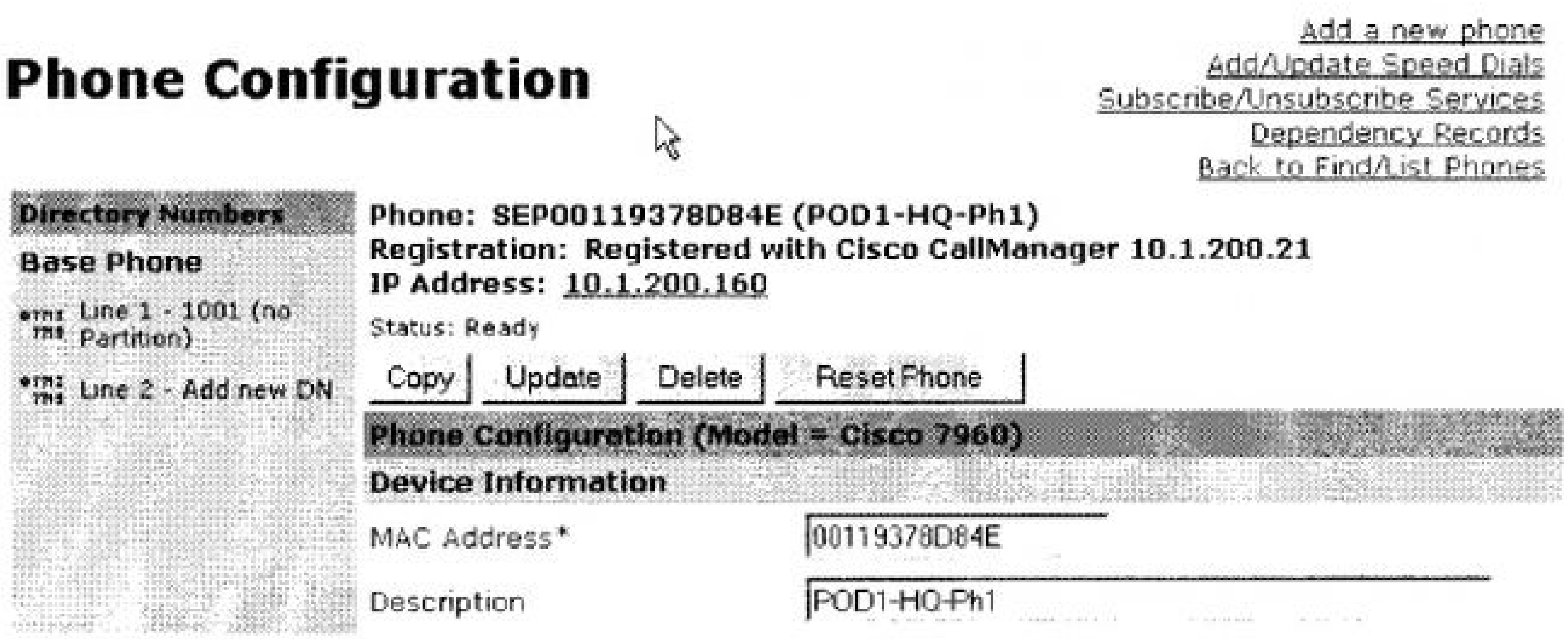
➔ **It is beyond the scope to cover how Publisher-Subscriber SQL replication takes place - however we recommend that you verify that replication is indeed working.**

➔ **The Database Layer Monitor service must be started and NetBIOS name resolution must be working on each server (edit the "lmhosts.sam" file in c:\WINNT\system32\drivers\etc directory with the IP Addresses and names of the Call Manager servers and save the file as LMHOSTS without the extension.). You can check what is currently in the NETBIOS name cache by issuing the nbtstat –c command from a command prompt. Issue the nbtstat –R command if the servers do not appear in the list. Check replication via SQL Enterprise Manager (for more information check the Troubleshooting IP Telephony book by Giralt).**

➔ **Once you have started services on the Publisher (and Subscriber) we would suggest turning on auto-registration (using a range that does not overlap with the DN assignment) if the Cluster has not already been converted to Mixed-Mode – which in the case of Proctor Labs equipment, this has been done for you. If you can't auto-register, pay special attention to whether the phone is a 7960 or 7940! The number of candidates who fall at this hurdle is surprising since the phone does not register if the phone type is incorrect.**

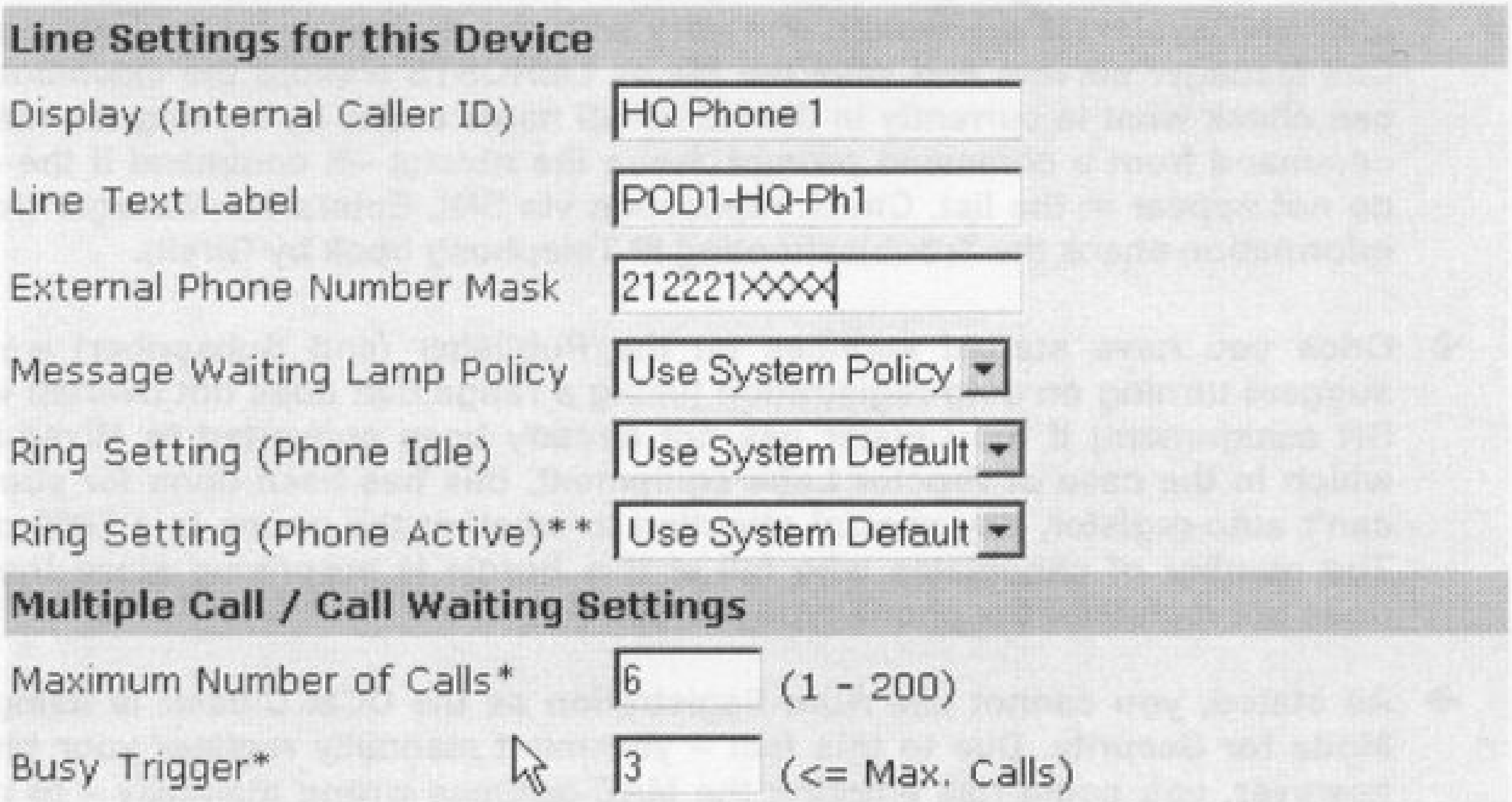
➔ **As stated, you cannot use Auto-Registration as the CCM Cluster is using Mixed Mode for Security. Due to this fact – you must manually register your phones – however, you could risk entering the MAC address wrong manually – to mitigate this problem, use "sh cdp neighbor" on the switch device where the phone is connected and Copy & Paste the MAC address into the CCM configuration page.**

➔ **From Device > Phone, create a new record for each phone and configure DN based on Tables 5 and 6.**



➔ **Ensure that devices register properly.**

➔ **Finally set the "Multiple Call / Call Waiting Settings" section on the DN for 6 and 3:**



➔ **Launch the IP Blue client (refer to the Demo instructions for details). You will need to change to the IP Blue directory and issue the "VTGO-PC.exe /d" command from a command prompt.**

➔ **You will register this phone as a 7960 IP Phone with a DN.**

➔ **Go into the phone administration page and configure the DN of each LINE.**

NOTE:

- The Partition of the LINE is dependent on any restrictions – the <None> of default partition (otherwise known as the Null Partition) can be used if you are not restricted from using the Default partition or there is no Calling Restriction between phones.

➔ **More information on the other settings are discussed in Section 2.**

Task 1.9

Start the telephony-service on BR2 router using the voice sub-interface as the source address. Register BR2 phones based on Table 7. Configure all lines such that two calls can be active per single DN.

➔ **Run the Telephony service wizard. Be careful to answer every question you are prompted to answer carefully otherwise you have to start again!**

```
P4-BR2-RTR(config)#telephony-service setup


 --- Cisco IOS Telephony Services Setup ---
```

➔ **As you have already configured DHCP skip that stage.**

```
Do you want to setup DHCP service for your IP Phones? [yes/no]: no

Do you want to start telephony-service setup? [yes/no]: yes
Configuring Cisco IOS Telephony Services:

 Enter the IP source address for Cisco IOS Telephony Services: 10.4.202.1
 Enter the Skinny Port for Cisco IOS Telephony Services:  [2000]:
 How many IP phones do you want to configure:  [0]: 2
 Do you want dual-line extensions assigned to phones? [yes/no]: yes
 What Language do you want on IP phones:
    0 English
    1 French
    2 German
    3 Russian
    4 Spanish
    5 Italian
    6 Dutch
    7 Norwegian
    8 Portuguese
    9 Danish
    10 Swedish
    11 Japanese
 [0]:
```

Which Call Progress tone set do you want on IP phones :
 0 United States
 1 France
 2 Germany
 3 Russia
 4 Spain
 5 Italy
 6 Netherlands
 7 Norway
 8 Portugal
 9 UK
 10 Denmark
 11 Switzerland
 12 Sweden
 13 Austria
 14 Canada
 15 Japan
[0]:

What is the first extension number you want to configure: 3001

➔ **For this particular Lab this is an optional step since PSTN is not required here. This is question has huge significance and will be covered in more detail later on.**

Do you have Direct-Inward-Dial service for all your phones? [yes/no]: yes
 Enter the full E.164 number for the first phone: 3313243001

Do you want to forward calls to a voice message service? [yes/no]: no
Do you wish to change any of the above information? [yes/no]: no

---- Setup completed config ---

➔ **Verify configuration once the wizard has completed adding the configuration.**

```
P4-BR2-RTR#sh run | b telephony-service
telephony-service
 max-ephones 2
 max-dn 2
 ip source-address 10.4.202.1 port 2000
 auto assign 1 to 2
 create cnf-files version-stamp Jan 01 2002 00:00:00
 dialplan-pattern 1 3313243... extension-length 4
 transfer-system full-consult

P2-BR2-RTR#sh ephone summ

ephone-1 Mac:0011.BBE0.5775 TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
IP:10.2.202.51 Telecaster 7940  keepalive 6387  1:1

ephone-2 Mac:0011.BBEF.6901 TCP socket:[2] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
IP:10.2.202.52 Telecaster 7940  keepalive 6381  1:2
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 2: Call Manager Fundamentals

Estimated Time to Complete: 3 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 2 Call Manager Fundamentals

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

Use a Remote Desktop Protocol (RDP) client for access to Call Manager.

To complete this lab the infrastructure and Call Manager sections in Section 1 must be performed.

The devices which are plugged into the actual switches in the POD are there to test that the Infrastructure and QoS Section are configured correctly. The devices will auto-answer after 5 seconds and you should be able to hear a recorded message. To test dial plan we recommend you bring up Cisco IP Communicator and multiple instances of IP Blue. The PSTN phone is a 7960 attached to a Catalyst switch that you do not have access to – however it will ring and auto-answer when called properly out of your gateways.

Section 2 Configuration Tasks

Task 2.1

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **From System-Region rename the Default Region to HQ and create another Region called BR1, and one called BR2 (you will use this later for an H323 BR2 ICT to CME as well as for your GK configuration). Codec within Regions should be set to G711 and between Regions should be set to G729.**

➔ **See this snippet below for what Cisco briefly points out are supported speeds on a Cisco VTA (Video Telephony Advantage) camera:**

Supported Video Codecs on Cisco VT Advantage

These video codecs are supported in Cisco VT Advantage.

- H.263 (128 Kbps - 1.5 Mbps)
- Cisco VT Camera wideband video codec (7 Mbps)

➔ **Also see this snippet below for a much expanded view detailing Video and Audio codec breakouts:**

Call Speed	Audio Codec and Rate	Video Codec and Rate
128 kbps	G.711 at 64 kbps	H.261, H.263, or H.264 at 64 kbps
128 kbps	G.728 at 16 kbps	H.261, H.263, or H.264 at 112 kbps
128 kbps	G.729 at 8 kbps	H.261, H.263, or H.264 at 120 kbps
384 kbps	G.711 or G.722 at 64 kbps	H.261, H.263, or H.264 at 320 kbps
384 kbps	G.729 at 8 kbps	H.261, H.263, or H.264 at 376 kbps
768 kbps	G.711 or G.722 at 64 kbps	H.261, H.263, or H.264 at 704 kbps
768 kbps	G.729 at 8 kbps	H.261, H.263, or H.264 at 760 kbps
1.5 Mbps (1.472 Mbps)	G.711 or G.722 at 64 kbps	H.261, H.263, or H.264 at 1.408 Mbps
1.5 Mbps (1.472 Mbps)	G.729 at 8 kbps	H.261, H.263, or H.264 at 1.464 Mbps
2.048 Mbps	G.711 or G.722 at 64 kbps	H.264 at 1.984 Mbps
2.048 Mbps	G.729 at 8 kbps	H.264 at 2.040 Mbps
7 Mbps	G.711 at 64 kbps	Cisco VT Advantage Wideband at approximately 7 Mbps
7 Mbps	G.729 at 8 kbps	Cisco VT Advantage Wideband at approximately 7 Mbps

Region Configuration

Add a New Region
Back to Find/List Regions
Dependency Records

Region: HQ
Status: Ready

Update | Delete | Restart Devices

Region Information

Region Name* HQ

Call Information

The maximum audio codec/video bandwidth supported within this region and between 2 other regions are:

Region	Audio Codec	Video Call Bandwidth
BR1	G.729	None ⦿ 128 kbps
BR2	G.729	None ⦿ 128 kbps
HQ (Within this Region)	G.711	None ⦿ 7168 kbps

Items per page 10 First Previous Next Last Page 1 of 1

➔ **Rename the Default Device Pool to HQ and create another Device Pool called BR1, and one called BR2. Assign the appropriate Region to each.**

Find and List Device Pools

Add a New Device Pool

3 matching record(s) for Device Pool Name begins with ""

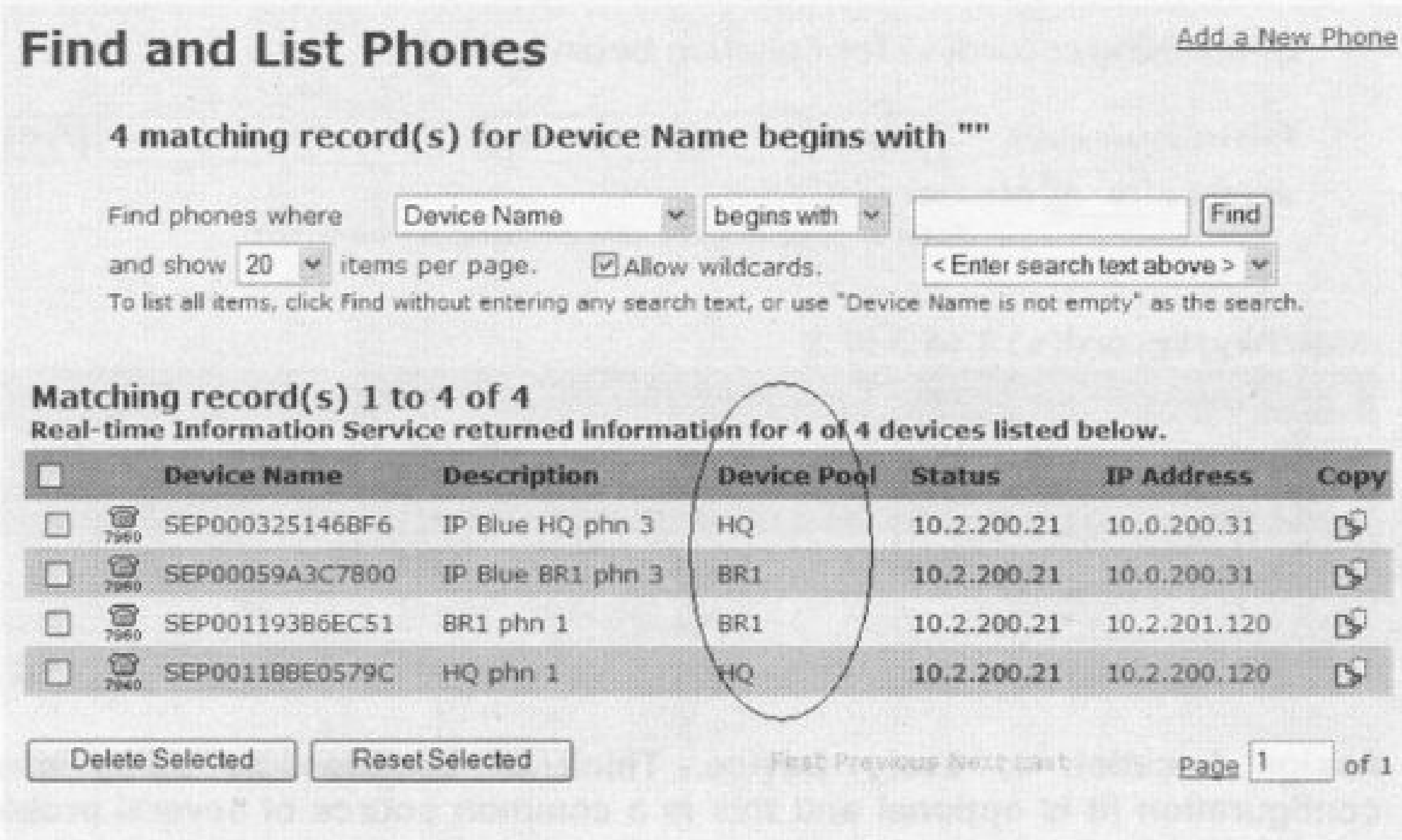
Find Device Pools where Device Pool Name begins with Find
and show 20 items per page
To list all items, click Find without entering any search text.

Matching record(s) 1 to 3 of 3

	Device Pool Name	Call Manager Group	Region	Date/Time Group	Copy
	BR1	Pod1-Primary	BR1	CMLocal	
	BR2	Pod1-Primary	BR2	CMLocal	
	HQ	Pod1-Primary	HQ	CMLocal	

Delete Selected First Previous Next Last Page 1 of 1

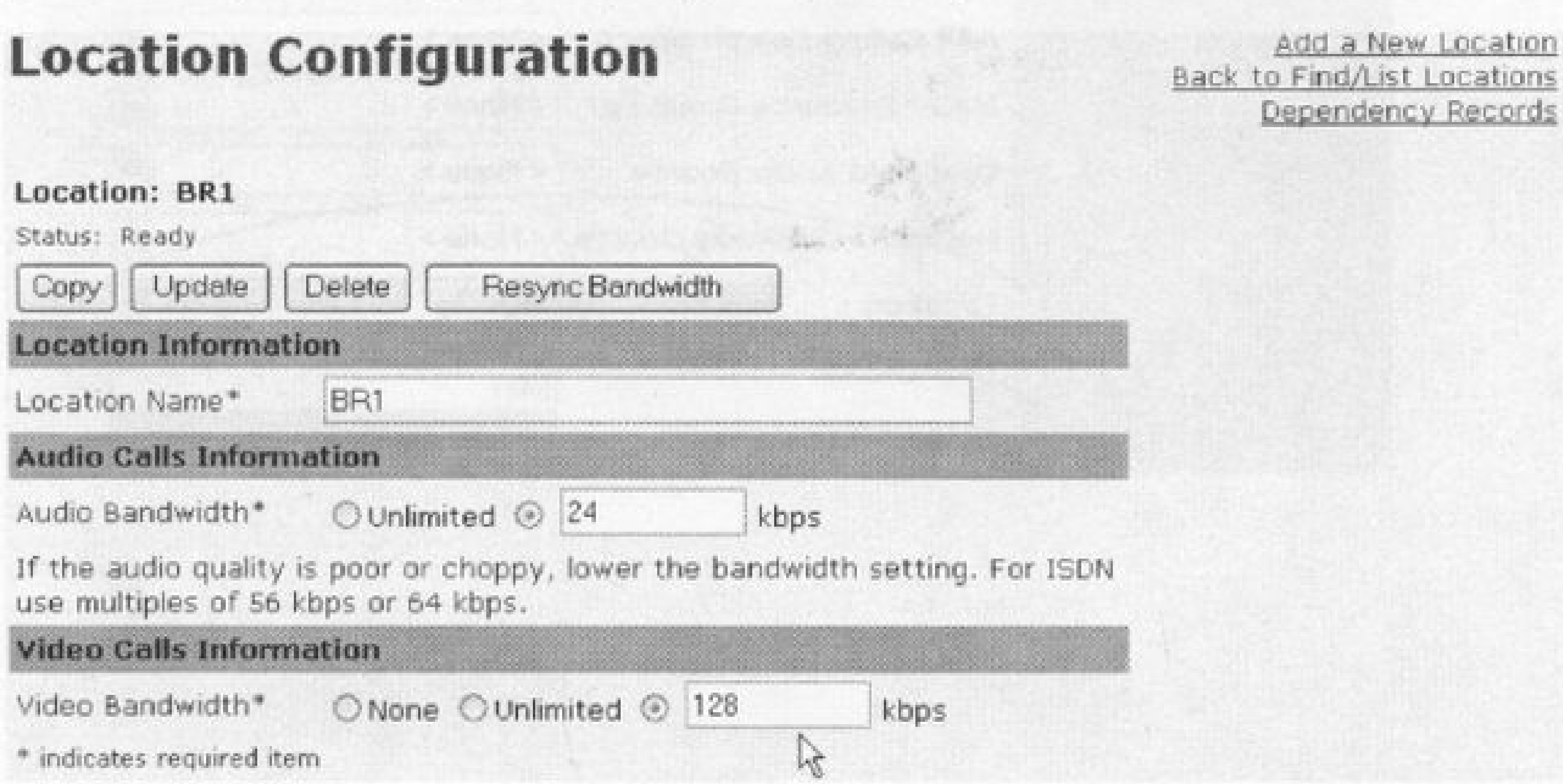
➔ **Assign the correct Device Pool to the appropriate Device.**

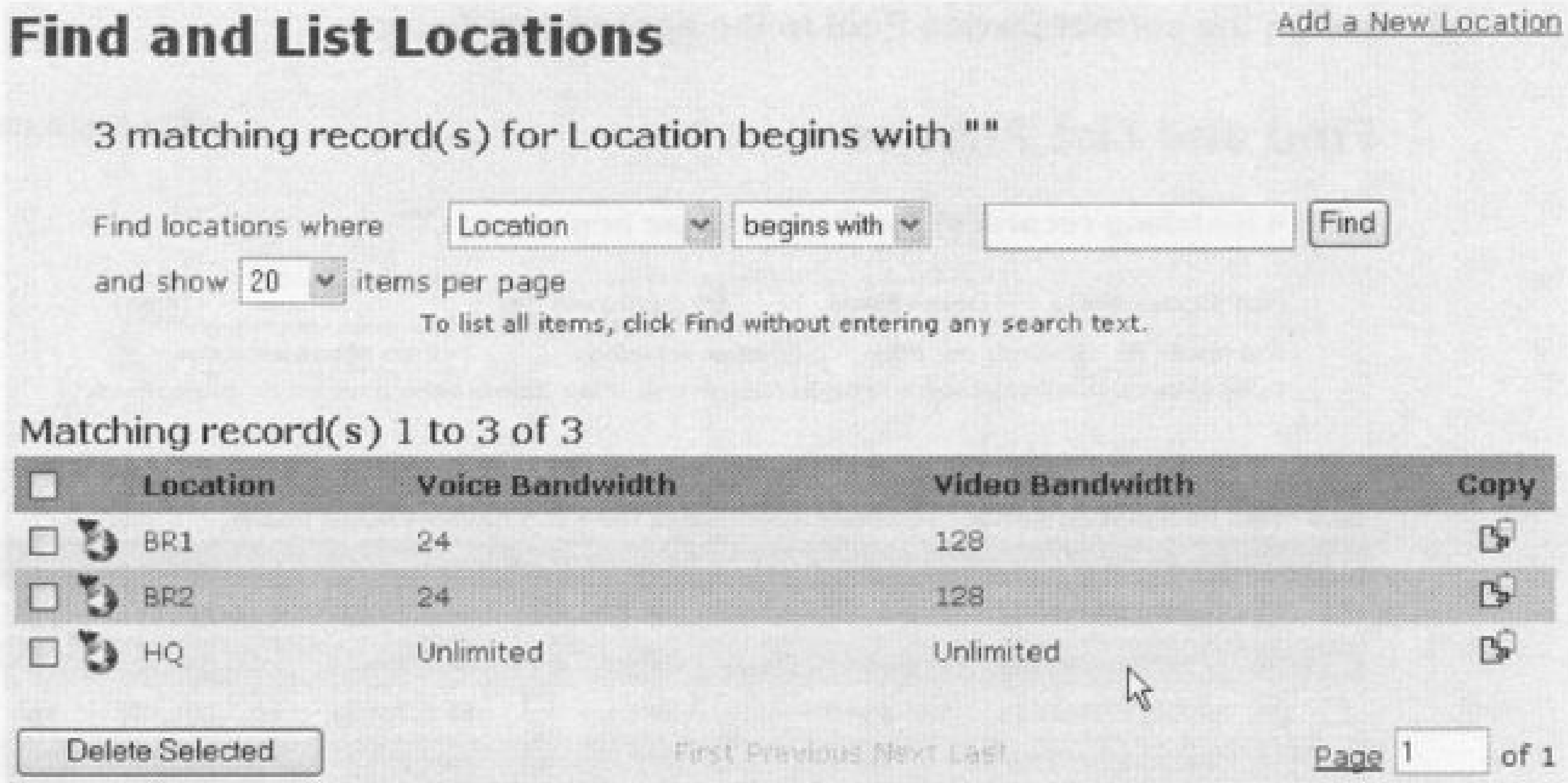


Task 2.2

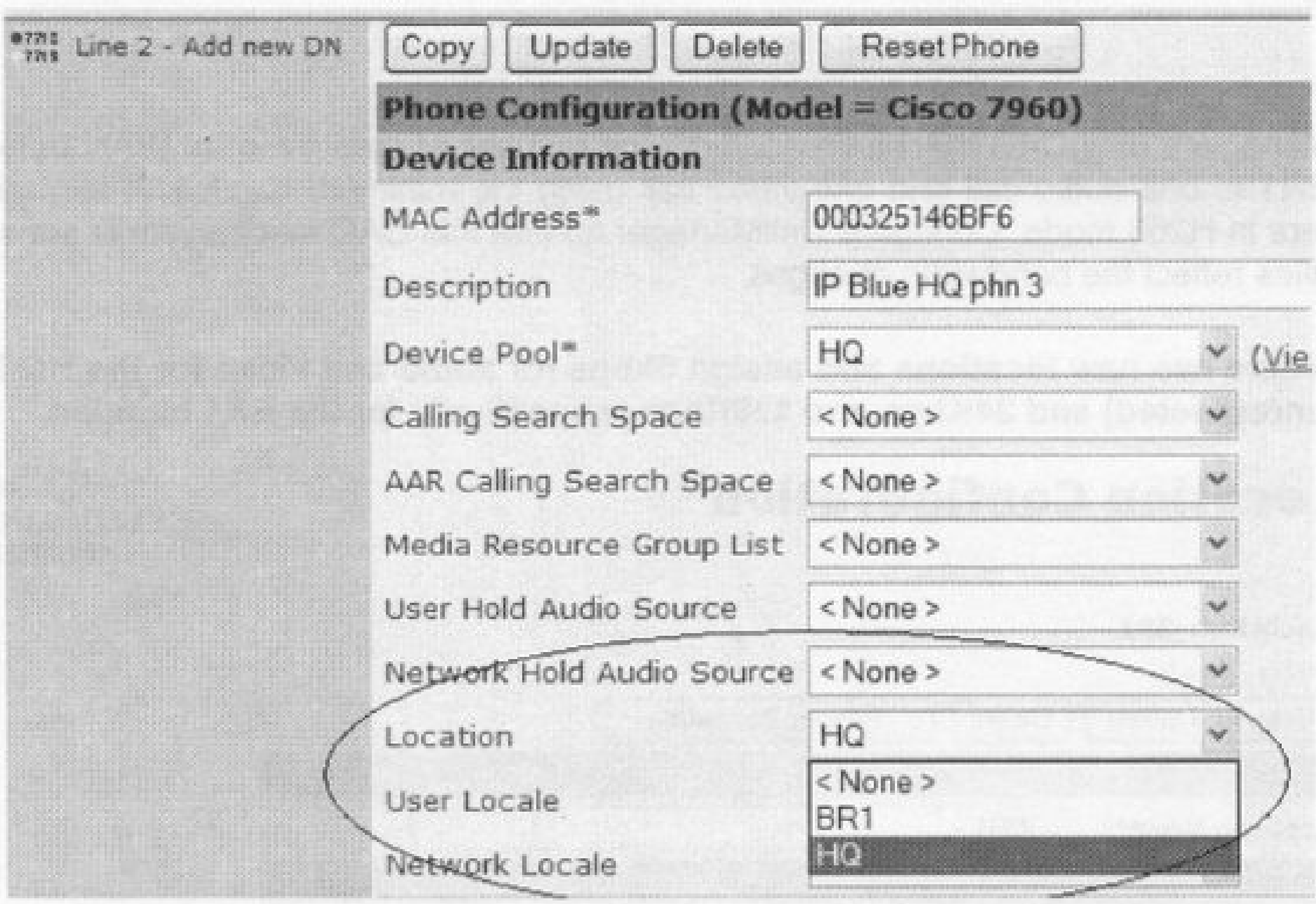
Use CallManager's only CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **Create two new locations and assign 0kbps for audio and video for the HQ location (unrestricted) and 24Kbps and 128Kbps respectively for the BR1 location.**





➔ **Assign Location to every Device. Think of Location as being mandatory configuration (it is optional and this is a common source of several problems for candidates).**



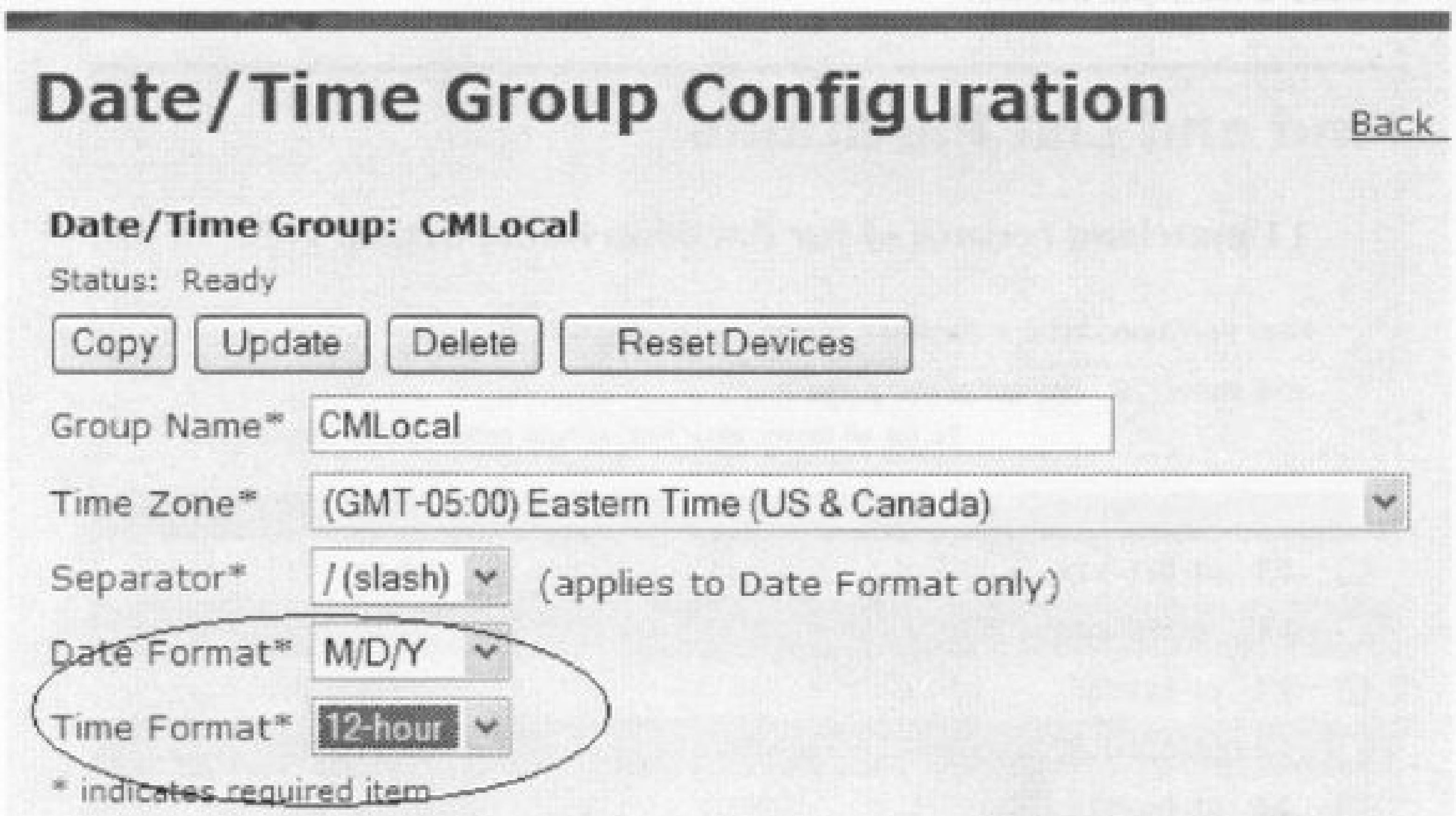
➔ **Enable Detailed Locations Tracing by changing the CCM Service Parameter.**

Clusterwide Parameters (System - Location and Region)		
Parameter Name	**Parameter Value**	**Suggested Value**
Enforce Millisecond Packet Size*	True	True
Locations Initialization Timer (sec)*	90	90
Locations Trace Details Enabled*	True	False

Task 2.3

Change the display on the HQ and BR1 phones so that the clock is using 12-hour format.

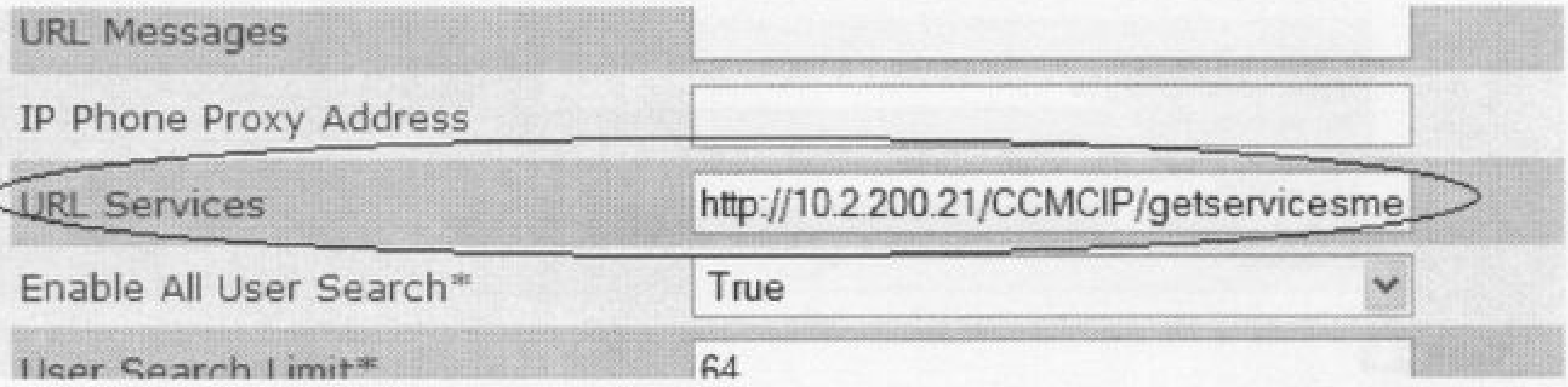
➔ **In Date/Time Group Configuration change the clock to 12-hour display. Verify settings on the IP Communicator.**



Task 2.4

Ensure that when a user presses the 'Services' or 'Directories' button the error message is not displayed.

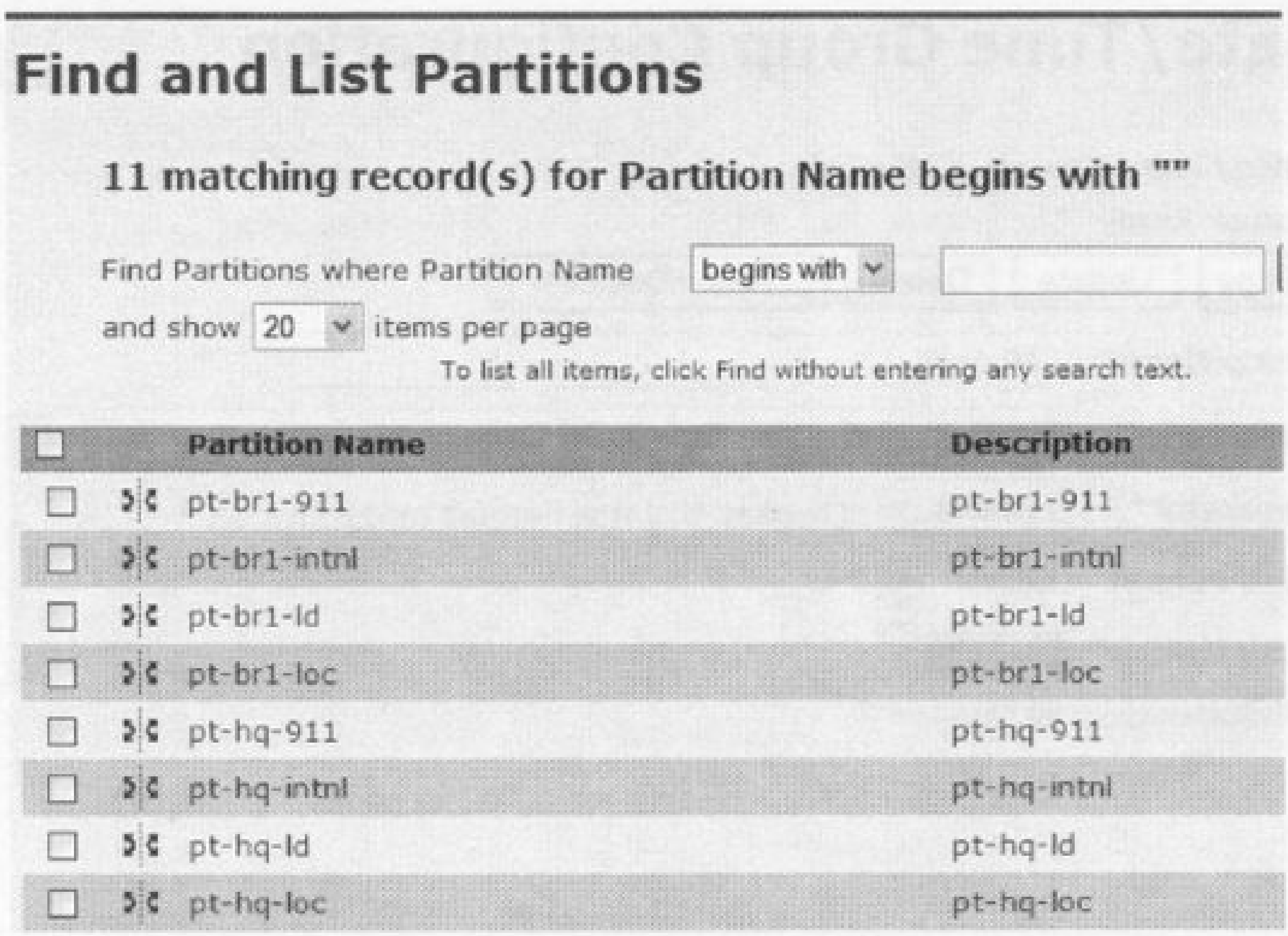
➔ **Change Enterprise Parameters and place IP Address in the Services URL and verify by pressing "Services" button on IP Communicator.**



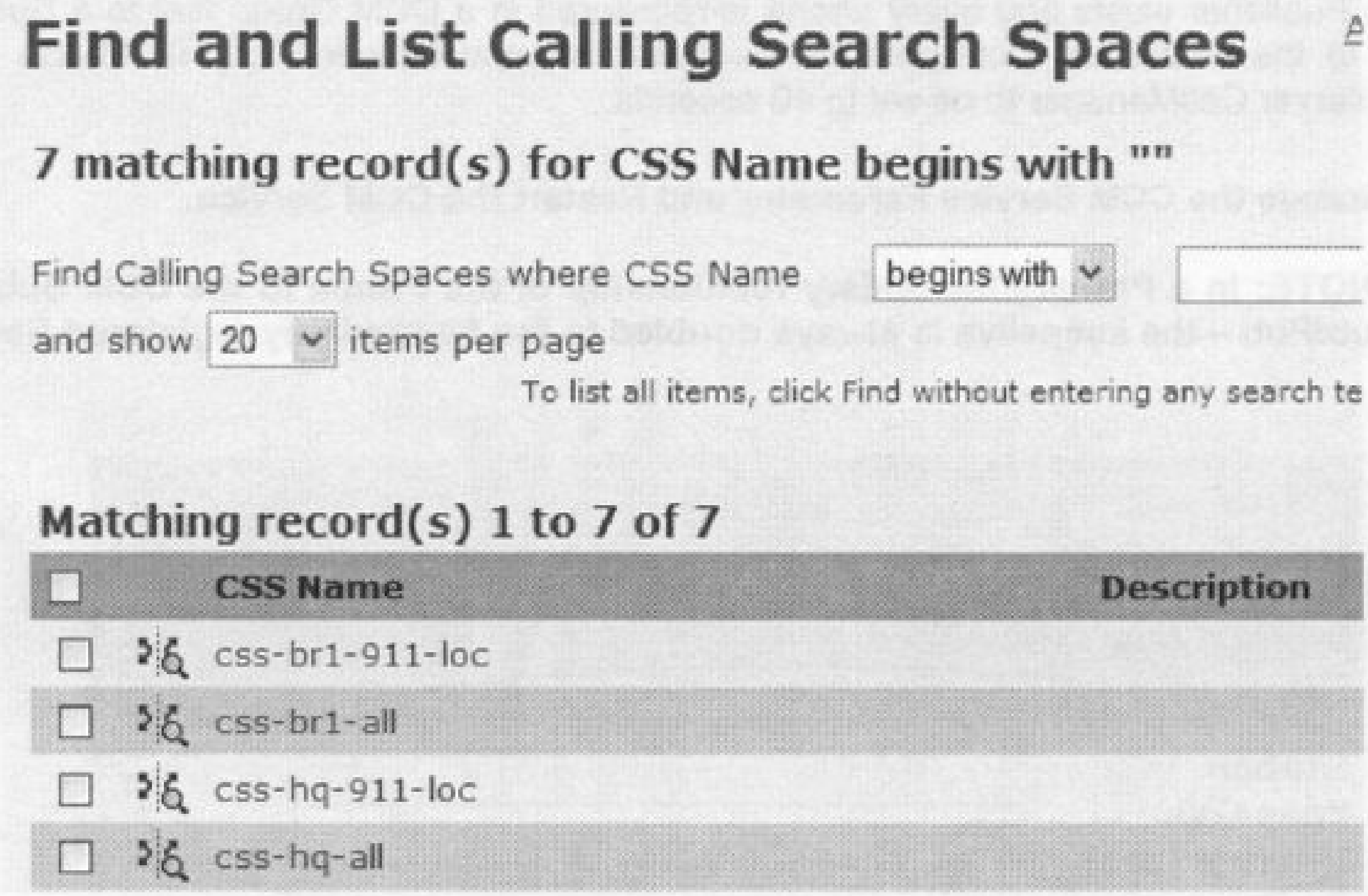
Task 2.5

Configure Calling Restriction based on Table 1.

➔ **Create 8 new partitions.**



➔ **Create 4 new CSS and assign relevant partitions into each partition.**



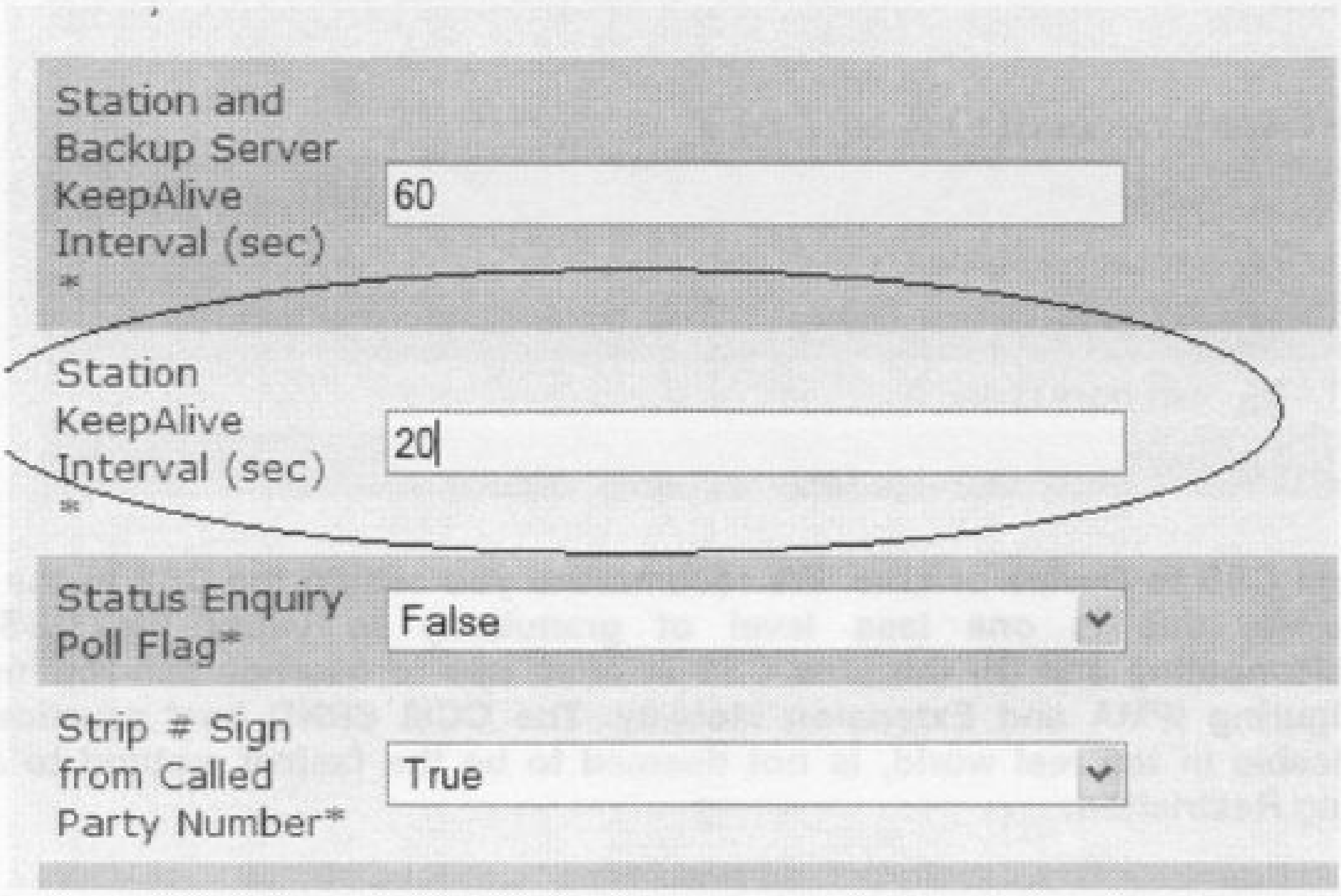
➔ **Assign CSS to Device or Line. We recommend you assign the CSS to the Device since (a) this is one less level of granularity to verify the CSS when troubleshooting and (b) the Line CSS is often use to override call routing when configuring IPMA and Extension Mobility. The CCM SRND best practice, while applicable in the real world, is not deemed to be the fastest method to achieve Calling Restriction.**

Task 2.6

Assume a Publisher exists and every phone is registered in a CCM Group first to a Subscriber, and then to the Publisher. Configure the keepalive interval between any IP Phone and the Publisher server CallManager to be set to 40 seconds.

➔ **Change the CCM Service Parameter and Restart the CCM Service.**

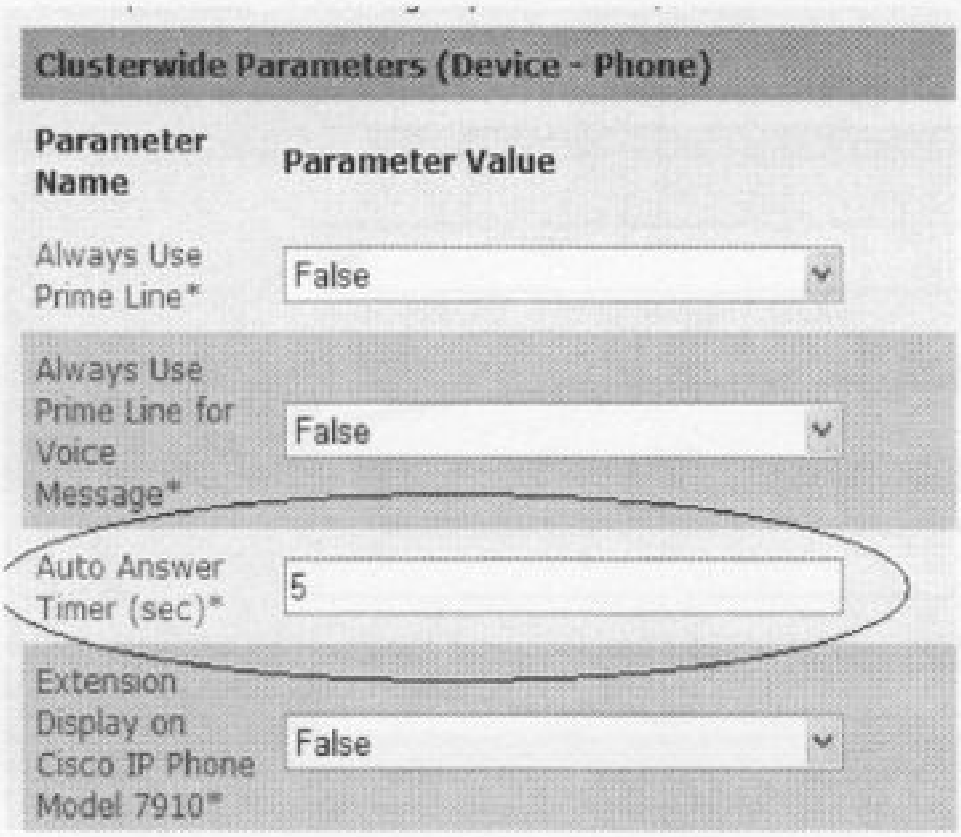
➔ **(NOTE: In a Primary/Secondary relationship of the Phone to the CCM Sub/Sub or Sub/Pub – the keepalive is always doubled to the Secondarily registered Server)**

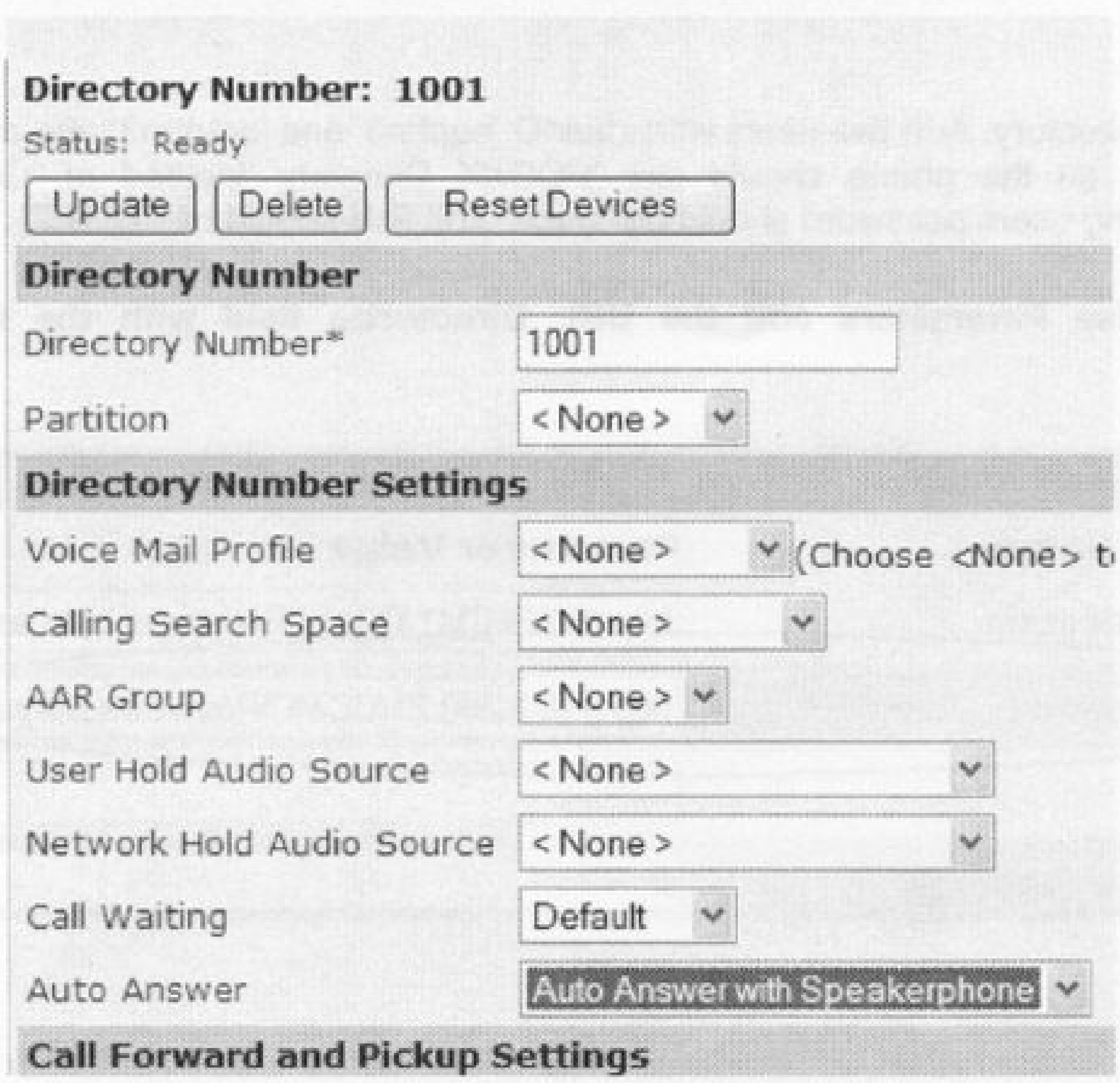


Task 2.7

Set the phones that reside in the POD (all 79XX not physically accessible to you) to auto-answer. Phones must only auto-answer after 5 seconds.

➔ **Change the CCM Service Parameter and Restart the CCM Service. Test by calling the phones in your POD and verify auto-answer is no longer immediate.**





Task 2.8

Configure Call Manager so that the Inter-digit timeout is 10 seconds.

➔ **Change the CCM Service Parameter and Restart the CCM Service.**

Interval (sec) *	
Status Enquiry Poll Flag*	False
Strip # Sign from Called Party Number*	True
T301 Timer (msec)*	180000
T302 Timer (msec)*	10000
T303 Timer (msec)*	4000
T304 Timer	

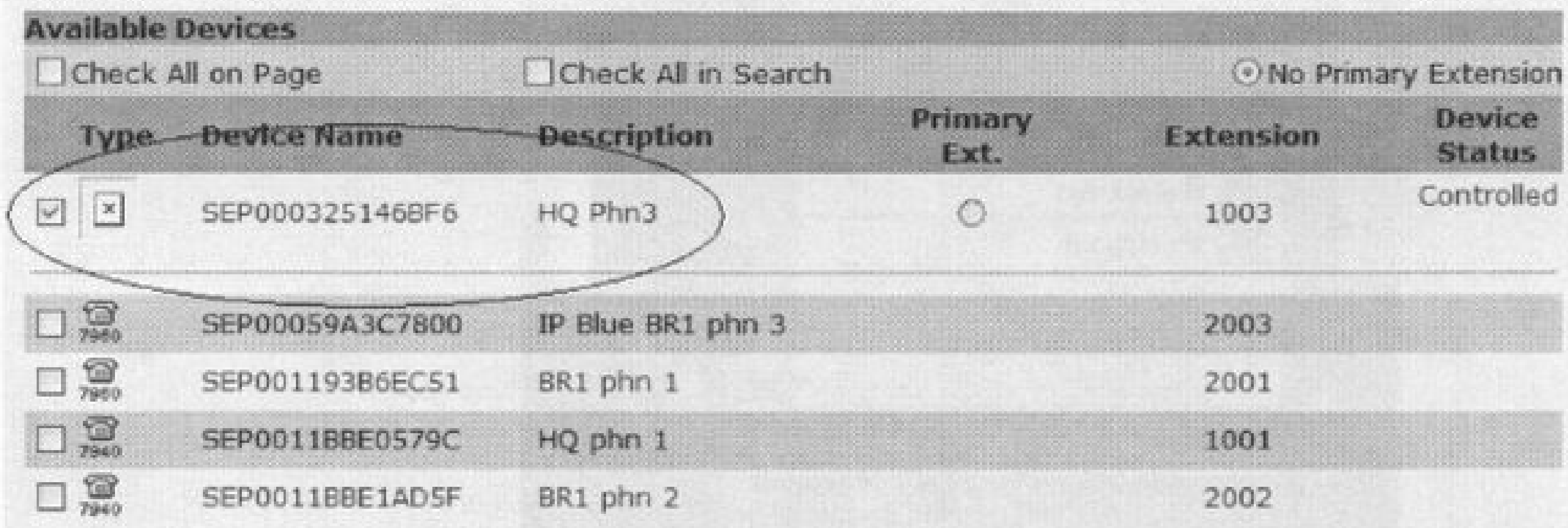
Task 2.9

Enable the Corporate Directory. Add two users with UserID 'hqphn3' and 'br1phn3' and associate relevant devices. Text on the phone should say 'PODXX Directory' instead of 'Corporate Directory'. [When creating users password should be "cisco" and PIN should be "12345"].

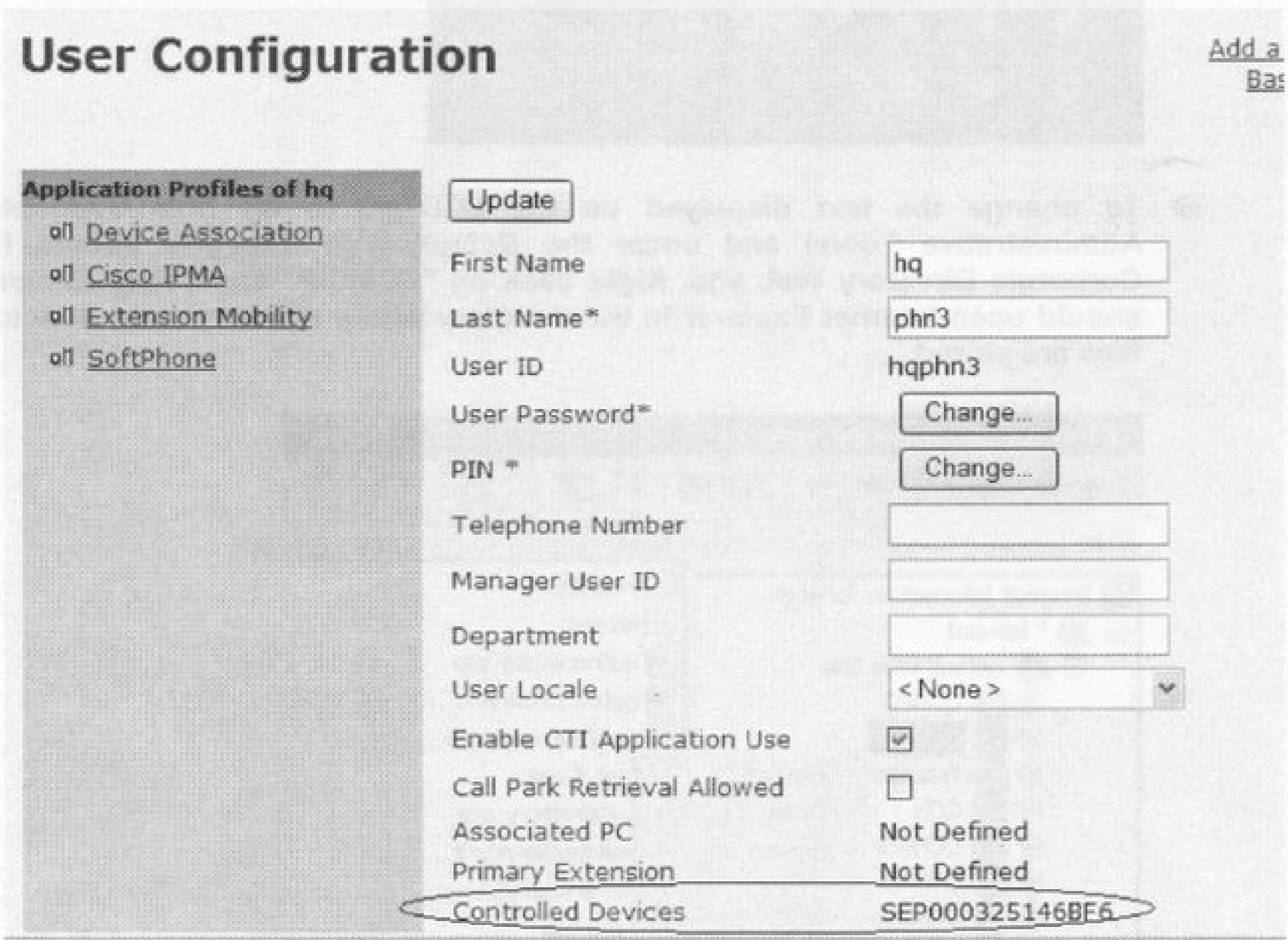
➔ **From Enterprise Parameters edit the URL Directories field with the CCM IP Address.**

Phone URL Parameters	
Parameter Name	**Parameter Value**
URL Authentication	http://LAB-CM1/CCMCIP/authenticate.asp
URL Directories	http://10.2.200.21/CCMCIP/xmldirectory.as
URL Idle	
URL Idle Time (sec)	0

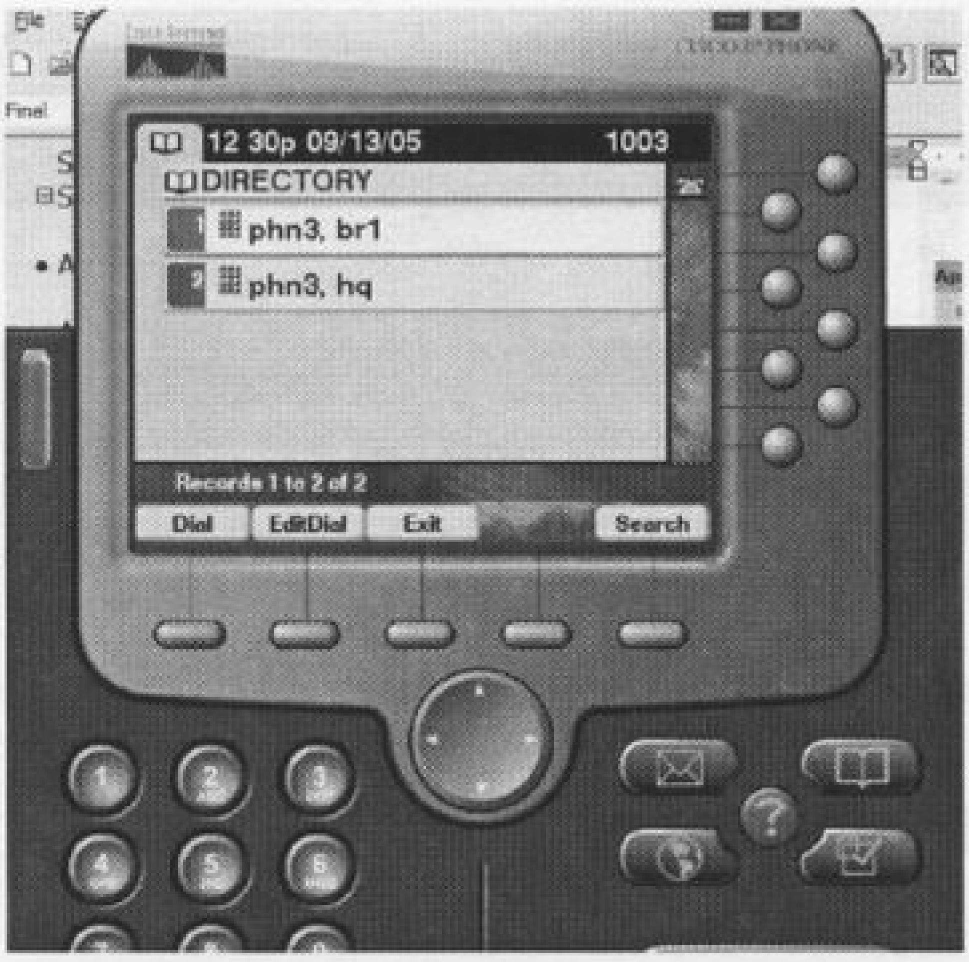
➔ **Add a User and Associate the appropriate Device. No Primary Extension checkbox should be marked.**



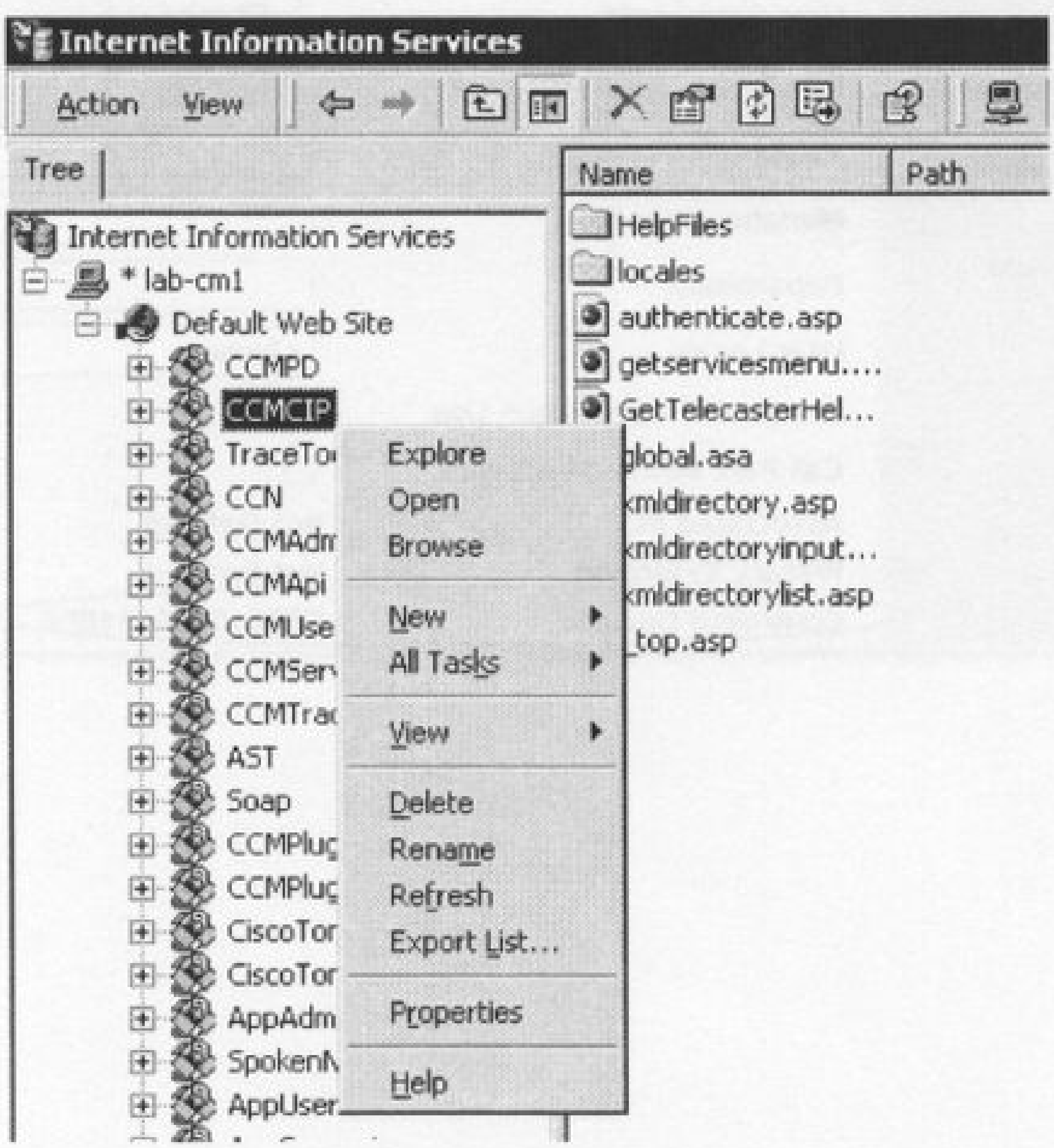
➔ **Verify that the user page is showing the controlled device.**



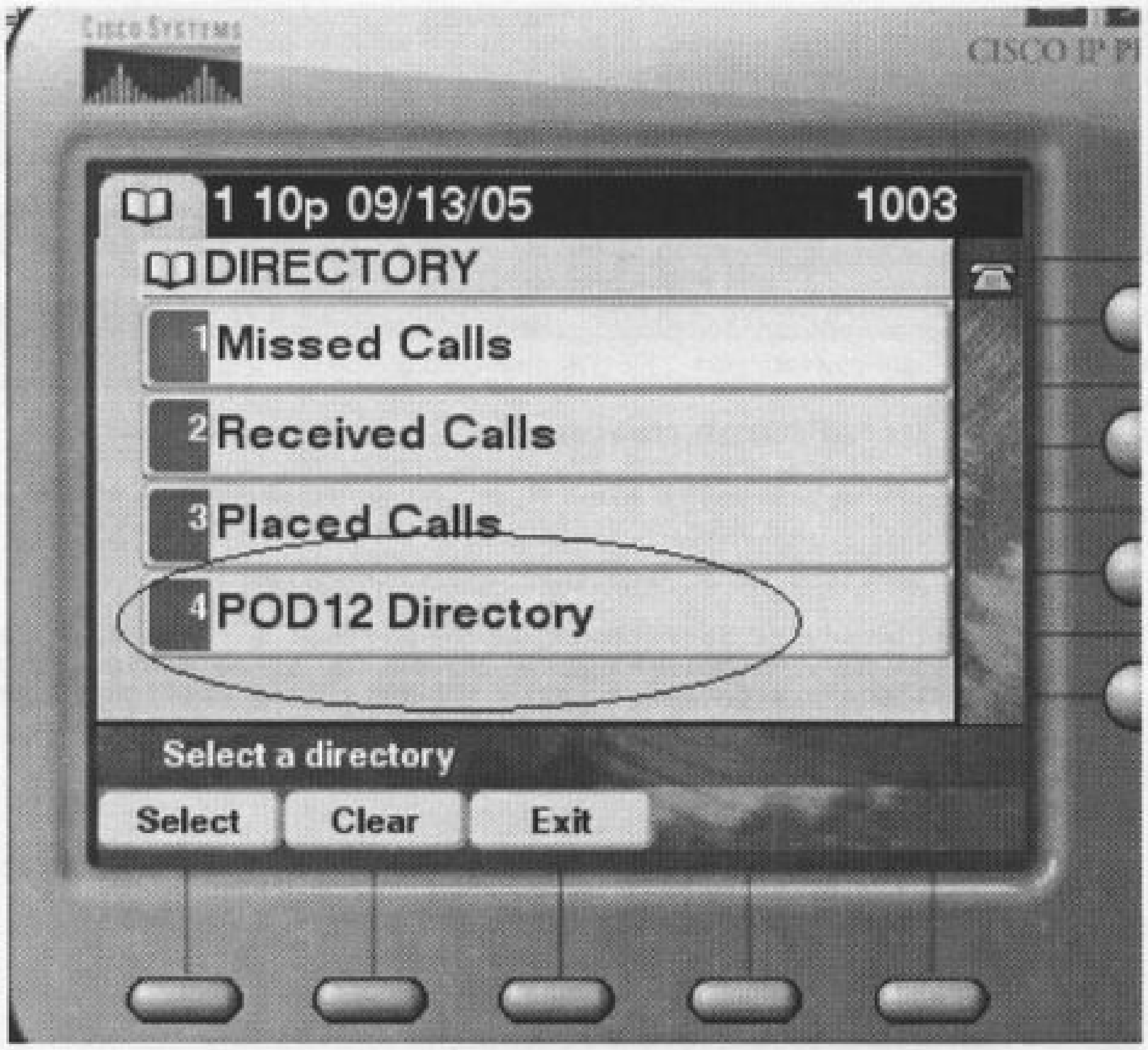
➔ **Either using the IP Blue client or IP Communicator search on Corporate Directory and check the users you have added earlier are displayed.**



➔ **To change the text displayed on the LCD go to IIS (Start-Program Files-Administrative Tools) and under the Default Web Site you should find the Corporate Directory Web site. Right click on "CCMCIP" and select Explore - this should open Internet Explorer in the directory where the Corporate Directory ASP files are stored.**



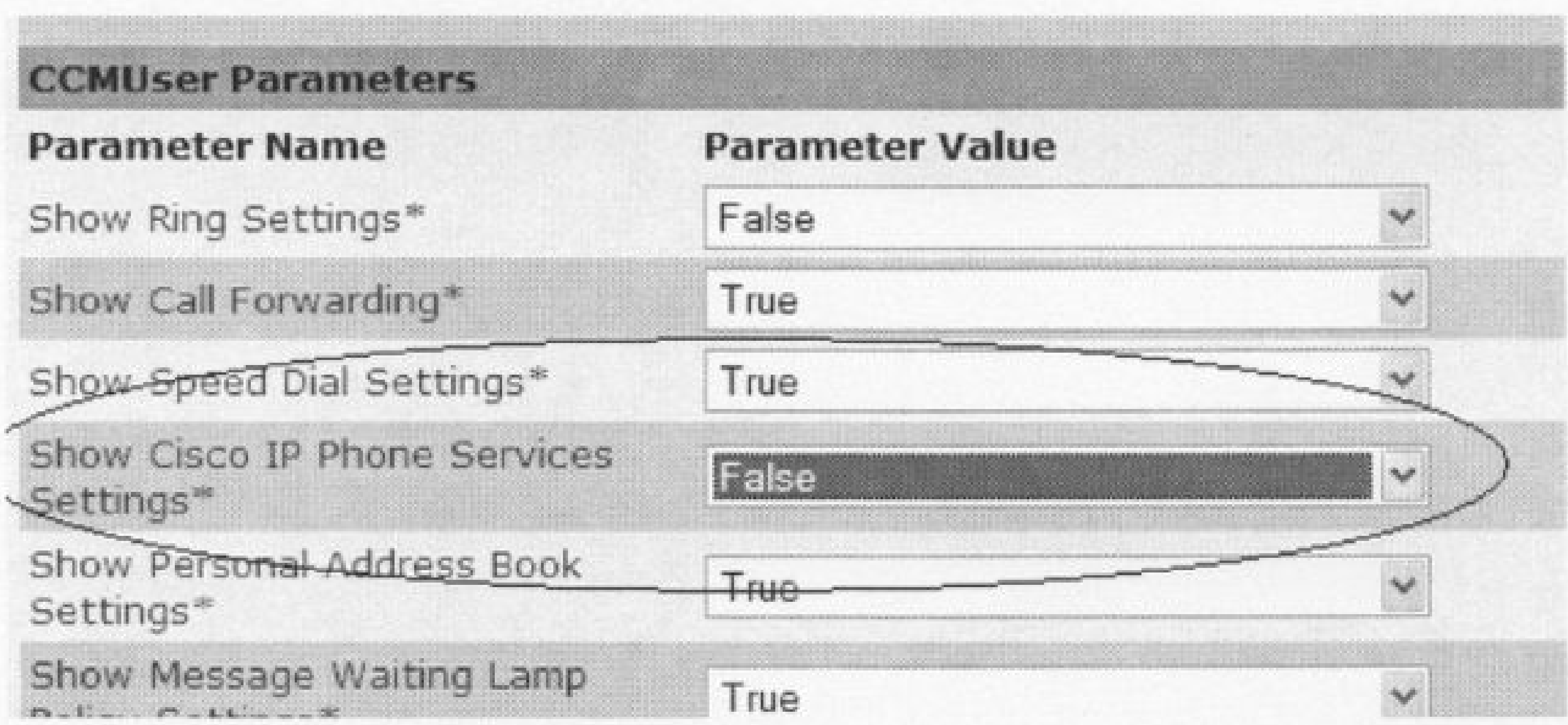
➔ **Verify the text has changed by pressing the Directory button on IP Communicator.**



Task 2.10

Configure Call Manager such that users logging into CCMUSER web page should **not** be able to subscribe or configure IP Phone Services.

➔ **Change the following Enterprise Parameter.**

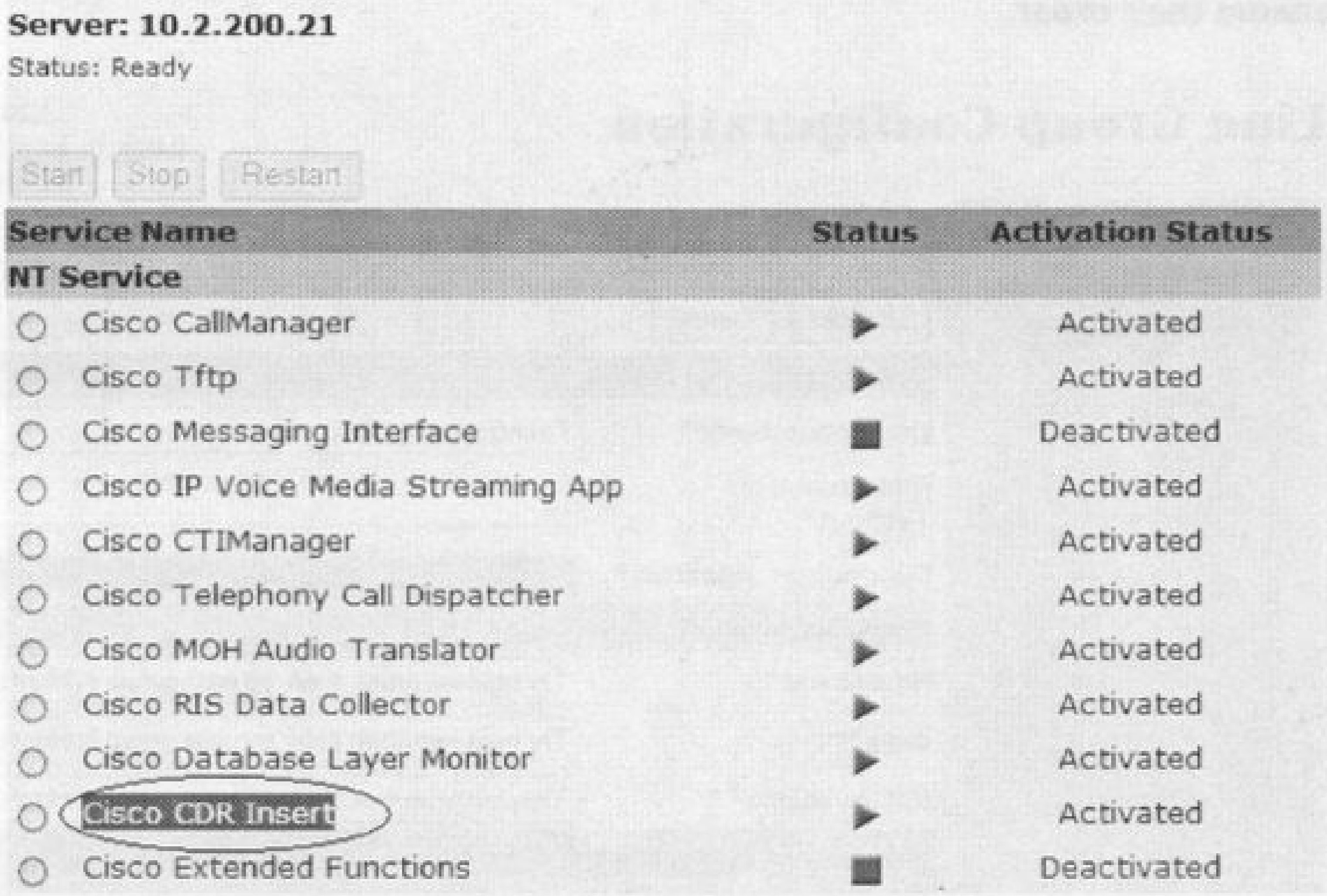


CCMUser Parameters	
Parameter Name	**Parameter Value**
Show Ring Settings*	False
Show Call Forwarding*	True
Show Speed Dial Settings*	True
Show Cisco IP Phone Services Settings*	False
Show Personal Address Book Settings*	True
Show Message Waiting Lamp	True

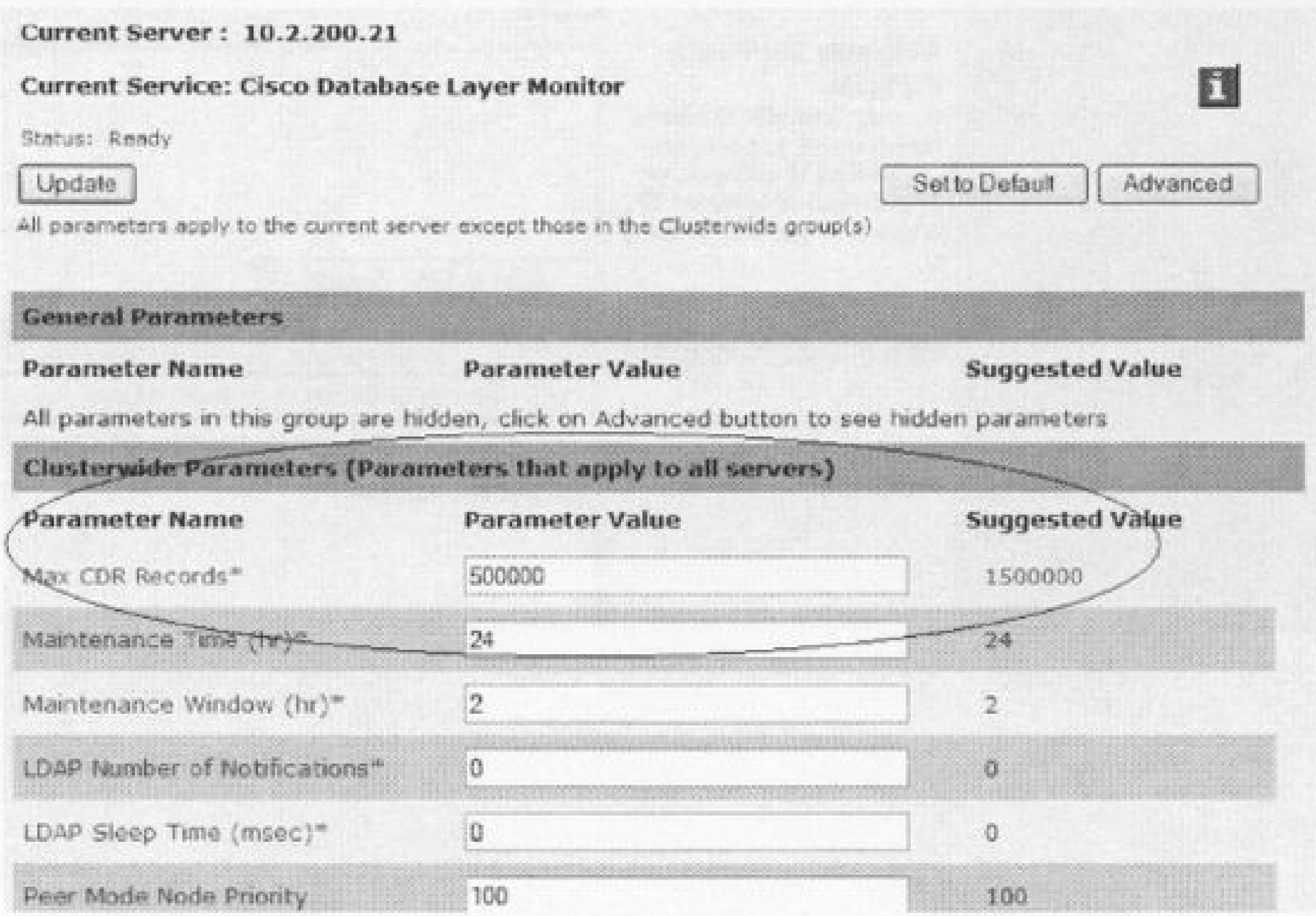
Task 2.11

Configure Call Manager so that CDRs are created for all connected calls. Ensure only calls that are answered create a CDR. Only a maximum of 500 000 CDRs should be held in the database.

➔ **Ensure that the CDR Insert Service is activated from Call Manager Serviceability.**



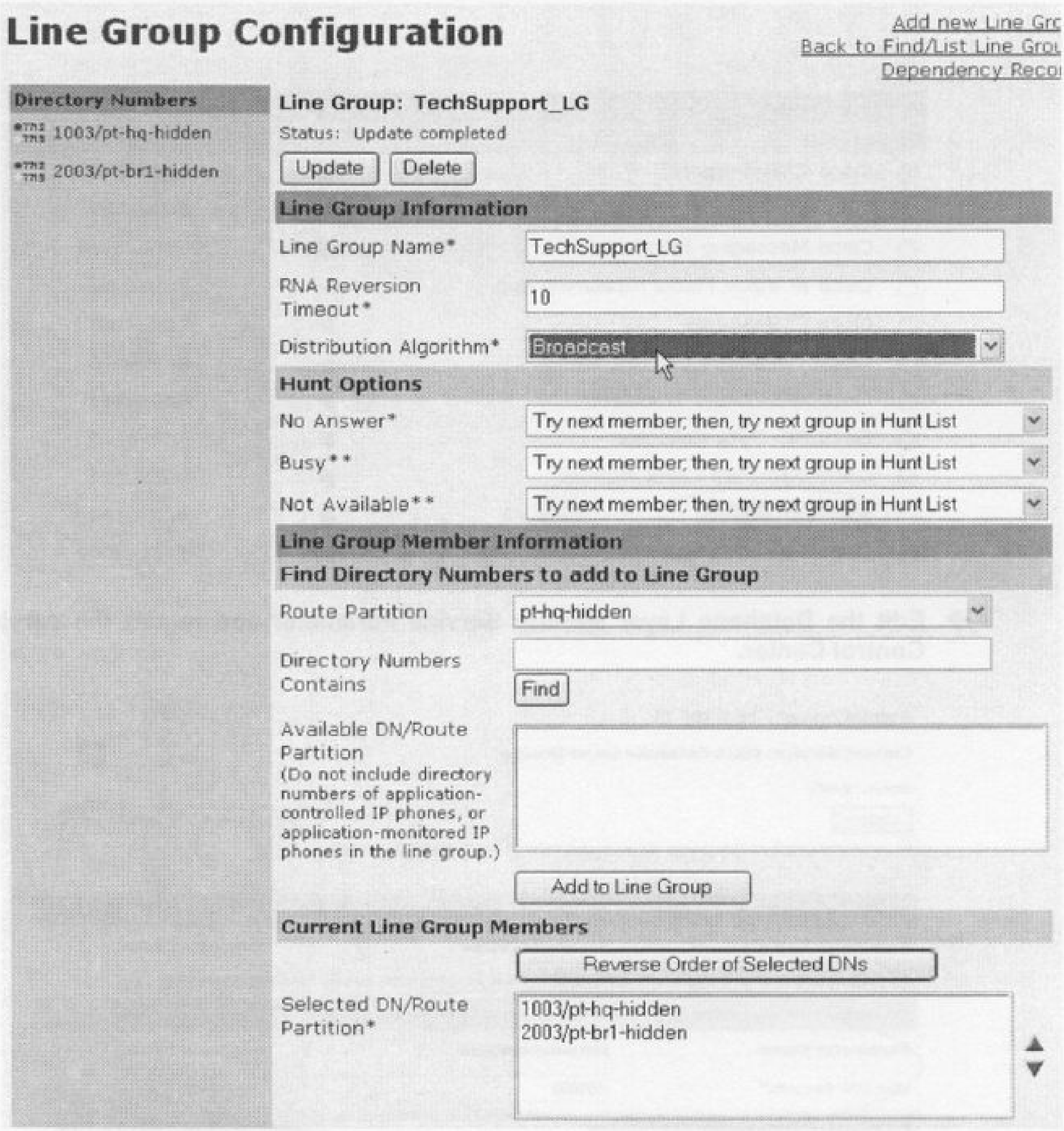
➔ **Edit the Database Layer Monitor Service Parameter and restart the service from Control Center.**



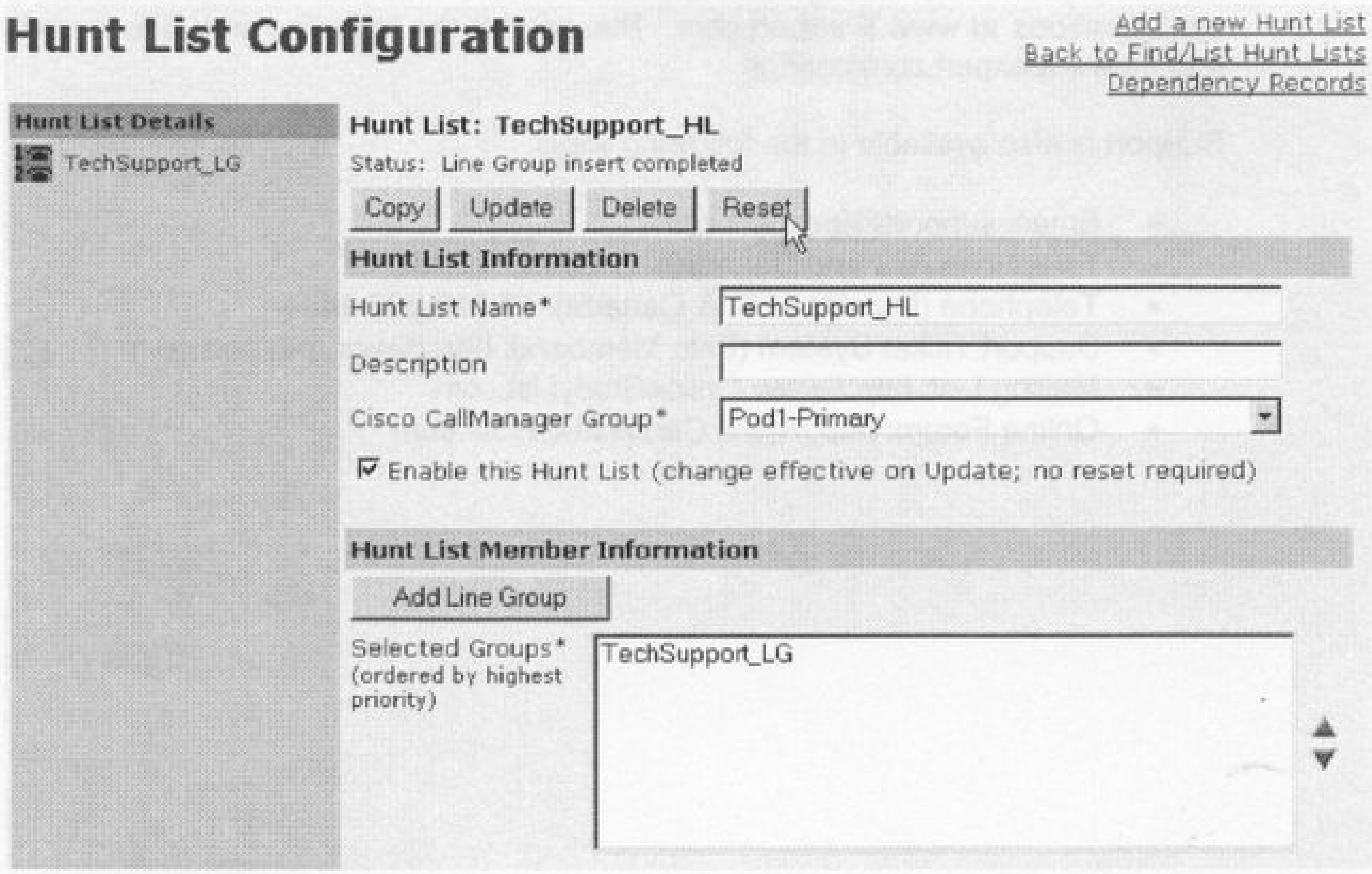
Task 2.12

Create a DN of 1005 for Tech Support. Make HQ phone 3 and BR1 Phone 3 ring simultaneously when this DN is called. You may not use a shared line to accomplish this task.

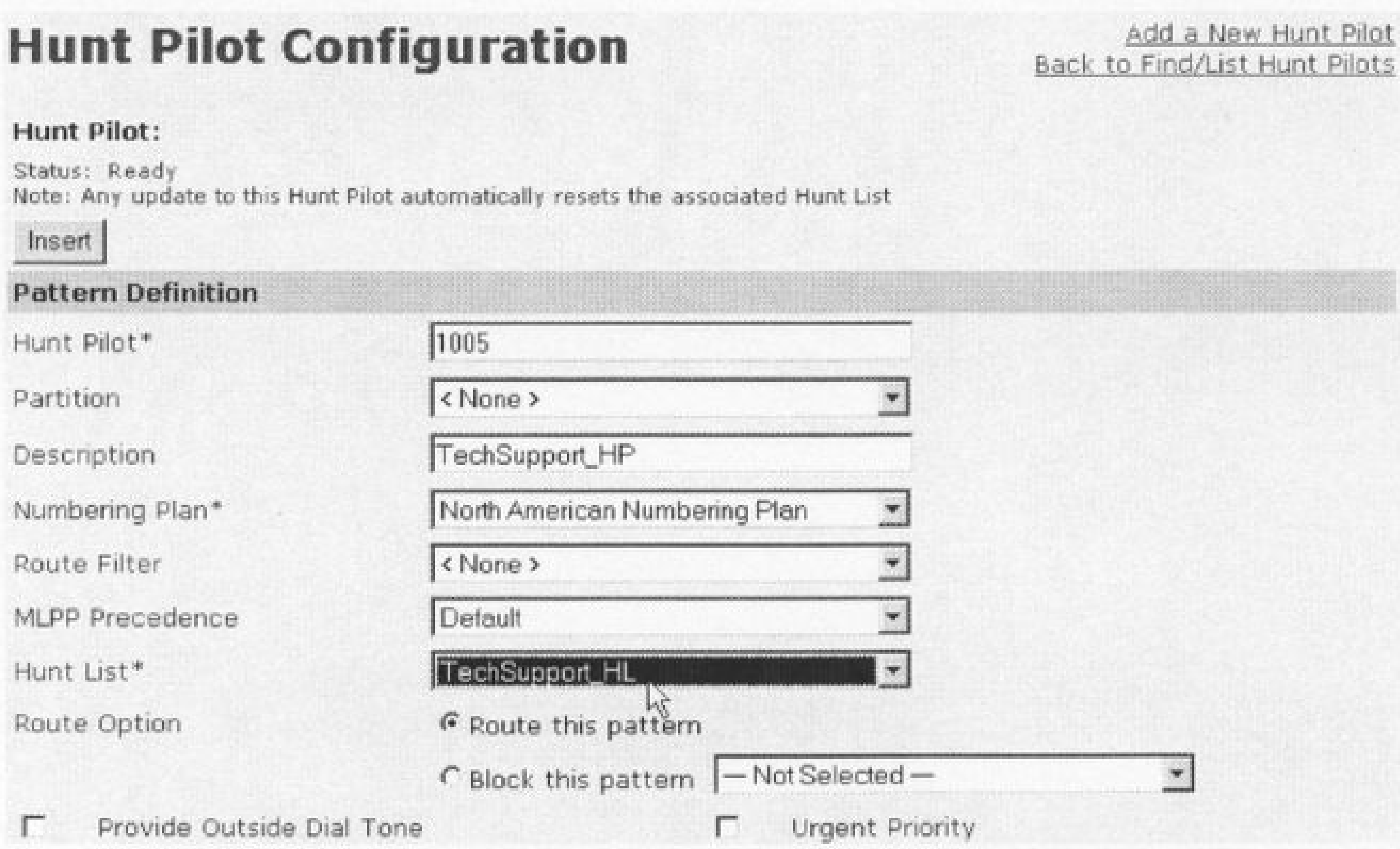
➔ **Add a new Line Group called TechSupport_LG, ensure that it follows a Top Down Distribution Algorithm, and include the DNs 1001, 1002, and 1003 as members and ensure their order.**



➔ **Add a new Hunt List called TechSupport_HL, add the Line Group you just created, and be sure to reset the Hunt List once you've inserted it.**



➔ **Create a Hunt Pilot with the DN of 1005 and make sure that it points to ring the Hunt List you just created.**



Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 3: CME Fundamentals

Estimated Time to Complete: 3 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 3 CME Fundamentals

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure and CME sections in Section 1 must be performed.

The devices which are plugged into the actual switches in the POD are there to test that the Infrastructure and QoS Section are configured correctly. The devices will auto-answer after 5 seconds and you should be able to hear a recorded message. To test dial plan we recommend you bring up Cisco IP Communicator and multiple instances of IP Blue. The PSTN phone is a 7960 attached to the Catalyst 6000.

Section 3 Configuration Tasks

Task 3.1

Create a shared line on the BR2 phones 1 and 3 with DN 3010. The first call coming into the shared line must ring both phones. When a second call comes into the shared line (while the first call to the shared line is still connected) the unused phone that has the shared line must ring **while at the same time** displaying 'call waiting' on the first phone. Ensure that the shared lines have the second media channel enabled.

- ➔ **Use the CME telephony-service setup wizard. For the shared line manually add the ephones. Given the choice ephone-DNs should be configured as dual-lines to replicate the CCM devices.**

- ➔ **A note about dual-lines - An ephone configured with a single-line ephone-dn does NOT have an option to see call waiting, use consultative transfer or have a second call using that particular line or ephone-dn. This is because each line or ephone-dn requires the second "channel" to be enabled – this is configured using dual-line on the ephone-dn. By default the second channel is enabled on Call Manager phones.**

- ➔ **When the ephone-DNs are configured as dual-lines, a second concurrent call into a shared line will hunt on the second channel resulting in Caller ID being displayed on the phone involved in the first call. When an ephone-dn is configured as a shared line the device assigned the unused instance of the shared line is dormant if we use the Overlay component. However if we use the new Call-Waiting for Overlaid lines, we can accomplish all that we wish. This is done using a 'c' between the button number and the ephone-dn we wish to assign.**

```
ephone-dn 1 dual-line
 number 3001
!
ephone-dn 2 dual-line
 number 3003
!
ephone-dn 3 dual-line
 number 3010
 huntstop channel
 no huntstop
```



```
!
ephone-dn 4 dual-line
 number 3010
 preference 1
 huntstop channel
!
ephone 1
 mac-address 0011.BBEF.6901
 type 7940
 button 1:1 2c3,4
!
ephone 2
 mac-address 0011.BBE0.5775
 type 7940
 button 1:2 2c3,4
```

Task 3.2

Configure Class of Restriction (COR) based on Table 1.

➔ **Configuration is done using the steps below - we shall use the same terminology as Call Manager uses to implement Calling Restriction, namely Calling Search Spaces (CSS) and Partitions.**

➔ **First configure dial-peer cor custom and assign a meaningful name that specifies the way CORs apply to dial-peers - this is in effect defining the list of partitions.**

```
dial-peer cor custom
 name pt-911
 name pt-loc
 name pt-ld
 name pt-internl
```

➔ **Create the actual lists of the restrictions that apply to the dial-peer - this is the equivalent of CSS the difference between COR and Call Manager CSS/Partitions is that we apply CSS to the incoming AND outgoing leg of the call whereas in CCM CSS is applied to the incoming call leg only.**

```
dial-peer cor list css-911
 member pt-911
!
dial-peer cor list css-loc
 member pt-loc
!
dial-peer cor list css-ld
 member pt-ld
!
dial-peer cor list css-intnl
 member pt-internl
```



```
!
dial-peer cor list css-911-loc
 member pt-911
 member pt-loc
!
dial-peer cor list css-ALL
 member pt-911
 member pt-loc
 member pt-ld
 member pt-internl
```

➔ **Apply COR list (or CSS) to the outgoing dial-peer.**

```
dial-peer voice 911 pots
 corlist outgoing css-911
!
dial-peer voice 7 pots
 corlist outgoing css-loc
!
dial-peer voice 11 pots
 corlist outgoing css-ld
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
```

NOTE:

- If no outgoing COR list is applied to an outgoing dial-peer, that particular dial-peer has no restrictions and is visible by all incoming dial-peers and hence all phones registered to CCME and SRST.

➔ **The next step is to apply COR to the incoming dial-peer. In CCME this is done on the "ephone-dn" (in SRST all steps are the same as for CCME except this step - applying COR to the incoming dial-peer is configured inside call-manager-fallback for SRST).**

```
ephone-dn 1 dual-line
 number 3001
 cor incoming css-911-loc
!
!
ephone-dn 2 dual-line
 number 3002
 cor incoming css-ALL
```

NOTE:

- If there is no incoming COR list applied for a particular ephone then that phone has visibility to all outgoing dial-peers since the incoming dial-peer, by default, has the highest COR priority when no COR is applied. Therefore, if you apply no COR for an incoming call leg to a dial-peer, then this dial-peer can make calls out of any other dial-peer, irrespective of the COR configuration on the outgoing dial-peer.

Task 3.3

Set up the CME GUI and allow the administrator to add/remove DNs through the web interface.

```
P2-BR2-RTR(config)#ip http server
P2-BR2-RTR(config)#ip http path flash:

P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)#web admin system name ipexpert password ipexpert
P2-BR2-RTR(config-telephony)#dn-webedit
P2-BR2-RTR(config-telephony)#time-webedit
```

Task 3.4

Configure the inter-digit timer to 7 seconds.

```
P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)#timeouts interdigit 7
```

Task 3.5

Configure the BR2 phones so that the system display shows the message "BR2 site" instead of "Cisco CME".

```
P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)#system message BR2 site
```

Task 3.6

Create 3 paging groups with DN = 1007, 1008 and 1009. When 1007 is dialed BR2 phone 1 will be paged. When 1008 is dialed BR2 phone 2 will be paged. When 1009 is dialed all the BR2 phones will be paged.

➔ **As a general rule of thumb, the Documentation CD is very useful when it comes to CME and you should be adept at using it. The only exception to the rule is COR where the DocCD is confusing since the names of the CSS are the same as the names of the Partitions.**

```
ephone-dn 1 dual-line
 number 3001
!
ephone-dn 2 dual-line
 number 3002
!
ephone-dn 3 dual-line
 number 3010
 huntstop channel
 no huntstop
!
!
ephone-dn 4 dual-line
 number 3010
 preference 1
 huntstop channel
 no huntstop
!
ephone-dn 11
 number 1007
 paging
!
!
ephone-dn 12
 number 1008
 paging
!
!
ephone-dn 13
 number 1009
 paging
 paging group 11,12
!
!
ephone 1
 mac-address 0011.BBEF.6901
 paging-dn 11
```



```
 type 7940
 button  1:1 2o3,4
!
!
!
ephone  2
 mac-address 0011.BBE0.5775
 paging-dn 12
 type 7940
 button  1:2 2o3,4
```

Task 3.7

International calls should be blocked from all phones Mon-Fri outside office hours. Office hours are 9am-5pm.

➔ **To block calls define the pattern to block and then the times during which calls to the defined numbers will be blocked. If you want to block certain calls all the time then use the "7-24" keyword. Otherwise define the day/time. When specifying times, use a start time and an end time. If the end time is a smaller value than the start time then the end time applies to the following day.**

```
telephony-service
!
after-hours block pattern 1 9011
 after-hours day Sun 23:59 09:00
 after-hours day Mon 17:00 09:00
 after-hours day Tue 17:00 09:00
 after-hours day Wed 17:00 09:00
 after-hours day Thu 17:00 09:00
 after-hours day Fri 17:00 09:00
```

Task 3.8

A call from another site supporting only G729 may ring into a BR2 site CME phone, and that phone may be busy and have set to forward busy calls into CUE VM. If this is the case, ensure that G729 call into CUE will not fail.

➔ **What we wish to accomplish here is to create the ability to invoke a transcoder local on the BR2 router. As long as we have a few DSP resources left over, we can accomplish this by using the same configuration on the router that we would use in tying an IOS Transcoder to CallManager. Only difference being that instead of putting in the IP address of CallManager Pub or Sub as who we want to register to, we put the IP of the CME source address in the telephony-service section. Then add a few 'sdspfarm' commands in the same section.**

```
voice-card 0
 dspfarm
 dsp services dspfarm
!
```



```
interface FastEthernet0/0.2
 encapsulation dot1Q 210
 ip address 10.1.202.1 255.255.255.0
 no snmp trap link-status
!
sccp local FastEthernet0/0.2
sccp ccm 10.1.202.1 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register mtp00128031d058          ←MAC Add of FastEth 0/0.2
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 maximum sessions 6
 associate application SCCP
!
telephony-service
 max-ephones 20
 max-dn 48
 ip source-address 10.1.202.1 port 2000
 sdspfarm units 1
 sdspfarm transcode sessions 6
 sdspfarm tag 1 mtp00128031d058
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 4: Gateways

Estimated Time to Complete: 1.5 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 4 Gateways

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure Section 1 must be completed along with the basic Call Manager/CCME tasks in Section 2 and 3.

There are two methods of testing - complete section 5 and 6 and test gateways having complete dial plan. If this is not desired then you may find it beneficial to create a '911' Route Pattern to test the HQ and BR1 gateways and a Dial-peer with destination-pattern 911 to test the CME - this is purely to verify the gateway configuration.

Section 4 Configuration Tasks

Task 4.1

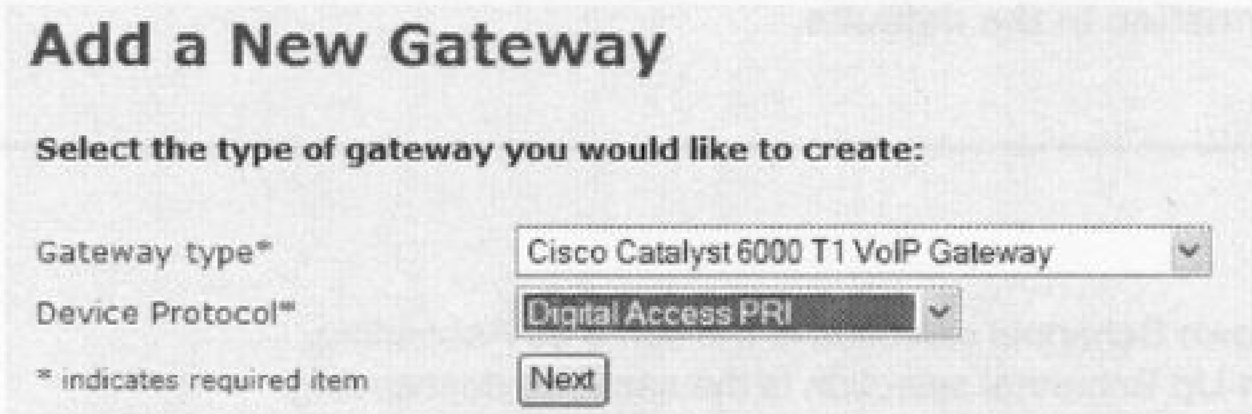
Configure the HQ 6608 T1 PRI gateway based on Table 1. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed.

- ➔ **Log onto the Cat 6608 and place the assigned port into the correct Vlan - if unspecified enable DHCP.**

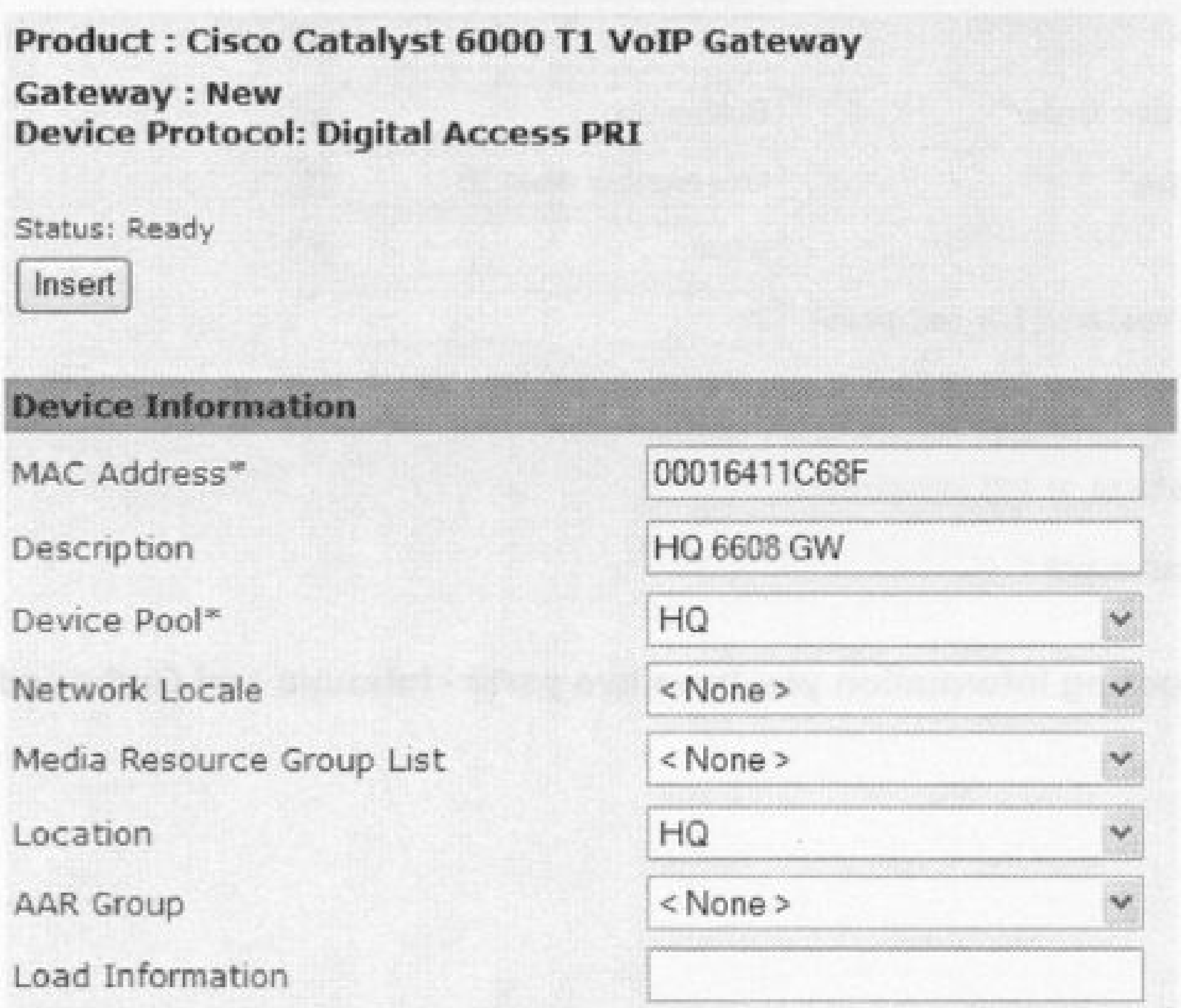
- ➔ **Show port to retrieve the MAC address - this will be used in the Call Manager administration. You may also wish to verify that the T1 port has been allocated an IP Address from the DHCP Server.**

```
Console> (enable) set port voice int 4/4 dhcp enable vlan 240
Port 4/4 DHCP enabled.
Console> (enable) sh port 4/4
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status    Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 4/4                     enabled   240        full    - unknown

Port     DHCP   MAC-Address      IP-Address     Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 4/4    enable 00-02-7e-38-c7-97 10.4.200.104    255.255.255.0

Port     Call-Manager(s)  DHCP-Server    TFTP-Server    Gateway
-------- ----------------- --------------- --------------- ---------------
 4/4     -               10.4.200.21    10.4.200.21    10.4.200.1

Port     DNS-Server(s)    Domain
-------- ----------------- -------------------------------------------------
 4/4     -               -
```

➔ **From the Call Manager Admin GUI add a gateway, selecting the Cat 6K T1 VoIP Gateway and Device Protocol to PRI.**



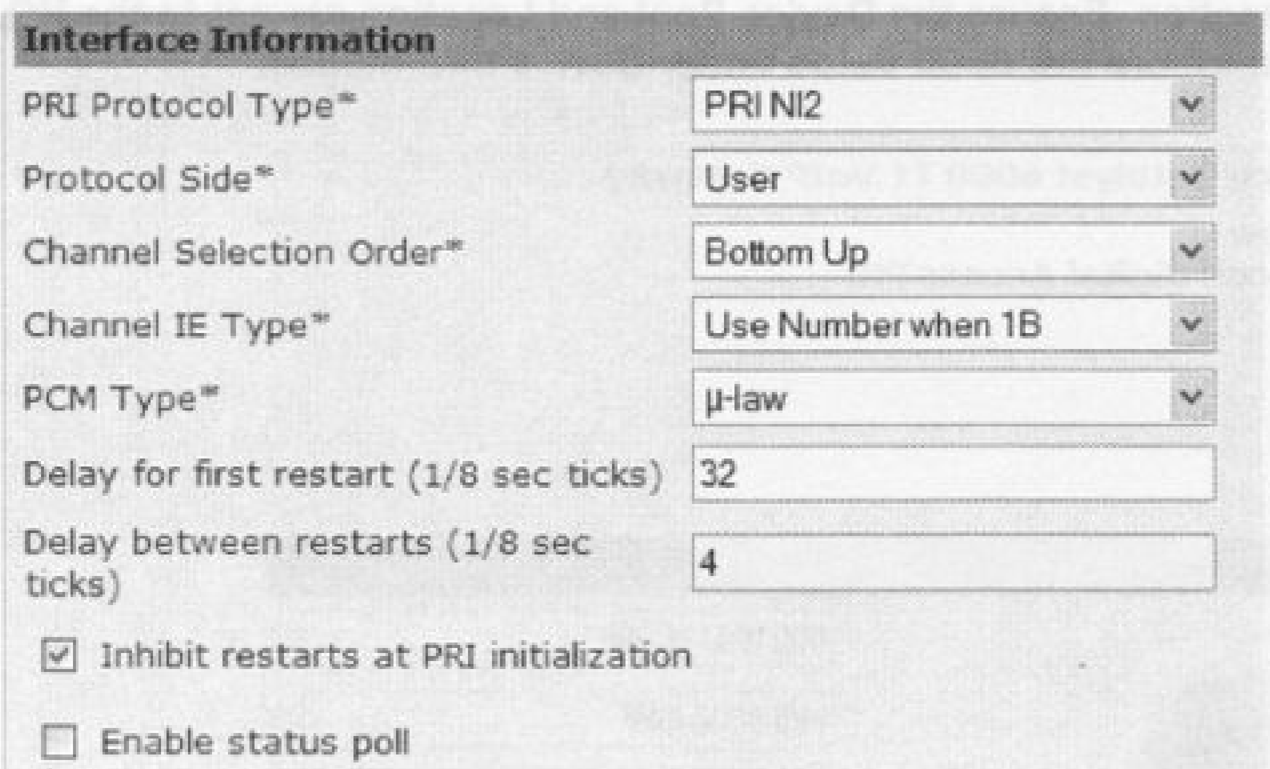
➔ **Earlier in this task you should have done a "show port" on the T1 port on the 6608 (as a time-saver cut 'n paste this into notepad). Use the MAC address in the Device Information section. Ensure the Device Pool and Location are set to the HQ. At this stage you can ignore the other fields under Device Information.**



➔ **Under Interface Information select the correct Protocol Type/Side. Channel Selection is Bottom Up since the Telco is using Top-Down Bchannel Selection so we must do the opposite to minimize the chances of glare. Leave other fields under Interface Information to the defaults.**

NOTE:

- Top-Down Bchannel selection is the same as Ascending.
- Bottom-Up Bchannel selection is the same as descending.



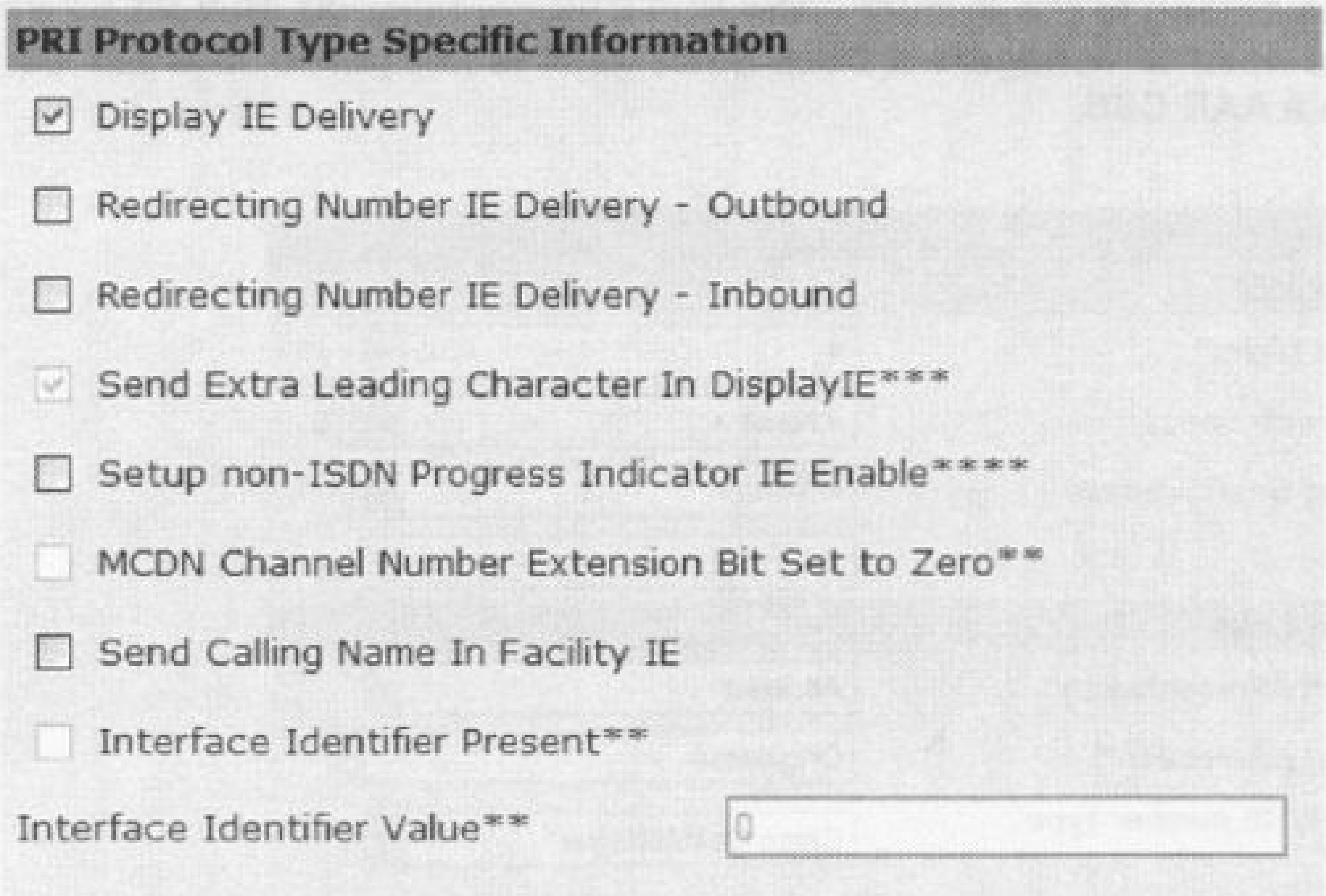
➔ **Under Call Routing Information you have two parts - Inbound and Outbound Calls.**

➔ **For inbound calls set the Incoming Significant digits to the amount of digits you are using for DNs of Devices - in this case 4. A CSS is required if the devices the gateway is supposed to be able to dial are in the non-default partition - in this case all devices belong to the Null PT – the Null CSS contains the Null PT by default so we do not need to configure a CSS. Since AAR is not part of this lab we will not configure a AAR CSS.**

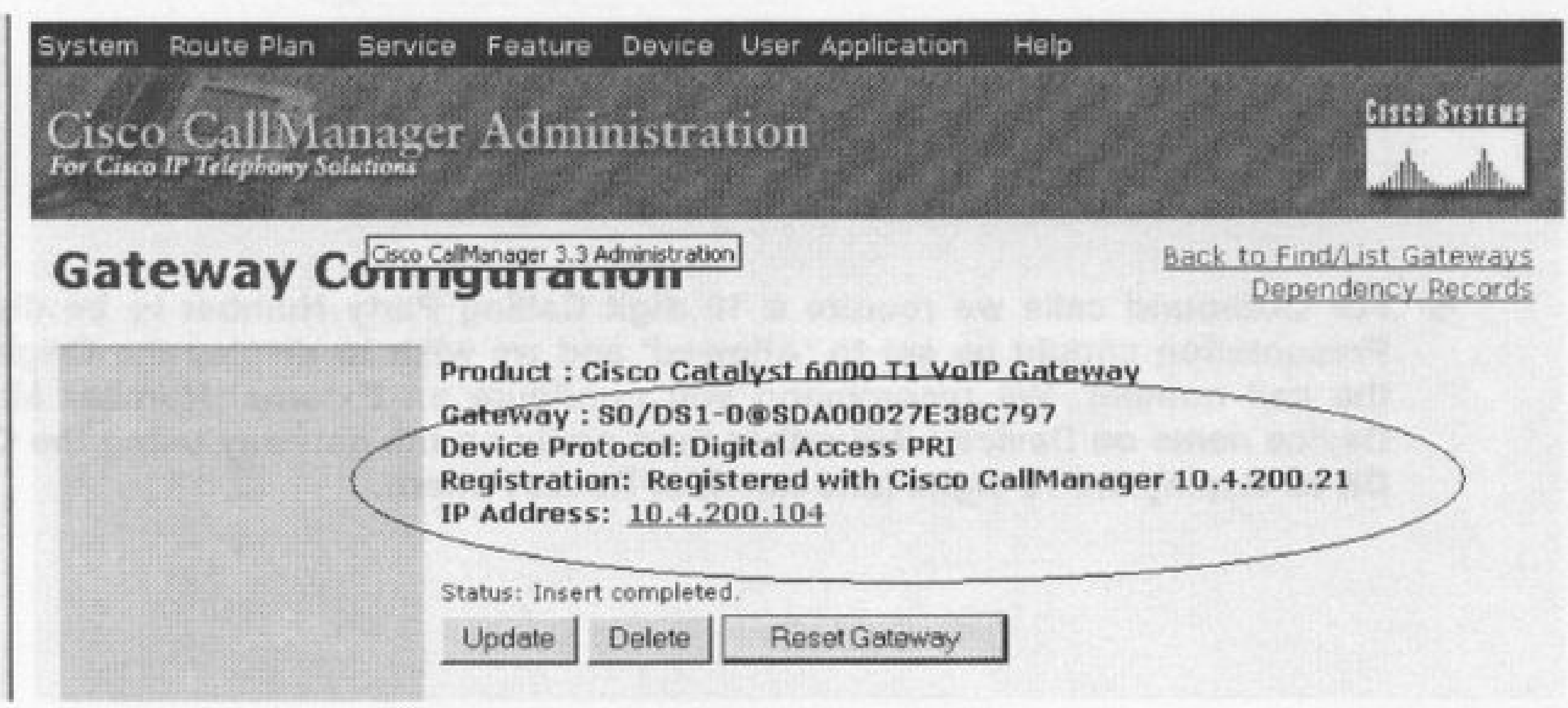
Call Routing Information	
Inbound Calls	
Significant Digits*	4
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	
Outbound Calls	
Calling Party Presentation*	Allowed
Calling Party Selection*	Originator
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Number of digits to strip*	0
Caller ID DN	
SMDI Base Port*	0

➔ **For Outbound calls we require a 10 digit Calling Party Number to be displayed. Presentation should be set to 'Allowed' and we wish to display the Originator of the call number. We recommend you configure an External Number Mask and Device name on Device LINE rather than prefix on the gateway using the Caller ID DN to display the 10 digits (and not 4) or Route Pattern.**

➔ **Under PRI Protocol Type mark the Display IE Delivery checkbox - this will ensure the calling name will be displayed to the Called Party.**



➔ **Leave all other settings to the default. After updating and resetting verify the registration status.**



➔ **Also verify from the Catalyst - you should see that the port has registered to the Call Manager.**

```
Console> (enable) sh port 4/4
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
4/4                        connected  240        full   1.544       T1

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
4/4      enable  00-02-7e-38-c7-97 10.4.200.104    255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
4/4      10.4.200.21       10.4.200.21     10.4.200.21     10.4.200.1
```

➔ **At this stage with Bottom UP BChannel Selection, Call Manager will attempt to use channel 23 (the last Bchannel). We have to manually instruct Call Manager that this is a partial PRI using the following procedure (this step is only required for the 6608 T1 PRI and not the IOS MGCP PRI in the next task).**

➔ **Copy the name of the 6608 gateway into the clipboard.**

Product : Cisco Catalyst 6000 T1 VoIP Gateway
Gateway : S0/DS1-0@SDA00016411C68F
Device Protocol: Digital Access PRI
Registration: Registered with Cisco CallManager 10.2.200.21
IP Address: 10.2.200.122

Status: Ready

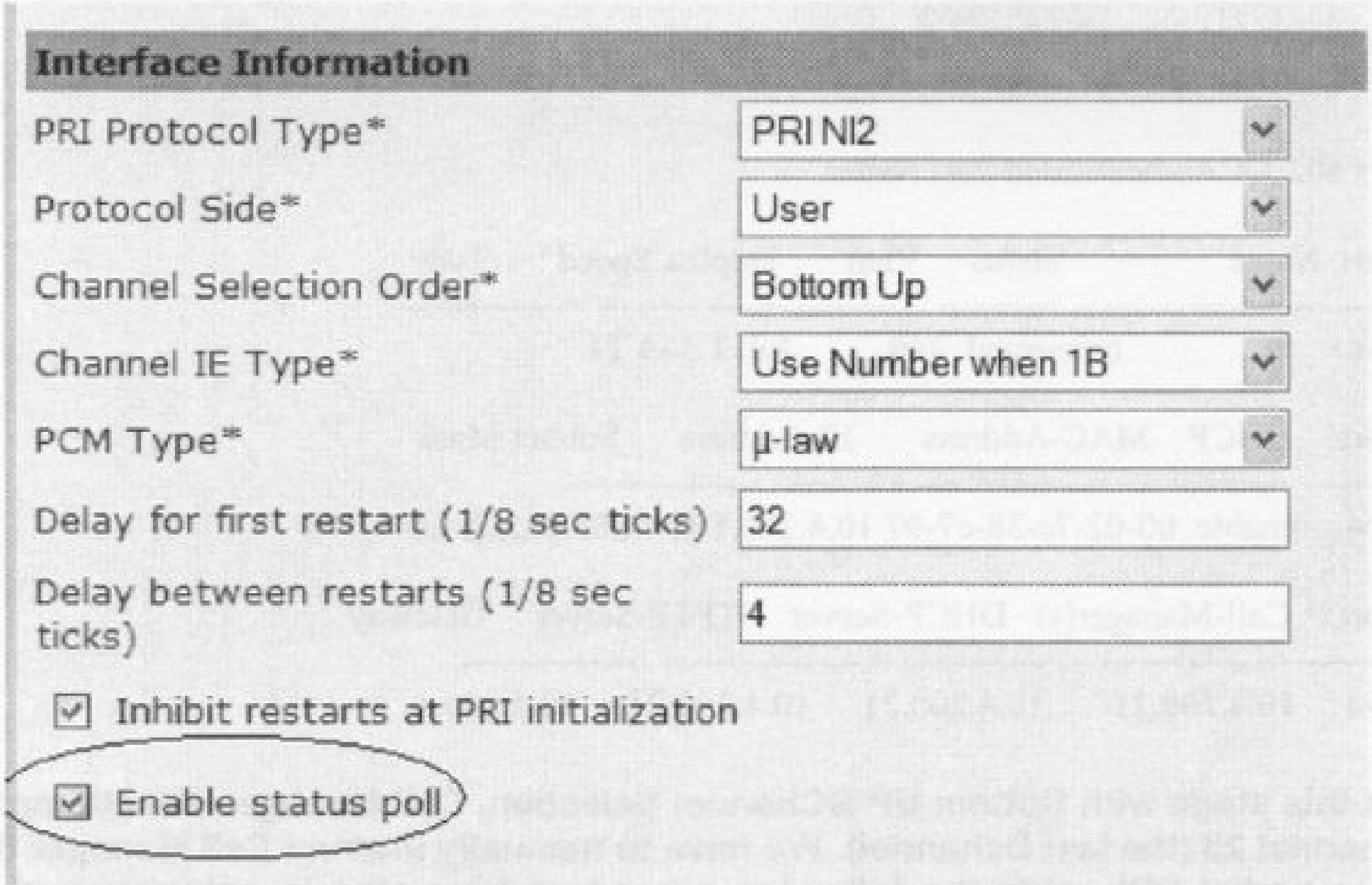
➔ **Edit the CCM Service Parameter shown below (you will have to click on the Advanced button to display this Service Parameter.**

Change B-Channel Maintenance Status 1	S0/DS1-0@SDA00016411C68F=0001 111

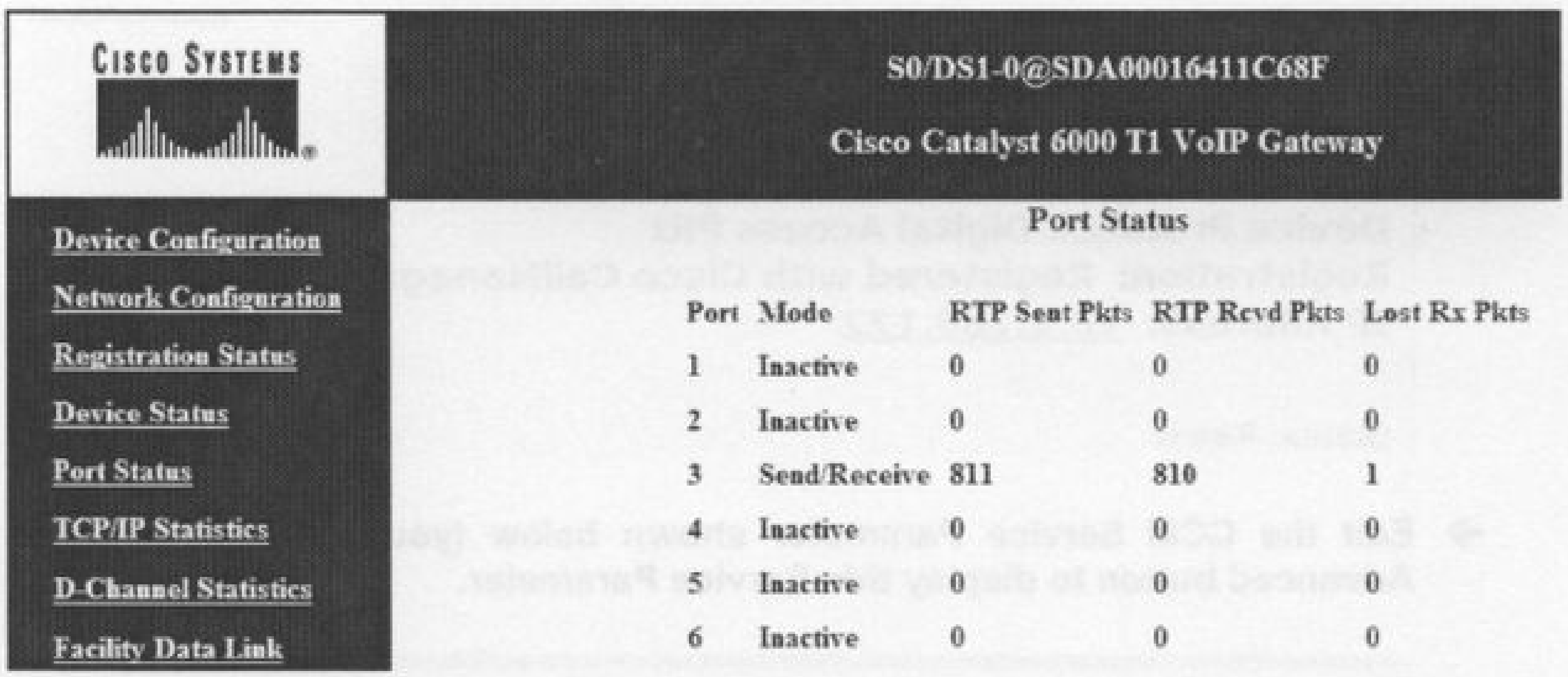
➔ **The full value of the parameter is:**

"S0/DS1-0@SDA00016411C68F=0001 1111 1111 1111 1111 1111", where '0' signifies an active timeslot and '1' is out of service.

➔ **In the 6608 gateway page mark the checkbox shown below and Reset the gateway (you might need to restart the CCM Service if not already done after previous step).**



➔ **Verify which Bchannel the call to 911 is using by clicking on the IP Address of the 6608 gateway and selecting "Port Status".**



Task 4.2

Configure BR1 as an MGCP gateway, based on information in Table 1. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed.

➔ **With MGCP the Layer 3 (Q931) Signaling channel of the T1 PRI is backhauled back to Call Manager. Q921 terminates on the gateway.**

➔ **The first step in configuring a MGCP gateway is to enable the physical interface and Layer 2 Q921.**

```
P4-BR1-RTR(config)# isdn switch-type primary-ni
P4-BR1-RTR(config)# controller T1 2/0/0
P4-BR1-RTR(config-controller)# pri-group timeslots 1-3 service mgcp
*Jun 22 15:31:08.906: %LINK-3-UPDOWN: Interface 2/0/0:23(1), changed state to up
*Jun 22 15:31:08.906: %LINK-3-UPDOWN: Interface 2/0/0:23(2), changed state to up
*Jun 22 15:31:08.906: %LINK-3-UPDOWN: Interface 2/0/0:23(3), changed state to u
*Jun 22 15:31:09.894: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0/0:0,
changed state to down
*Jun 22 15:31:09.894: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0/0:1,
changed state to down
*Jun 22 15:31:09.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0/0:2,
changed state to down
*Jun 22 15:31:09.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0/0:23,
changed state to up
*Jun 22 15:31:10.898: %LINK-3-UPDOWN: Interface Serial2/0/0:23, changed state to up
```

➔ **The last line of the output following configuration of the controller states that the Serial interface has been created and has changed state to UP. This interface will not show before the controller has been configured.**

```
P4-BR1-RTR(config-controller)# int Serial2/0/0:23
P4-BR1-RTR(config-if)# isdn bind-l3 ccm-manager
```

➔ **If not already configured, assign a unique hostname to the gateway so that the Cisco CallManager server can identify it.**

```
router(config)# hostname P4-BR1-RTR
```

➔ **Configure the router to run MGCP as a signaling protocol.**

```
P4-BR1-RTR(config)# mgcp
```

➔ **Configure the IP address (or DNS name) for the Cisco CallManager server.**

```
P4-BR1-RTR(config)# mgcp call-agent 10.4.200.21
```

➔ **Bind Control and Media packets to the voice vlan interface.**

```
P2-BR1-RTR(config)#mgcp bind control source-interface Vlan220
P2-BR1-RTR(config)#mgcp bind med source-interface Vlan220
```

NOTE:

- To configure redundant Cisco CallManagers in the CallManager cluster, issue the following commands:

P4-BR1-RTR(config)# ccm-manager redundant-host <IP Address PUB>
P4-BR1-RTR(config)# ccm-manager switchback {graceful | immediate |schedule-time hh:mm | uptime-delay minutes}

➔ **To enable support for Cisco CallManager within MGCP, issue the following command:**

P4-BR1-RTR(config)# ccm-manager mgcp

➔ **Bind the MGCP application to the voice ports in a POTS dial-peer.**

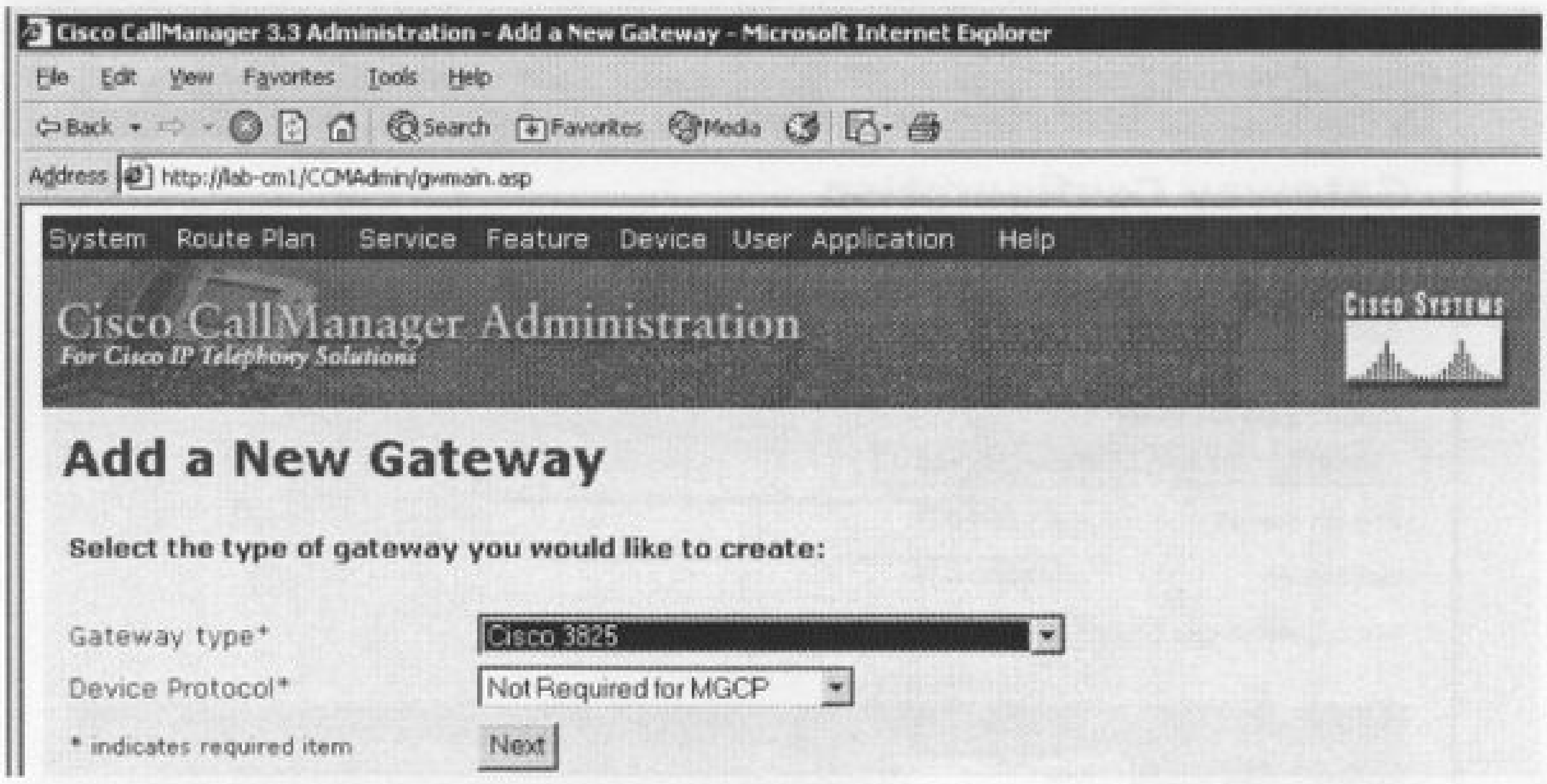
P4-BR1-RTR(config)# dial-peer voice 1 pots
P4-BR1-RTR(config)# application MGCPAPP
P4-BR1-RTR(config)# port 2/0/0:23

➔ **Before adding the gateway to Call Manager, the hardware type, module and card type must be derived. This is done using the following method:**

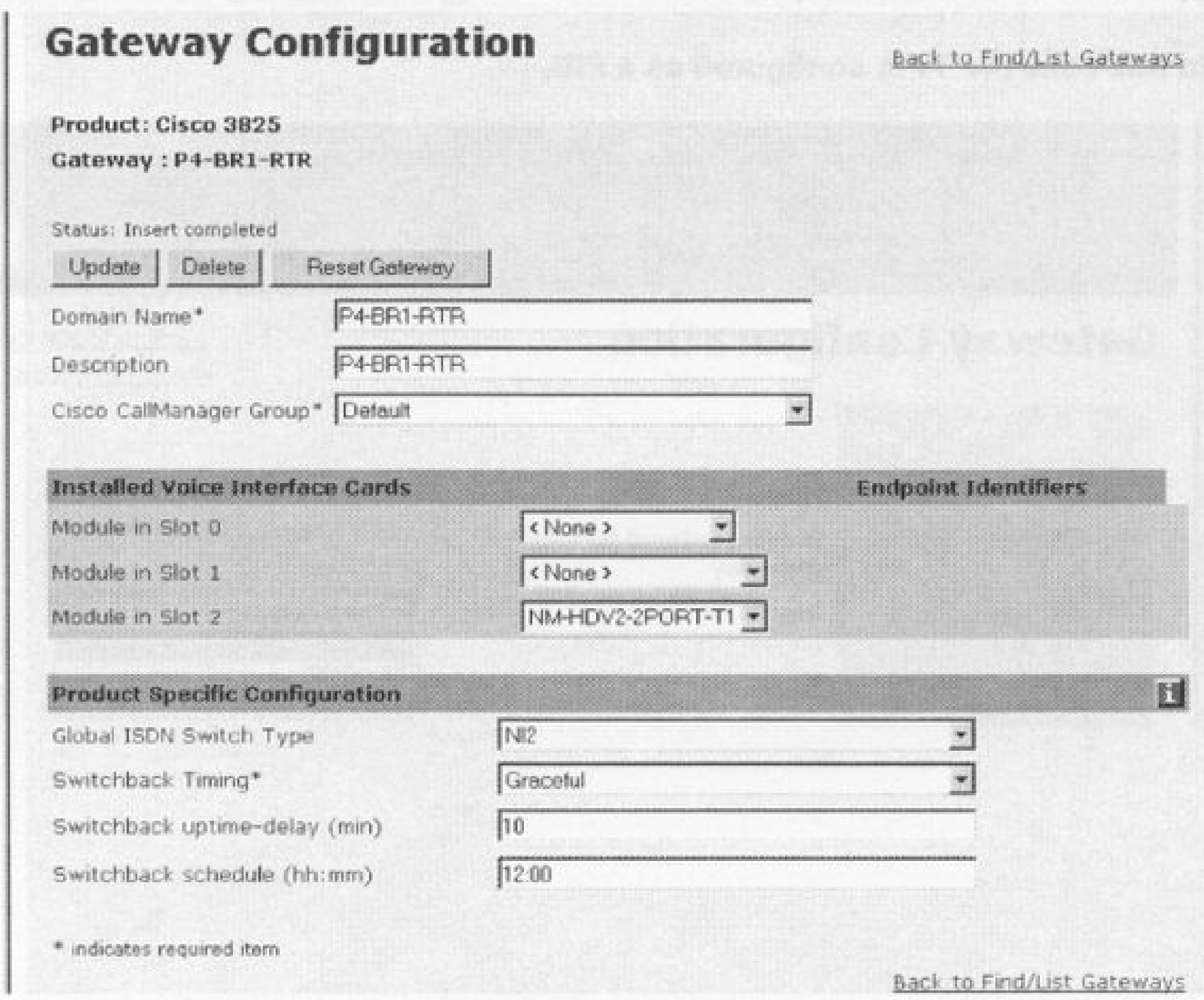
P4-BR1-RTR#sh diag
Slot 0: **C3825** Mother board 1GE(TX,SFP),1GE(TX), integrated VPN and 4W Port adapter, 3 ports
.....
Slot 2:
High Density Voice **NM-HDV2-2T1/E1** Port adapter
WIC Slot 0:
T1 (1 Port) Multi-Flex Trunk WAN Daughter Card
.....
P4-BR1-RTR#sh run | b controller
controller T1 2/0/0
framing esf
linecode b8zs
pri-group timeslots 1-3,24 service mgcp

➔ **The module is NM-HDV2-2T1/E1 and the card is VWIC1-MFT-1T1 which resides in port 2/0/0.**

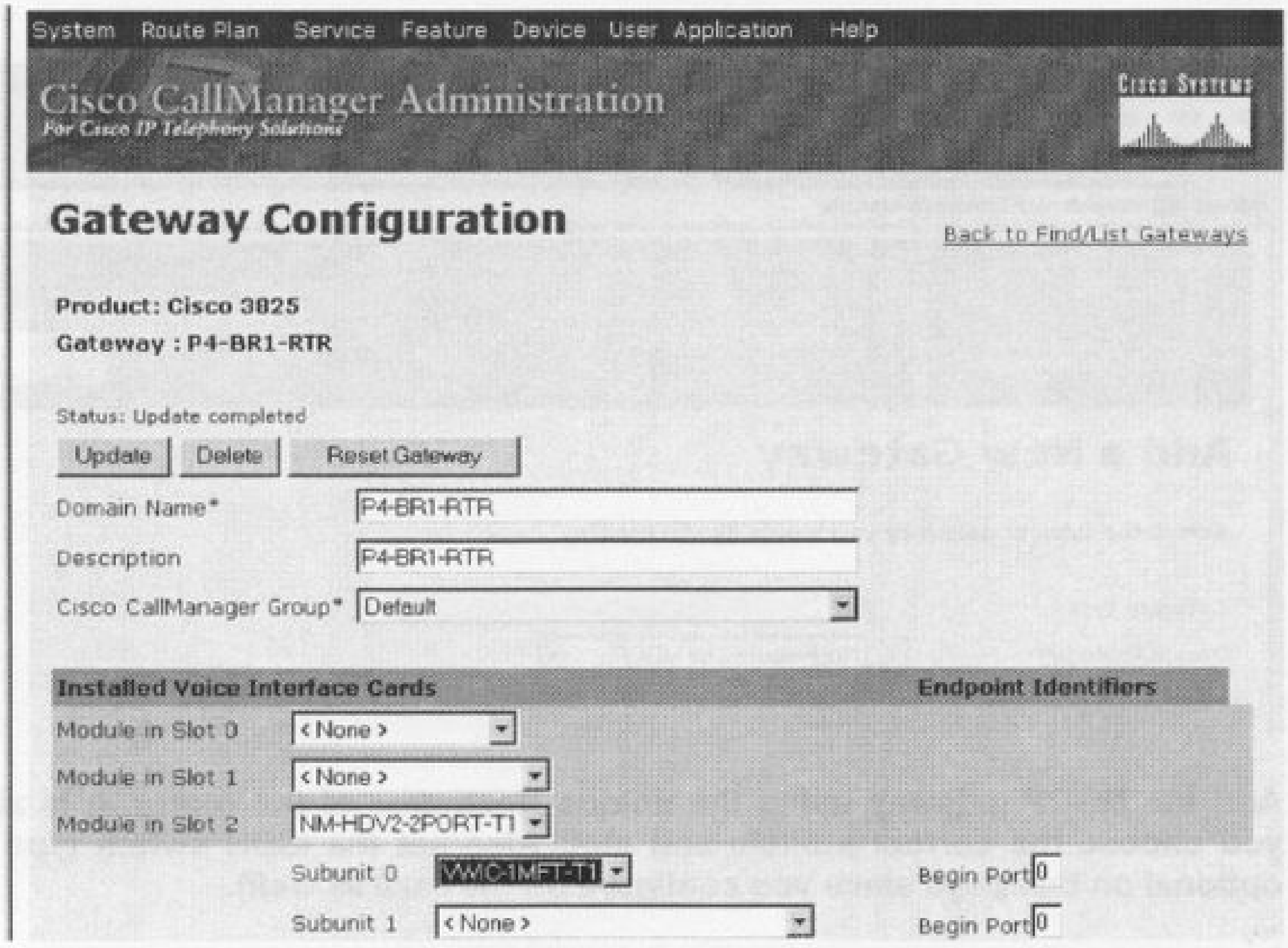
➔ **Now we are ready to add the gateway to the Call Manager using the information above.**



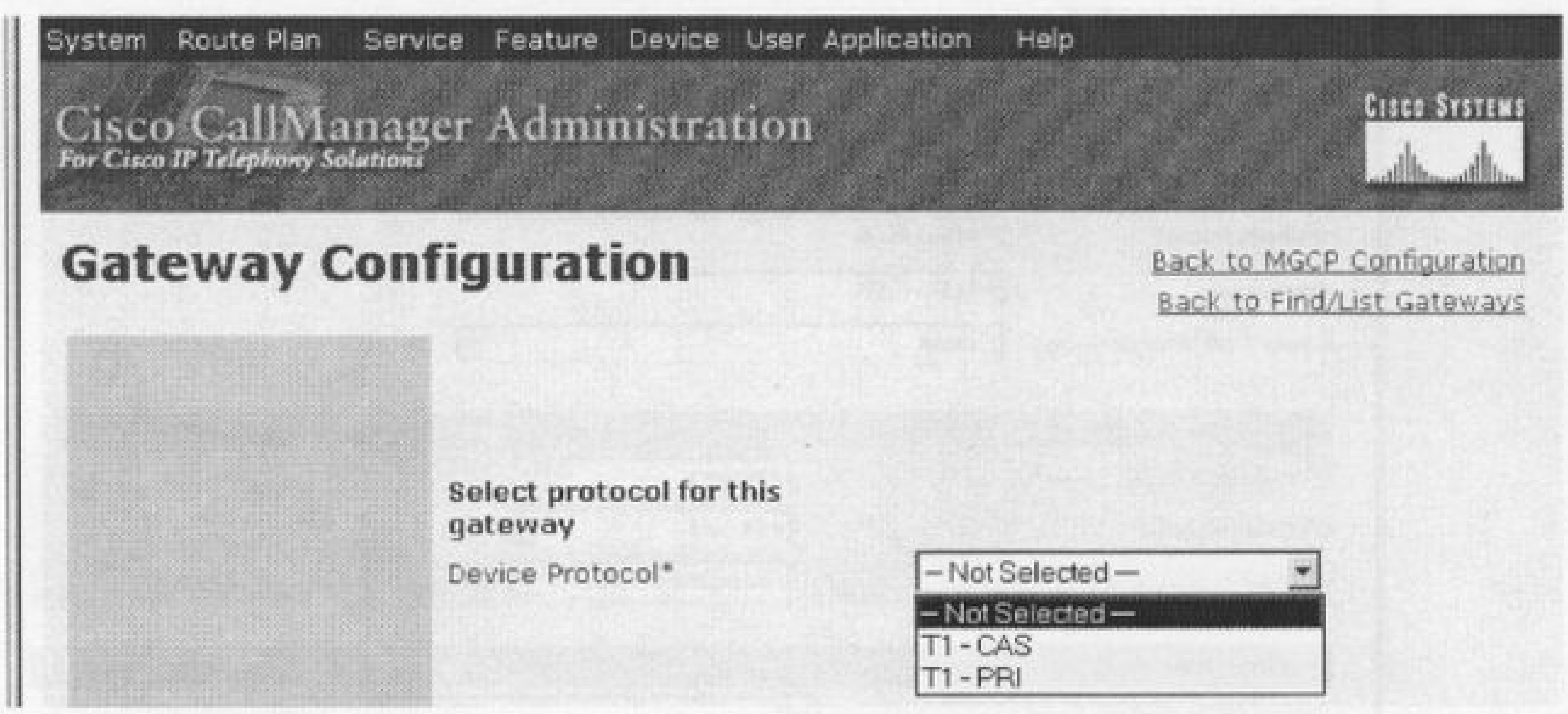
➔ **Add the MGCP gateway using the unique Hostname of the router. It is also vital you choose the correct module and slot! Also set the ISDN switch type (this is optional on this page since you configure on the card as well).**



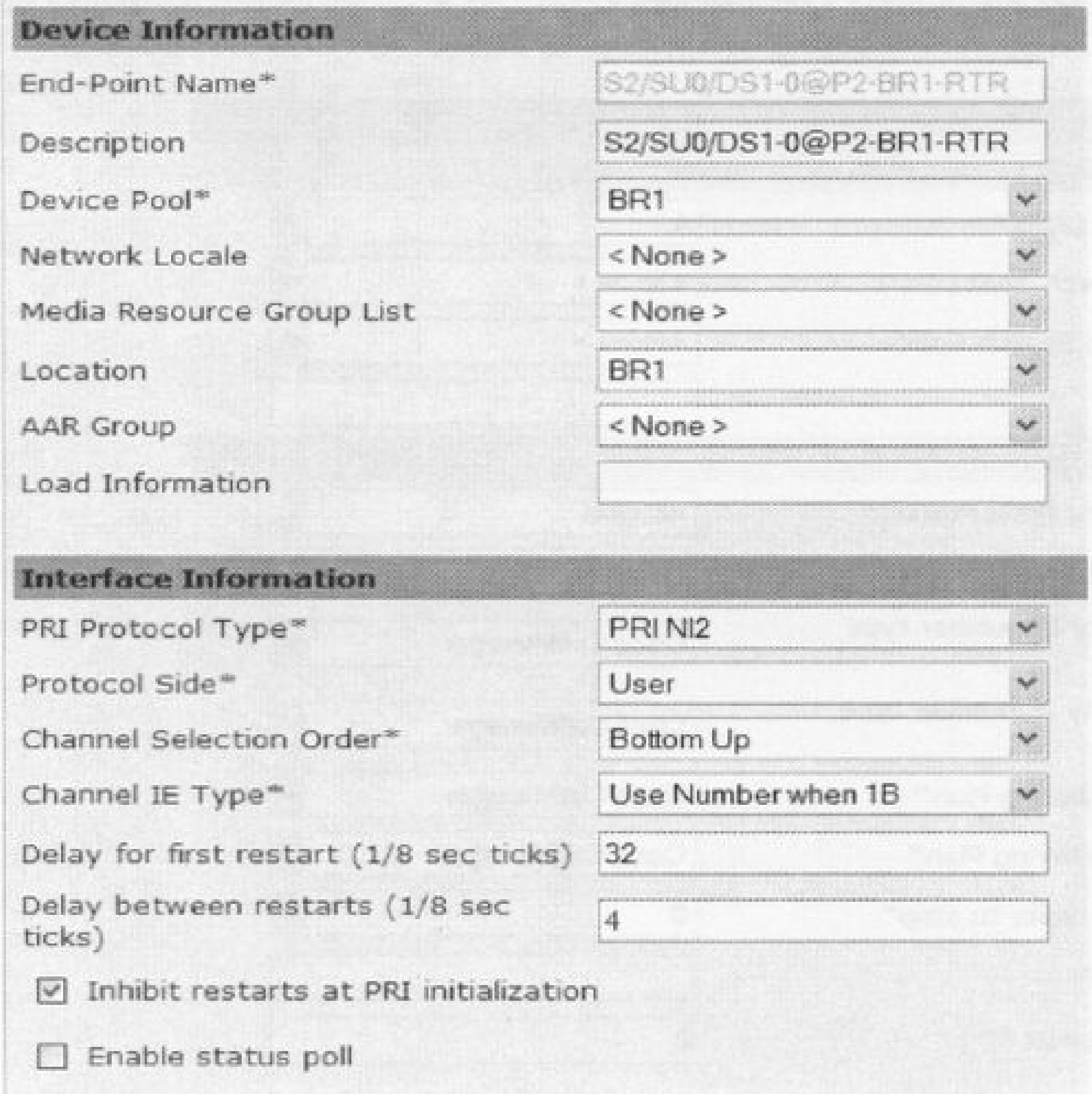
➔ **Select the correct card based on earlier information.**



➔ **In this case the T1 is configured as a PRI.**



➔ **Under Device Information select the relevant Device Pool, Location and PRI Protocol Type.**



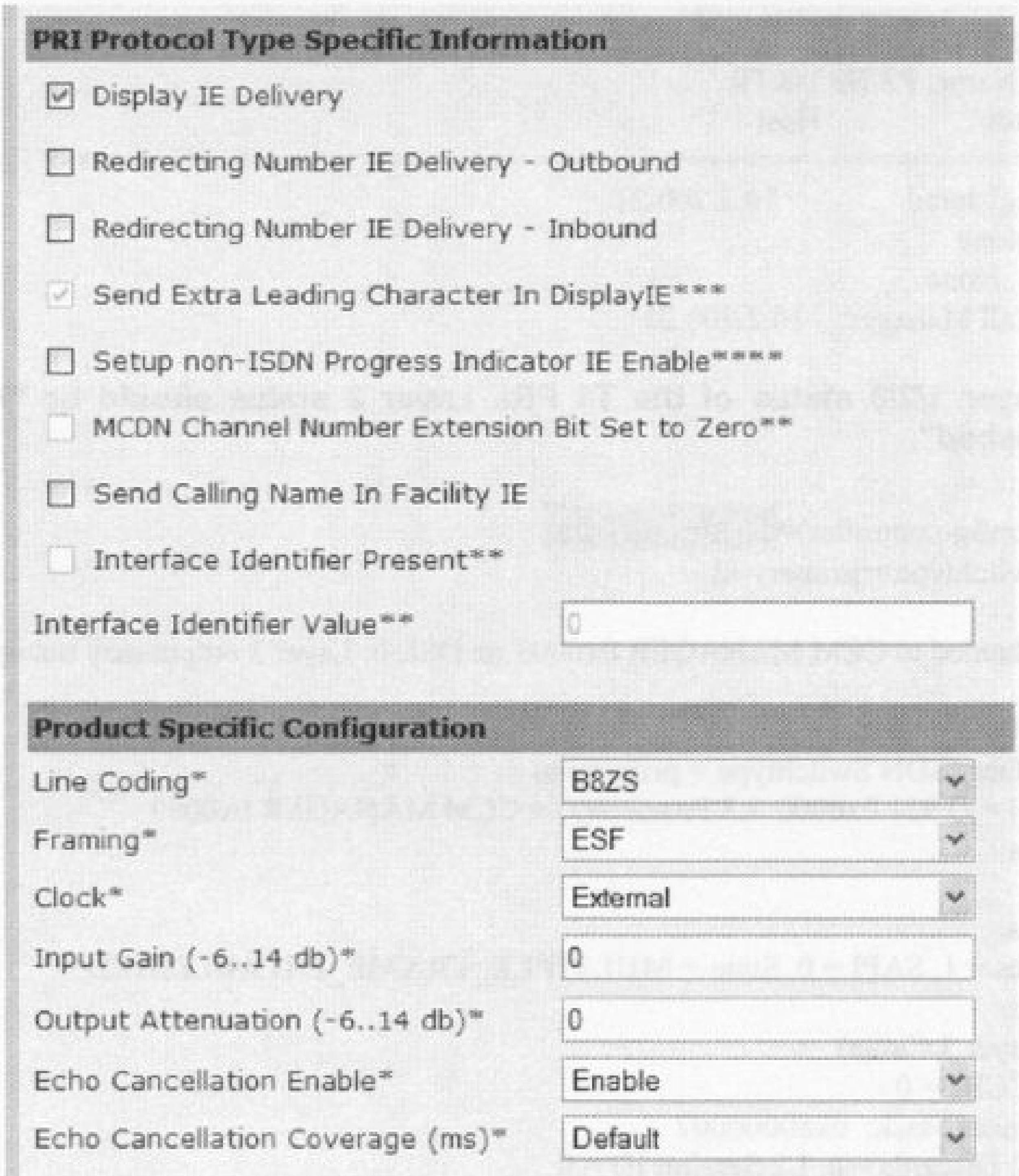
➔ **The Channel Selection is important in this case since the question implies that the Telco is using the Top-Down B Channel Selection algorithm. To minimize chances of glare we must there use the Bottom-up algorithm.**

➔ **Call Routing Information must have the correct Significant Digits set - assuming the Devices registered to Call Manager are using 4 digit extension this is set to '4'. Also the gateway needs to be configured with a Calling Search Space that can see the Phone Partitions - in.**

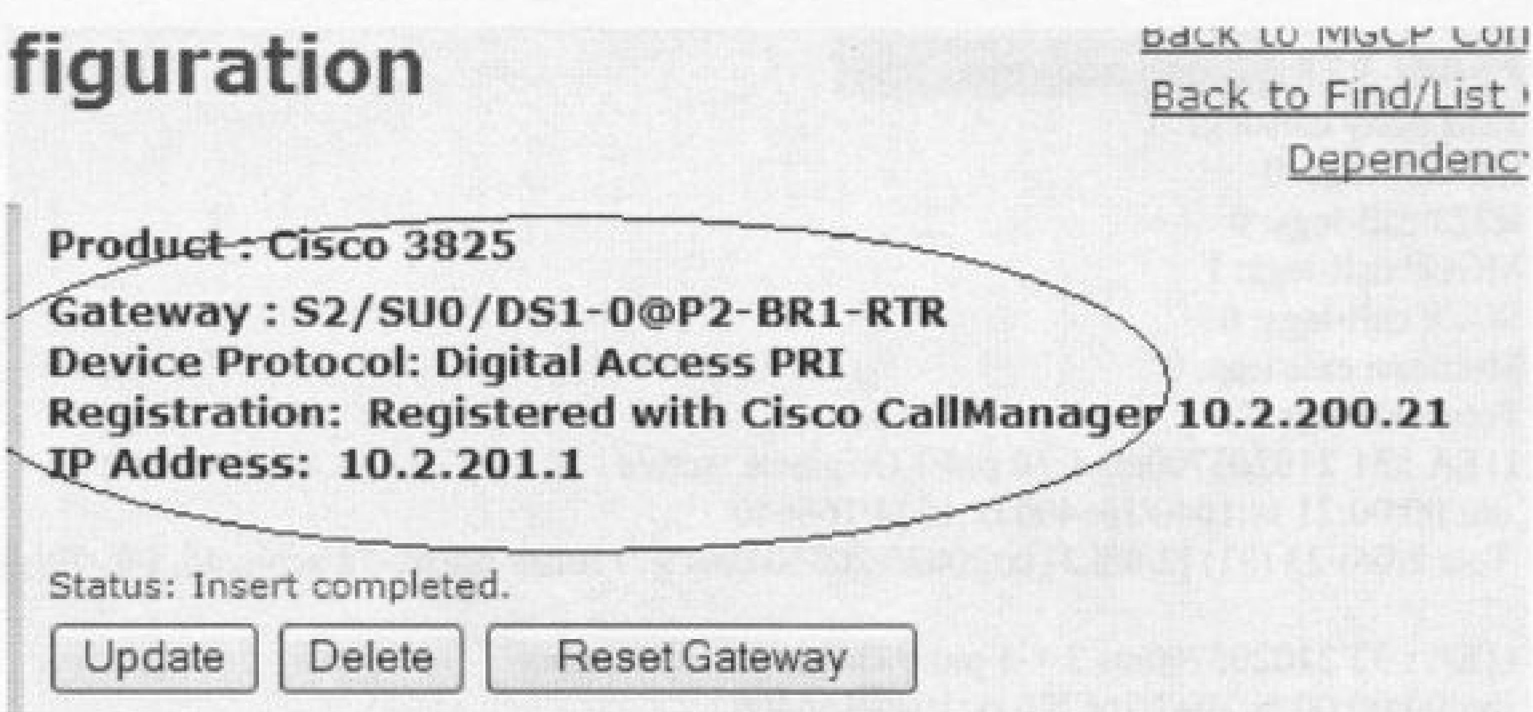
Call Routing Information	
Inbound Calls	
Significant Digits*	4
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	
Outbound Calls	
Calling Party Presentation*	Allowed
Calling Party Selection*	Originator
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Number of digits to strip*	0
Caller ID DN	
SMDI Base Port*	0

➔ **To display 10 digit Calling Party Number we will need to ensure that Presentation is Allowed. For Calling Party Name we mark the Display IE Delivery checkbox. We will then need to ensure the External Number Mask and Display name on the LINE is configured with the 10 digit number.**

➔ **Ensure that the Framing, LineCoding and clock parameters are correct.**



➔ **Once you have configured the gateway 'Update' and 'Reset'. You should see the gateway's registration status change to 'Registered'.**



➔ **Verify from the gateway itself.**

```
P2-BR1-RTR(config)#do sh ccm-manager
MGCP Domain Name: P2-BR1-RTR
Priority        Status                   Host
============================================================
Primary         Registered               10.2.200.21
First Backup    None
Second Backup   None
Current active Call Manager:    10.2.200.21
```

➔ **Check the Layer 1/2/3 status of the T1 PRI. Layer 2 status should be "Multiple Frame Established".**

```
P2-BR1-RTR(config-controller)#do sh isdn stat
Global ISDN Switchtype = primary-ni

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 0. Layer 3 output may not apply

ISDN Serial2/0/0:23 interface
        dsl 0, interface ISDN Switchtype = primary-ni
        L2 Protocol = Q.921 0x0000  L3 Protocol(s) = CCM MANAGER 0x0003
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000007
    Number of L2 Discards = 0, L2 Session ID = 0
    Total Allocated ISDN CCBs = 0
```

➔ **Make a call and verify which BChannel the call is using.**

```
P2-BR1-RTR#sh call act voice brief
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 1
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
11EA : 31 210205700ms.1 +0 pid:1 Originate  active
 dur 00:00:21 tx:1040/166400 rx:1054/168640
 Tele 2/0/0:23 (31) [2/0/0.3] tx:20830/20830/0ms g711ulaw noise:-78 acom:45  i/0:-79/-36 dBm

11EA : 32 210205700ms.2 +-1 pid:0 Originate  connecting
 dur 00:00:00 tx:1042/166720 rx:1040/166400
 IP 10.0.200.33:22377 SRTP: off rtt:0ms pl:19080/20ms lost:1/1/0 delay:55/55/65ms g711ulaw
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
Telephony call-legs: 1
```

Task 4.3

Ensure that the correct transport for DTMF digits is used for the BR1 gateway.

➔ **Configure the DTMF relay method - you will need to make sure all DTMF digits are transported out-of-band.**

```
P4-BR1-RTR(config)# mgcp dtmf-relay codec all mode out-of-band
```

Task 4.4

Configure BR2 as an E1 R2/H323 gateway based on the information in Table 1. Outbound ANI should be displayed (10 digits).

➔ **E1 R2 is similar to T1 CAS – create a DS0 group and define the active timeslots. We are using ITU-U Q421 type which is r2-digital and semi-compelled for inter-register signaling. The "ani" command at the end of the line enabled outbound caller-id.**

➔ **In R2 signaling, the exchanges (or BR2 and PSTN routers) are considered registers and the signaling between them is called interregister signaling. Interregister signaling uses forward and backward in-band multifrequency signals in each time slot to transfer called and calling party numbers, as well as the calling party category. There are 3 different type of Interregister signaling.**

➔ **R2-Compelled—When a tone-pair is sent from the switch (forward signal), the tones stay on until the remote end responds (sends an ACK) with a pair of tones that signals the switch to turn off the tones. The tones are compelled to stay on until they are turned off.**

➔ **R2-Non-Compelled—The tone-pairs are sent (forward signal) as pulses so they stay on for a short duration. Responses (backward signals) to the switch (Group B) are sent as pulses. There are no Group A signals in non-compelled interregister signaling.**

➔ **R2-Semi-Compelled—Forward tone-pairs are sent as compelled. Responses (backward signals) to the switch are sent as pulses. It is the same as compelled, except that the backward signals are pulsed instead of continuous.**

```
controller E1 0/0/0
 ds0-group 0 timeslots 1-3 type r2-digital r2-semi-compelled ani
```

Task 4.5

Configure the E1 R2 such that calls from the PSTN are set up 3 seconds quicker (where possible) than the default. Our carrier instructs that they will send us 10 digits.

➔ **Add a cas-custom group in the ds0-group created in the previous task.**

```
controller E1 0/0/0
ds0-group 0 timeslots 1-3 type r2-digital r2-semi-compelled ani
cas-custom 0
 dnis-digits min 3 max 11
```

Task 4.6

➔ **Block incoming calls to the BR2 router that have no Caller ID.**

```
controller E1 0/0/0
 ds0-group 0 timeslots 1-3 type r2-digital r2-semi-compelled ani
 cas-custom 0
  dnis-digits min 3 max 11
  ani-digits min 1 max 65
```

Task 4.7

Assume the PSTN has SIP Registrar servers according to Table 11. Configure the BR2 gateway to register all of its FXS and soon to be ephone-dn numbers to these 2 servers as primary and fallback respectively. Increase the default retry registration time by half of one second. You must use FQDNs to accomplish this task.

➔ **On BR2**

```
ip host sip1.ipexpert.com 192.20.200.51
ip host sip2.ipexpert.com 192.20.200.52
!
sip-ua
 timers register 1000
 registrar dns:sip1.ipexpert.com expires 3600
 registrar dns:sip2.ipexpert.com expires 3600 secondary
```

➔ **NOTE: You may need to undo this task in the future in order to get calls to route properly – this was done only to enlighten you how to register an IOS GW to a SIP Registar/Proxy/Location server should one be present in the actual Lab (which is a distinct possibility).**

➔ **Another thing to keep in mind is that you might be asked to authenticate to the SIP Register / Proxy Server. This would be done in the global-config SIP-UA subsection as follows:**

```
sip-ua
 timers register 1000
 registrar dns:sip1.ipexpert.com expires 3600
 registrar dns:sip2.ipexpert.com expires 3600 secondary
 authentication username BR2 password 094F471A1A0A realm IPEXPERT
```

➔ **Also – should you need to point a Dial-Peer to send a call to the SIP Proxy Server (much like a H323 GW sends a call to a GK with a 'session target ras' command) this is how you would configure it:**

```
dial-peer voice 1 voip
 destination-pattern xxxx
 session protocol sipv2
 session target dns:sip1.ipexpert.com
 codec g711ulaw

dial-peer voice 2 voip
 destination-pattern xxxx
 preference 1
 session protocol sipv2
 session target dns:sip2.ipexpert.com
 codec g711ulaw
```

Task 4.8

Unity needs to be able to accept in-bound faxes at the mailbox of IncomingFax@voip.lab (we will configure Unity for this task later). Unity will also be your DNS server. Configure the BR1 GW to intercept these faxes from the PSTN PRI as an On-Ramp gateway and email all incoming faxes to this mailbox. Refer to Table 7 of this section for FaxDN ranges. All the files you will need are in BR1 Flash memory.

➔ **NOTE: In setting up faxing we will need to first configure an "ip domain-name" on the BR1 GW. THIS WILL BREAK YOUR MGCP CONFIGURATION!!!**

➔ **So we need to go back to our GW configuration page in CCM and re-configure it so that our BR1 GW not only has the Host Name, but now the FQDN of "P1-BR1-RTR.voip.lab"**

➔ **Make sure to RESET your GW both on the CCM, and by issuing a "no mgcp", "mgcp" on the IOS GW.**

➔ **Also when testing Faxing later when you have setup the Unity piece of the puzzle – you will need to create an ACL to block MGCP traffic from get to the CCM or stop the CCM service all together (it might also be a good time to test SRST) – this way the PRI will be handed back over to the Default Application away from MGCP so that the Fax application can intercept the specific call**

➔ **Also note that after you have configured the command "fax interface-type fax-mail" and finished the rest of your configuration – that you MUST reboot the router in order for the GW to work as a Fax On or Off Ramp GW**

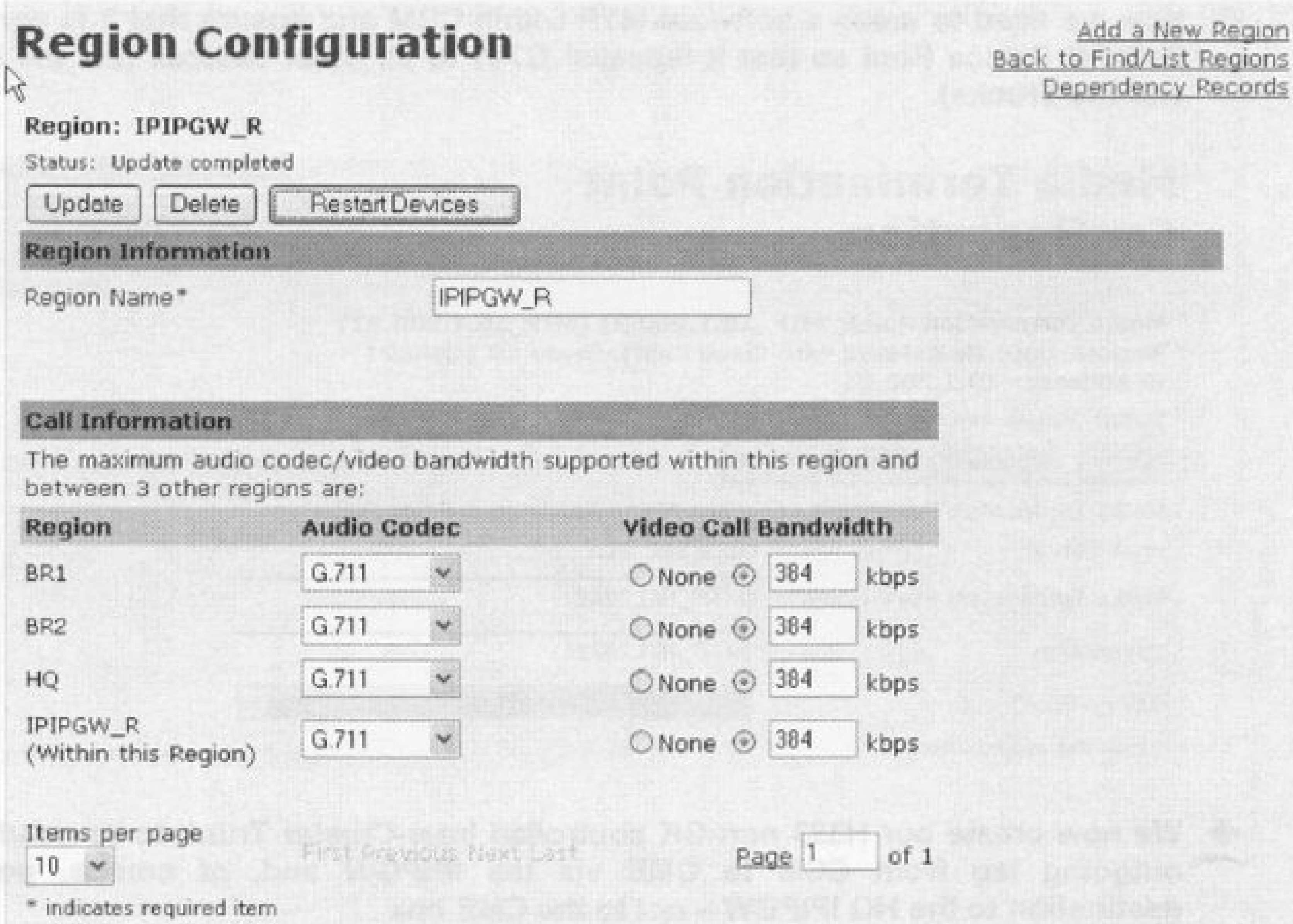
➔ **Now on the BR1 GW:**

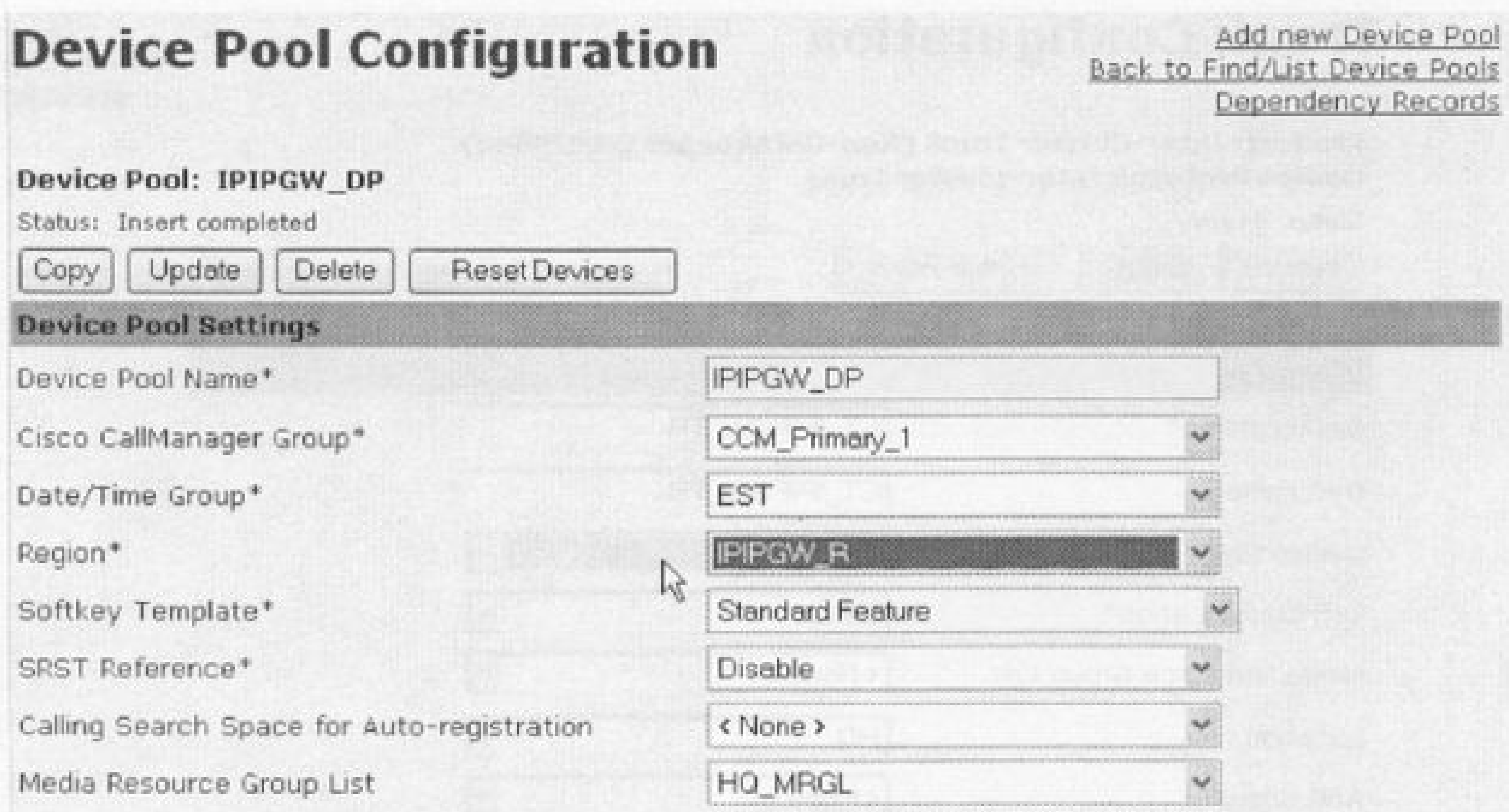
```
ip domain-name voip.lab
ip name-server 10.1.200.22
!
fax receive called-subscriber $d$
fax interface-type fax-mail
mta send server unity-lab.voip.lab port 25
mta send with-subject both
mta send postmaster administrator@voip.lab
mta send mail-from hostname P1-BR1-RTR.voip.lab
mta send mail-from username $s$
mta send return-receipt-to hostname voip.lab
mta send return-receipt-to username administrator
!
application
 service fax-onramp flash:app_faxmail_onramp.2.0.1.3.tcl
  !
!
!
dial-peer voice 10 pots
 service fax-onramp
 incoming called-number 617521280.
 direct-inward-dial
!
dial-peer voice 20 mmoip
 service fax_on_vfc_onramp_app out-bound
 destination-pattern 617521280.
 information-type fax
 session target mailto:FaxInboundMailbox @voip.lab
!
```

Task 4.9

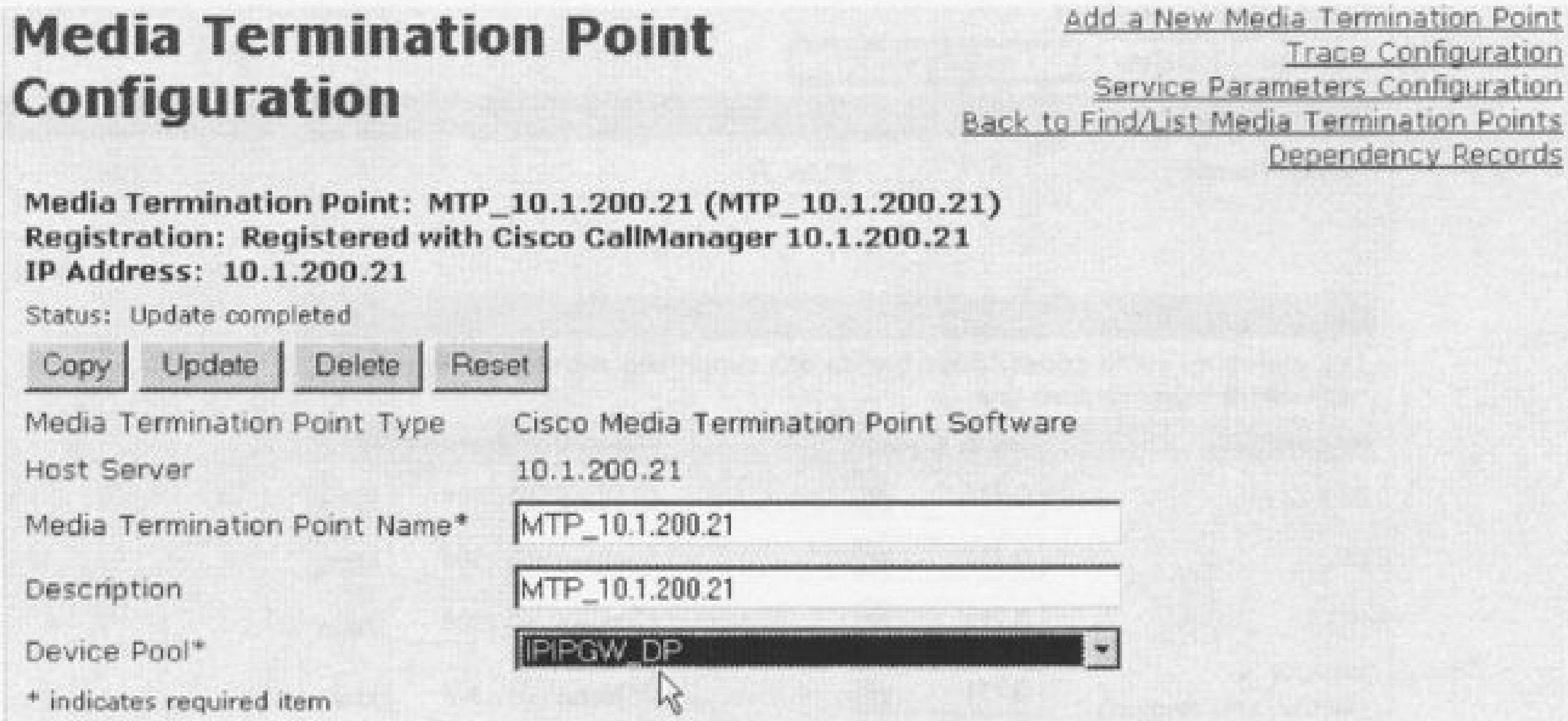
Configure the HQ-RTR as an IPIPGW. Calls will be coming into it from CCM via H323 using G711ulaw and then be routed out to the BR2 CME via SIP using G729 (see Table 9 for DNs at CME). Calls will also be coming from CME via H323 using G729 and routed to CCM via SIP using G711ulaw (see Table 10 for DNs at in CCM). Also ensure when calls are coming from SIP to H323 that RFC 2833 is properly stripped. Ensure that if calls are coming from H323 to SIP, that RFC 2833 is used for the SIP side.

➔ **First we need to setup a new Region and Device Pool that will speak G711ulaw to every other Region/DP. The reason that we do this is that our IPIPGW will only allow a specific codec to come into it – it will not negotiate the codec with us like an endpoint would.**

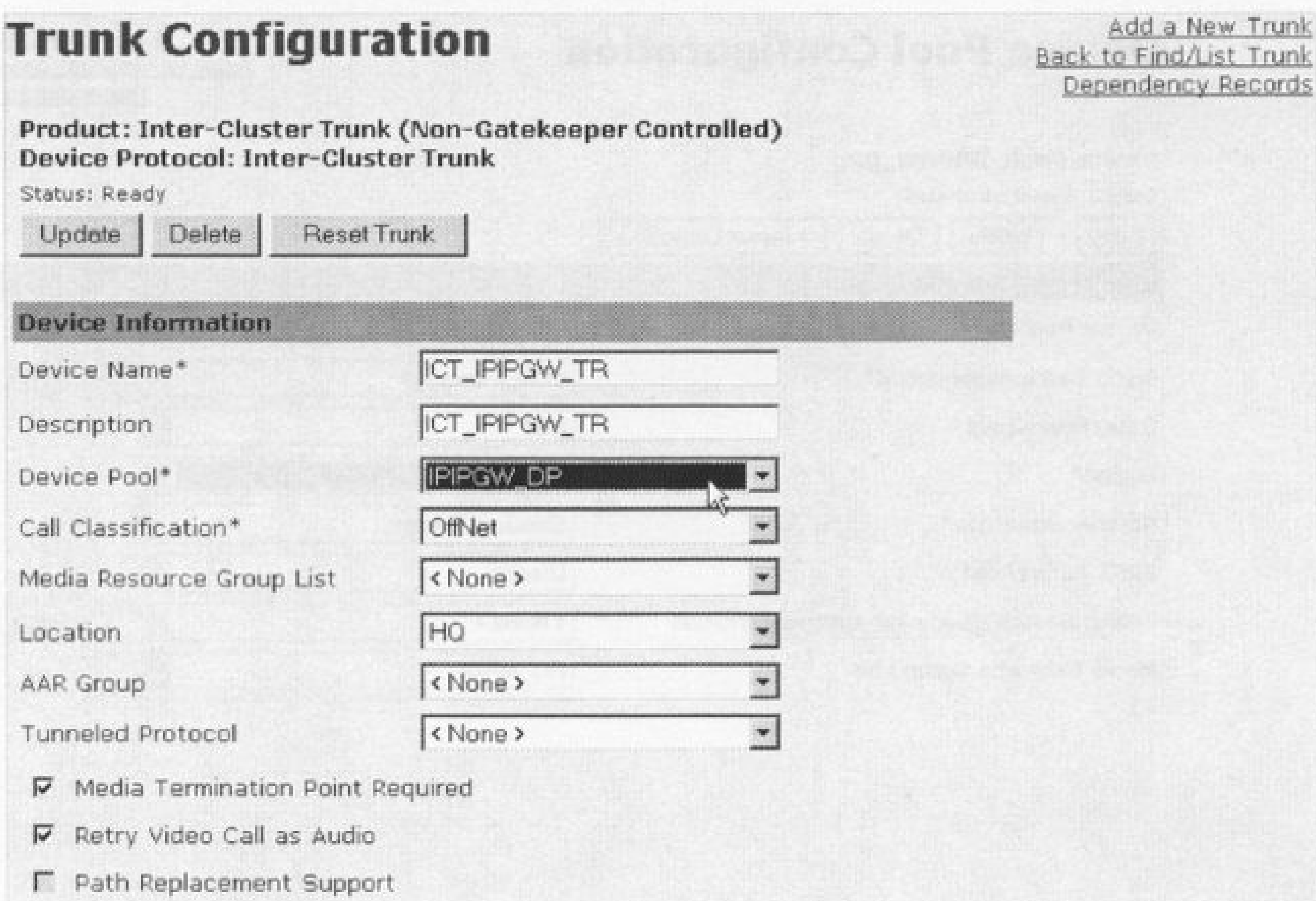

Region Configuration
Add a New Region
Back to Find/List Regions
Dependency Records
Region: IPIPGW_R
Status: Update completed
Update
Delete
Restart Devices
Region Information
Region Name*
IPIPGW_R
Call Information
The maximum audio codec/video bandwidth supported within this region and between 3 other regions are:
Region
Audio Codec
Video Call Bandwidth
BR1
G.711
None
384
kbps
BR2
G.711
None
384
kbps
HQ
G.711
None
384
kbps
IPIPGW_R (Within this Region)
G.711
None
384
kbps
Items per page
10
First Previous Next Last
Page 1 of 1
* indicates required item

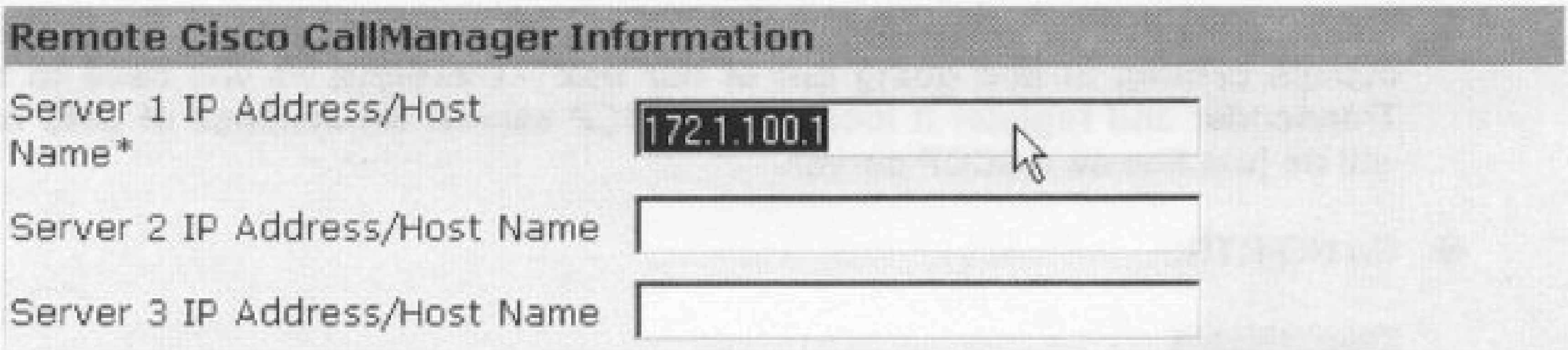

Device Pool Configuration
Add new Device Pool
Back to Find/List Device Pools
Dependency Records
Device Pool: IPIPGW_DP
Status: Insert completed
Copy
Update
Delete
Reset Devices
Device Pool Settings
Device Pool Name*
IPIPGW_DP
Cisco CallManager Group*
CCM_Primary_1
Date/Time Group*
EST
Region*
IPIPGW_R
Softkey Template*
Standard Feature
SRST Reference*
Disable
Calling Search Space for Auto-registration
< None >
Media Resource Group List
HQ_MRGL

➔ **Now we need to setup a software MTP within CCM and ensure that it is part of the IPIPGW Device Pool so that it 'speaks' G711 to all other devices (i.e. the Phones and the Trunks).**

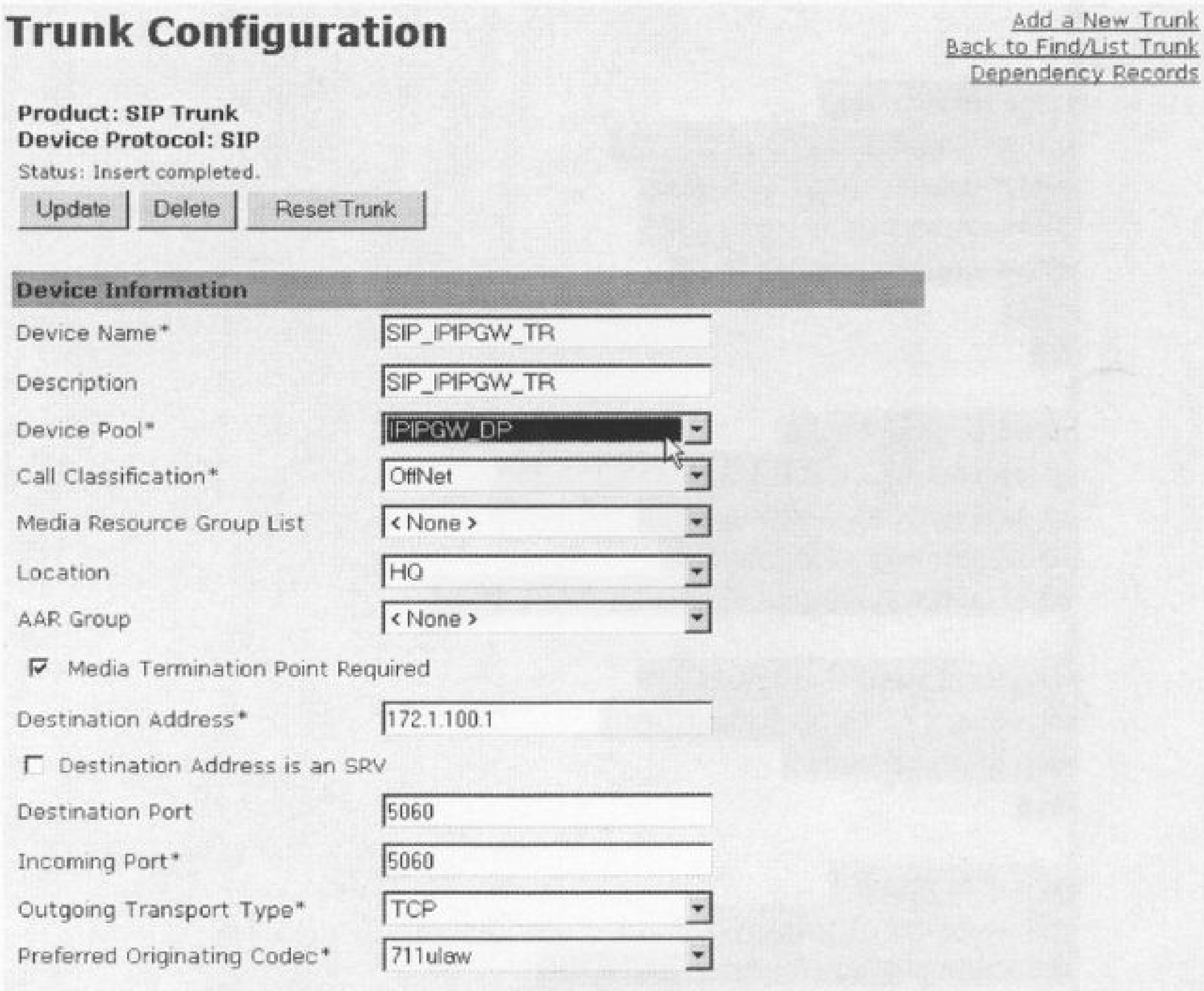


➔ **We now create our H323 non-GK controlled Inter-Cluster Trunk to be used on the outgoing leg from CCM to CME via the IPIPGW and, of course, point the destination to the HQ IPIPGW – not to the CME box**





➔ **We now create our SIP Trunk to allow calls to come in from the CME via the IPIPGW**



➔ **Next let us create the incoming dial-peer on the BR2 CME box to allow incoming calls via the IPIPGW (we will setup the outgoing dial-peer to the IPIPGW in the section for Dial Plan)**

➔ **On BR2 RTR:**

```
dial-peer voice 10 voip
 incoming called-number 3…
 session protocol sipv2
 dtmf-relay rtp-nte
```

➔ **Finally we need to setup our IPIPGW keeping in mind that we have 2 different codecs coming in and going out of our box – therefore we will need to setup a Transcoder and register it locally to a SCCP server. An instance of CME or SRST will do just fine as a SCCP server.**

➔ **On HQ-RTR:**

```
voice-card 2
 dspfarm
 dsp services dspfarm
!
!
!
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 h323
 sip
!
interface Loopback0
 ip address 172.1.100.1 255.255.255.255
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 172.1.100.1
!
sccp local FastEthernet0/0.210
sccp ccm 172.1.100.1 identifier 1
sccp ip precedence 3
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCODER
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 codec g729br8
 maximum sessions 2
 associate application SCCP
!
```

```
!
telephony-service
 max-conferences 12 gain -6
 ip source-address 172.1.100.1 port 2000
 max-ephones 10
 max-dn 10
 sdspfarm tag 1 XCODER
 sdspfarm units 1
 sdspfarm transcode sessions 1
!
dial-peer voice 10 voip                         ←(Incoming Dial-Peer for CCM-to-CME)
 incoming called-number 3...
 codec g711ulaw
 dtmf-relay h245-alphanumeric
!
dial-peer voice 11 voip                         ←(Outgoing Dial-Peer for CCM-to-CME)
 destination-pattern 3...
 session protocol sipv2
 session target ipv4:10.1.202.1
 dtmf-relay rtp-nte digit-drop h245-alphanumeric
!
dial-peer voice 20 voip                         ←(Incoming Dial-Peer for CME-to-CCM)
 incoming called-number [12]...
 dtmf-relay h245-alphanumeric
!
dial-peer voice 21 voip                         ←(Outgoing Dial-Peer for CME-to-CCM)
 destination-pattern [12]...
 session protocol sipv2
 session target ipv4:10.1.200.21
 codec g711ulaw
 dtmf-relay rtp-nte
!
```

Task 4.10

Unity also needs to be able to send out-bound faxes to the PSTN (we will configure Unity for this task later). Configure the BR1 GW to accept these faxes via email from Unity and then to send them out through the PSTN PRI as an Off-Ramp gateway. Refer to Table 8 of this section for PSTN FaxDN ranges. Again, all the files you will need are in BR1 Flash memory.

➔ **Again when testing Faxing later when you have setup the Unity piece of the puzzle – you will need to create an ACL to block MGCP traffic from get to the CCM or stop the CCM service all together (it might also be a good time to test SRST) – this way the PRI will be handed back over to the Default Application away from MGCP so that the Fax application can intercept the specific call**

➔ **Also note that after you have configured the command "fax interface-type fax-mail" and finished the rest of your configuration – that you MUST reboot the router in order for the GW to work as a Fax On or Off Ramp GW**

➔ **Now on the BR1 GW:**

```
ip domain-name voip.lab
ip name-server 10.1.200.22
!
fax interface-type fax-mail
fax send transmitting-subscriber $s$
fax send left-header FROM: $s$
fax send center-header FAX NO: $d$
fax send right-header D:$a$ $t$ P:$p$
fax send coverpage enable
fax send coverpage comment FAX FROM POD1-BR1-RTR
mta receive aliases P1-BR1-RTR.voip.lab
mta receive maximum-recipients 23
mta receive generate mdn
!
application
 service fax-offramp flash:app_faxmail_offramp.2.0.1.1.tcl
  !
!
dial-peer voice 100 mmoip
 service fax-offramp
 information-type fax
 incoming called-number 16175212223
!
dial-peer voice 110 pots
 destination-pattern 16175212223
 port 2/0/0:23
 forward-digits all
```


Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 5: Gatekeeper

Estimated Time to Complete: 1.5 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 5 Gatekeeper

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure Section 1 must be completed along with the CCME Gateway section. The Basics in Section 2 and 3 must also be completed.

Section 5 Configuration Tasks

Task 5.1

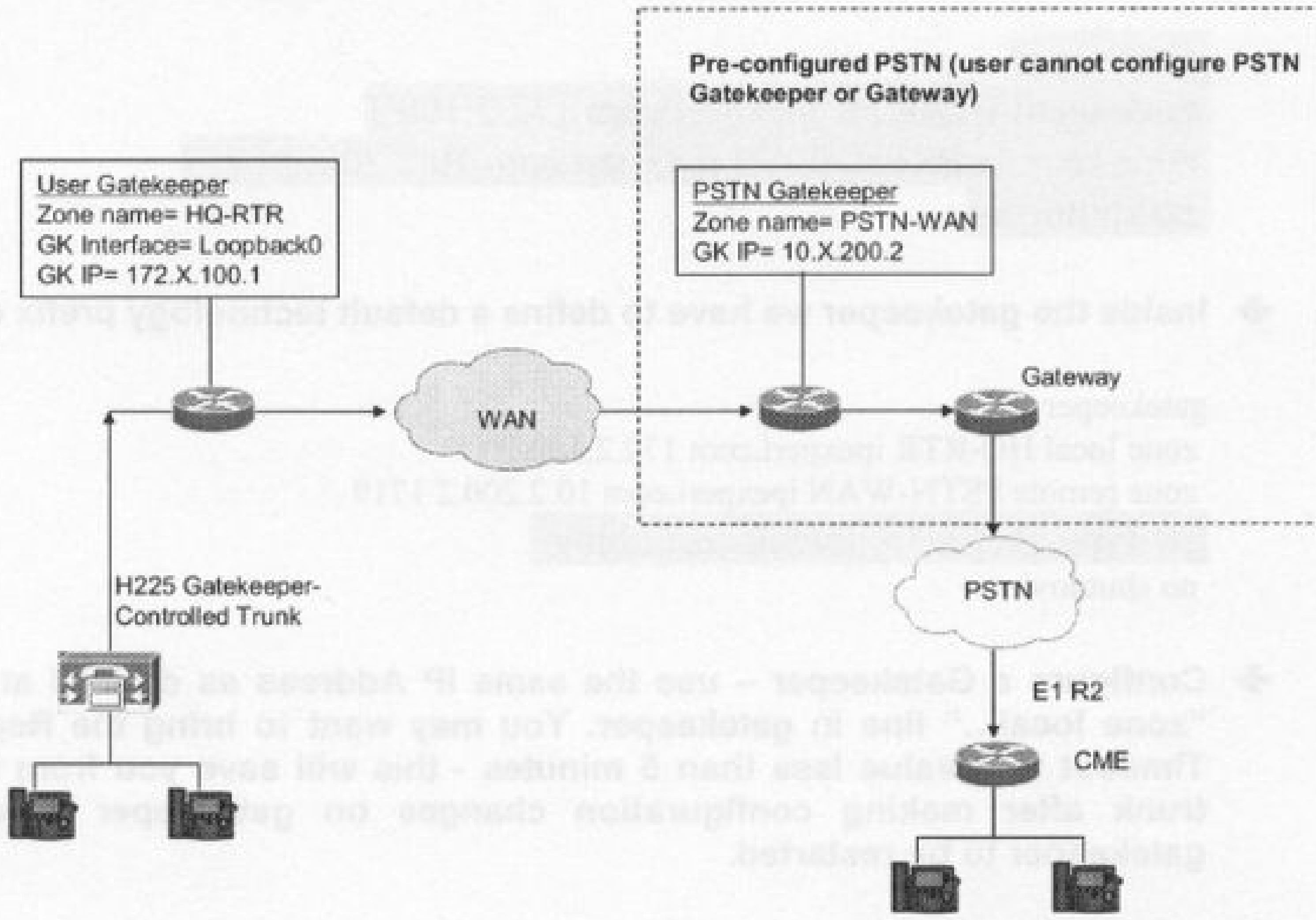
Configure gatekeeper on HQ-RTR with the following information:

Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

Register Call Manager to the gatekeeper using the default tech prefix 1#

→ **Be careful to study the exact topology for routing calls to CCME. Most people automatically assume this is an end-to-end VOIP call – which in this case is not true.**



Call Routing: CM TO CME VIA GK

➔ **As far as you are concerned the call leaves the HQ-RTR gatekeeper and arrives into the CCME via the PSTN - in other words for the call to be successful you are reliant on the E1 R2 working correctly.**

➔ **In this scenario you have no control of the PSTN gatekeeper and the PSTN gateway.**

➔ **The first step in configuring the gatekeeper is to define the local zone using the "zone local" command.**

```
zone local HQ-RTR domain-name 172.2.100.1
```

➔ **Note that the zone name is case sensitive. A domain name is mandatory even if DNS resolution is not being used. The RAS IP Address is optional but it is recommended that one is defined to avoid gatekeeper registration problems.**

➔ **Remote zones can be defined in using the same command except the keyword "…local…" is replaced with "remote".**

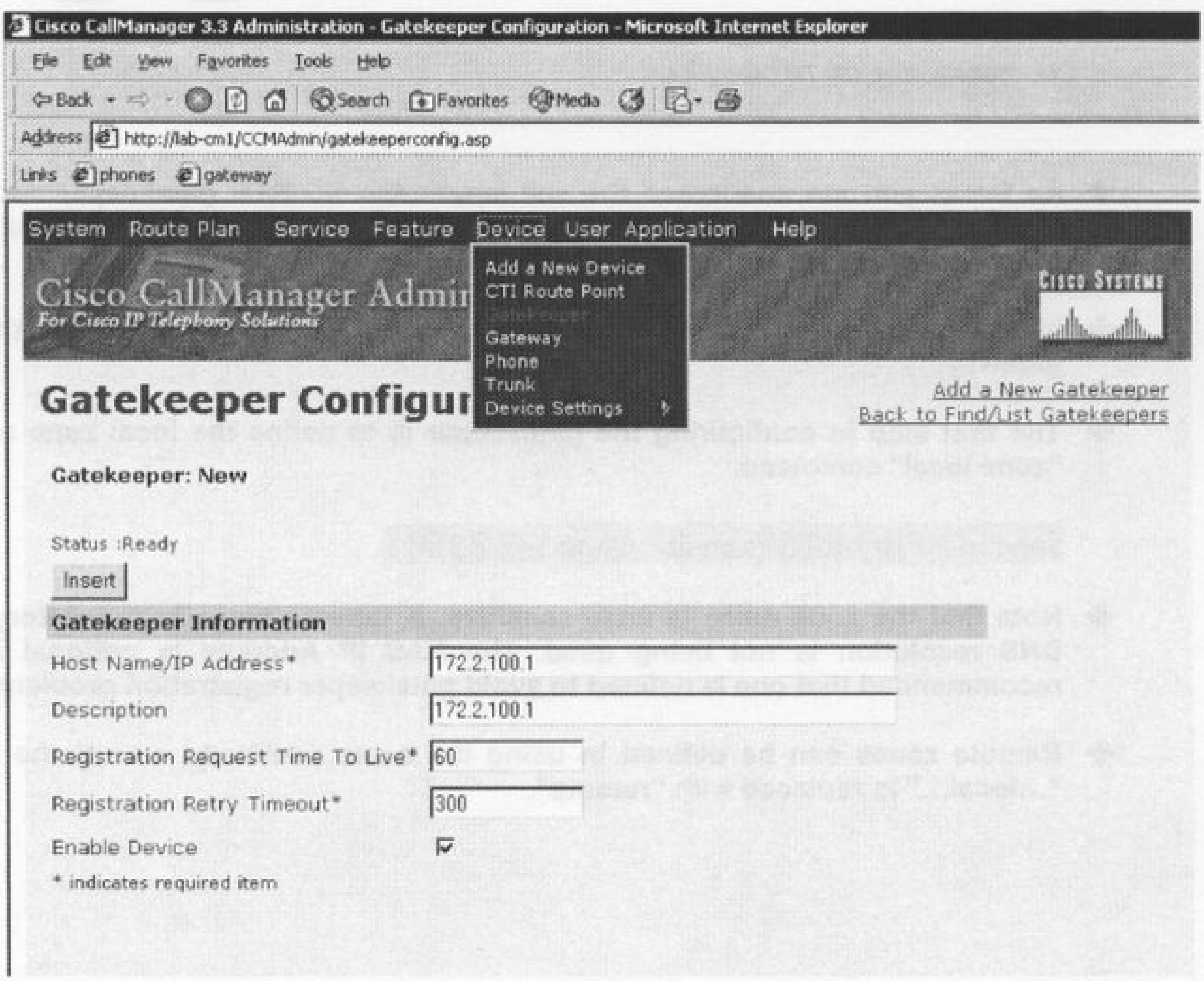
➔ **The configuration for this particular question is displayed below.**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.2.100.1
 zone remote PSTN-WAN ipexpert.com 10.2.200.2 1719
 no shutdown
```

➔ **Inside the gatekeeper we have to define a default technology prefix of 1#.**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.2.100.1
 zone remote PSTN-WAN ipexpert.com 10.2.200.2 1719
gw-type-prefix 1# default-technology
 no shutdown
```

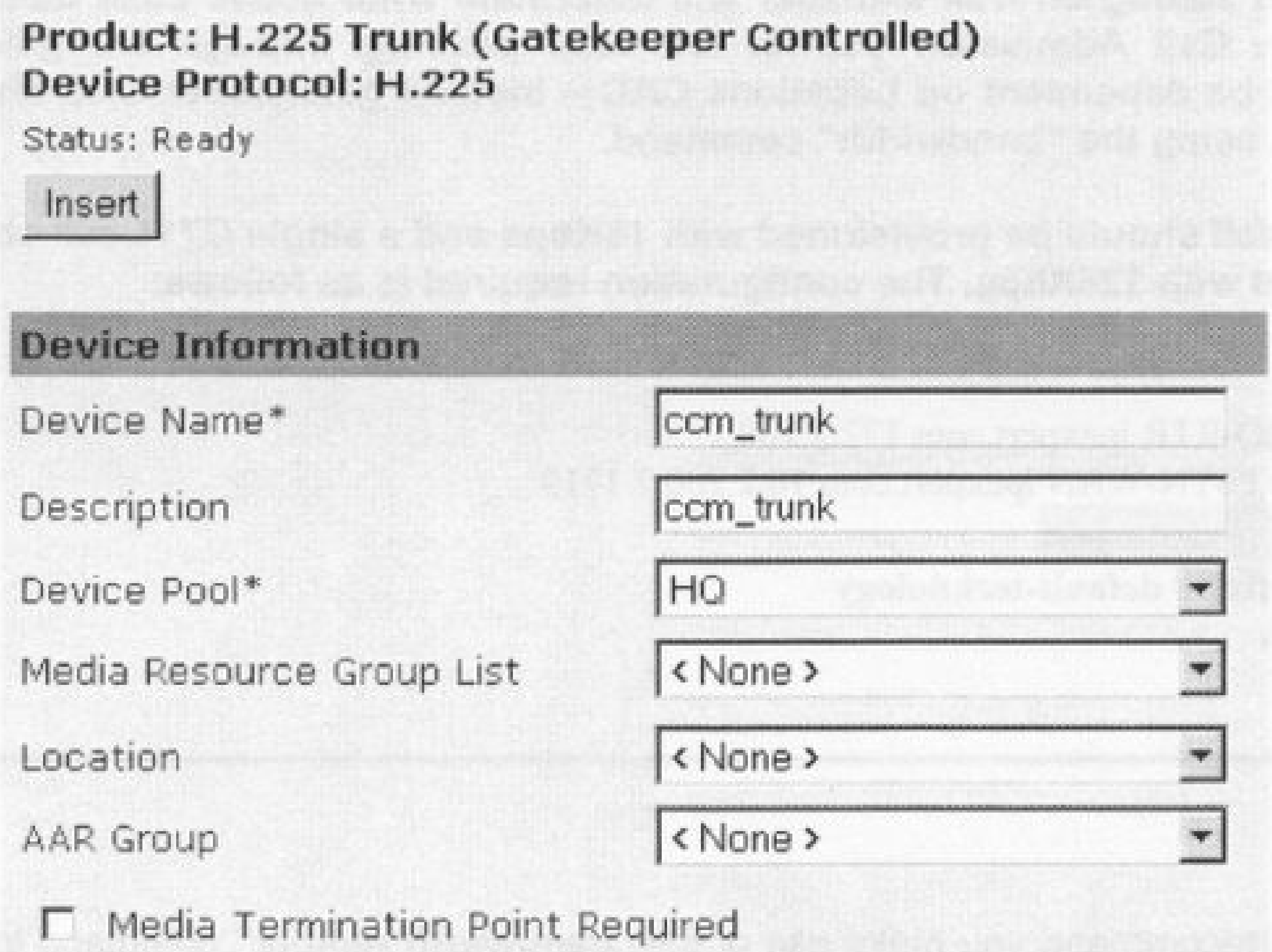
➔ **Configure a Gatekeeper – use the same IP Address as defined at the end of the "zone local..." line in gatekeeper. You may want to bring the Registration Retry Timeout to a value less than 5 minutes - this will save you from having to reset trunk after making configuration changes on gatekeeper which require the gatekeeper to be restarted.**



➔ **From Device-Trunk add a H225 Trunk (Gatekeeper Controlled) and give it a unique name. Also don't forget to set Device Pool and Location information. The Location should be the unrestricted location (either None or HQ) and the Device Pool should contain the relevant region setting.**

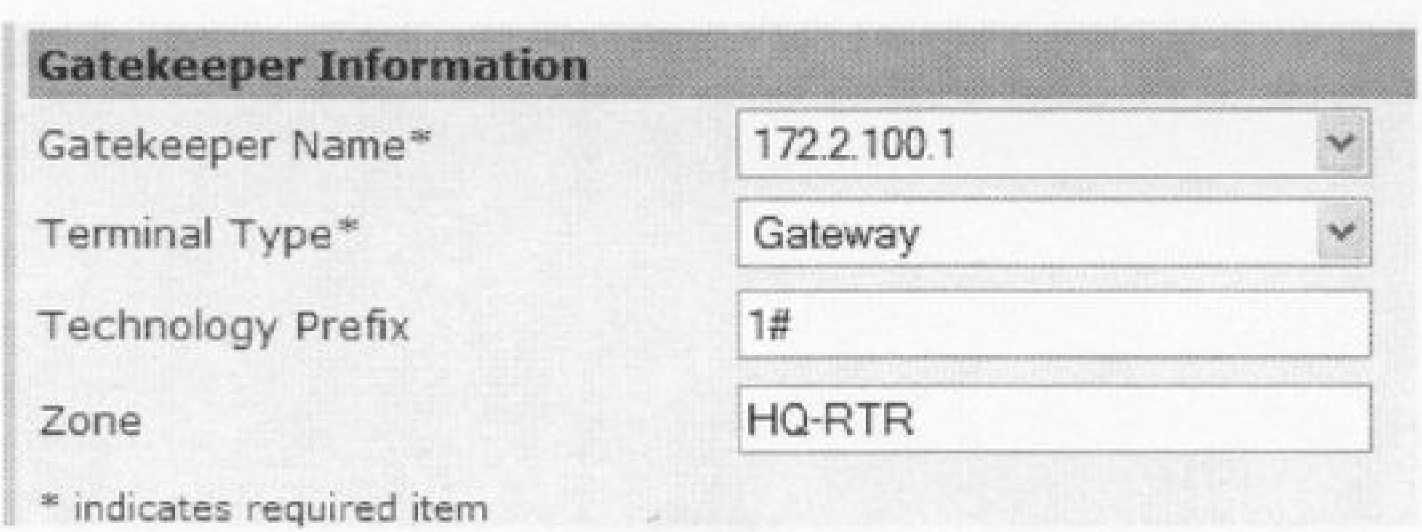
NOTE:

- We recommend you avoid using gatekeeper CAC at the same time as Locations based CAC – think of the gatekeeper as sitting in the WAN and not on any particular LAN even though it is physically configured on the HQ router. Using more than one method of CAC is redundant and un-needed and only causes more headache when trying to troubleshoot a problem – not to mention that they each use a different number for bandwidth and that alone can be confusing.



➔ **In the Call Routing section of the Trunk Configuration, the same logic discussed in the Gateway section applies to the Gatekeeper Trunk.**

➔ **Be careful not to forget the parameters at the bottom of the trunk page.**



➔ **Update/Reset the trunk and verify using the registration status as shown below:**

```
P2-HQ-RTR#sh gatek end
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name     Type    Flags
--------------- ----- --------------- ----- ---------     ----    -----
10.2.200.21     64534 10.2.200.21     64535 HQ-RTR        VOIP-GW
   H323-ID: ccm_trunk_1
   Voice Capacity Max.= Avail.= Current.= 0
Total number of active registrations = 1
```

Task 5.2

Configure CAC to allow one G711 call and one G729 call.

➔ **Gatekeeper is not involved with codec selection – codec negotiation takes place between the two endpoints for example Call Manager and an IOS gateway or ATA. The Region setting on Call Manager will determine what codec calls through the gatekeeper. Call Admission control for calls passing through the gatekeeper should not be dependent on Locations CAC – instead gatekeeper CAC should be configured using the "bandwidth" command.**

➔ **One G729 call should be provisioned with 16Kbps and a single G711 call should be provisioned with 128Kbps. The configuration required is as follows:**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.2.100.1
 zone remote PSTN-WAN ipexpert.com 10.2.200.2 1719
bandwidth remote 144
gw-type-prefix 1# default-technology
 no shutdown
```

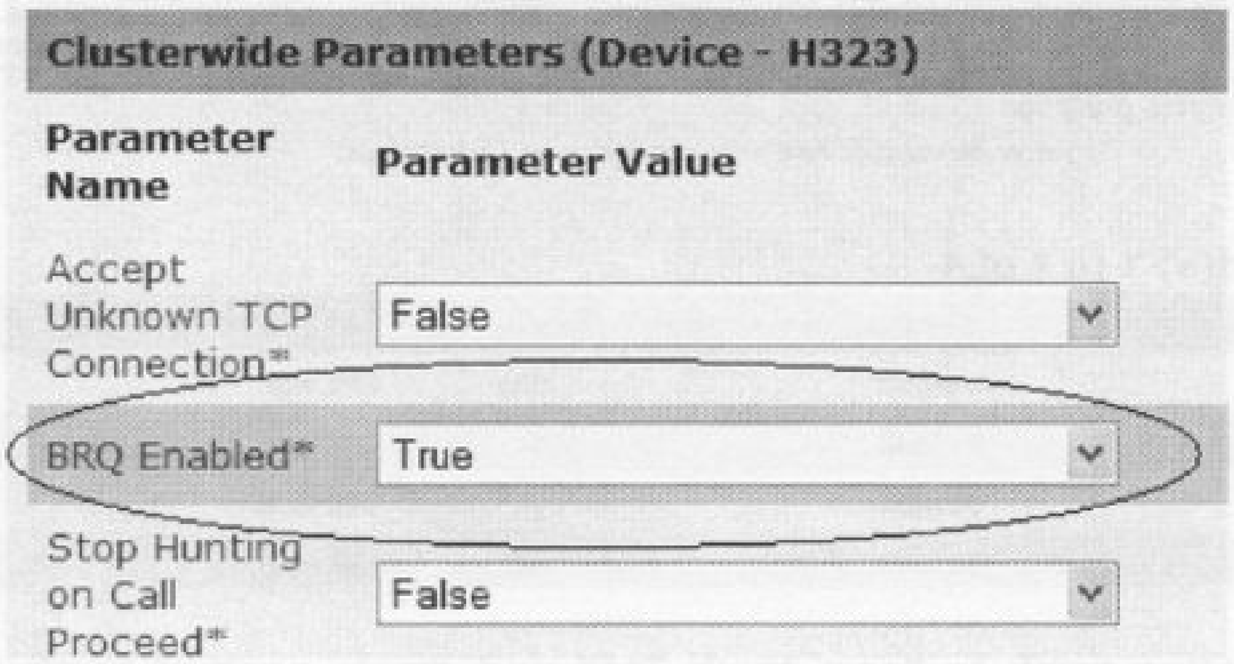
NOTE:

- We recommend you make use of the "***bandwidth remote***" command instead of using "***bandwidth total***". When gatekeeper is managing more than one zone use "***bandwidth interzone***". The "***bandwidth total***" command can cause issues in some configurations.

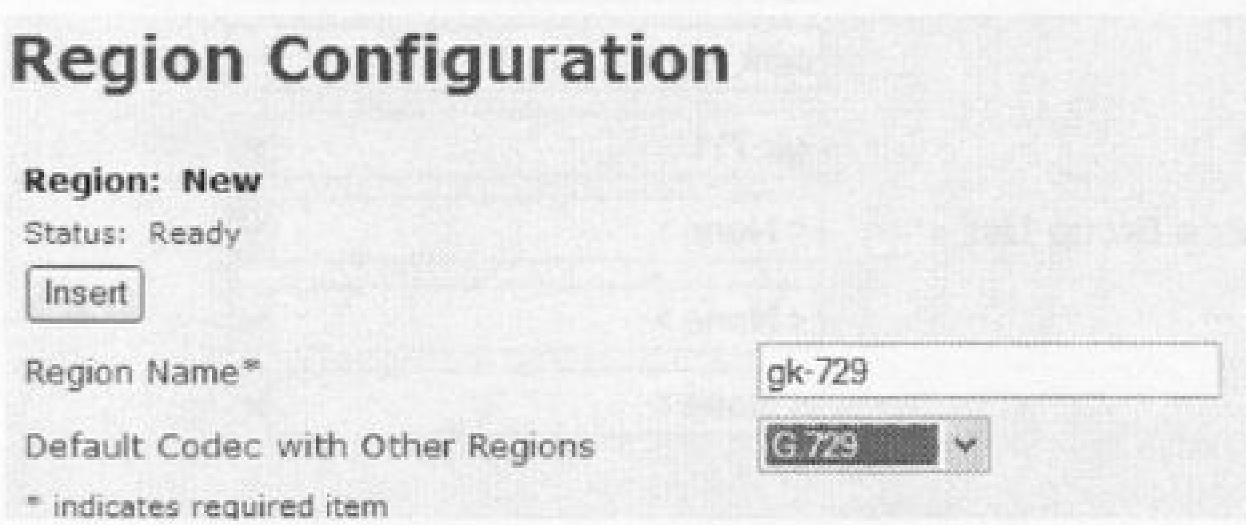
Task 5.3

Calls should attempt to use G711. If the call fails due to there not being enough bandwidth over the WAN provisioned, then the G729 codec should be selected.

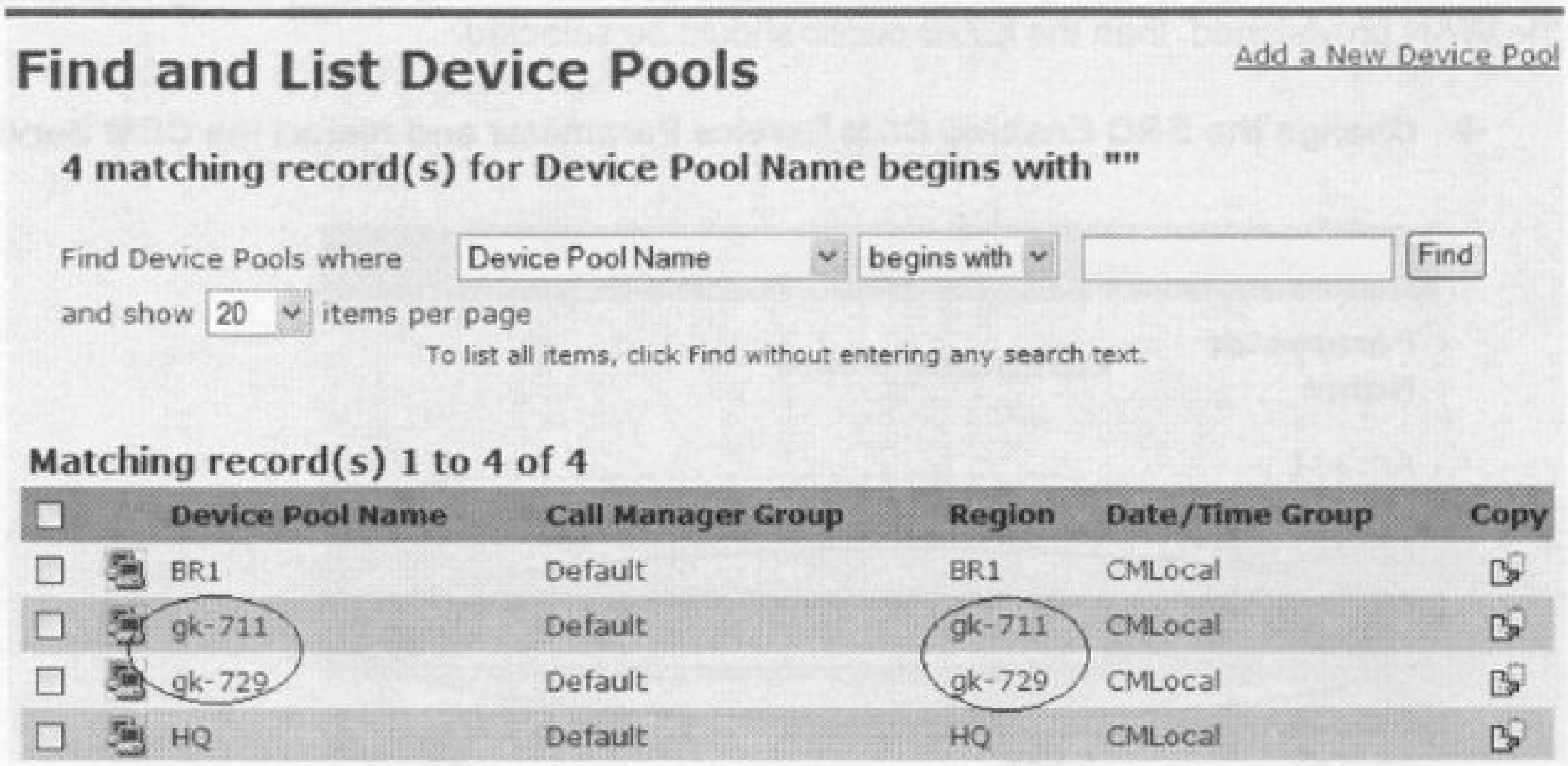
➔ **Change the BRQ Enabled CCM Service Parameter and restart the CCM Service.**



➔ **Create two new Regions and Device Pools – one that uses G711 to other Regions and one that uses G729 to other Regions.**

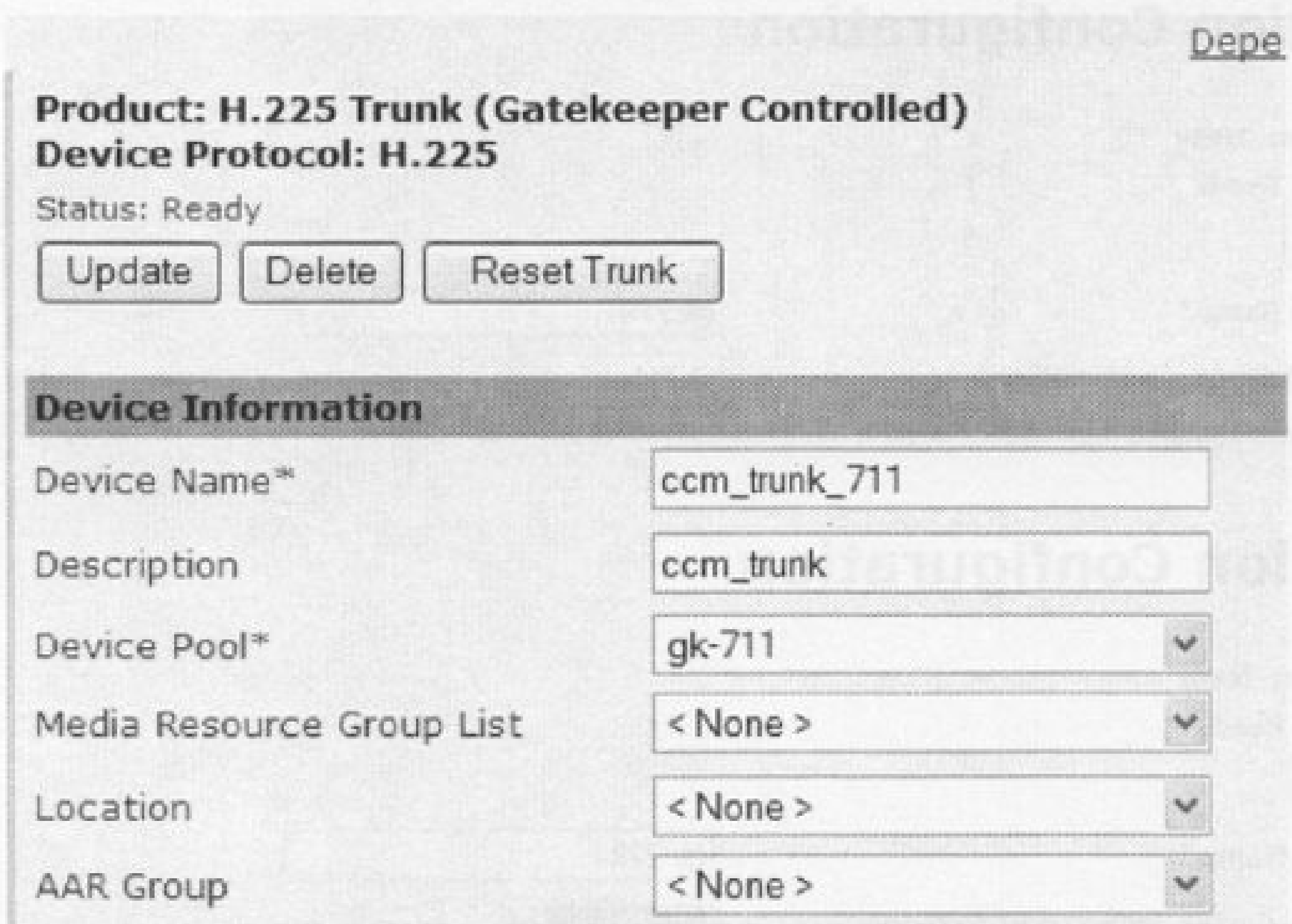


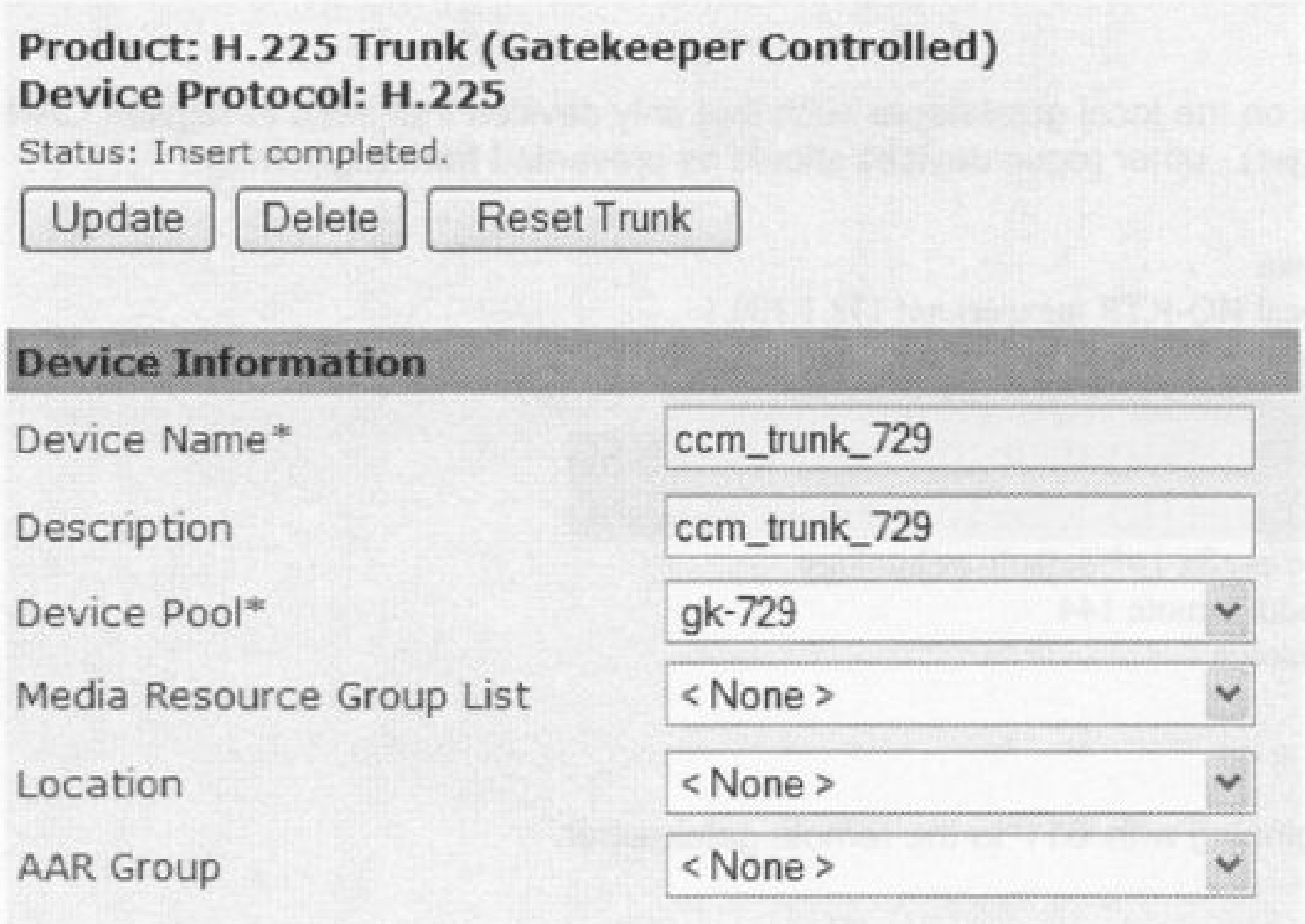
➔ **Assign these Regions to the new Device Pools - call the Device Pools GK-711 and GK-729.**



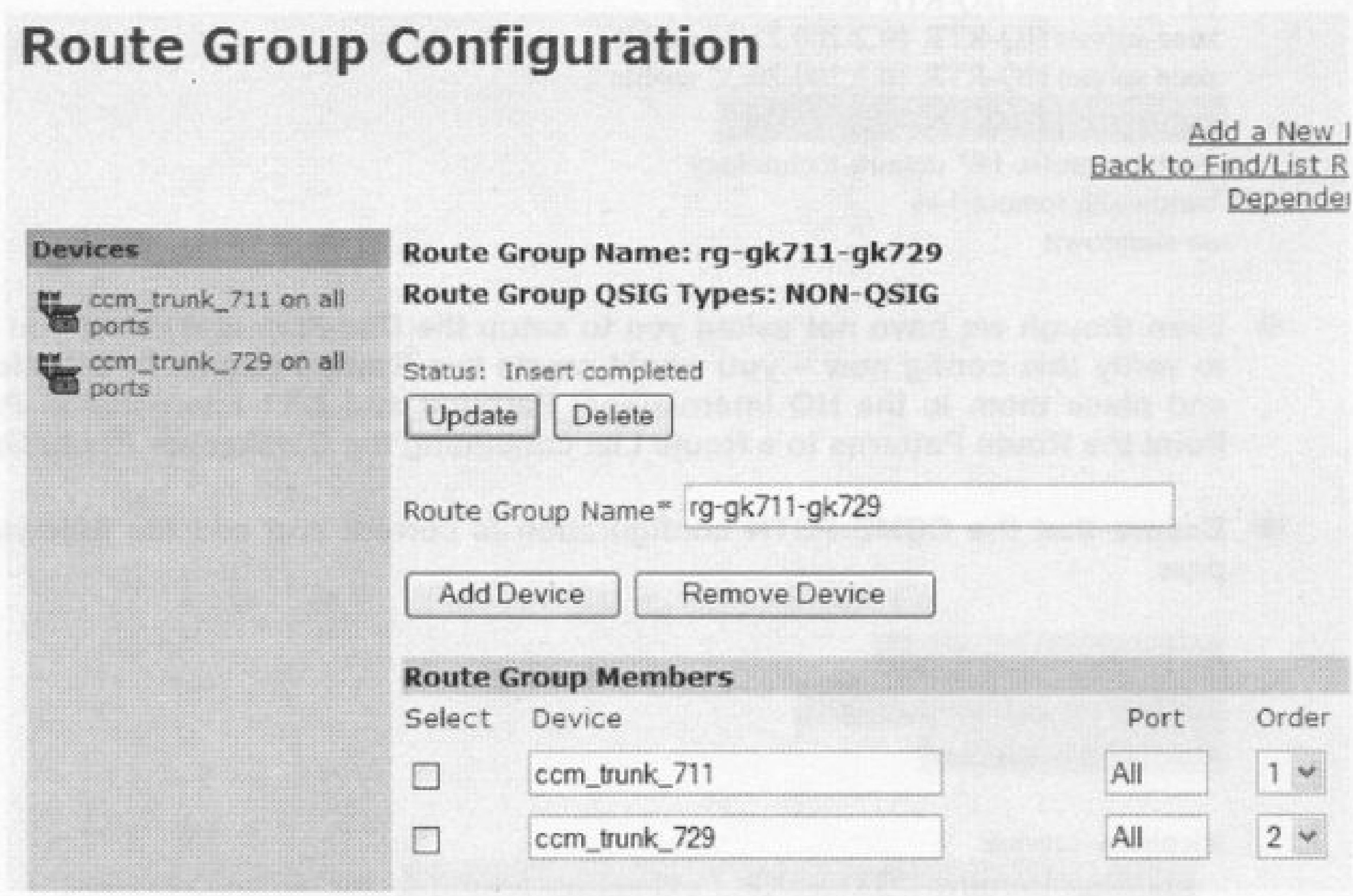
Device Pool Name	Call Manager Group	Region	Date/Time Group	Copy
BR1	Default	BR1	CMLocal	
gk-711	Default	gk-711	CMLocal	
gk-729	Default	gk-729	CMLocal	
HQ	Default	HQ	CMLocal	

➔ **Rename the existing trunk to "ccm_trunk_711" and create another trunk called "ccm_trunk_729". Assign the ccm_trunk_711 to the gk-711 Device Pool, assign the ccm_trunk_729 to the gk-729 Device Pool. Other parameters in the new trunk should be identical to the trunk created in the earlier task within this section.**





➔ **Create a Route Group as follows.**



Task 5.4

Enable security on the local gatekeeper such that only devices that need to register CAN register (e.g. CallManager) - other rogue devices should be prevented from registering.

```
gatekeeper
 zone local HQ-RTR ipexpert.net 172.1.100.1
 zone remote PSTN-WAN ipexpert.net 10.1.200.2 1719
 no zone subnet HQ-RTR default enable
 zone subnet HQ-RTR 10.1.200.21/32 enable
 zone subnet HQ-RTR 10.1.200.20/32 enable
 gw-type-prefix 1#* default-technology
 bandwidth remote 144
 no shutdown
```

Task 5.5

Route calls beginning with '011' to the remote gatekeeper.

```
gatekeeper
 zone local HQ-RTR ipexpert.net 172.2.100.1
 zone remote PSTN-WAN ipexpert.net 10.2.200.2 1719
 no zone subnet HQ-RTR default enable
 zone subnet HQ-RTR 10.2.200.21/32 enable
 zone subnet HQ-RTR 10.2.200.20/32 enable
 zone prefix PSTN-WAN 011*
 gw-type-prefix 1#* default-technology
 bandwidth remote 144
 no shutdown
```

➔ **Even though we have not asked you to setup the Dial-Plan just yet, if you wanted to verify this config now – you would create two Route Patterns in CCM for 011!# and place them in the HQ International Partition and BR1 International Partition. Point the Route Patterns to a Route List containing the Gatekeeper Route Group.**

➔ **Ensure that the CCME PSTN configuration is correct and add the following dial-peer.**

```
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial

telephony-service
   dialplan-pattern 1 33132X3... extension-length 4
```

➔ **Make a call from the HQ or BR1 phone client to the CCME phone. Turn on the debug on the HQ-RTR.**

```
P2-HQ-RTR#deb gatekeeper main 10
*Sep 14 16:38:32.768: gk_process: QUEUE_EVENT (minor 0) wakeup
*Sep 14 16:38:38.064: gk_process: QUEUE_EVENT (minor 0) wakeup
*Sep 14 16:38:38.064: gk_rassrv_arq: arqp=0x441CC2C0, crv=0x1, answerCall=0
*Sep 14 16:38:38.068: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
*Sep 14 16:38:38.068: gk_dns_query: No Name servers
```

➔ **The above output shows the ARQ message sent by the CCM. DNS is not being used.**

```
*Sep 14 16:38:38.068: rassrv_get_addrinfo: (0113313223003) Tech-prefix match failed.
*Sep 14 16:38:38.068: rassrv_get_addrinfo: (0113313223003) Matched zone prefix 011 and
remainder 3313223003
*Sep 14 16:38:38.068: rassrv_get_addrinfo: No tech prefix
*Sep 14 16:38:38.068: rassrv_get_addrinfo: Alias not found
*Sep 14 16:38:38.068: rassrv_put_remote_zones_from_zone_list: zone PSTN-WAN
```

➔ **The above output shows the digit string received by the gatekeeper. There is no Tech-Prefix but there is a Zone Prefix match to the remote zone PSTN-WAN.**

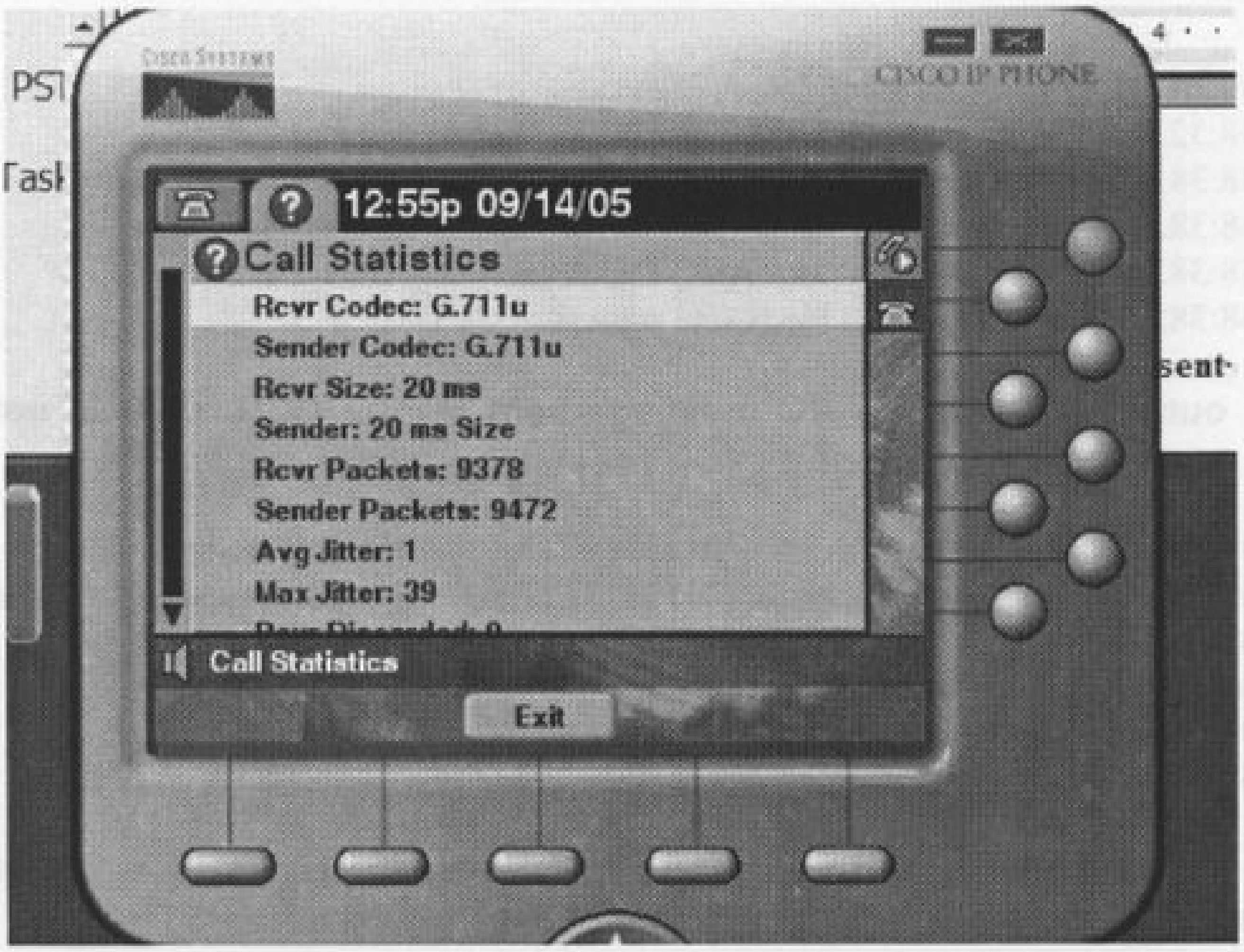
```
*Sep 14 16:38:38.068: send_lrq: seq_lrq 1, use_be 0, rzone_cnt 1
*Sep 14 16:38:38.068: send_lrq: lrq array index 0, lap 450F7EE8
*Sep 14 16:38:38.068: send_lrq: sent lrq - zonecount 1
*Sep 14 16:38:38.072: gk_process: QUEUE_EVENT (minor 0) wakeup
*Sep 14 16:38:38.072: gk_zone_get_proxy_usage: local zone= HQ-RTR, remote zone= PSTN-
WAN, call direction= 1, eptype= 2050 be_entry= 0
*Sep 14 16:38:38.072: gk_zone_get_proxy_usage: returns proxied = 0
*Sep 14 16:38:44.732: gk_process: got a TIMER event
```

➔ **The above output shows the LRQ message being sent out – proxy is not turned on.**

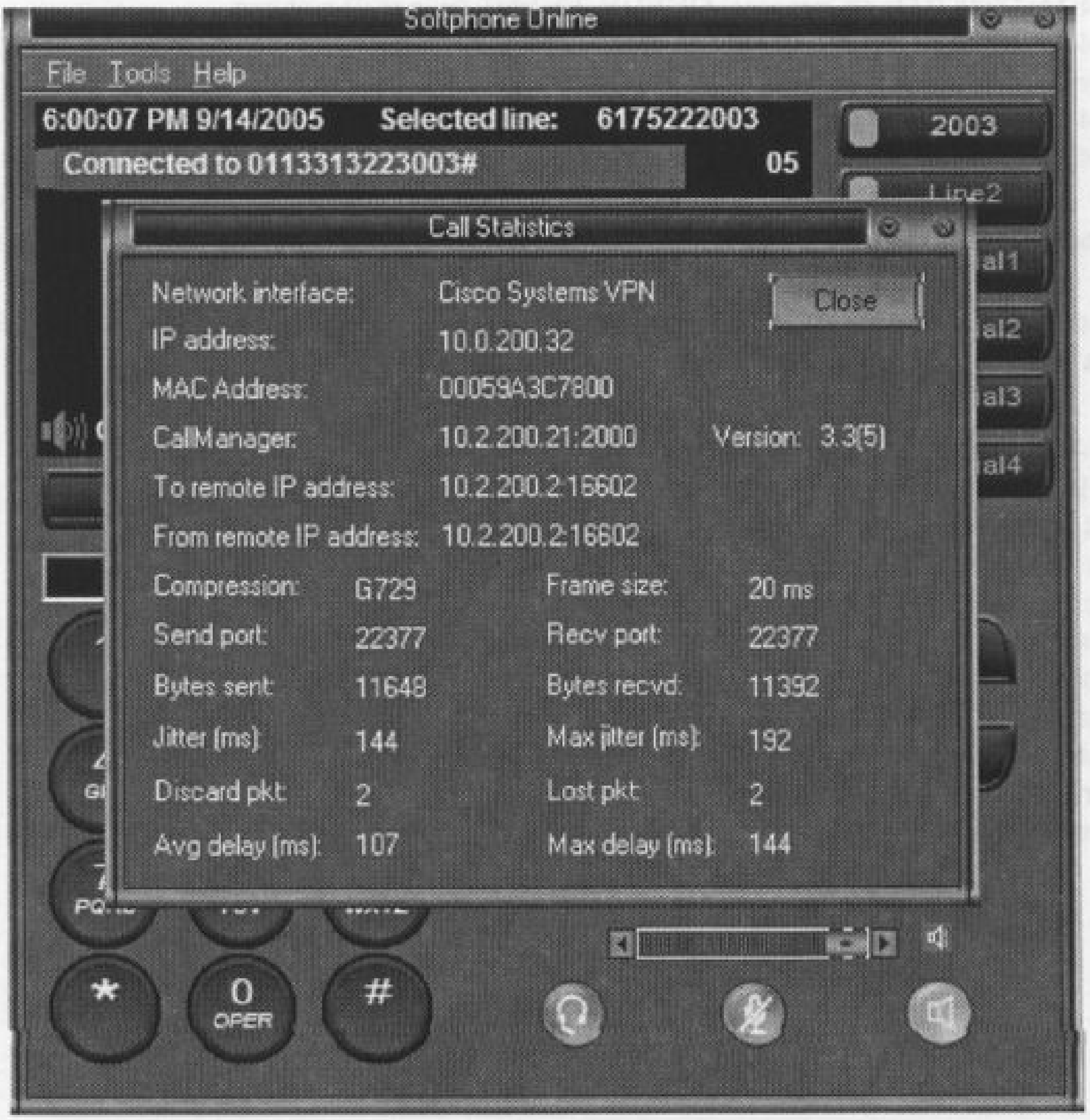
➔ **Now let's take a look at the amount of bandwidth consumed - the output below shows 128Kbps bandwidth being consumed.**

```
P2-HQ-RTR#sh gatek status
   Gatekeeper State: UP
   Load Balancing:   DISABLED
   Flow Control:     DISABLED
   Zone Name:        HQ-RTR
   Accounting:       DISABLED
   Endpoint Throttling:      DISABLED
   Security:         DISABLED
   Maximum Remote Bandwidth:           144 kbps
   Current Remote Bandwidth:          128 kbps
   Current Remote Bandwidth (w/ Alt GKs): 128 kbps
```


➔ **Similarly pressing the '?' button twice on the IP phone will display codec.**



➔ **Now it is time to make the second call – we are hoping that the call will succeed which would have meant G729 would be the codec used.**



➔ **Verify on the gatekeeper.**

```
P2-HQ-RTR#sh gatek stat
   Gatekeeper State: UP
   Load Balancing:  DISABLED
   Flow Control:   DISABLED
   Zone Name:     HQ-RTR
   Accounting:    DISABLED
   Endpoint Throttling:     DISABLED
   Security:     DISABLED
   Maximum Remote Bandwidth:          144 kbps
   Current Remote Bandwidth:          144 kbps
   Current Remote Bandwidth (w/ Alt GKs): 144 kbps
```

Task 5.6

Add on to your Gatekeeper configuration and create a new zone to enable the GK to route calls through your IPIPGW located on the same HQ-RTR. Allow your ATA to register with a new DN of 2080 to the GK in a new local zone. Ensure that calls from CCM routed to the ATA will succeed and terminate both sides of their RTP stream via the IPIPGW. Also Ensure the call comes from CCM in a G711 format and flows to the ATA using a G729 codec.

New Local zone for CCM = CCM-GK
domain name = ipexpert.com

New Local zone for IPIPGW = VGK
domain name = ipexpert.com

New Local zone for ATA = ATA-GK
domain name = ipexpert.com

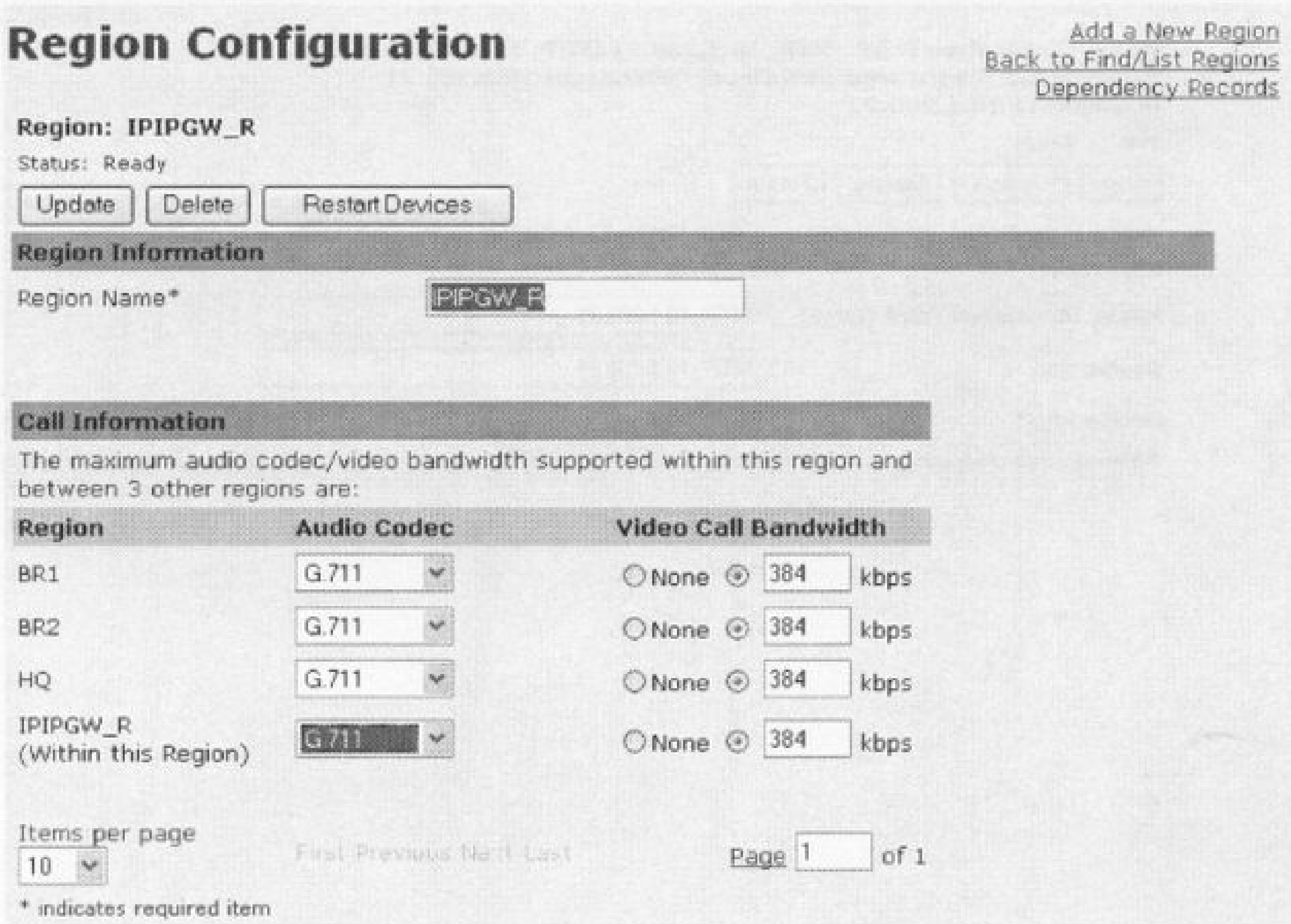
➔ **On HQ-RTR**

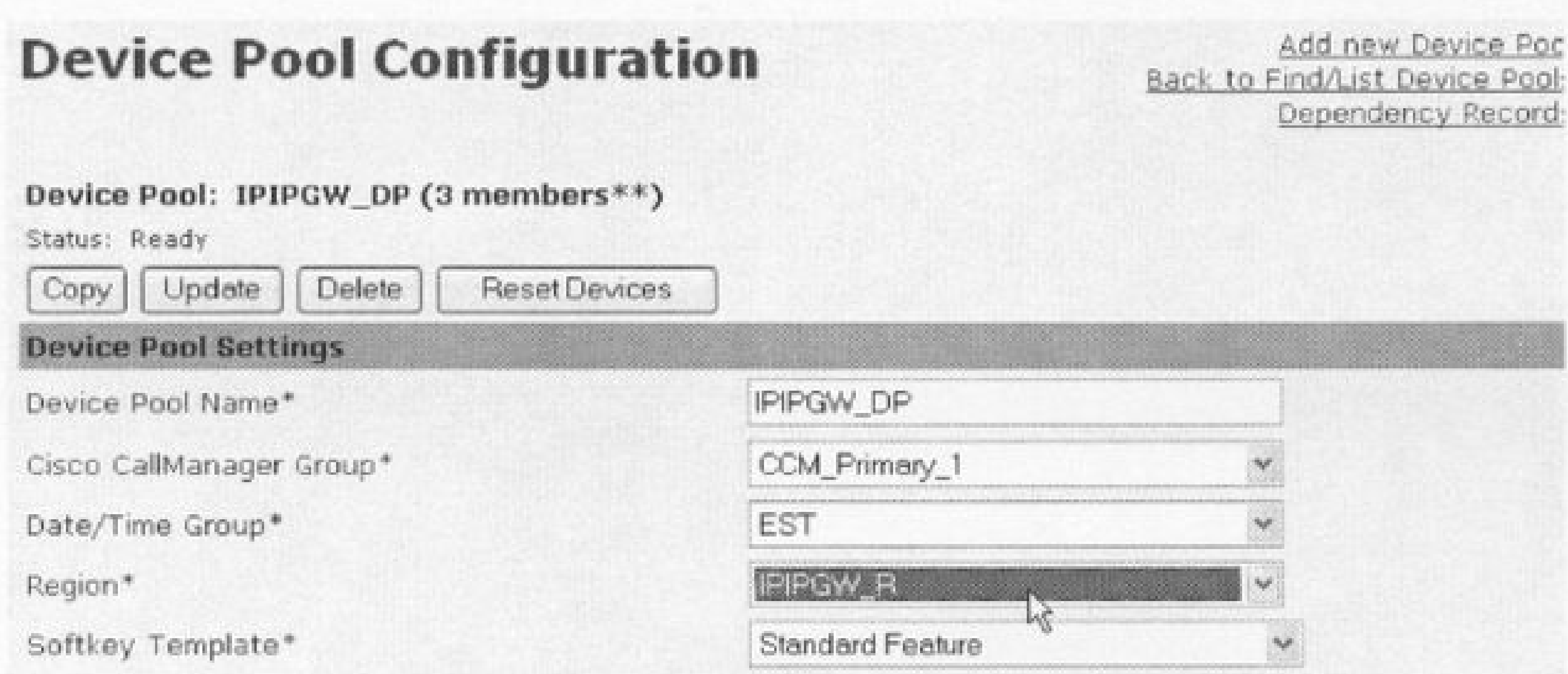
```
voice service voip
 allow-connections h323 to h323
!
interface Loopback0
 ip address 172.1.100.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id VGK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip bind srcaddr 172.1.100.1
!
dial-peer voice 10 voip
 destination-pattern 2080
 session target ras
!
dial-peer voice 12 voip
 destination-pattern 1...
 session target ras
```

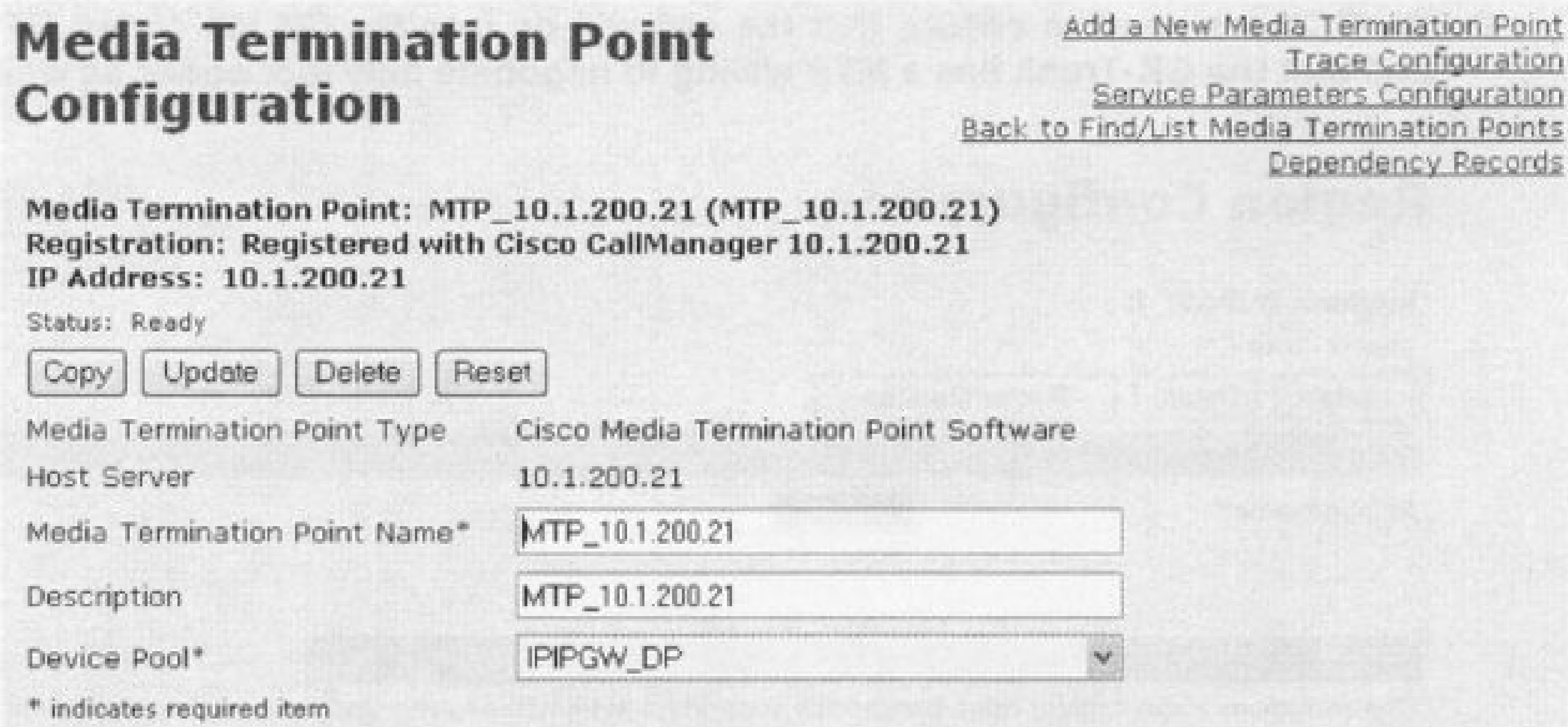


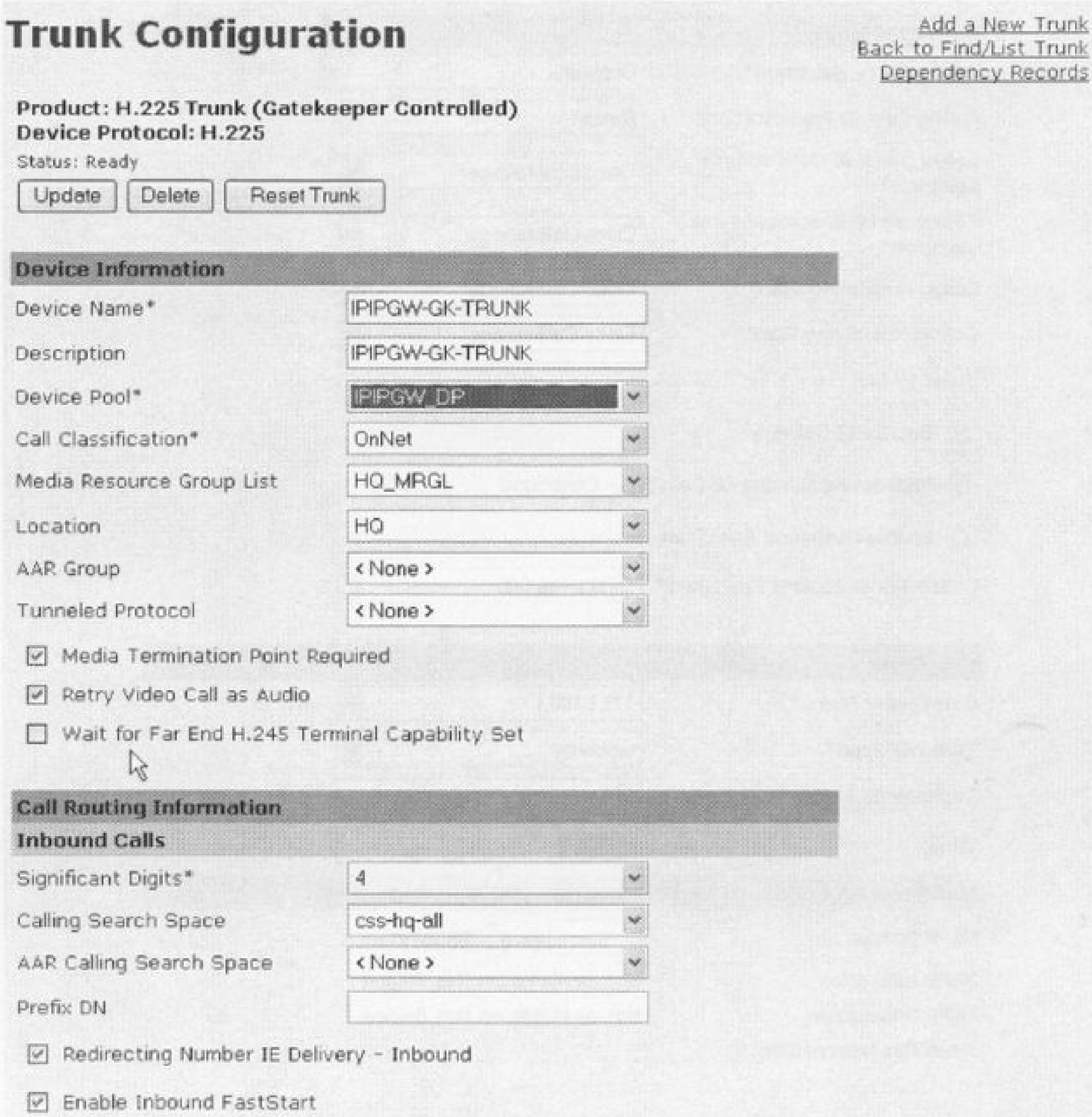
```
codec g711ulaw
!
gateway
!
!
gatekeeper
 zone local VGK ipexpert.com 172.1.100.1
 zone local ATA-GK ipexpert.com invia VGK outvia VGK enable-intrazone
 zone local CCM-GK ipexpert.com
 zone prefix ATA-GK 208.
 no use-proxy ATA-GK default inbound-to terminal
 no use-proxy ATA-GK default outbound-from terminal
 no shutdown
!
voice-card 2
 no dspfarm
 dsp services dspfarm
!
sccp local FastEthernet0/0.210
sccp ccm 10.1.200.3 identifier 1
sccp ip precedence 3
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCODER
 keepalive retries 5
 switchover method immediate
 switchback interval 15
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g729ar8
 codec g729abr8
 maximum sessions 2
 associate application SCCP
 no shutdown
!
call-manager-fallback
 ip source-address 10.1.200.3 port 2000
 max-ephones 10
 max-dn 10
 sdspfarm units 1
 sdspfarm transcode sessions 2
```

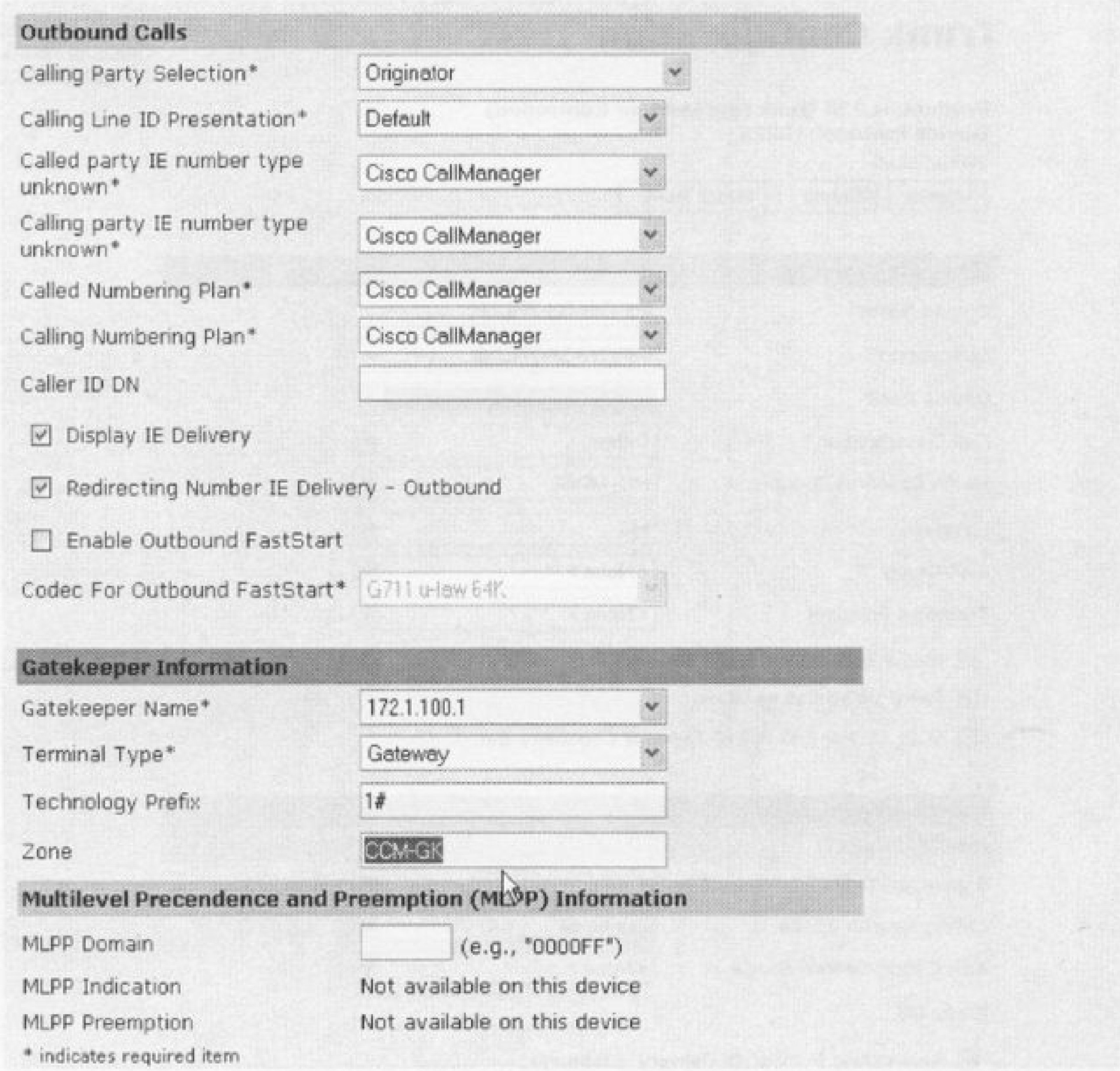
➔ **On CCM we need to ensure that the call will go into the GK via codec G711ulaw, and that the GK-Trunk has a MTP willing to negotiate only that codec as well**






Media Termination Point Configuration
Add a New Media Termination Point
Trace Configuration
Service Parameters Configuration
Back to Find/List Media Termination Points
Dependency Records
Media Termination Point: MTP_10.1.200.21 (MTP_10.1.200.21)
Registration: Registered with Cisco CallManager 10.1.200.21
IP Address: 10.1.200.21
Status: Ready
Copy
Update
Delete
Reset
Media Termination Point Type
Cisco Media Termination Point Software
Host Server
10.1.200.21
Media Termination Point Name*
MTP_10.1.200.21
Description
MTP_10.1.200.21
Device Pool*
IPIPGW_DP
* indicates required item


Trunk Configuration
Add a New Trunk
Back to Find/List Trunk
Dependency Records
Product: H.225 Trunk (Gatekeeper Controlled)
Device Protocol: H.225
Status: Ready
Update
Delete
Reset Trunk
Device Information
Device Name* IPIPGW-GK-TRUNK
Description IPIPGW-GK-TRUNK
Device Pool* IPIPGW_DP
Call Classification* OnNet
Media Resource Group List HQ_MRGL
Location HQ
AAR Group < None >
Tunneled Protocol < None >
Media Termination Point Required
Retry Video Call as Audio
Wait for Far End H.245 Terminal Capability Set
Call Routing Information
Inbound Calls
Significant Digits* 4
Calling Search Space css-hq-all
AAR Calling Search Space < None >
Prefix DN
Redirecting Number IE Delivery - Inbound
Enable Inbound FastStart



Outbound Calls

Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Caller ID DN	

- [x] Display IE Delivery
- [x] Redirecting Number IE Delivery - Outbound
- [ ] Enable Outbound FastStart

Codec For Outbound FastStart*	G711 u-law 64K

Gatekeeper Information

Gatekeeper Name*	172.1.100.1
Terminal Type*	Gateway
Technology Prefix	1#
Zone	CCM-GK

Multilevel Precendence and Preemption (MLPP) Information

MLPP Domain	(e.g., "0000FF")
MLPP Indication	Not available on this device
MLPP Preemption	Not available on this device

* indicates required item

➔ **Config from ATA H323 (http://IPAddressofATA/dev)**

Cisco ATA 186 (H323) Configuration

UIPassword:	*	UseTftp:	0
TftpURL:	*	CfgInterval:	3600
EncryptKey:	*	EncryptKeyEx:	0000000000000000000000
Dhcp:	1	StaticIP:	0.0.0.0
StaticRoute:	0.0.0.0	StaticNetMask:	255.255.255.0
UID0:	2080	PWD0:	*
UID1:	0	PWD1:	*
GkOrProxy:	172.1.100.1	Gateway:	0
UseLoginID:	0	LoginID0:	0
LoginID1:	0	AltGk:	0
AltGkTimeOut:	0	GkTimeToLive:	300
GkId:	ATA-GK	NATIP:	0.0.0.0
MediaPort:	16384	LBRCodec:	3
AudioMode:	0x00140014	RxCodec:	2
TxCodec:	2	NumTxFrames:	2
CallFeatures:	0xffffffff	PaidFeatures:	0xffffffff
CallerIdMethod:	0x00019e60	FeatureTimer:	0x00000000

➔ **Back on HQ-RTR we need to verify and send the call to test**

```
P1-HQ-RTR#sh gatek end
          GATEKEEPER ENDPOINT REGISTRATION
          ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name    Type    Flags
--------------- ----- --------------- ----- ---------    ----    -----
10.1.200.21     54080 10.1.200.21     49358 CCM-GK       VOIP-GW
   H323-ID: IPIPGW-GK-TRUNK_1
   Voice Capacity Max.=  Avail.=  Current.= 0
172.1.100.1     1720  172.1.100.1     53849 VGK          H323-GW
   H323-ID: IPIPGW
   Voice Capacity Max.=  Avail.=  Current.= 0
192.168.15.27   1720  192.168.15.27   1719  ATA-GK       TERM
   E164-ID: 2080
Total number of active registrations = 3
```

P1-HQ-RTR#debug gatek main 10
May 22 17:13:34.065: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 17:13:34.069: gk_rassrv_arq: arqp=0x45EB45F4, crv=0x2, answerCall=0
May 22 17:13:34.069: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
May 22 17:13:34.069: gk_dns_query: No Name servers
May 22 17:13:34.069: rassrv_get_addrinfo: (2080) Tech-prefix match failed.
May 22 17:13:34.069: rassrv_get_addrinfo: (2080) Matched zone prefix 208 and remainder 0
May 22 17:13:34.069: gk_rassrv_get_ingress_network: returning default ingress network = 1
May 22 17:13:34.069: rassrv_arq_select_viazone: about to check the source side, src_zonep=0x476A44B0
May 22 17:13:34.069: rassrv_arq_select_viazone: matched zone is CCM-GK, and z_invianamelen=0
May 22 17:13:34.069: rassrv_arq_select_viazone: about to check the destination side, dst_zonep=0x45E91214
May 22 17:13:34.069: rassrv_arq_select_viazone: matched zone is ATA-GK, and z_outvianamelen=3
May 22 17:13:34.069: rassrv_arq_select_viazone and z_outvianamep=VGK
May 22 1
P1-HQ-RTR#7:13:34.069: rassrv_arq_select_viazone: Received ARQ for a zone (ATA-GK) that has an outviazone (VGK) specified. Pick an IP-IP gateway in that viazone.
May 22 17:13:34.069: gk_gw_select_ipipgw: zonep: 0x4724ED54, tpp: 0x0, current_endpt: 1
May 22 17:13:34.069: gk_gw_select_ipipgw: Selecting any IPIPGW. qelemp.head=0x472C0BB0, use_count=1, current_endpt=1
May 22 17:13:34.069: gk_gw_select_ipipgw: Gateway selection will start at the top of the linked list. use_count=1, current_endpt=0
May 22 17:13:34.069: gk_gw_select_ipipgw: qelemp=0x472C0BB0, loop_count=0
May 22 17:13:34.069: gk_gw_select_ipipgw: Examining tgwp 0x472B0E60, g_supp_prots: 0x50 qelemp: 0x472C0BB0, loop_count: 1
May 22 17:13:34.069: gk_gw_select_ipipgw: Found an IPIPGW. tgwp: 0x472B0E60, endptsigIP: 172.1.100.1, endptrasIP: 172.1.100.1, zone: VGK
May 22 17:13:34.069: gk_gw_select_ipipgw: Selected an IPIPGW.
May 22 17:13:34.069: rassrv_get_addrinfo: (2080) successfully resolved IPIPGW and returning with return code 0
May 22 17:13:34.089: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 17:13:34.089: gk_rassrv_arq: arqp=0x45F11B10, crv=0x25, answerCall=1
May 22 17:13:34.089: gk_rassrv_dep_arq: ARQ Didn't use GK_AAA_PROC
May 22 17:13:34.105: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 17:13:34.105: gk_rassrv_arq: arqp=0x45F11B10, crv=0x26, answerCall=0
May 22 17:13:34.105: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
May 22 17:13:34.105: gk_dns_query: No Name servers
May 22 17:13:34.105: rassrv_get_addrinfo: (2080) Tech-prefix match failed.
May 22 17:13:34.105: rassrv_get_addrinfo: (2080) Matched zone prefix 208 and remainder 0
May 22 17:13:34.105: gk_rassrv_get_ingress_network: ARQ non-std ingress network = 2
May 22 17:13:34.105: rassrv_arq_select_viazone: about to check the destination side, dst_zonep=0x45E91214
May 22 17:13:34.105: rassrv_arq_select_viazone: matched zone is ATA-GK, and z_outvianamelen=3
May 22 17:13:34.105: rassrv_arq_select_viazone and z_outvianamep=VGK
May 22 17:13:34.105: rassrv_arq_select_viazone: Received ARQ for a zone (ATA-GK) that has an outviazone (VGK) specified, but I am that viazone. Continue normal ARQ processing
May 22 17:13:34.105: gk_zone_get_proxy_usage: local zone= ATA-GK, remote zone= VGK, call direction= 0, eptype= 2056 be_entry= 0
May 22 17:13:34.105: gk_zone_get_proxy_usage: returns proxied = 0
May 22 17:13:34.105: gk_gw_select_px: Source and destination endpoints in different local zones

May 22 17:13:34.105: gk_zone_get_proxy_usage: local zone= VGK, remote zone= ATA-GK, call direction= 1, eptype= 2114 be_entry= 0
May 22 17:13:34.109: gk_zone_get_proxy_usage: returns proxied = 0
May 22 17:13:34.109: rassrv_get_addrinfo: (2080) successfully resolved the alias locally and returning with 0x0
May 22 17:13:34.109: rassrv_get_addrinfo: We know this alias

May 22 17:13:34.241: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 17:13:34.245: gk_rassrv_arq: arqp=0x4768D4F8, crv=0x26, answerCall=1
May 22 17:13:34.245: gk_rassrv_dep_arq: ARQ Didn't use GK_AAA_PROC
May 22 17:13:35.513: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 17:13:35.517: gk_rassrv_irr: irrp=0x45E9887C, from 172.1.100.1:53849
May 22 17:13:35.521: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 17:13:35.525: gk_rassrv_irr: irrp=0x45E9887C, from 172.1.100.1:53849
May 22 17:13:37.089: gk_process: QUEUE_EVENT (minor 0) wakeup

```
P1-HQ-RTR#sh voip rtp connections
VoIP RTP active connections :
No. CallId dstCallId LocalRTP RmtRTP LocalIP        RemoteIP
1  45     46       17090   24598 172.1.100.1    10.1.200.21
2  46     45       18154   16384 172.1.100.1    192.168.15.27
3  47     48       16764   2000  10.1.200.3     10.1.200.3
4  49     48       19290   2000  10.1.200.3     10.1.200.3
Found 4 active RTP connections
P1-HQ-RTR#
```

```
P1-HQ-RTR#sh sdspfarm sessions active
Stream-ID:3 mtp:1 10.1.200.3  18214  Local:2000 START
 usage: Ip-Ip
 codec:G729  duration:20 vad:0 peer Stream-ID:4

Stream-ID:4 mtp:1 10.1.200.3  16754  Local:2000 START
 usage: Ip-Ip
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:3
P1-HQ-RTR#
```


Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 6: Dial Plan

Estimated Time to Complete: <u>4 hours</u>

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 6 Dial Plan

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure Section 1 must be completed along with the basic sections of Call Manager and CCME. The Gateway and Gatekeeper sections must also be completed.

Before proceeding with this task, place each gateway into a Route Group of its own (in addition to the GK Route Group created in the previous section).

The solutions and discussion to this section can be found at the end of this section.

Section 6 Configuration Tasks

Task 6.1

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

Task 6.2

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

Task 6.3

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed first out of the local Gatekeeper and then through the HQ-IPIPGW as a backup. Users must be able to dial the BR2 site using extension (4 digit) dialing. (**Test both** call routing methods one at a time before moving on to the next question).

Task 6.4

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway. You must 4 different types of methods to manipulate the digits sent to the PSTN (e.g. one method is by using the 'forward-digits' command inside the POTS dial-peer).

Task 6.5

Calls originating from BR2 to CallManager (both HQ and BR1) should use VoIP through the HQ IPIPGW and the PSTN as backup. 4-digit dialing must be preserved. Also, you must use the minimum amount of dial-peers possible.

Task 6.6

Enable DID for PSTN users dialing into the CM/CME (i.e. 2-stage dialing must not be used).

➔ **When implementing a dial plan it is a good idea to look at all the tasks together rather than treat each question as a separate question.**

➔ **Digit Manipulation should be done in the Route List.**

➔ **The following Route Groups should be created.**

Route Group	Gateway	Order
RG-GK	G711 GK-TRUNK	1
	G729 GK-TRUNK	2
RG-IPIPGW-ICT	H323 (non-GK controlled) InterClusterTrunk	1
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created.**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1-LOC	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-BR1-HQ-LOC	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617
RL-HQ-BR1-LD-INT	RG-HQ	PREDOT
	RG-BR1	PREDOT
RL-BR1-HQ-LD-INT	RG-BR1	PREDOT
	RG-HQ	PREDOT
RL-HQ-TOLLBY	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617
RL-BR1-TOLLBY	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-GK-ICT	RG-GK	PREFIX 01133132X
	RG-IPIPGW-ICT	

➔ **The following Route Patterns should be created.**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ-BR1-LOC
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ-LOC
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ-BR1-LD-INT
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1-HQ-LD-INT
91212.xxxxxxx	PT-BR1-LD	RL-BR1-TOLLBY
91617.xxxxxxx	PT-HQ-LD	RL-HQ-TOLLBY
9.011! 9.011!#	PT-HQ-INT	RL-HQ-BR1-LD-INT
9.011! 9.011!#	PT-BR1-INT	RL-BR1-HQ-LD-INT
3xxx	(Null PT)	RL-GK-ICT

➔ **For CCME use the following dial-peers.**

```
voice translation-rule 1
  rule 1 /^(1...\)/ /1212222\1/
  rule 2 /^(2...\)/ /1617522\1/
!
voice translation-profile PSTN-OUT
  translate called 1
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 destination-pattern 9911
corlist outgoing css-911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......T
 port 0/0/0:0
```

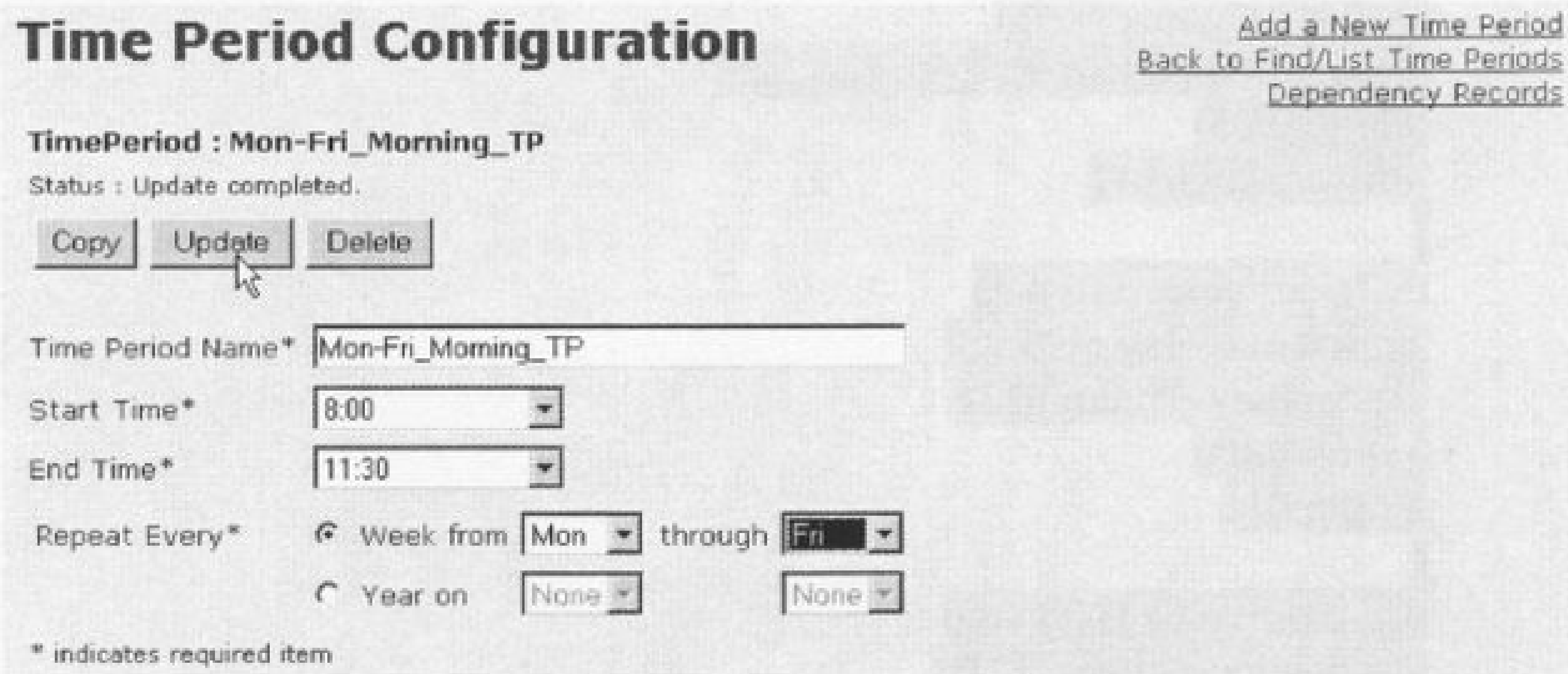
```
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1000 voip
 destination-pattern [12]...
 session target ipv4:172.1.100.1
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1001 pots
 preference 1
 destination-pattern [12]...
 port 0/0/0:0
 translation-profile outgoing PSTN-OUT
!
```

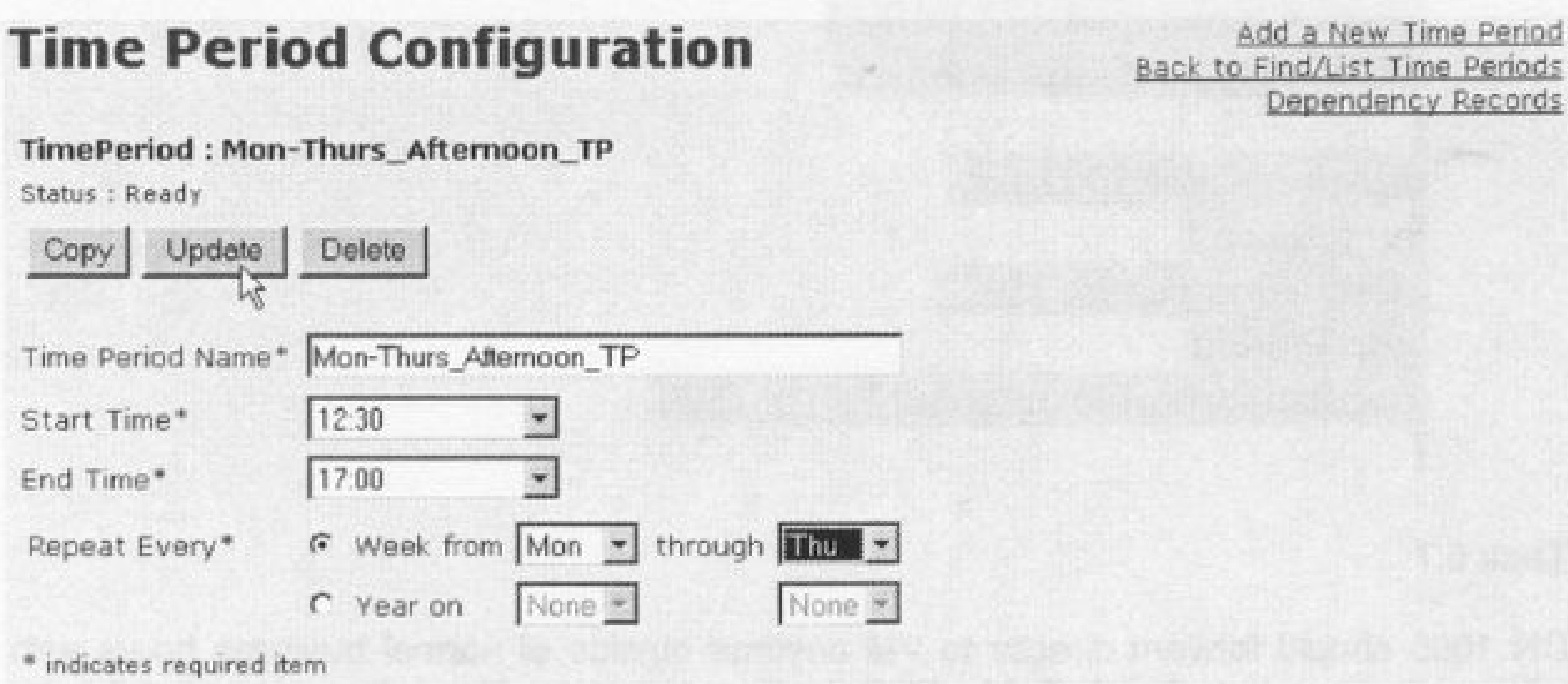
Task 6.7

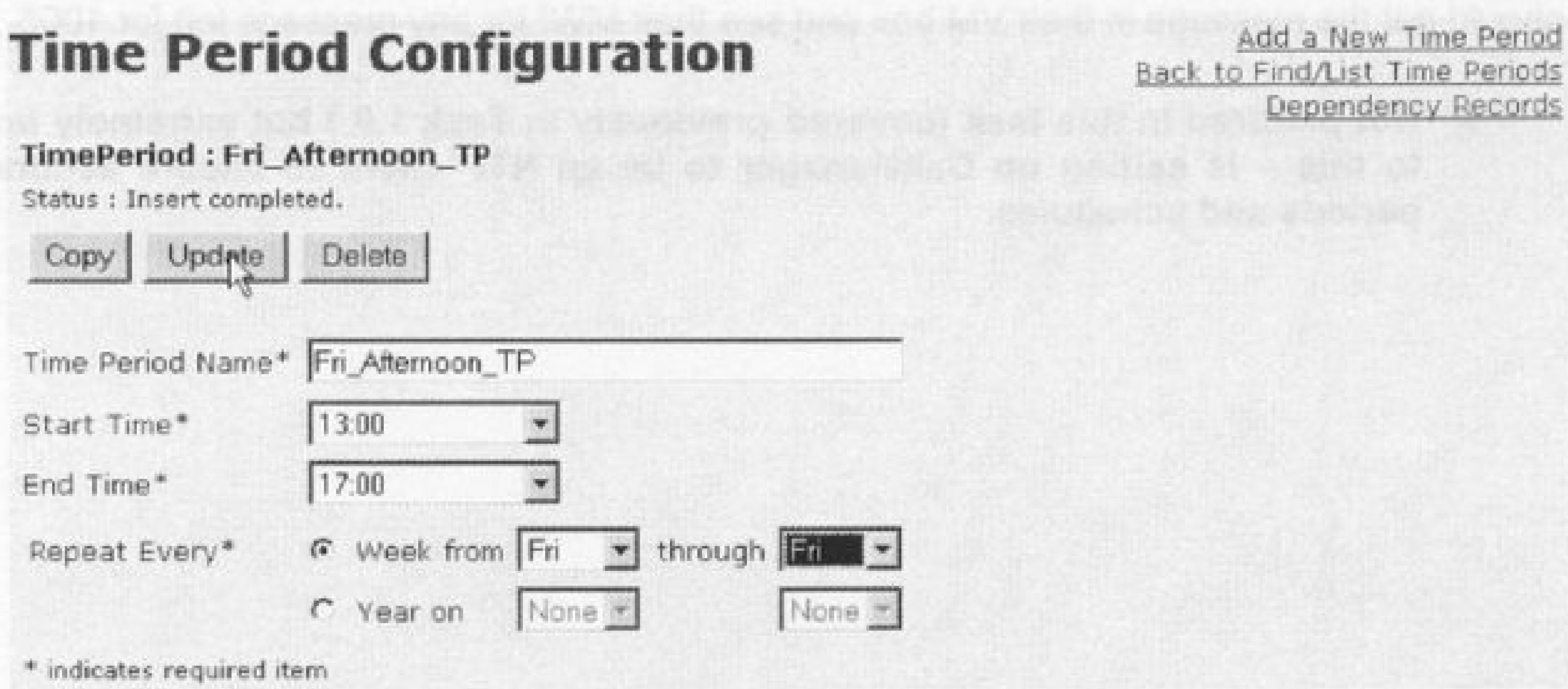
DN 1005 should forward directly to VM anytime outside of normal business hours with no user intervention needed. Check **Table 14** for a time schedule. Also, all members of this HuntGroup should get the message in their VM box and see their MWI for any message left for 1005.

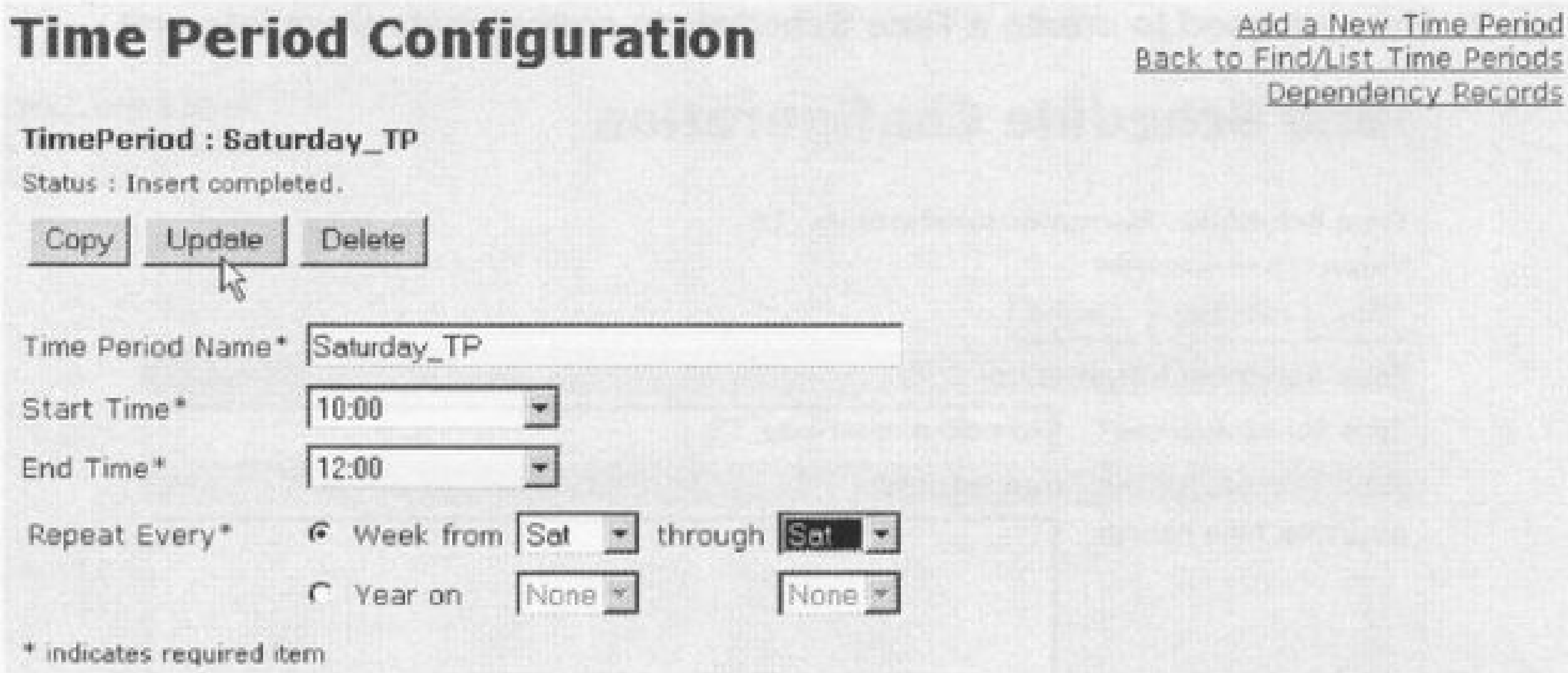
➔ **Not pictured in this task (covered previously in Task 1.6) but extremely important to this – is setting up CallManager to be an NTP client to ensure accurate time periods and schedules.**

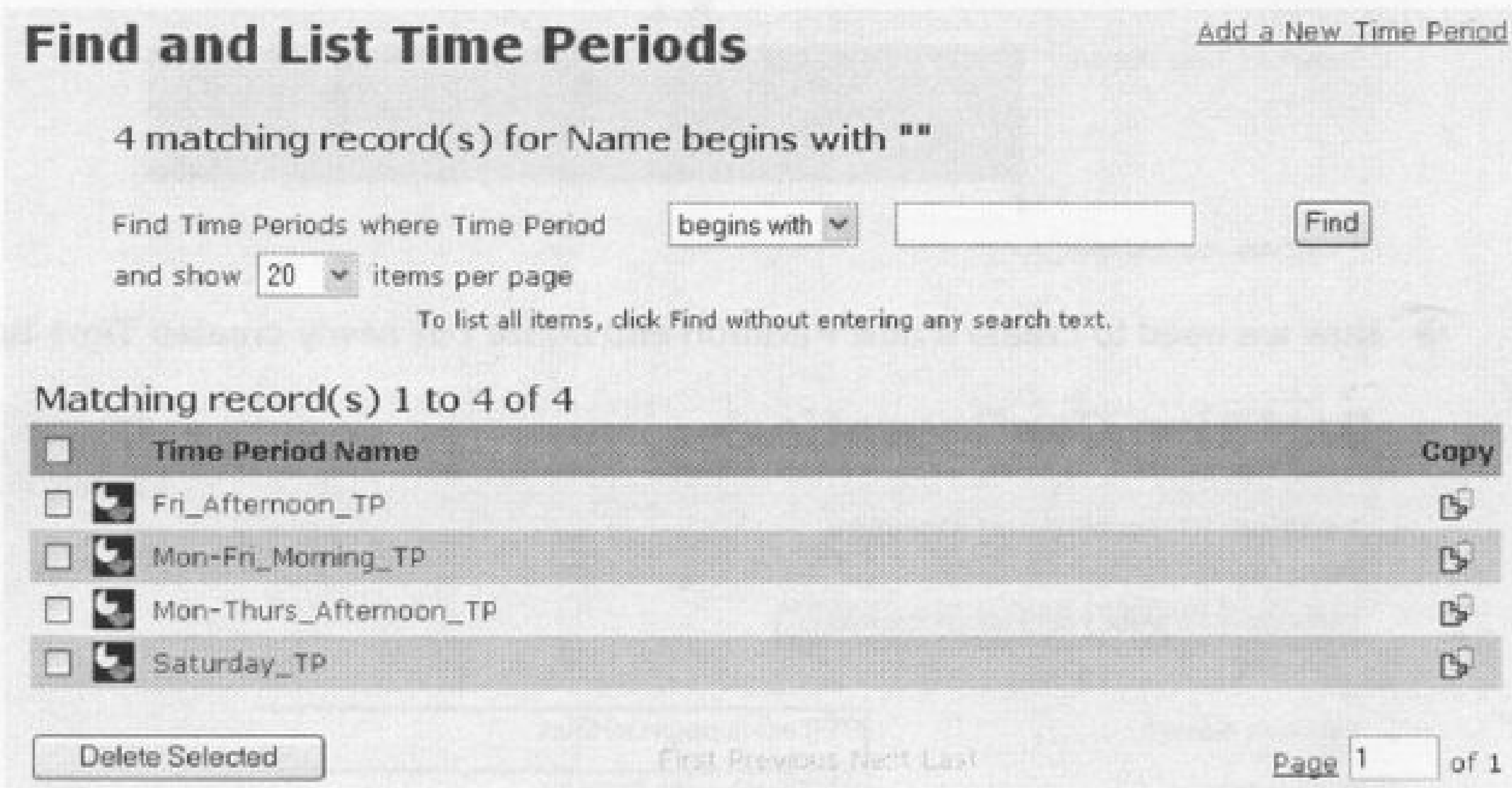
➔ **We will first need to create a series of Time Periods for Normal Business Hours (anything NOT falling within these hours and days specified will effectively turn the Partition OFF).**



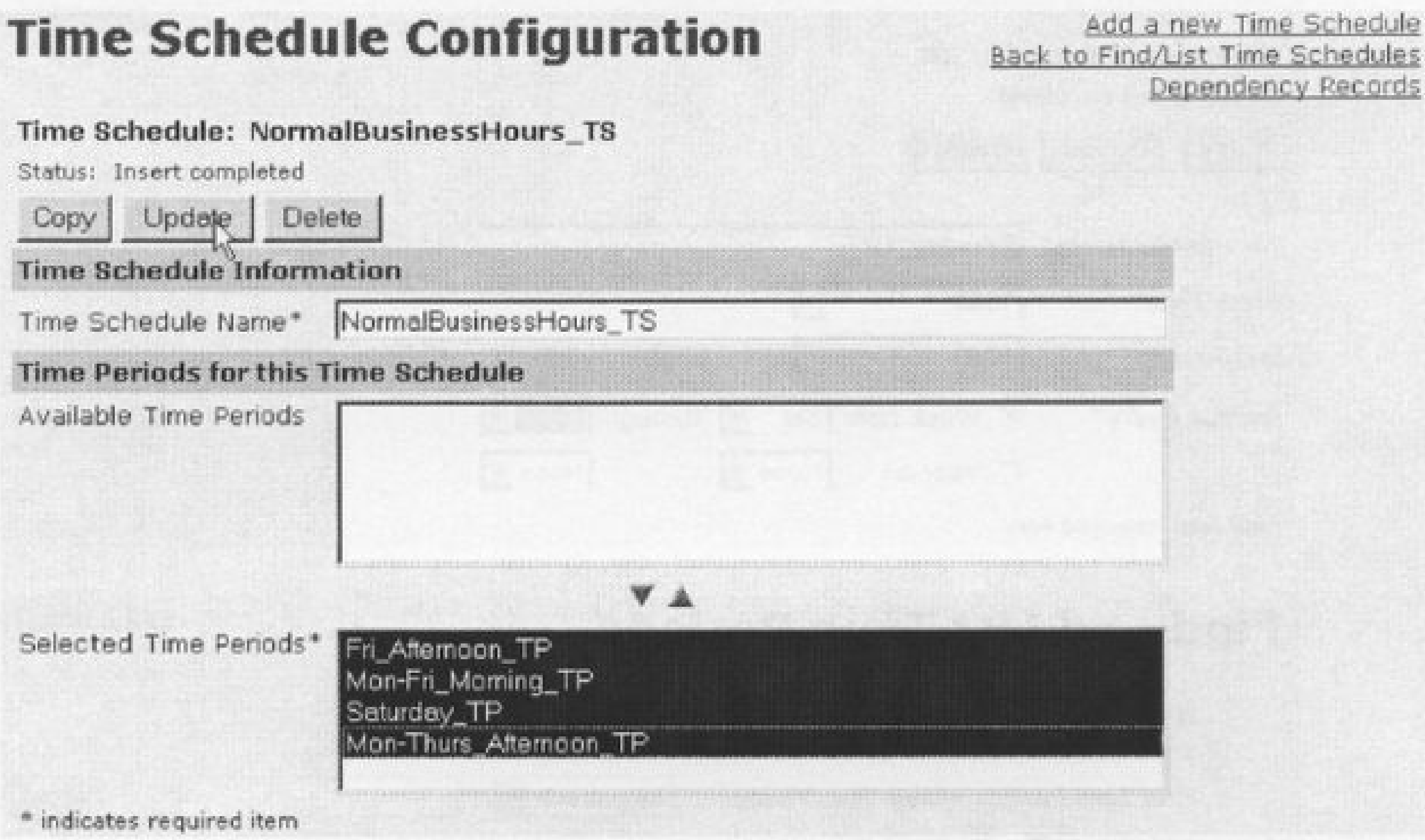




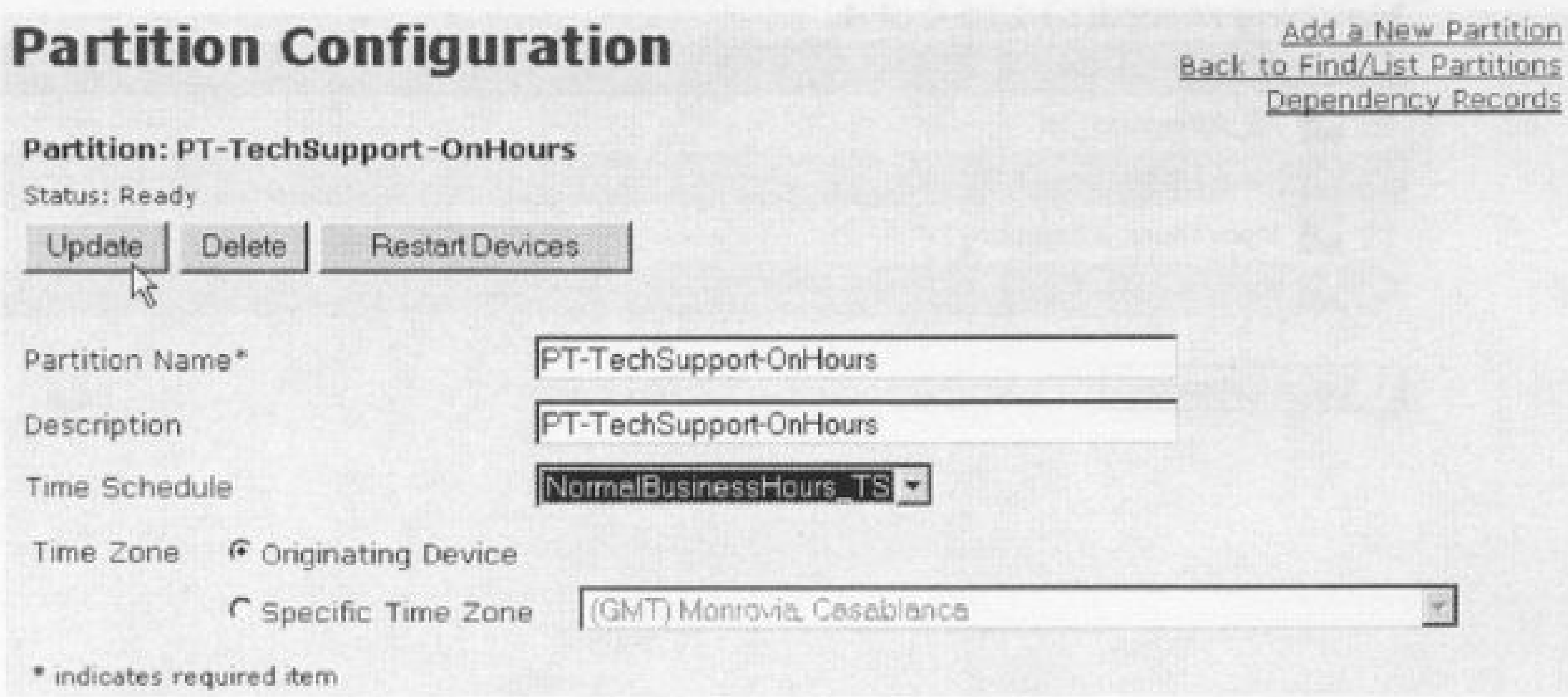

Time Period Configuration
Add a New Time Period
Back to Find/List Time Periods
Dependency Records
TimePeriod : Saturday_TP
Status : Insert completed.
Copy
Update
Delete
Time Period Name* Saturday_TP
Start Time* 10:00
End Time* 12:00
Repeat Every* Week from Sat through Sat
Year on None None
* indicates required item


Find and List Time Periods
Add a New Time Period
4 matching record(s) for Name begins with ""
Find Time Periods where Time Period begins with Find
and show 20 items per page
To list all items, click Find without entering any search text.
Matching record(s) 1 to 4 of 4
Time Period Name
Copy
Fri_Afternoon_TP
Mon-Fri_Morning_TP
Mon-Thurs_Afternoon_TP
Saturday_TP
Delete Selected
Page 1 of 1

➔ **Now we need to create a Time Schedule to concatenate them into one**

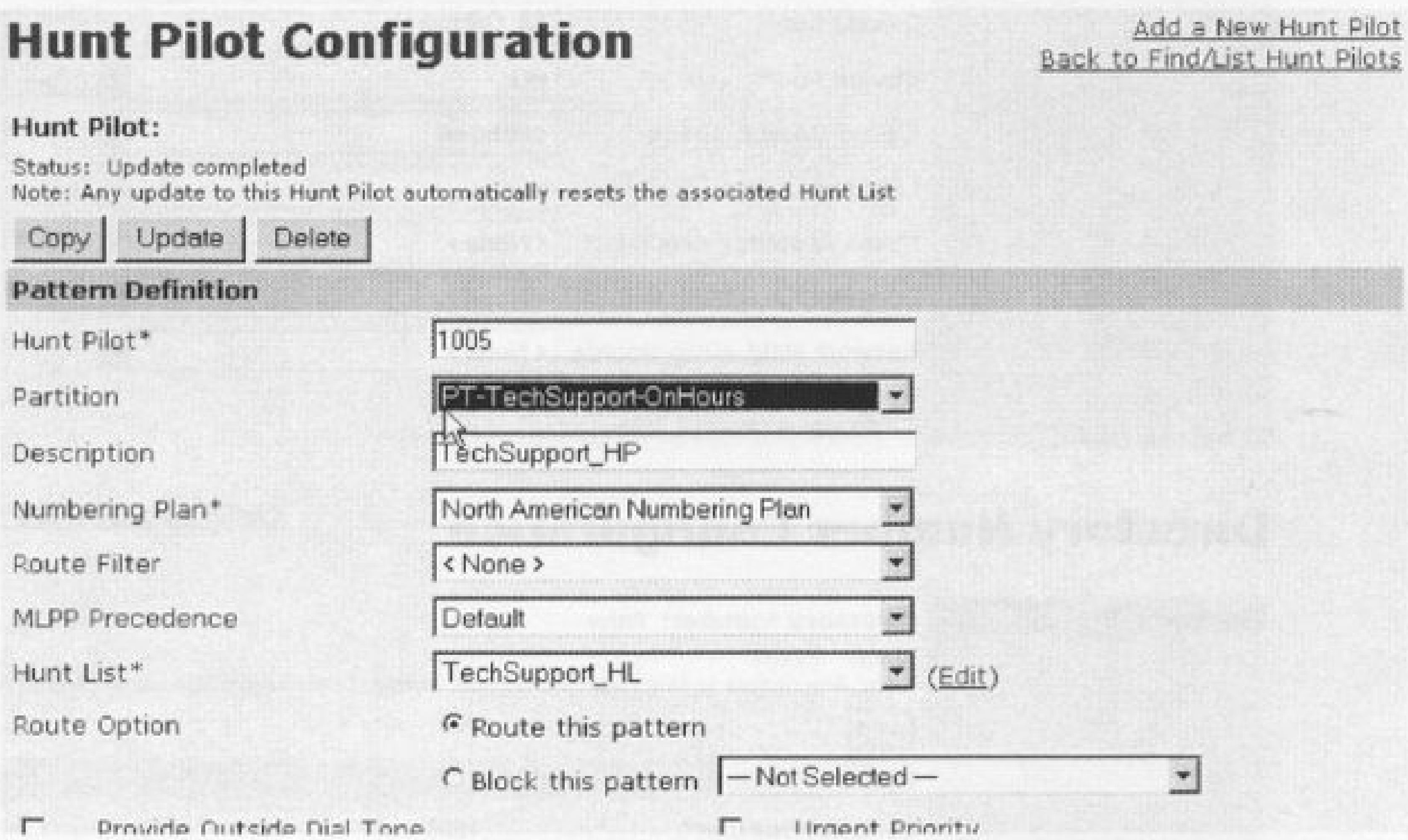


➔ **Now we need to create a new Partition and utilize our newly created Time Schedule**

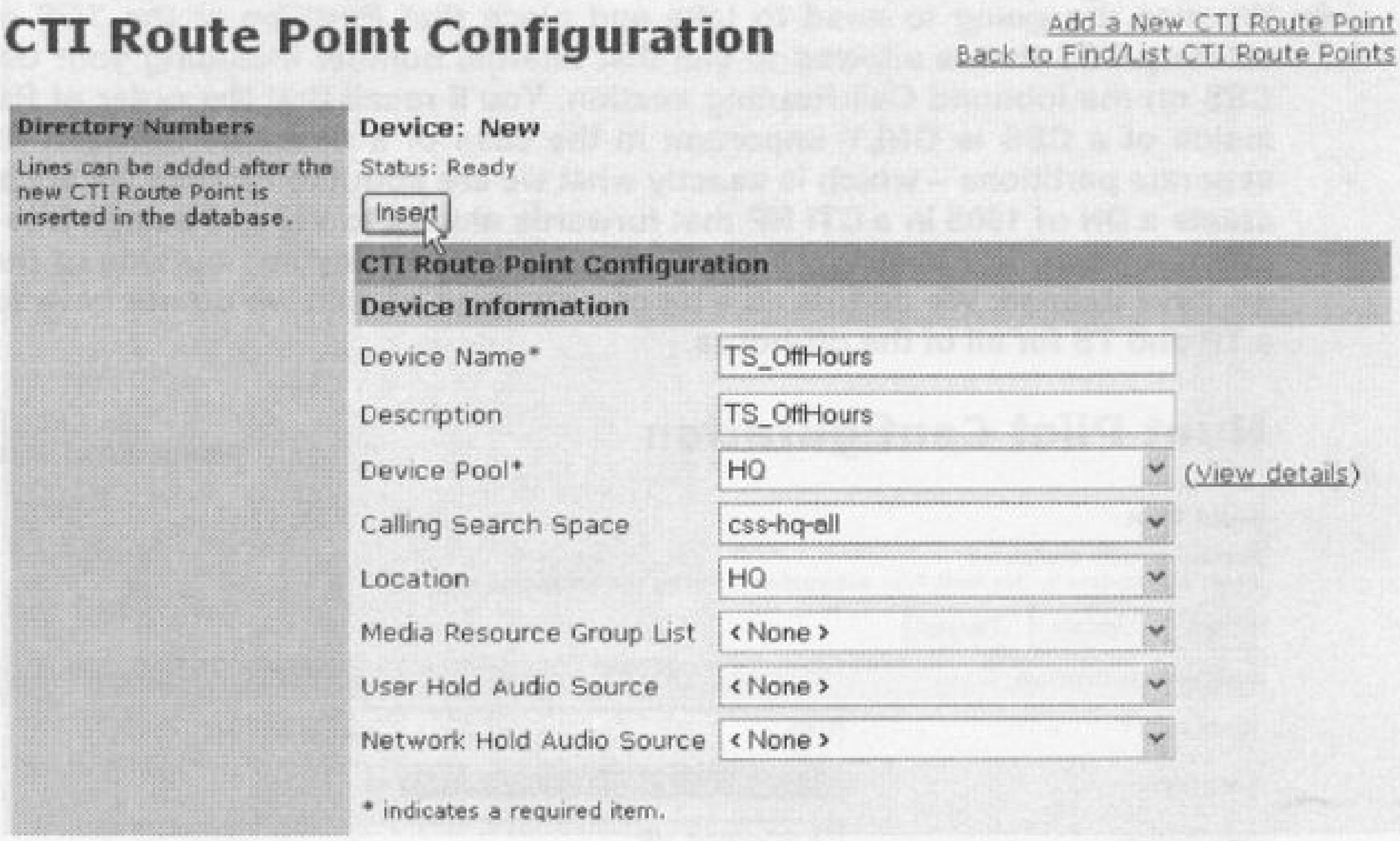


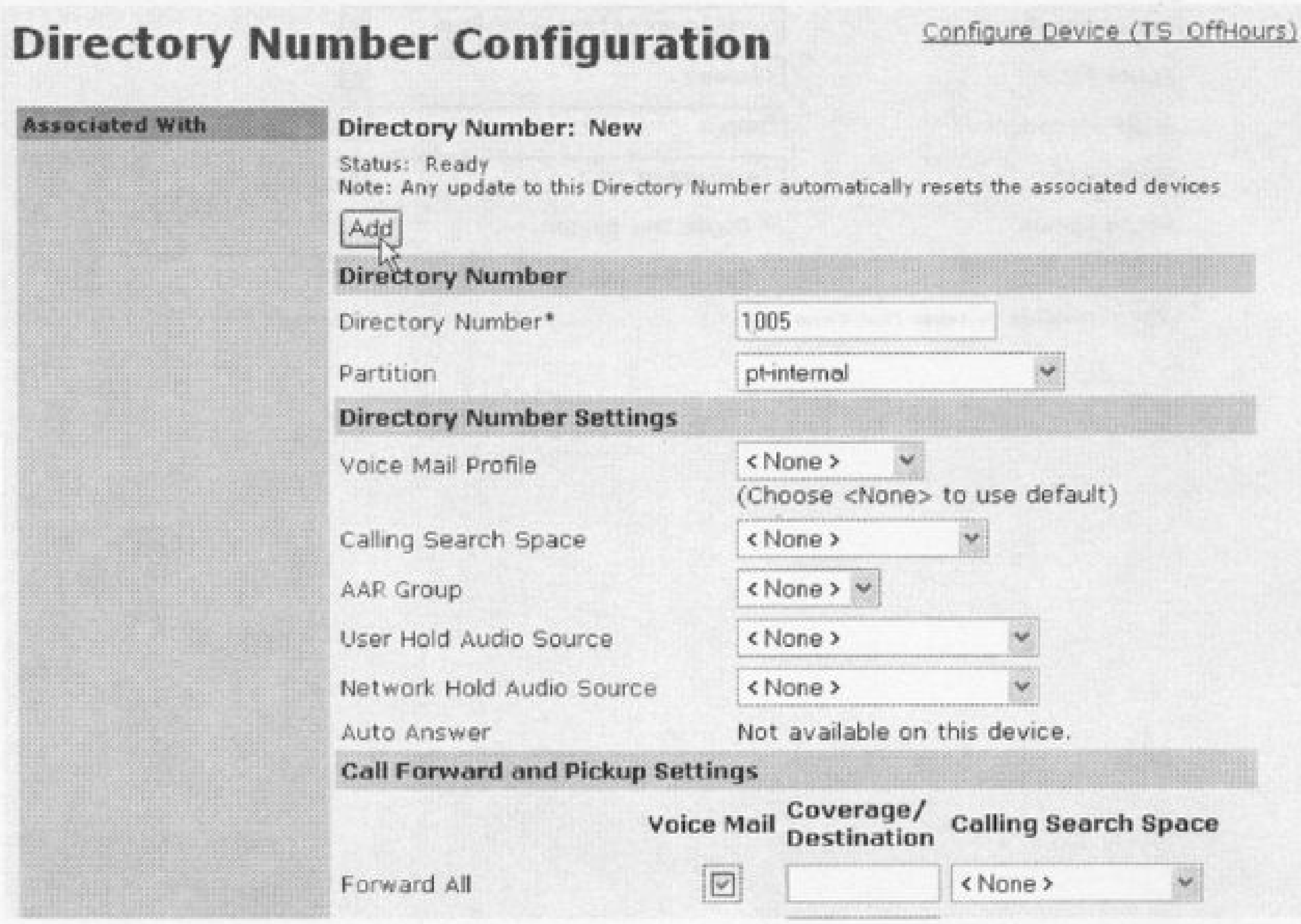
➔ **Now we need to assign that new Partition to our existing Hunt Pilot for Tech Support.**

➔ **We also are going to need to take and place that Partition at the TOP of every existing CSS that is allowed to call that internal number including your Gateways CSS on the Inbound Call Routing section. You'll recall that the order of Partitions inside of a CSS is ONLY important in the case of a direct tie between DNs in 2 separate partitions – which is exactly what we are about to have as we are about to create a DN of 1005 in a CTI RP that forwards always to VM and assign it to the PT-Internal which will basically "catch" the DN of 1005 anytime outside of the hours we have defined. We do this as a bit of a shortcut so that we do not have to create a TP and TS for all of the off-hours.**

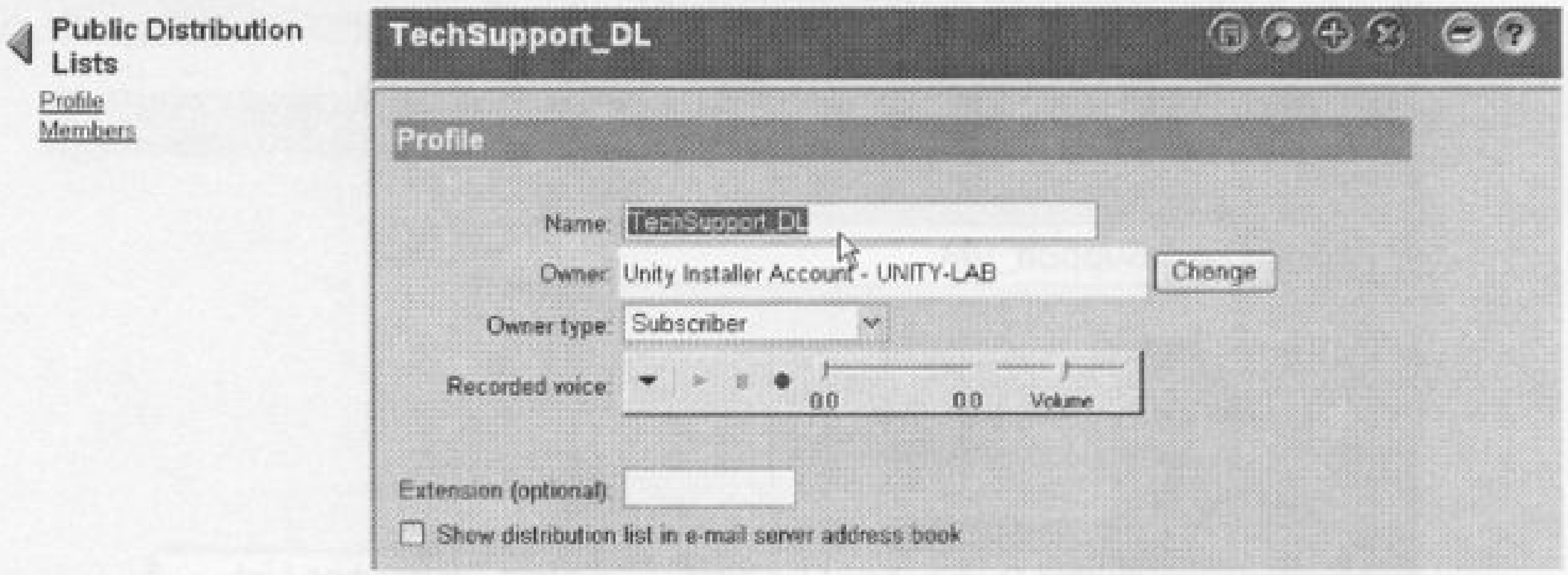


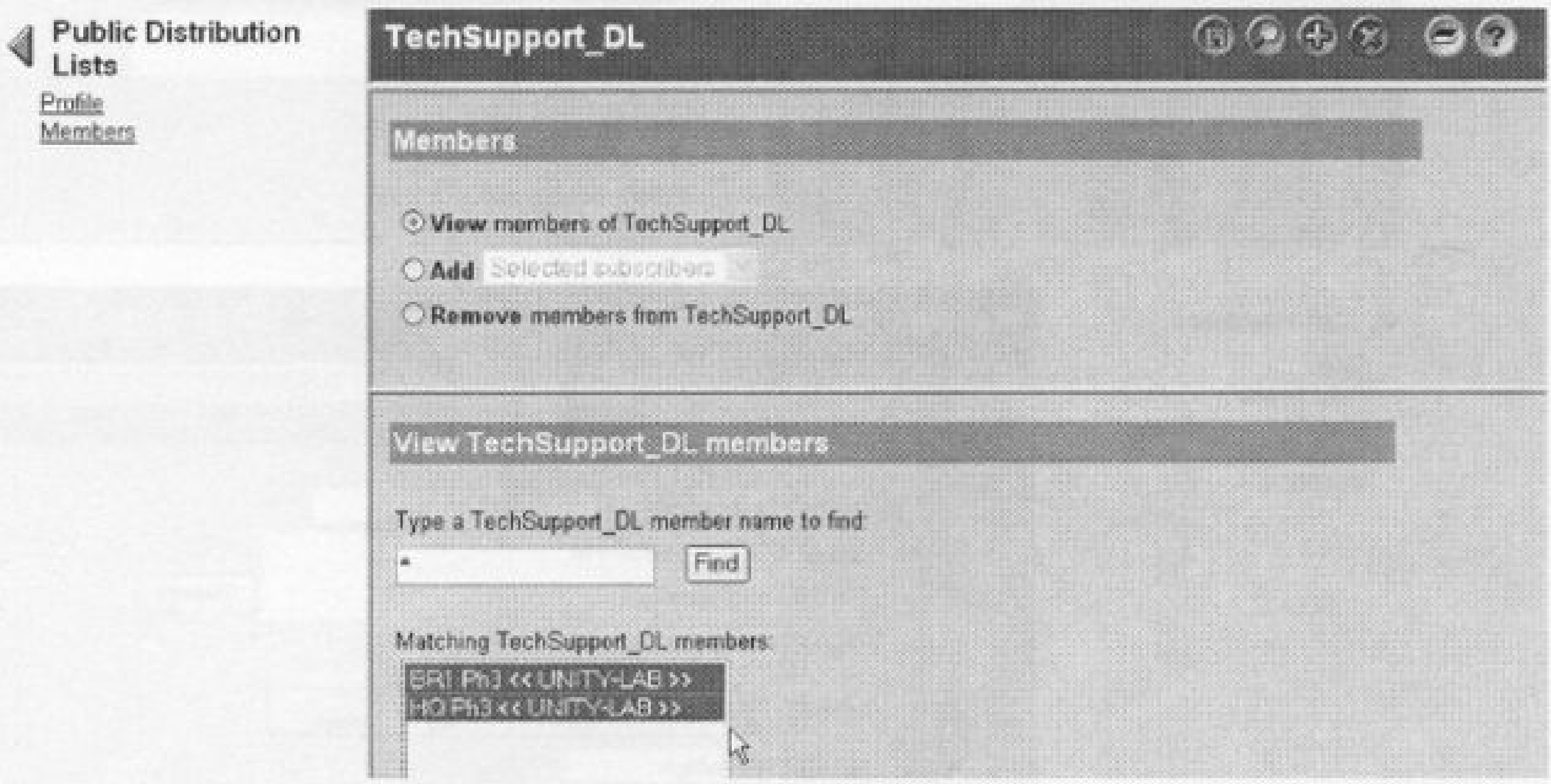
➔ **Now we will create the CTI RP we just discussed and assign it to the PT-Internal and forward it always to VM**



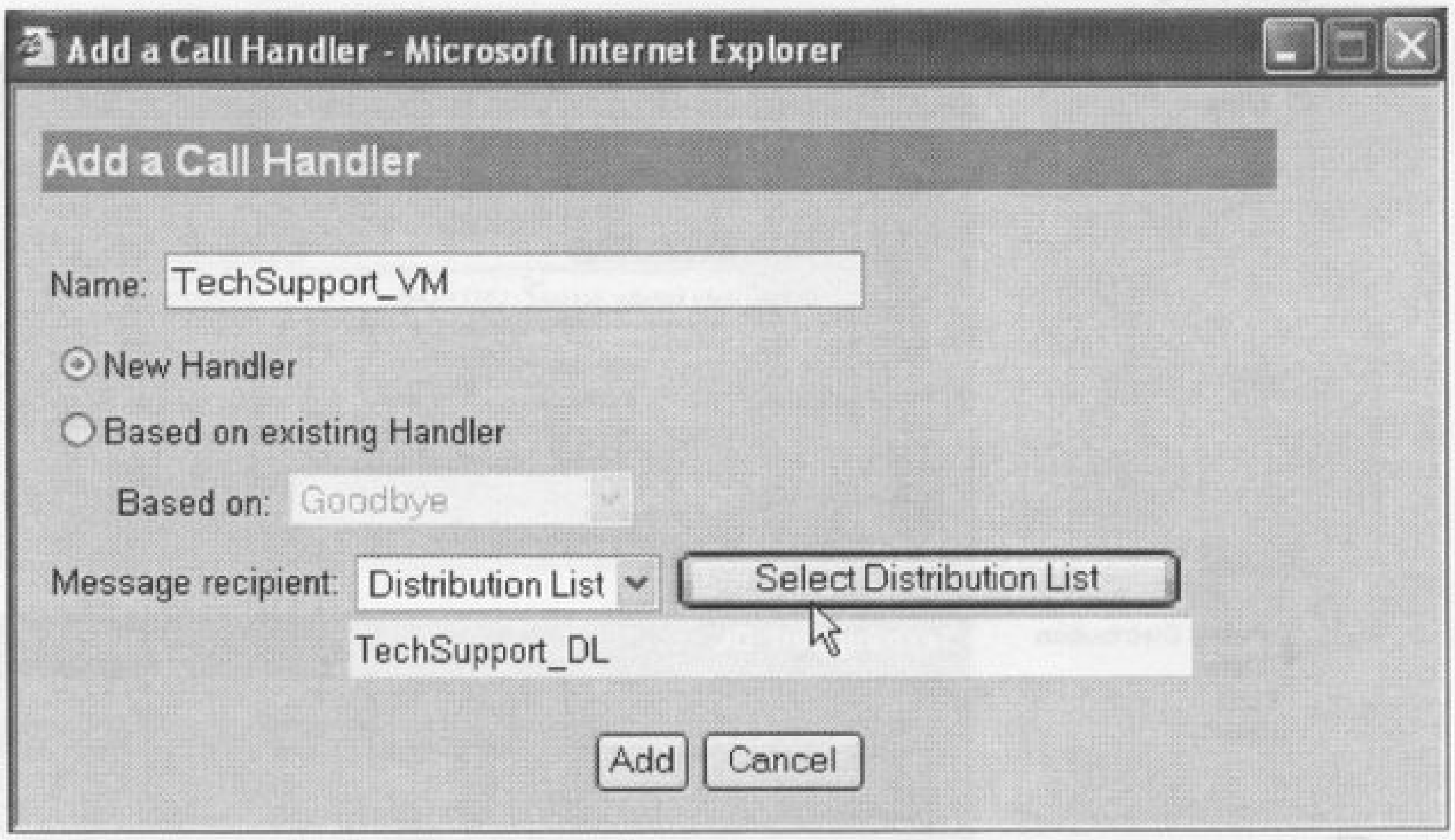


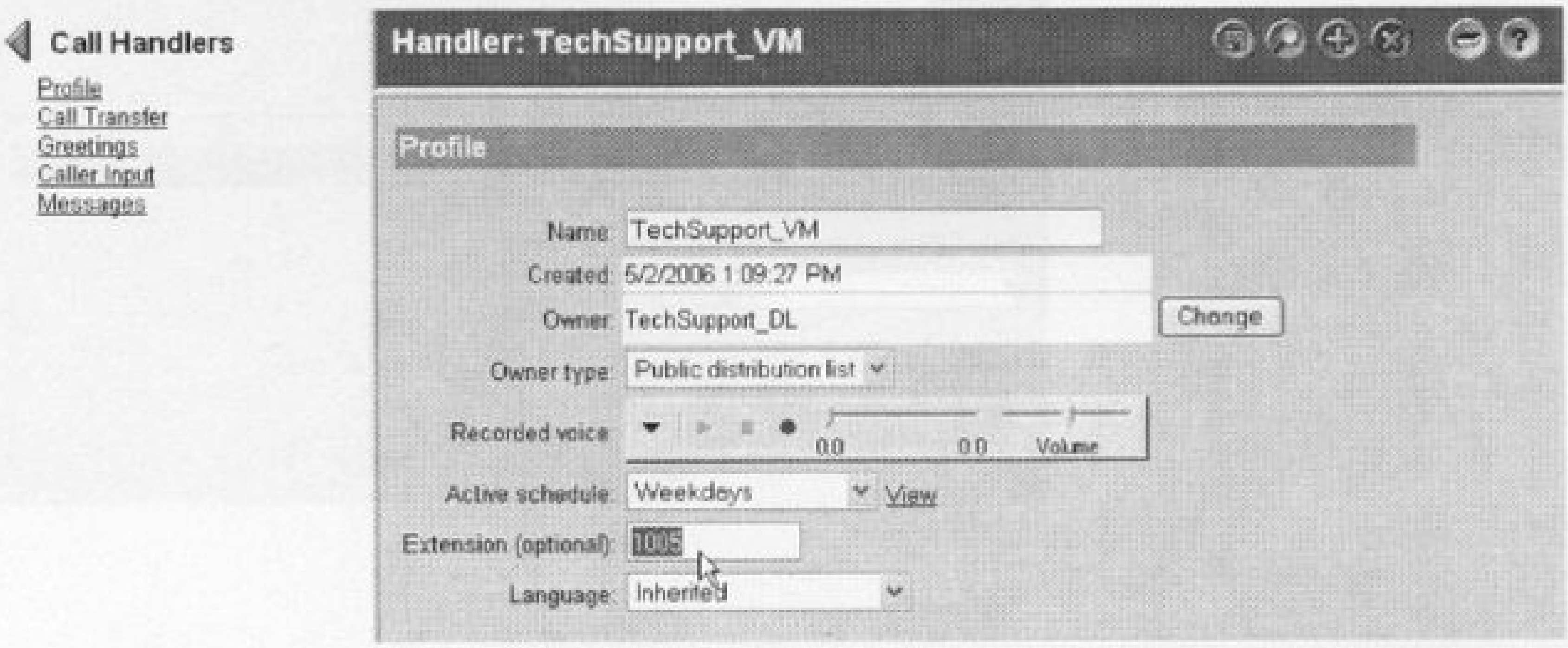
➔ **Next we skip over to Unity (even though it may not be integrated yet – that will come in Section 9) and create a Public Distribution List consisting of HQ Ph 3 and BR1 Ph 3**





➔ **Now we need to add a Call Handler with the message recipient as the Public Distribution list of TechSupport_DL and ensure that the Extension is set to 1005**





➔ **Now verify by ensuring that the Server time is set to a time that falls within our 'on-hours' Partition – ring the HG, and ensure proper operation.**

➔ **Next change the server time to anytime outside of our 'on-hours' and try ringing the HG again – this time the call should forward to Unity. Ensure that the MWI lights on all applicable phones.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 7: Media

Estimated Time to Complete: 2 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 7 Media

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure Section 1 must be completed along with the basic sections of Call Manager and CCME.

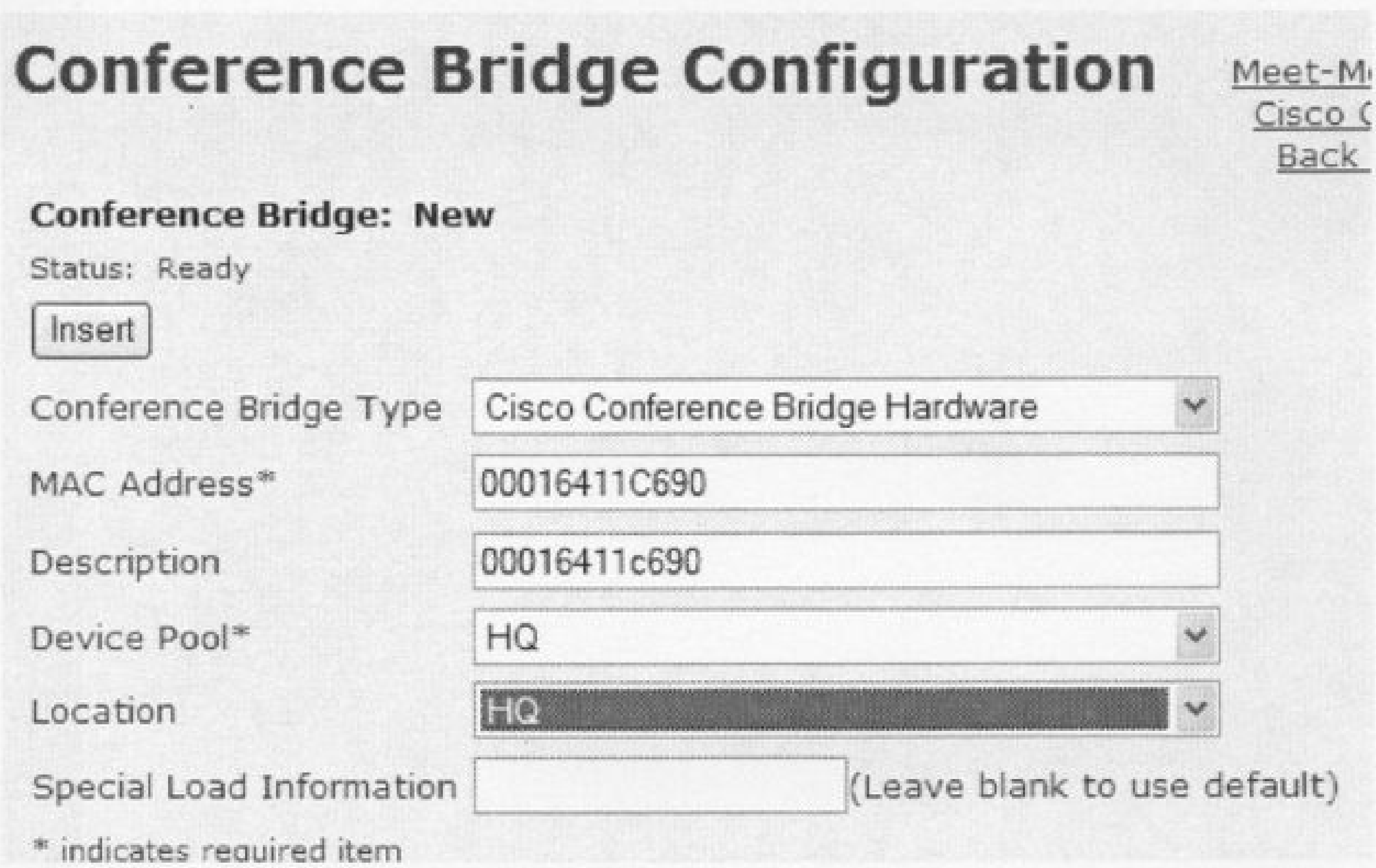
Section 7 Configuration Tasks

Task 7.1

Configure your assigned 6608 port as a conference bridge.

➔ **Put the conference bridge port in the correct VLAN - the command below gives you extra flexibility in case you wanted to assign a static IP Address and disable DHCP. Add the conference bridge as a Cisco Conference Bridge Hardware.**

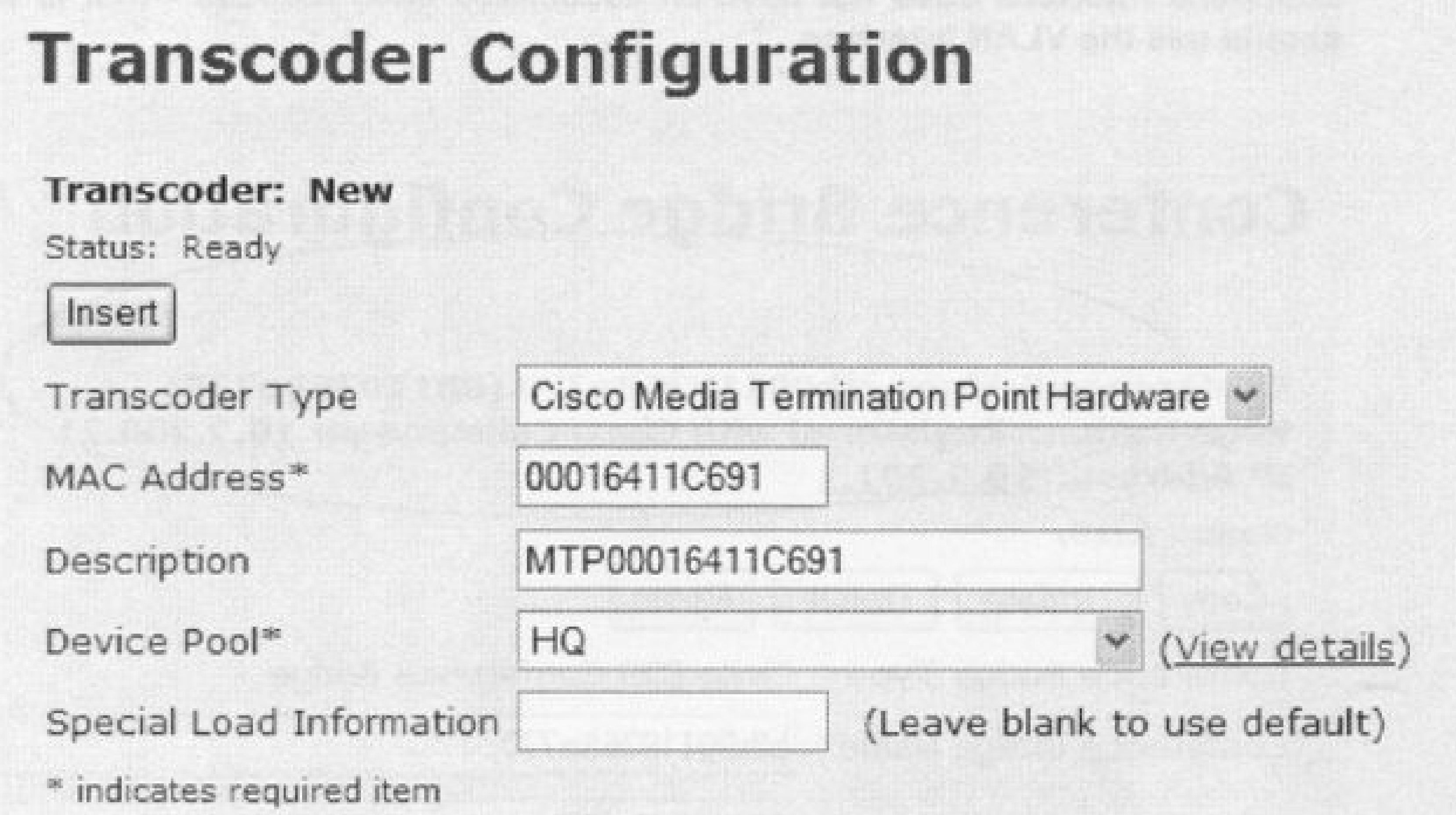
PL-VoicePod-6500> (enable) set port voice interface 3/5 dhcp en vlan 220



Task 7.2

Configure your assign 6608 port as a transcoder.

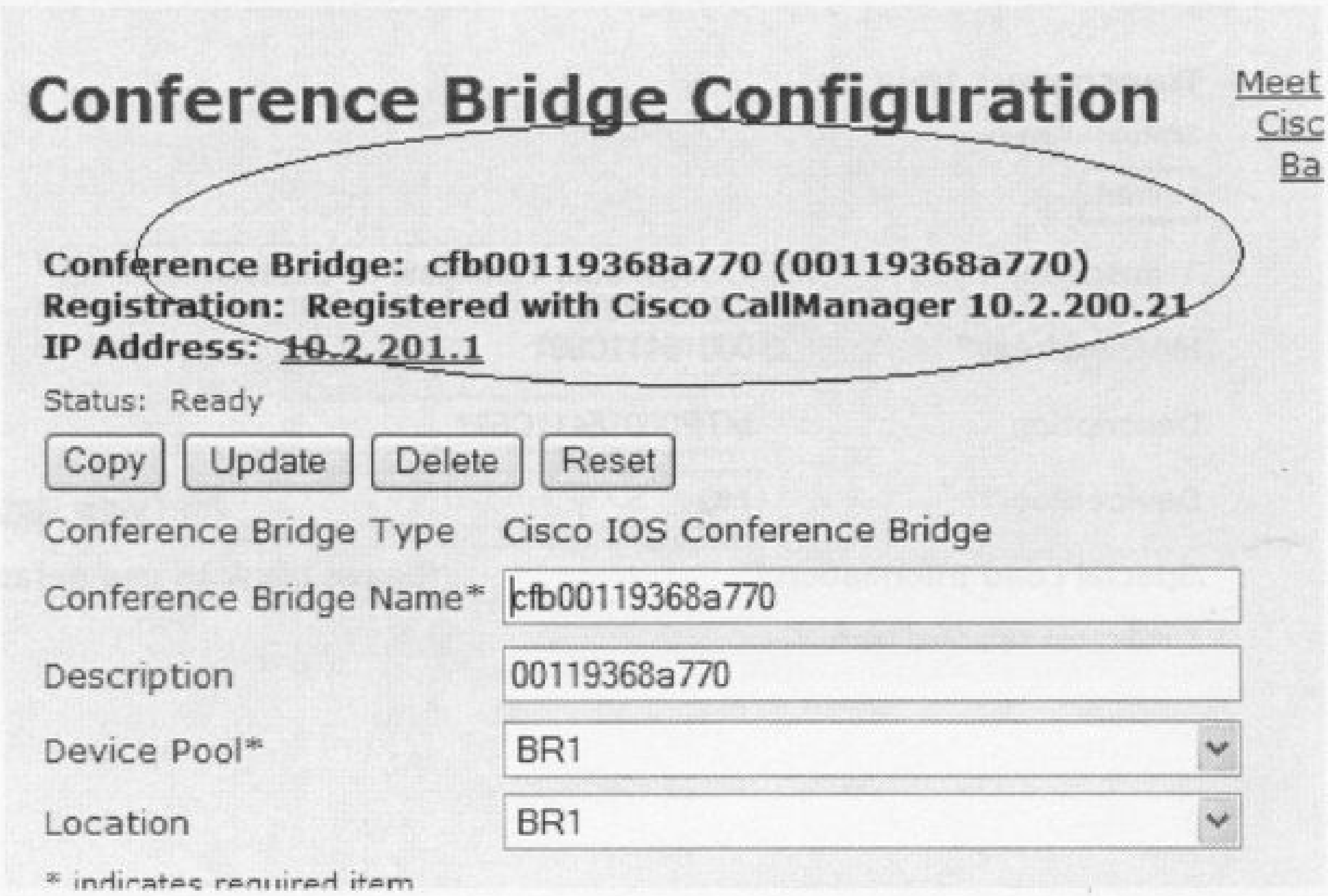
PL-VoicePod-6500> (enable) set port voice interface 3/6 dhcp en vlan 220



Task 7.3

Configure conference bridge on BR1 router. Use a maximum of 1 session.

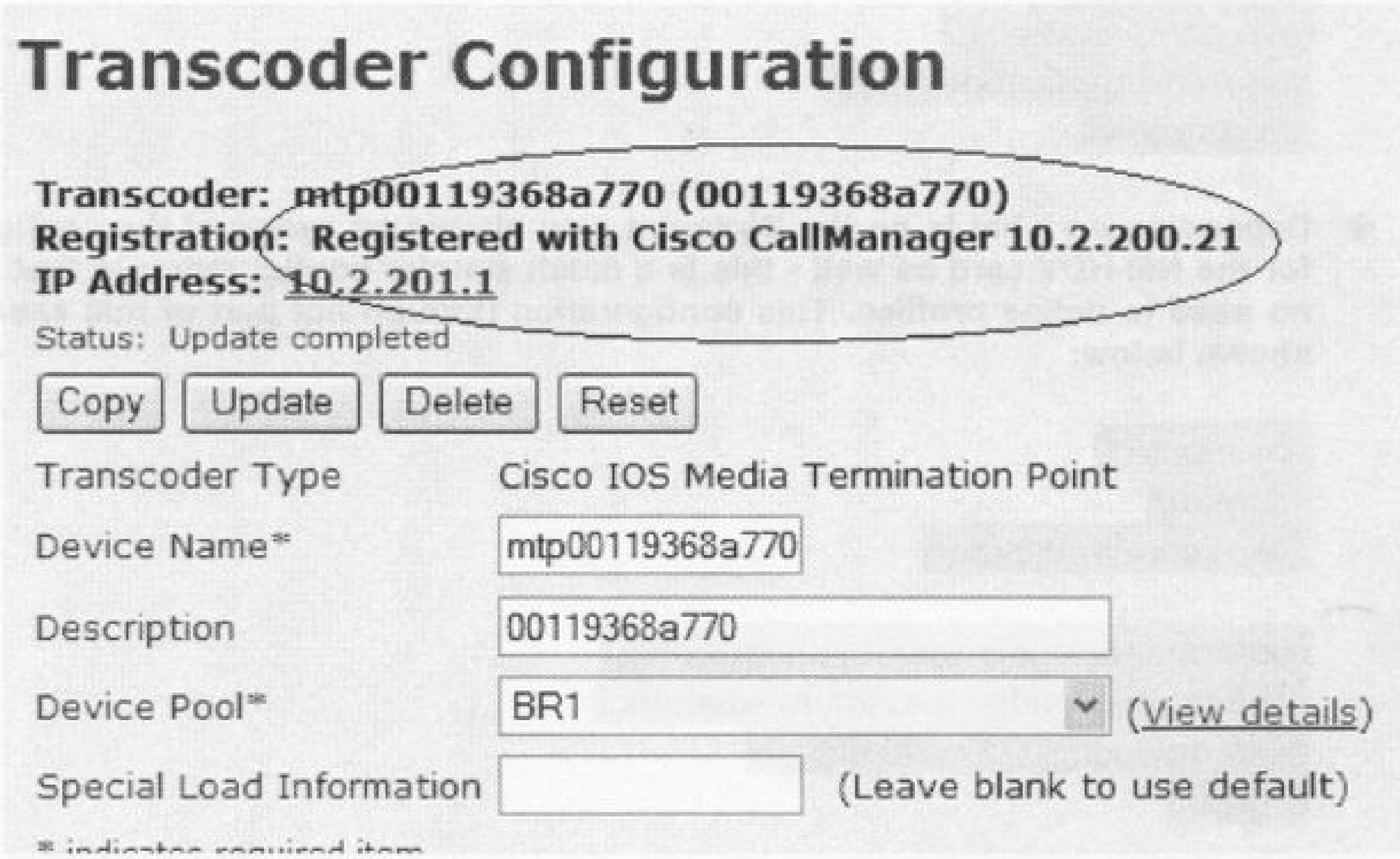
➔ **CCMAdmin configuration is shown below, for IOS configuration see next task. Use MAC Address of VLAN Interface and for IOS prefix MAC with "CFB". Remember the Loopback interface does not have an associated MAC address - that is why you should use the VLAN interface.**



Task 7.4

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **Add the transcoder in CCMAdmin - use MAC address of VLAN interface and prefix with "MTP" - you get the MAC address using the "show interface vlan220" command.**



➔ **IOS Conferencing and Transcoding configuration for PVDM2 DSPs directly on the motherboard is shown below. Configuration for an NM-HDV2 module would be the same.**

```
voice-card 0
 dspfarm
 dsp services dspfarm

sccp local VLan210
sccp ccm 10.1.200.21 identifier 1
sccp ccm 10.1.200.20 identifier 2
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate ccm 2 priority 2
 associate profile 2 register mtp00119368a770
 associate profile 1 register cfb00119368a770
!
dspfarm profile 2 transcode
 codec g711ulaw
 codec g729r8
```



```
 maximum sessions 2
 associate application SCCP
 no shutdown
!
dspfarm profile 1 conference
 codec g711ulaw
 codec g729r8
 maximum sessions 2
 associate application SCCP
 no shutdown
```

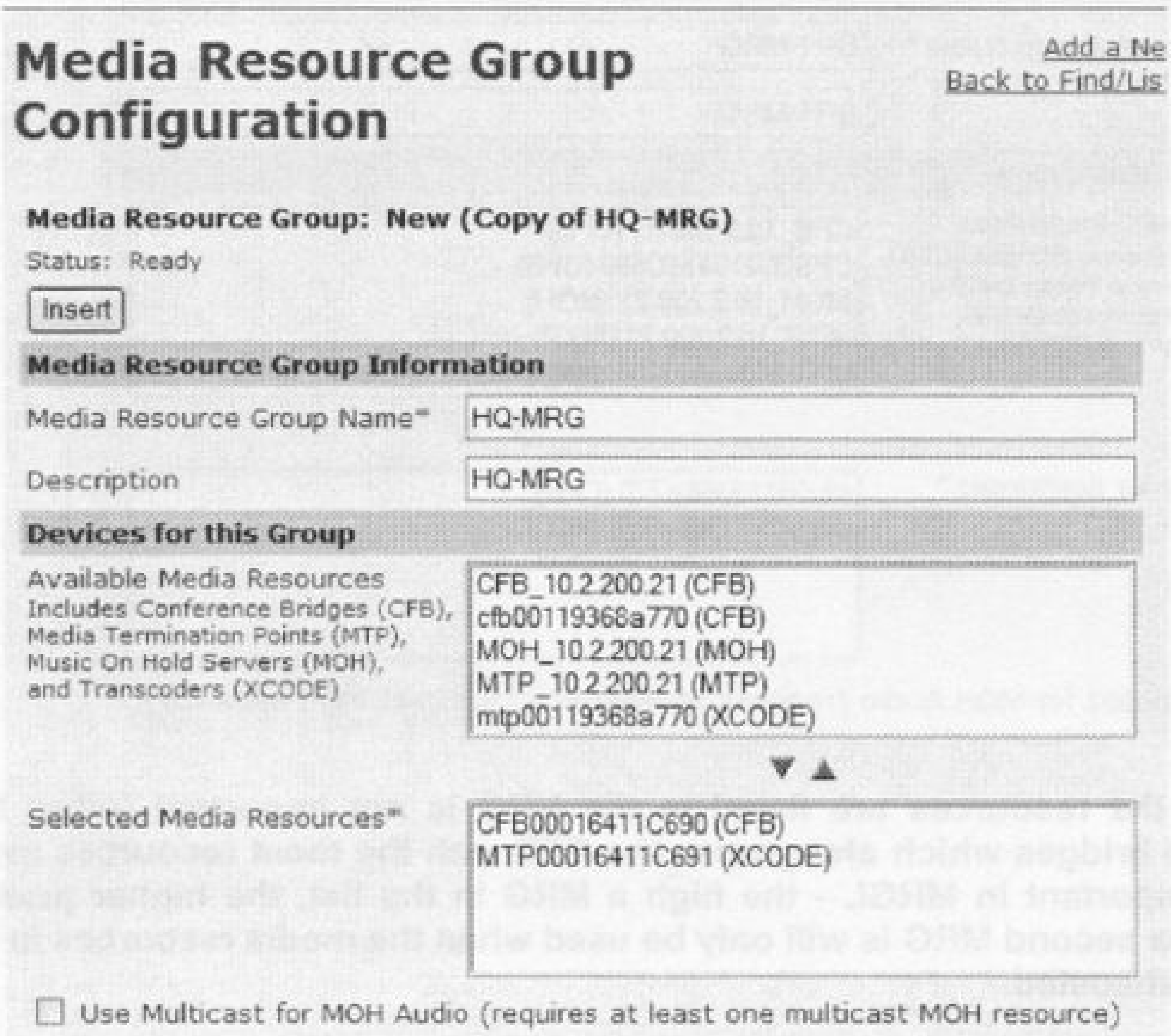
➔ **Depending on what is on the Blueprint, you should be aware of the configuration for the NM-HDV card as well - this is a much simpler configuration in that there is no need to define profiles. This configuration (though not part of this exercise) is shown below:**

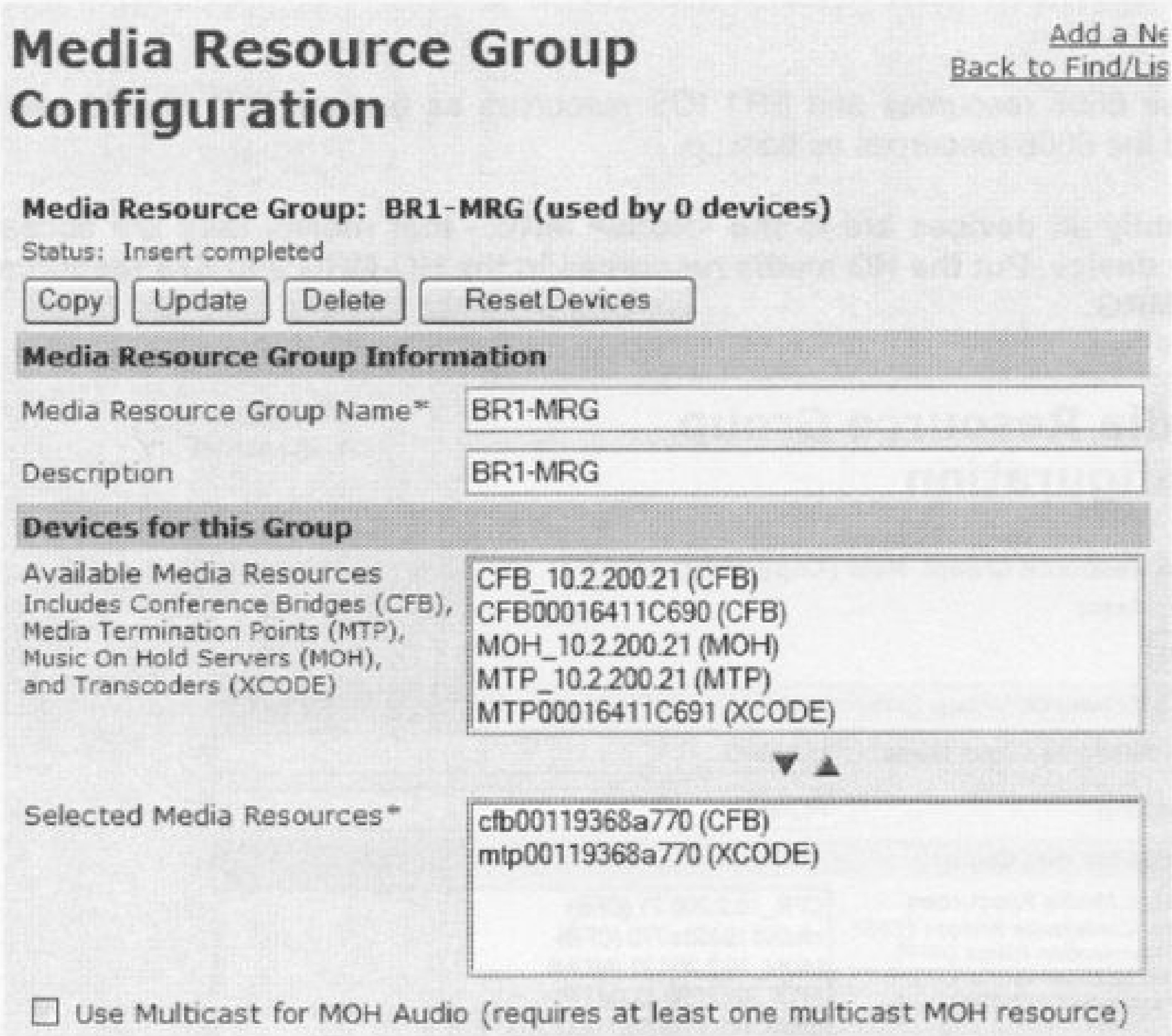
```
voice-card 0
 dspfarm
 dsp services dspfarm

dspfarm transcoder maximum sessions 2
dspfarm confbridge maximum sessions 1
dspfarm codec g729 vad disable
dspfarm

sccp
sccp local Vlan210
sccp ccm 10.1.200.21 priority 1
sccp ccm 10.1.200.20 priority 2
```

Task 7.5

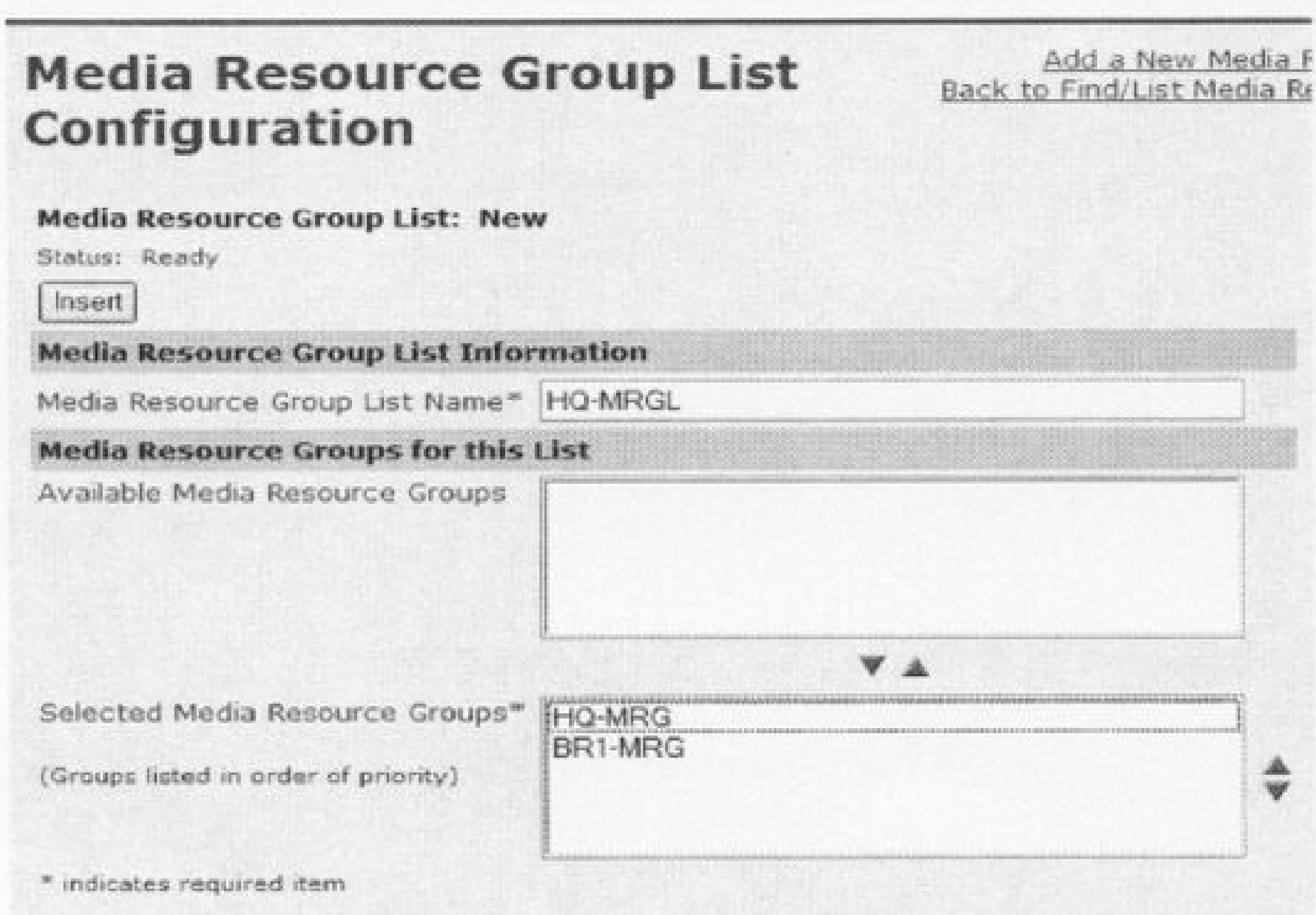
HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should use the IOS resources and the 6608 resources as backup.

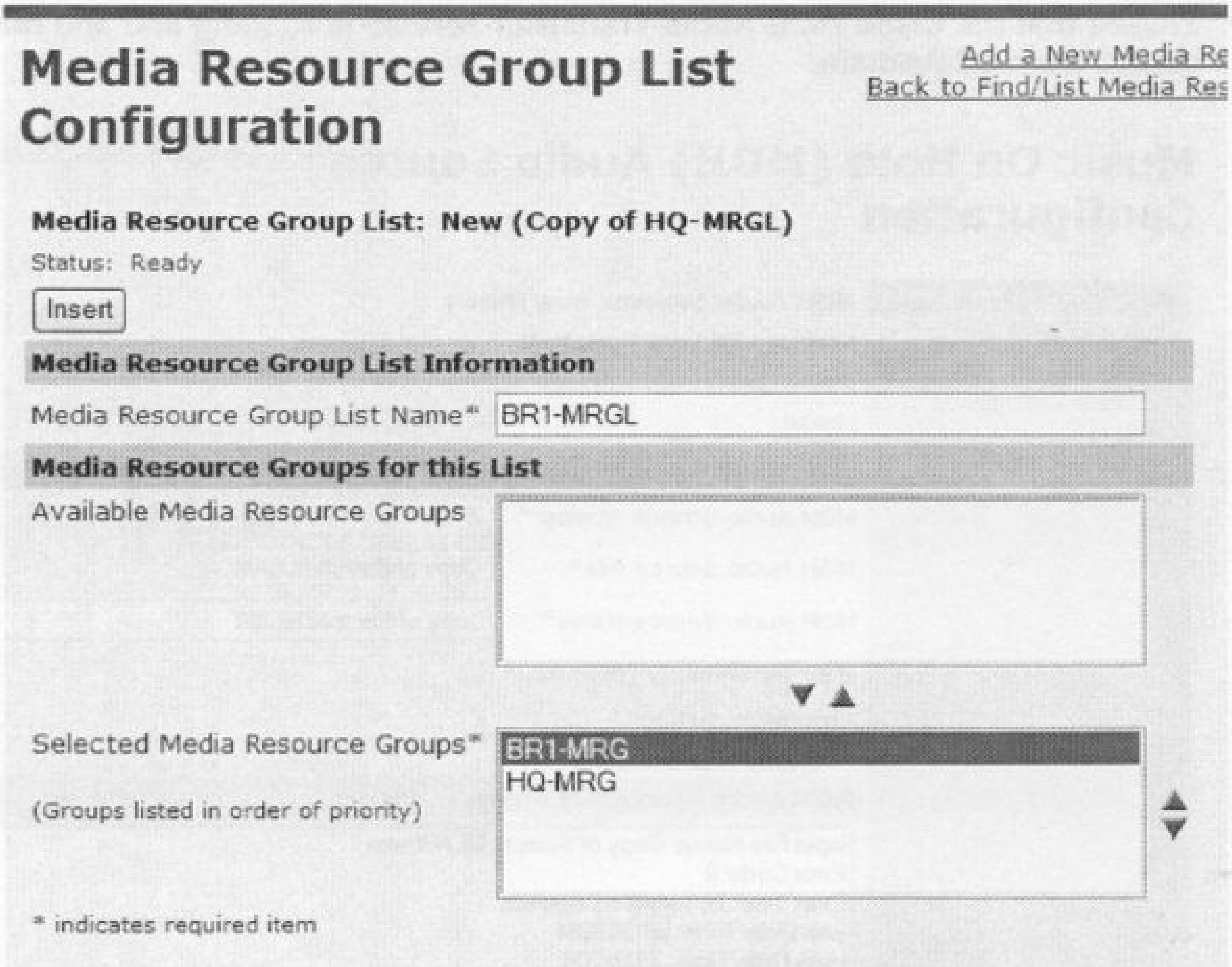
➔ **Currently all devices are in the <None> MRG - that means they are accessible to every device. Put the HQ media resources in the HQ-MRG and IOS resources in the BR1-MRG.**





➔ **The order the resources are listed in the MRG is not important (other than for conference bridges which always use the CFB with the most resources available). Order is important in MRGL - the high a MRG in the list, the higher priority that MRG is. The second MRG is will only be used when the media resources in the first MRG are exhausted.**



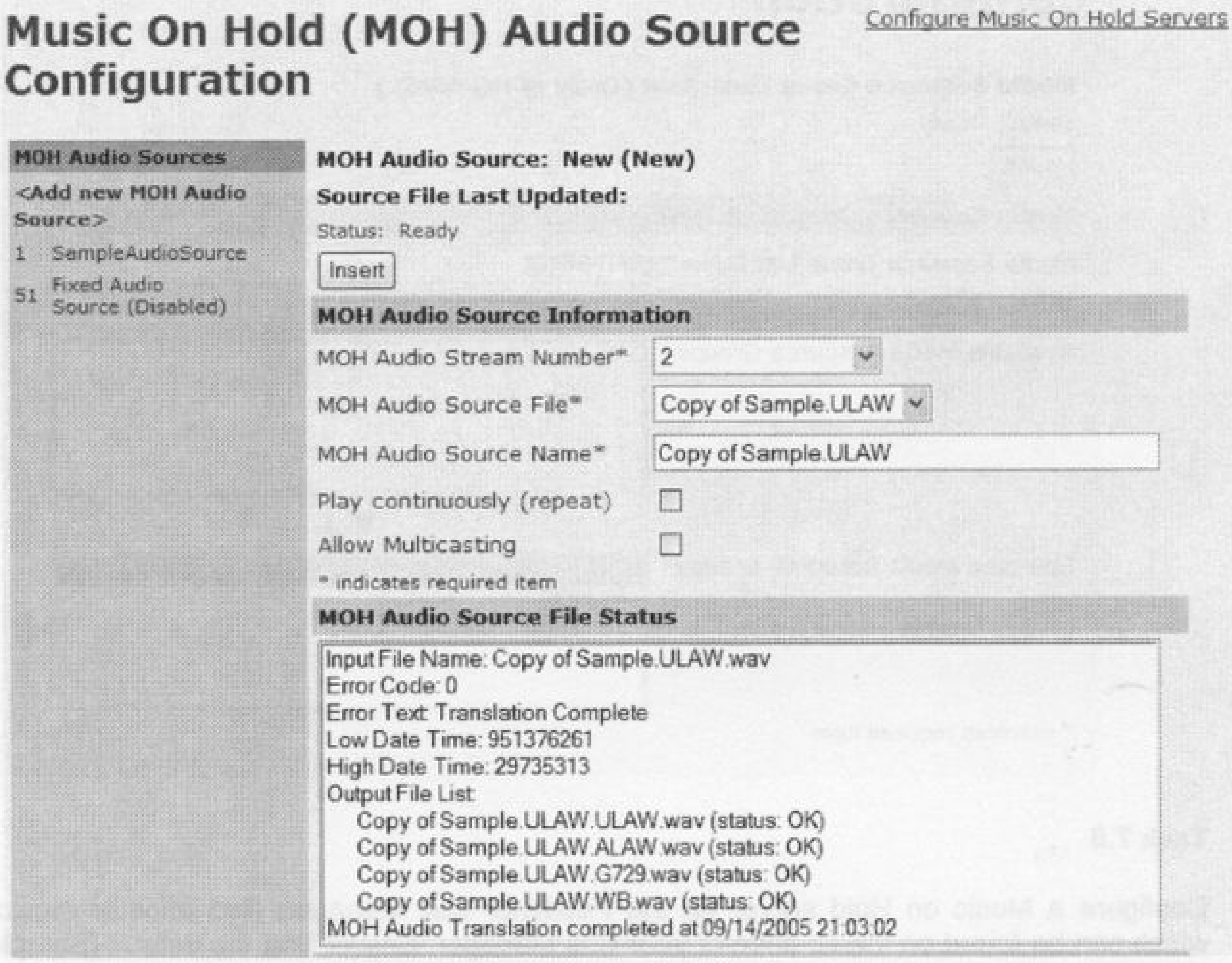


Task 7.6

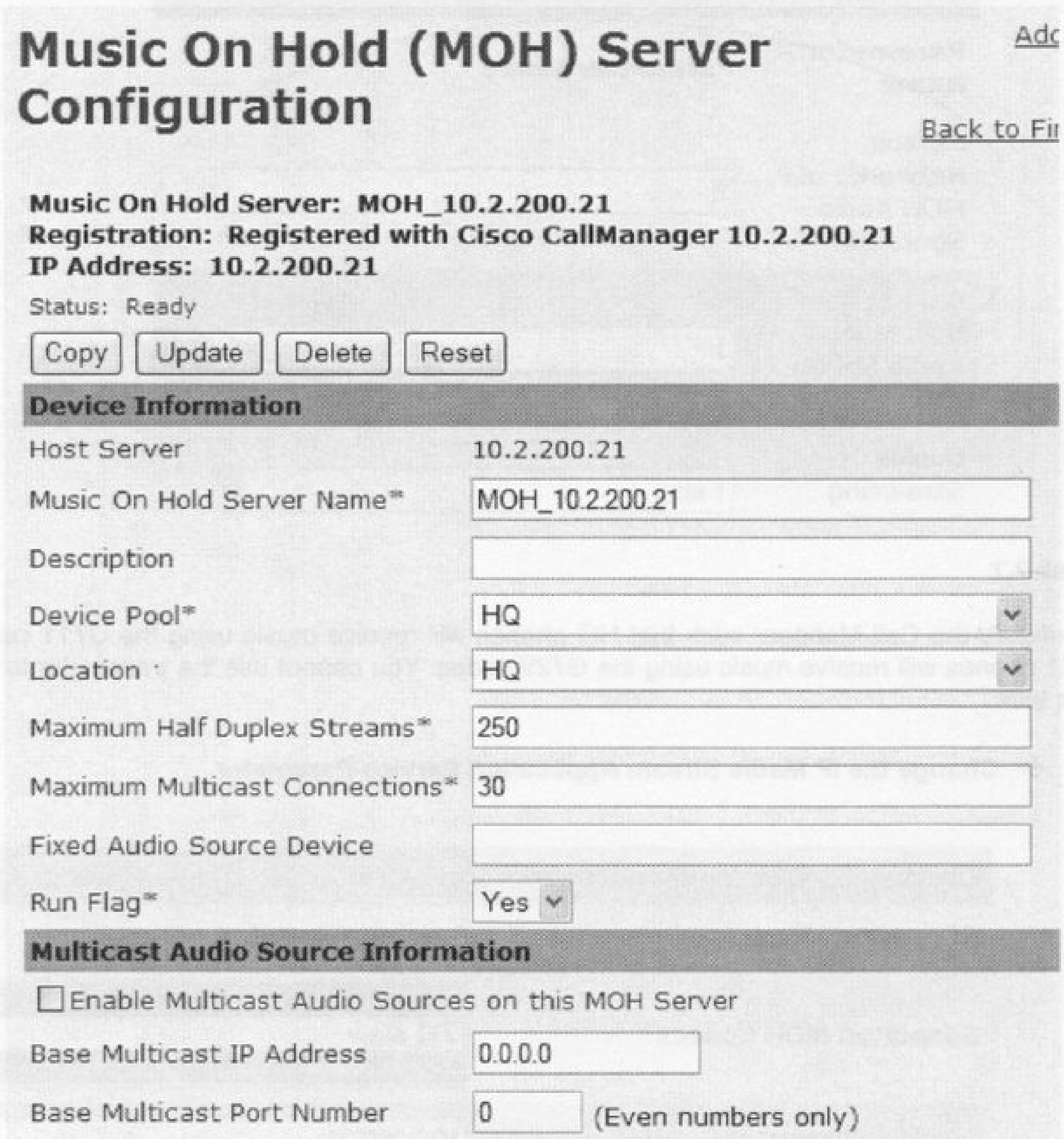
Configure a Music on Hold server on the Publisher Call Manager. Add another music source which can be found on the C: drive of your Call Manager. Ensure that the default (Sample) audio source is used when a User presses the 'Hold' button on his/her phone. For all other events that require music to be played use the newly added music source.

➔ **Make a copy of the "SampleAudioSource.ULAW.wav" file and call it something different. This can be located in the "C:\Program Files\Cisco\MOH" directory. Place this copy in the "C:\Program Files\Cisco\MOH\DropMOHAudioSourceFilesHere" directory.**

➔ **Ensure that the Cisco MOH Audio Translator service is running and add the music source from CCMAdmin.**

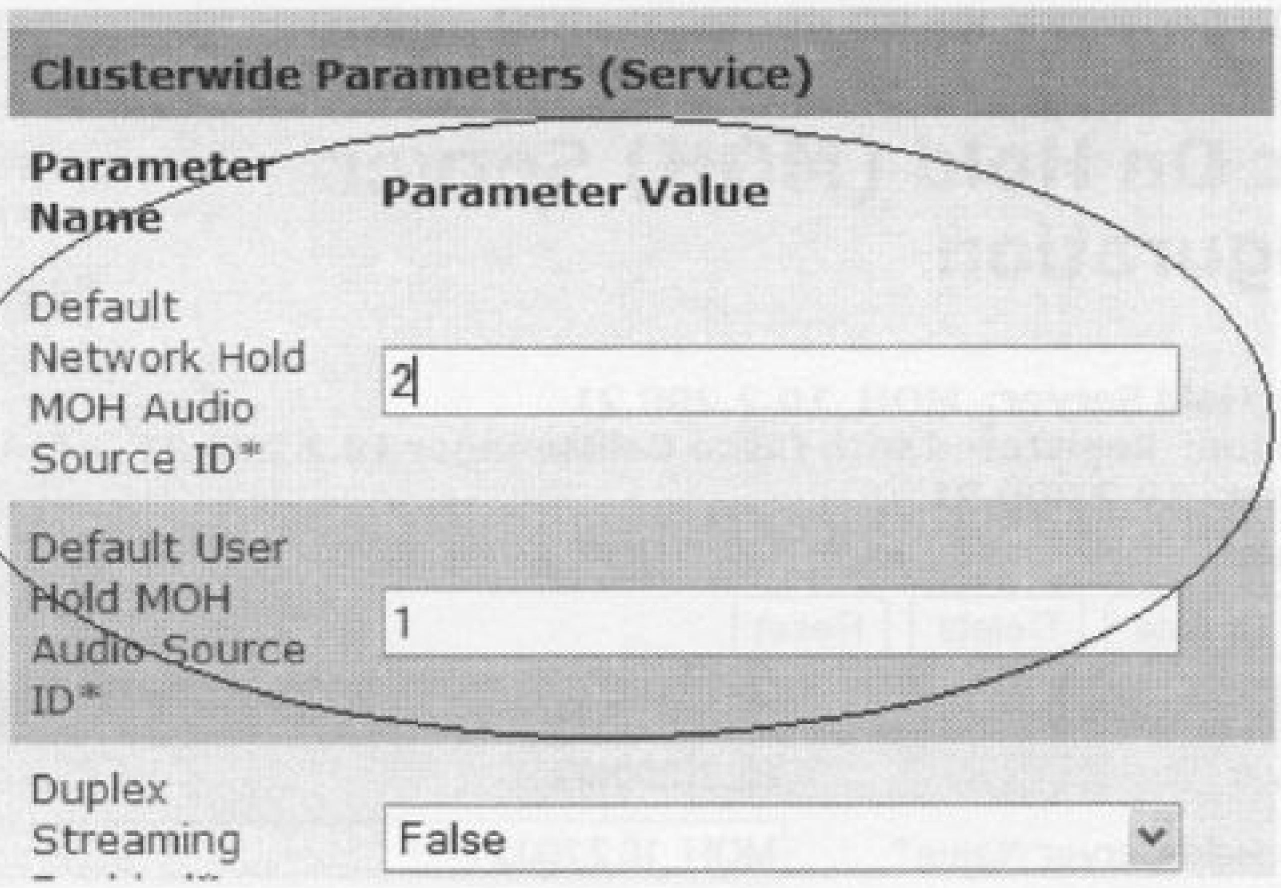


➔ **Configure the MOH Server with the correct Device Pool and Location. Looking ahead to the next task we can see that G729 should be used for BR1 phones and G711 should be used for HQ phones. Therefore the HQ DP should be used (given that the MOH Server is in the HQ site, use the HQ location).**



➔ **Add the MOH Server into the BR1-MRG and also the HQ-MRG.**

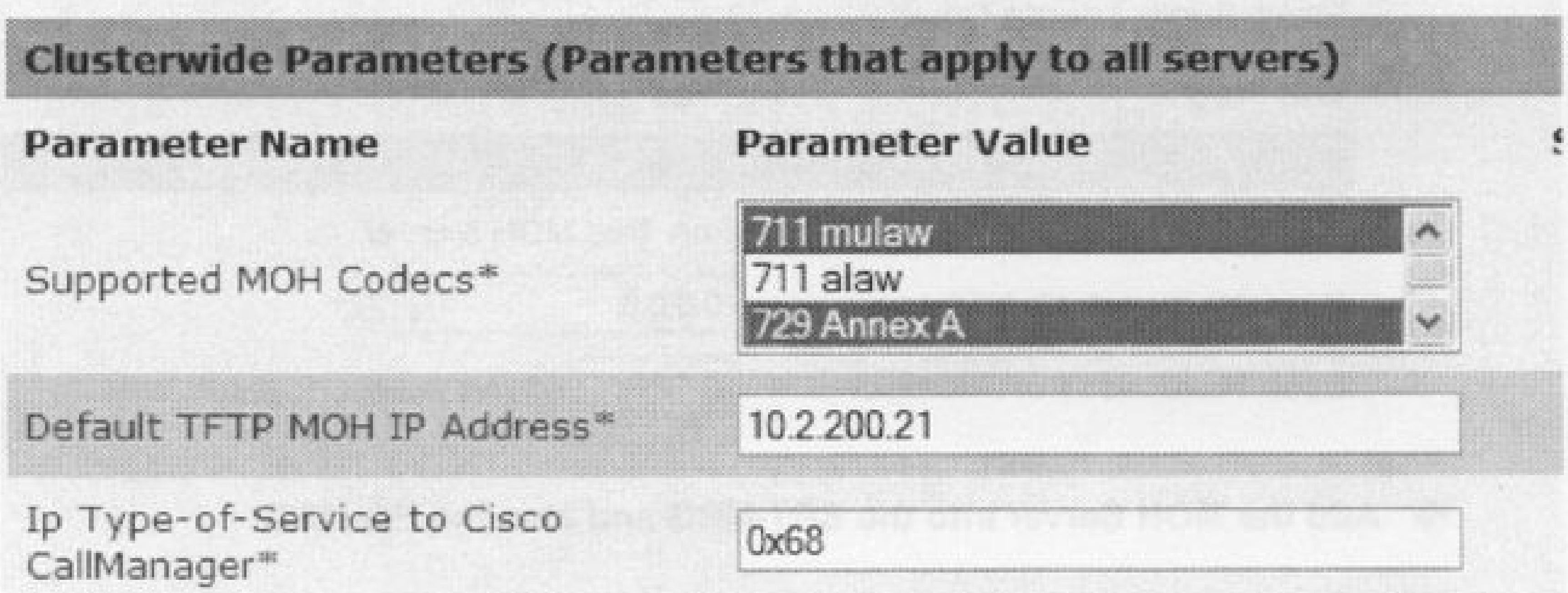
➔ **Configure the MOH Service Parameters to play the original Sample.wav file for User hold and the copy of Sample.wav for Network hold.**



Task 7.7

Configure the Call Manager such that HQ phones will receive music using the G711 codec and BR1 phones will receive music using the G729 codec. You cannot use the transcoder to achieve this task.

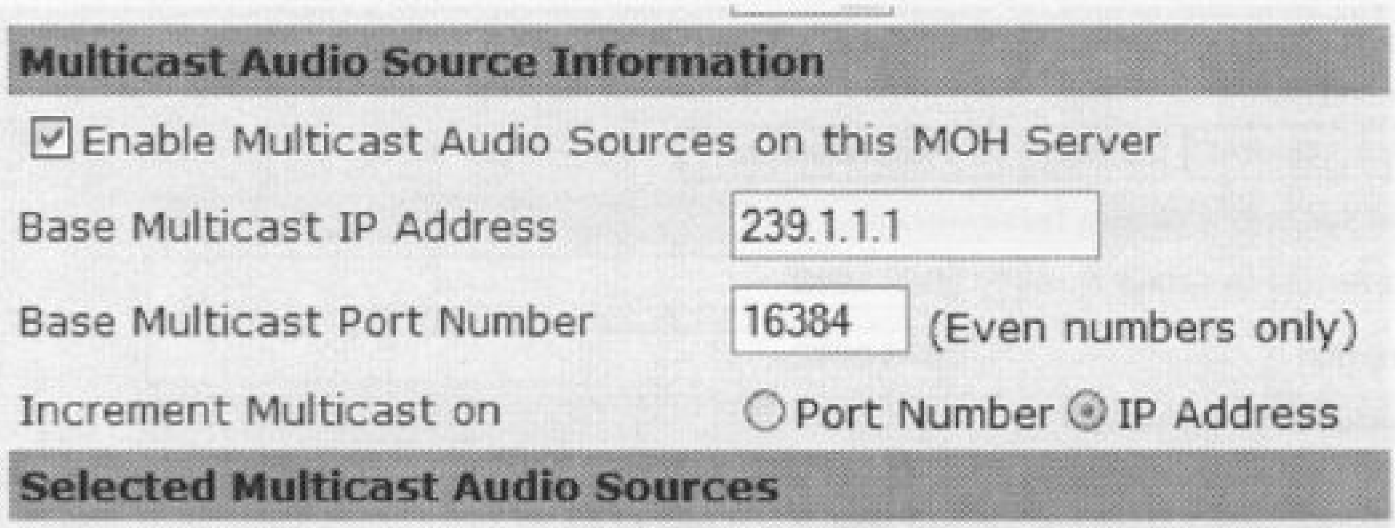
➔ **Change the IP Media Stream Application Service Parameter.**



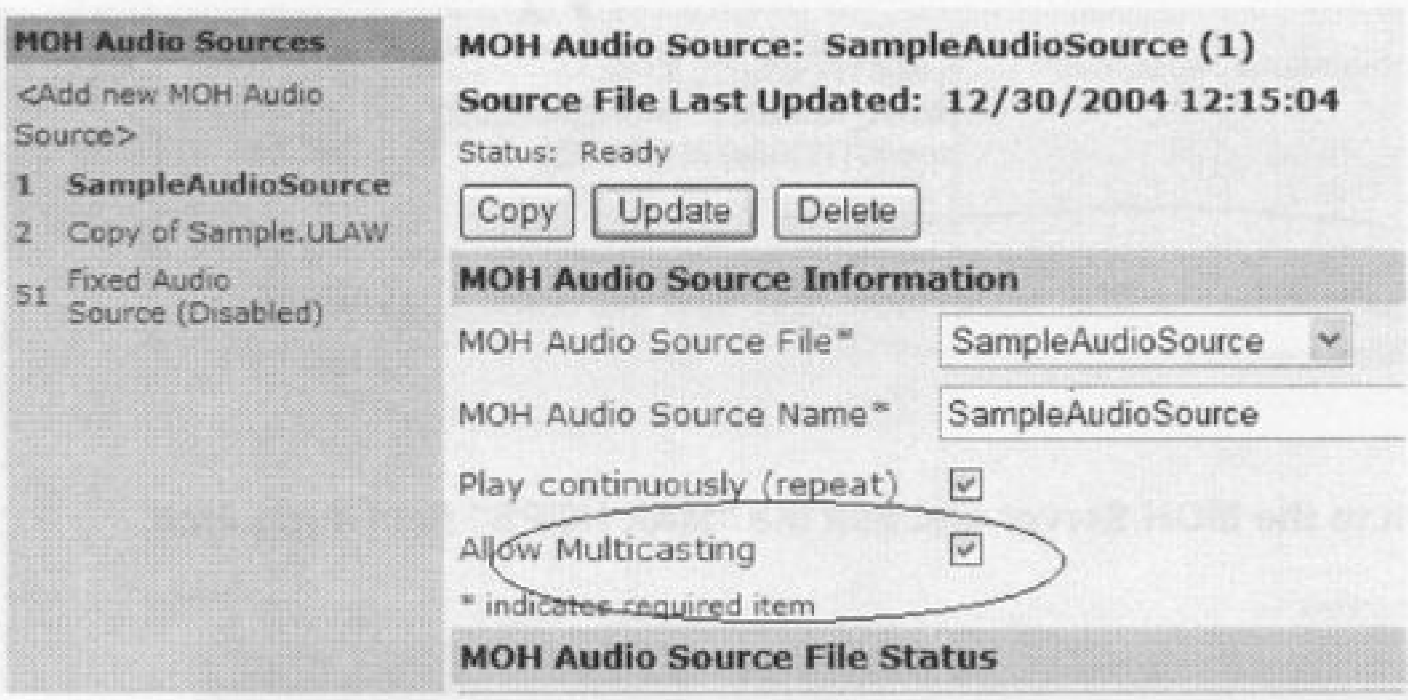
Task 7.8

Ensure that the HQ and BR1 phones receive multicast music on hold.

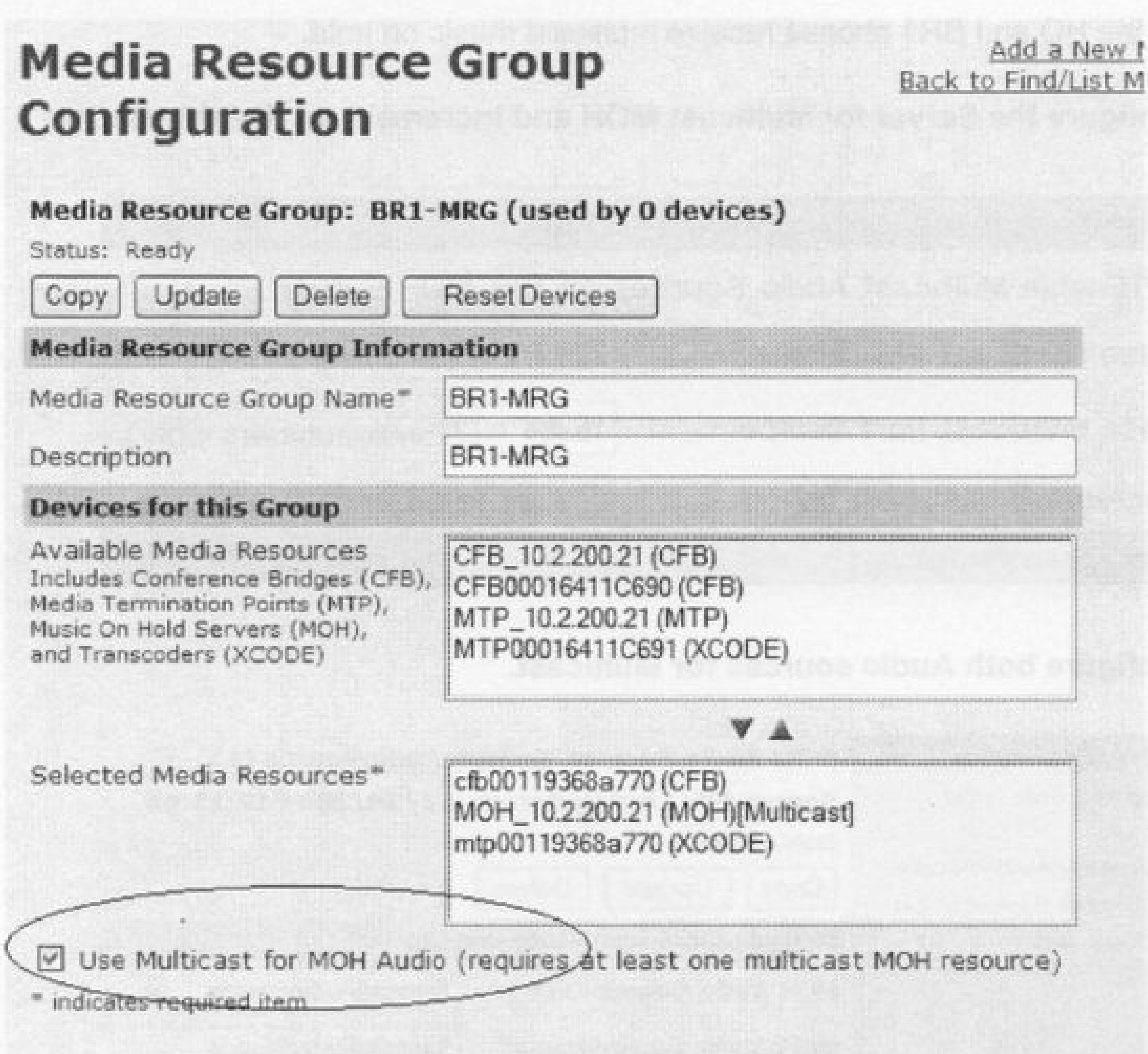
➔ **Configure the Server for Multicast MOH and increment on IP Address.**



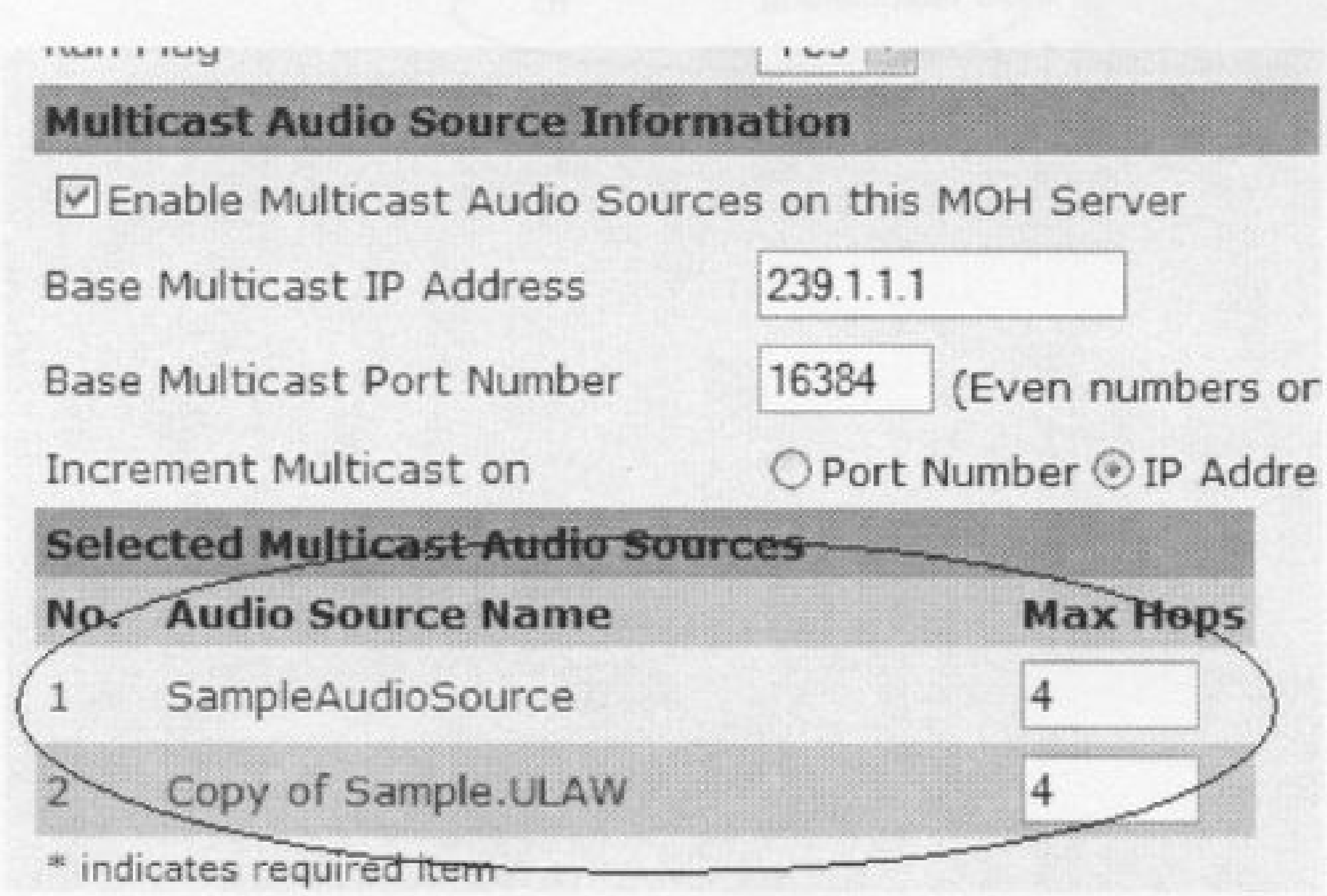
➔ **Configure both Audio sources for Multicast.**

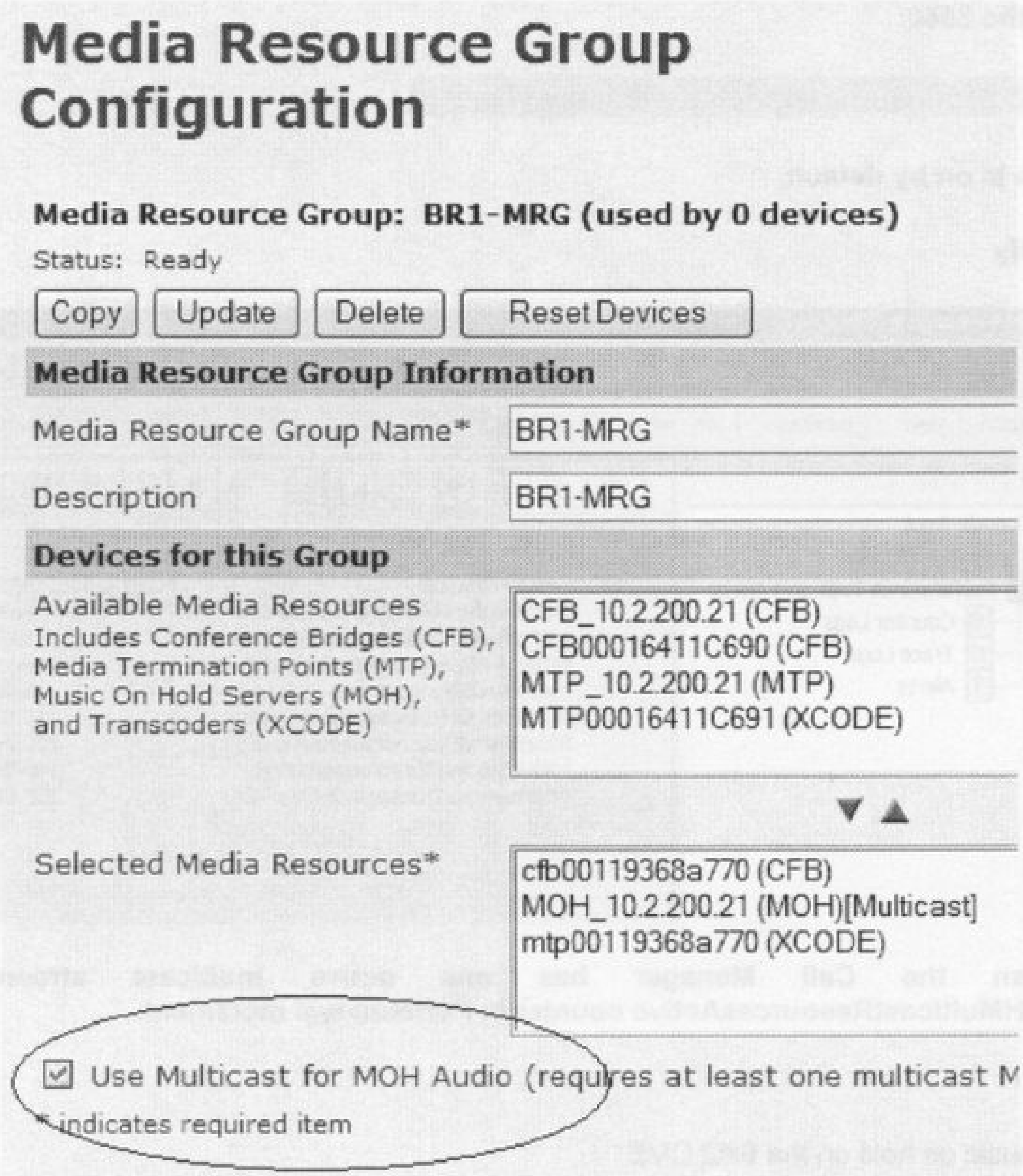


➔ **Configure both of the MRG for Multicast.**



➔ **Return to the MOH Server and edit the "MAX HOPS" field if required.**





➔ **Apply the appropriate MRGL to the corresponding Device Pool.**

➔ **The only remaining step is to configure multicast on the routers and switches.**

➔ **Multicast Routing needs to be enabled on all routers and pim dense-mode (or sparse-dense-mode) needs to be configured on all interfaces between the MOH server and the phones.**

```
P2-HQ-RTR(config)#
P2-HQ-RTR(config)#ip multicast-routing
P2-HQ-RTR(config)#int FastEthernet0/0.2
P2-HQ-RTR(config-subif)#ip pim dense-mode
```

➔ **On the 6500:**

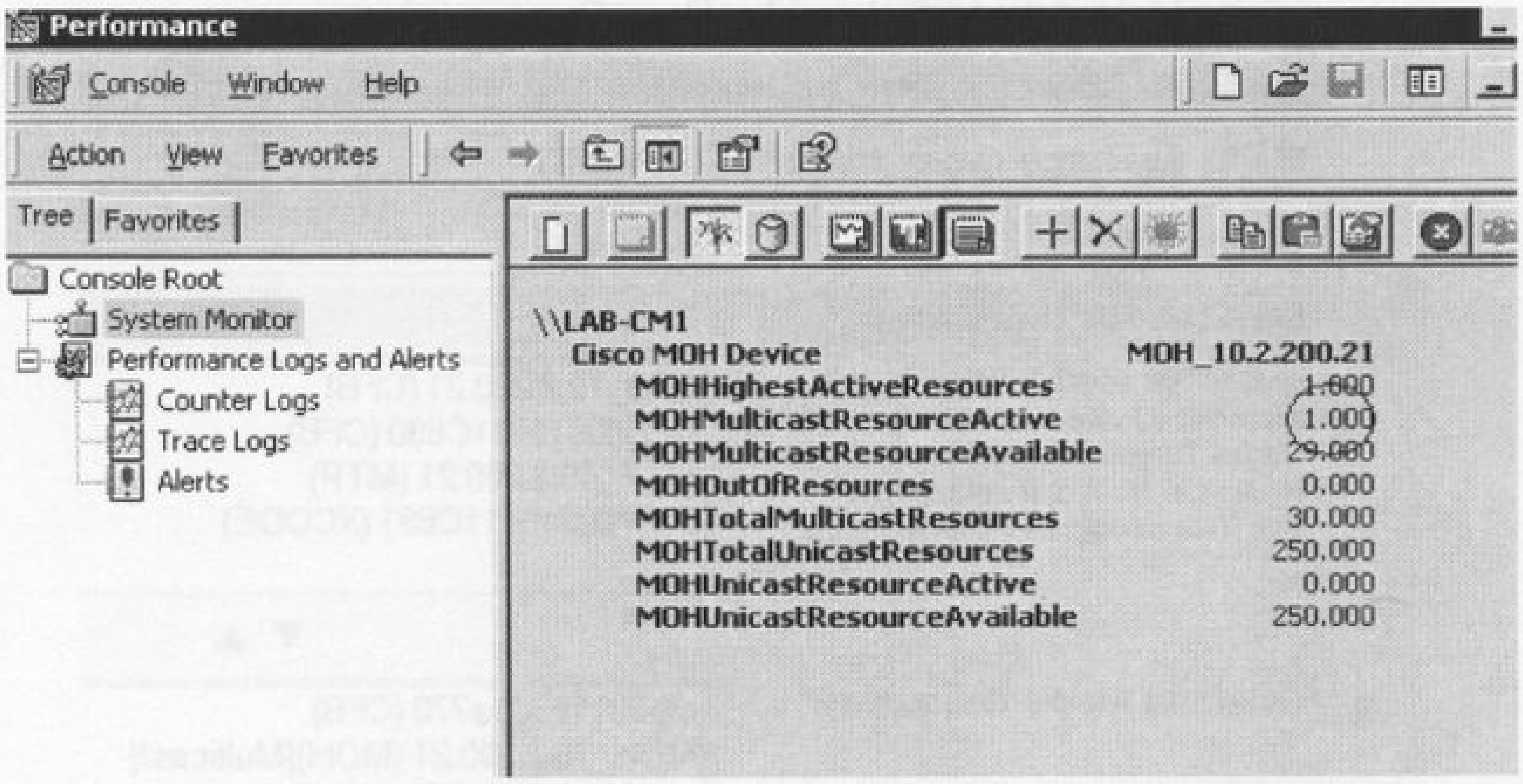
```
Console> (enable) set igmp enable
IGMP feature for IP multicast enabled
```

➔ **On the 3550:**

```
BR2-3550(config)#ip igmp snooping vlan 220
```

➔ **This is on by default.**

➔ **Verify**



➔ **When the Call Manager has one active multicast stream, the MOHMulticastResourcesActive counter in PerfMon will increment.**

Task 7.9

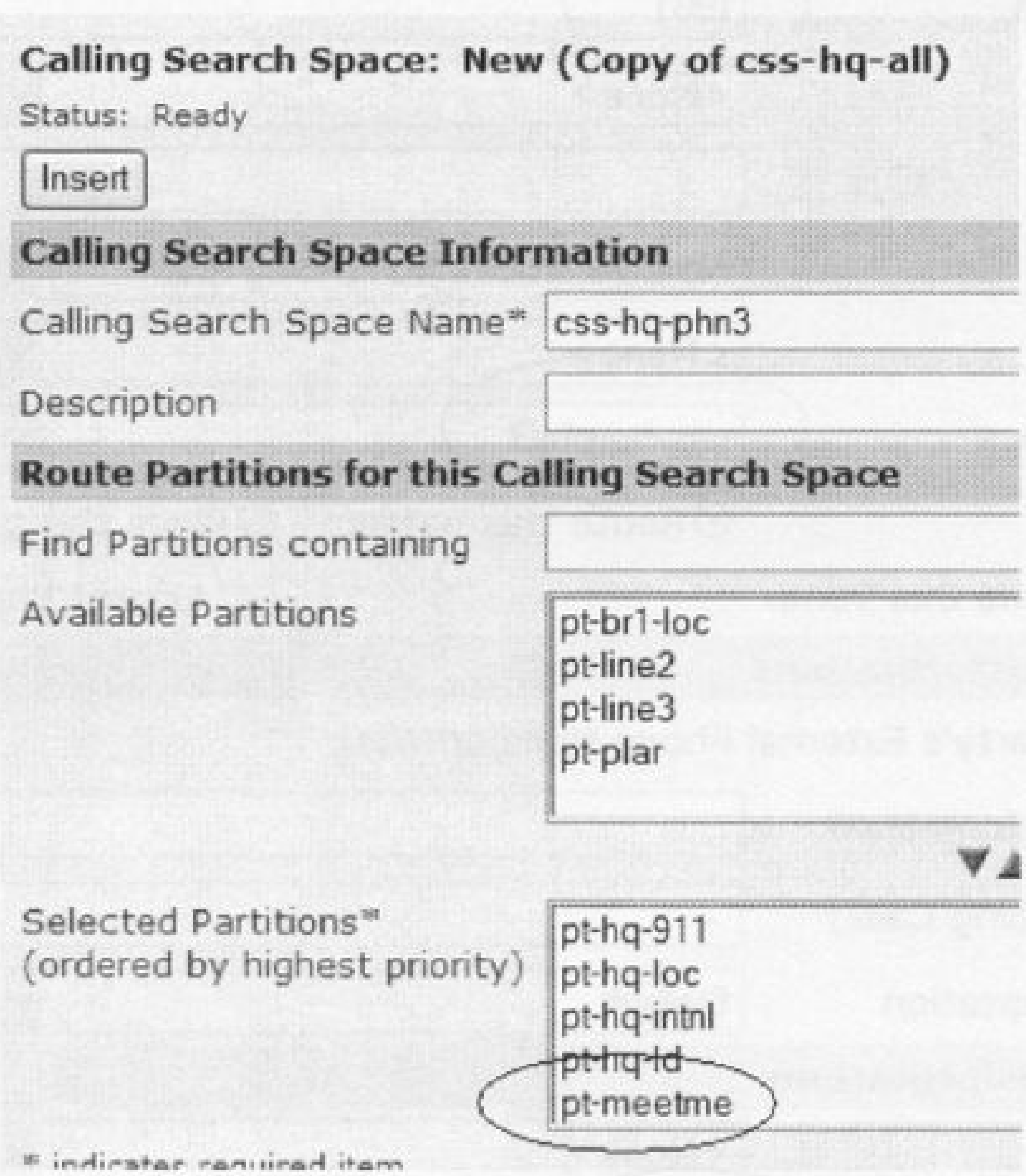
Configure music on hold on the BR2 CME.

```
telephony-service
 moh music-on-hold.au
```

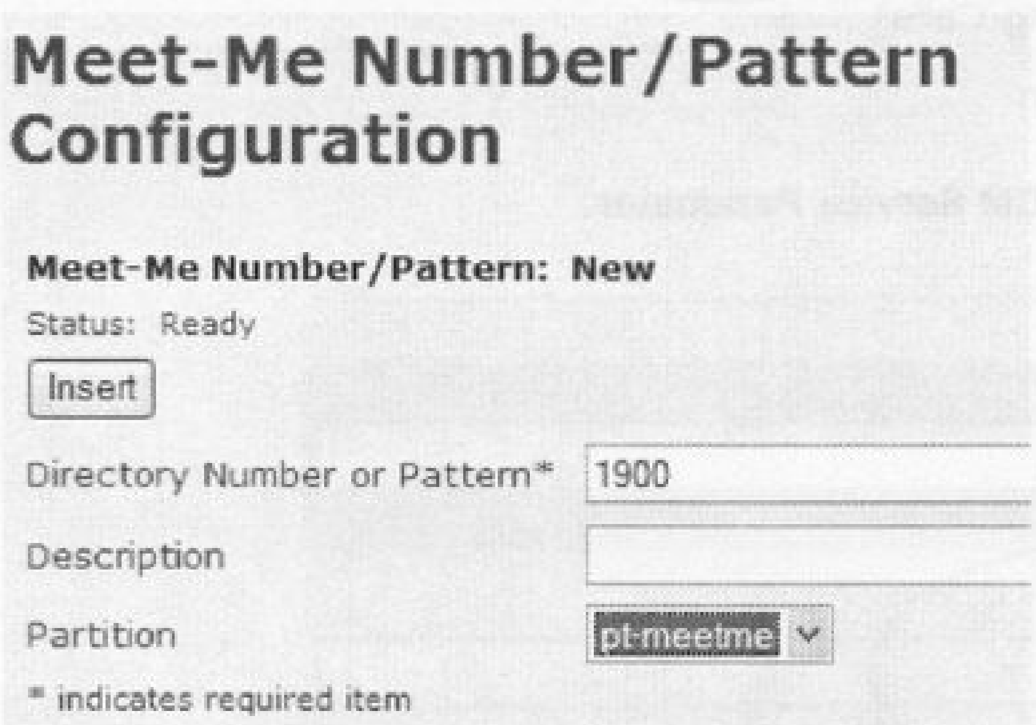
Task 7.10

Create a meet-me conference with DN=1900. Only HQ Phone 3 should be able to initiate the conference – other devices should be able to join/initiate this conference using DN=1901. Set the maximum number of participants of a single Meet-me conference to 6 conferencees.

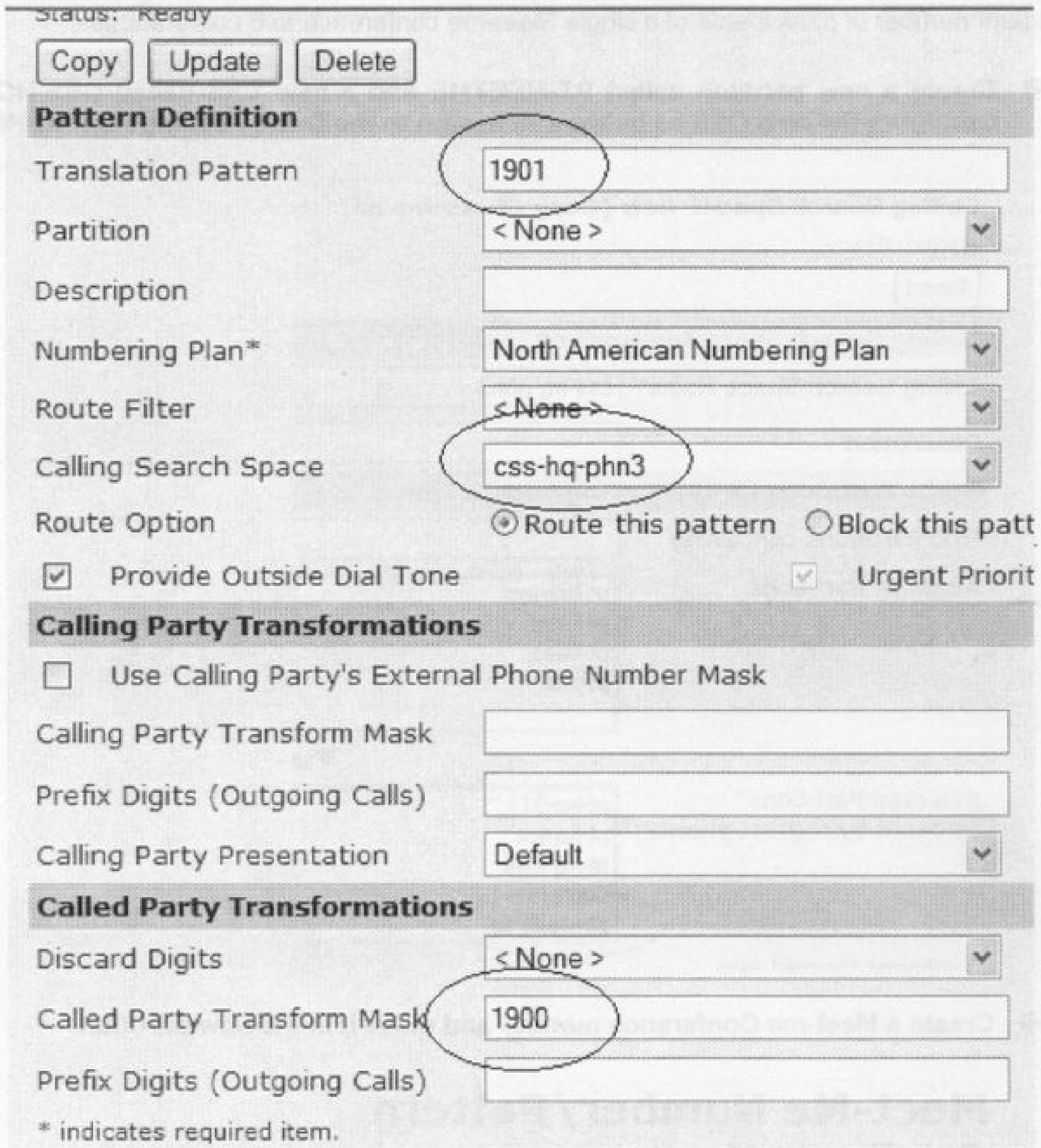
➔ **Create a new partition called PT-MEETME and a new CSS called CSS-HQ-PHN3. Configure the new CSS as below and assign to the Device settings on HQ Phone 3.**



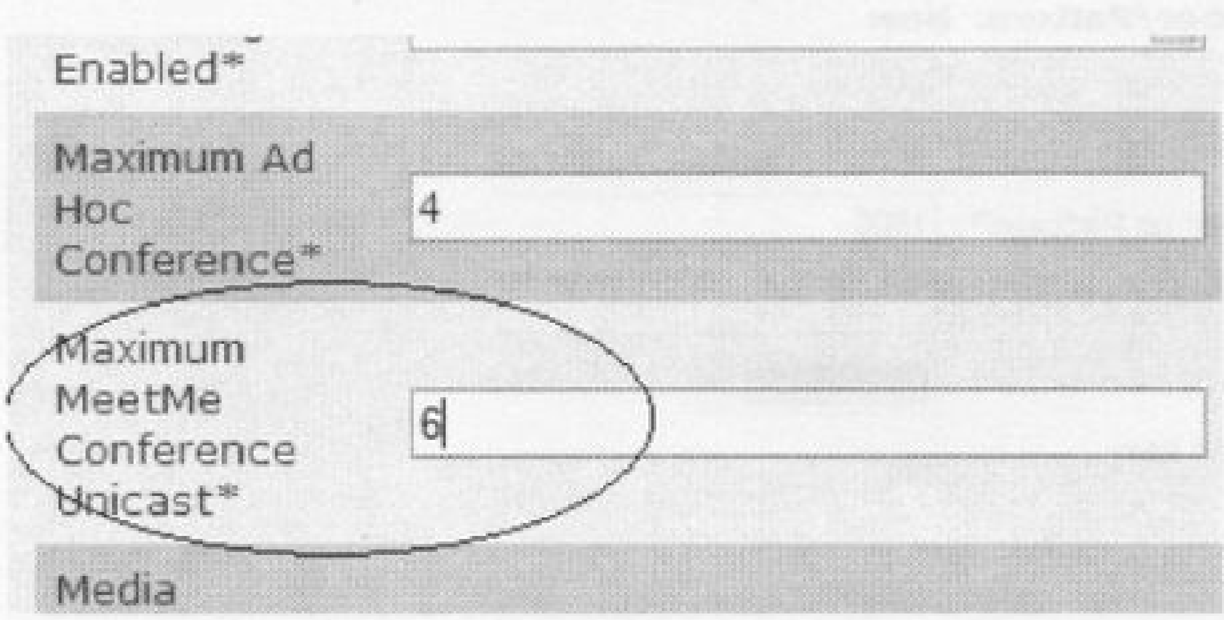
➔ **Create a Meet-me Conference number and place it in the new partition.**



➔ **Create a translation pattern in the Null Partition and Mask the Called Number as shown below. The Translation Pattern must be assigned a CSS with the Meet-me partition visible.**



➔ **Change the following CCM Service Parameter.**



Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 8: High Availability

Estimated Time to Complete: 2 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 8 High Availability

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

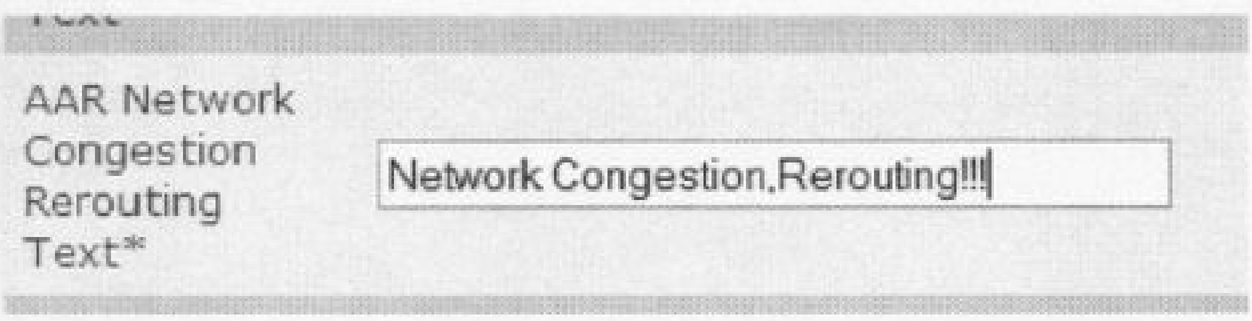
To complete this lab the dial plan section must have been completed (which implies all the pre-requisite sections of the dial plan).

Section 8 Configuration Tasks

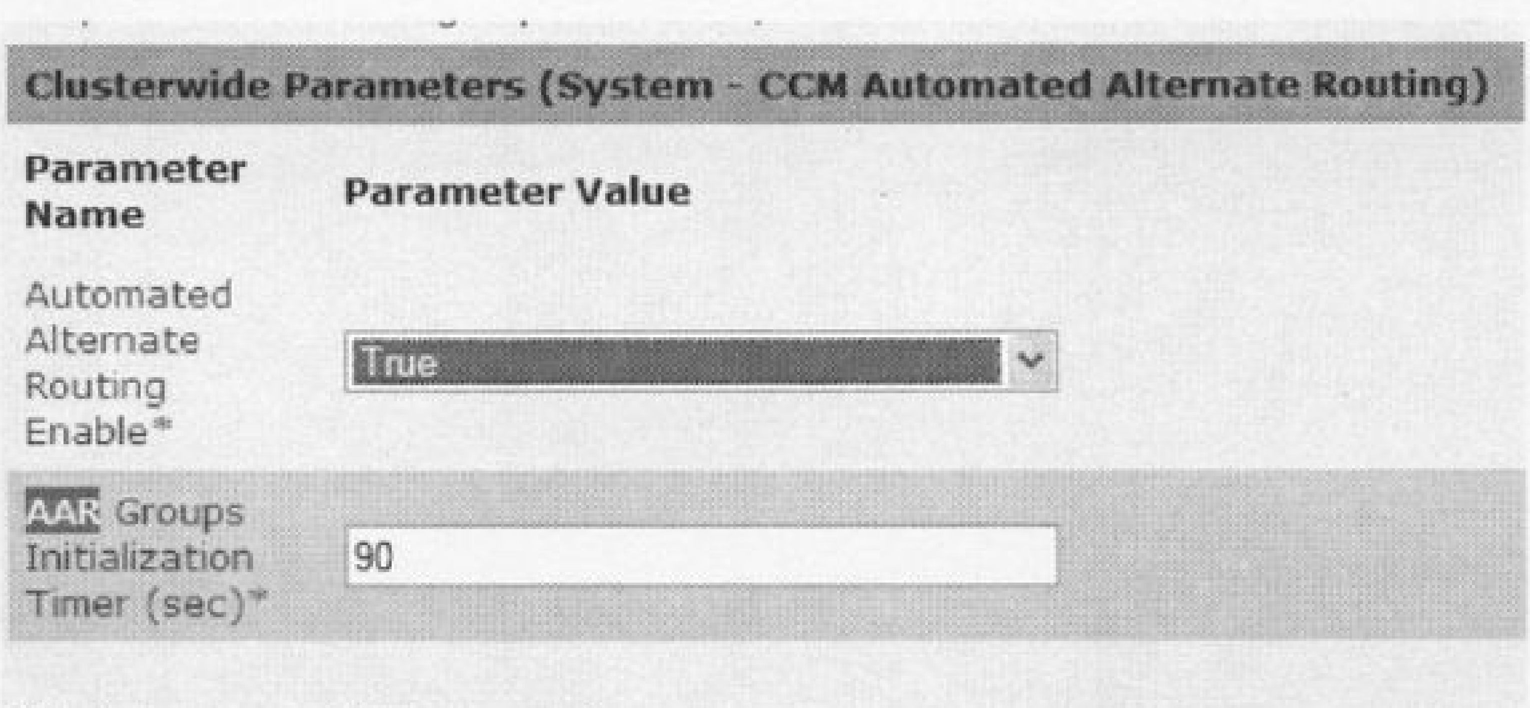
Task 8.1

Configure AAR such that calls between HQ and BR1 will be rerouted over the PSTN when there is not enough bandwidth over the WAN. You must preserve 10 digit Calling Number display. The text "*Network Congestion, Rerouting*!!!" must be displayed on the phone when AAR is being used.

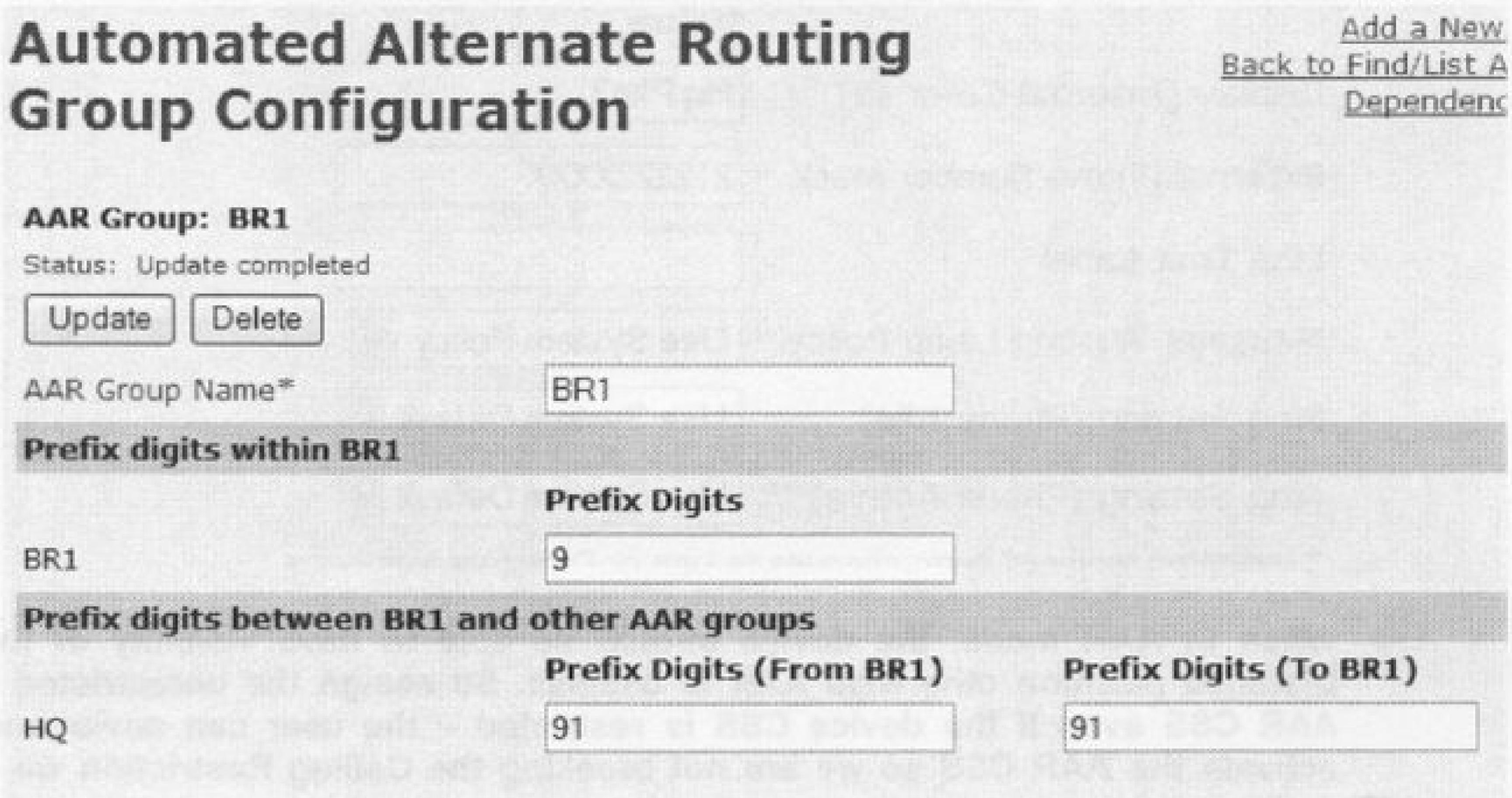
➔ **Change the text displayed on the phone when AAR is taking place. This is a CCM Service Parameter.**



➔ **Enable AAR system wide – this is a CCM Service Parameter in releases CCM3.3.4 and after, and in Enterprise Parameters in CCM3.3.3 and earlier releases of CCM3.3.**

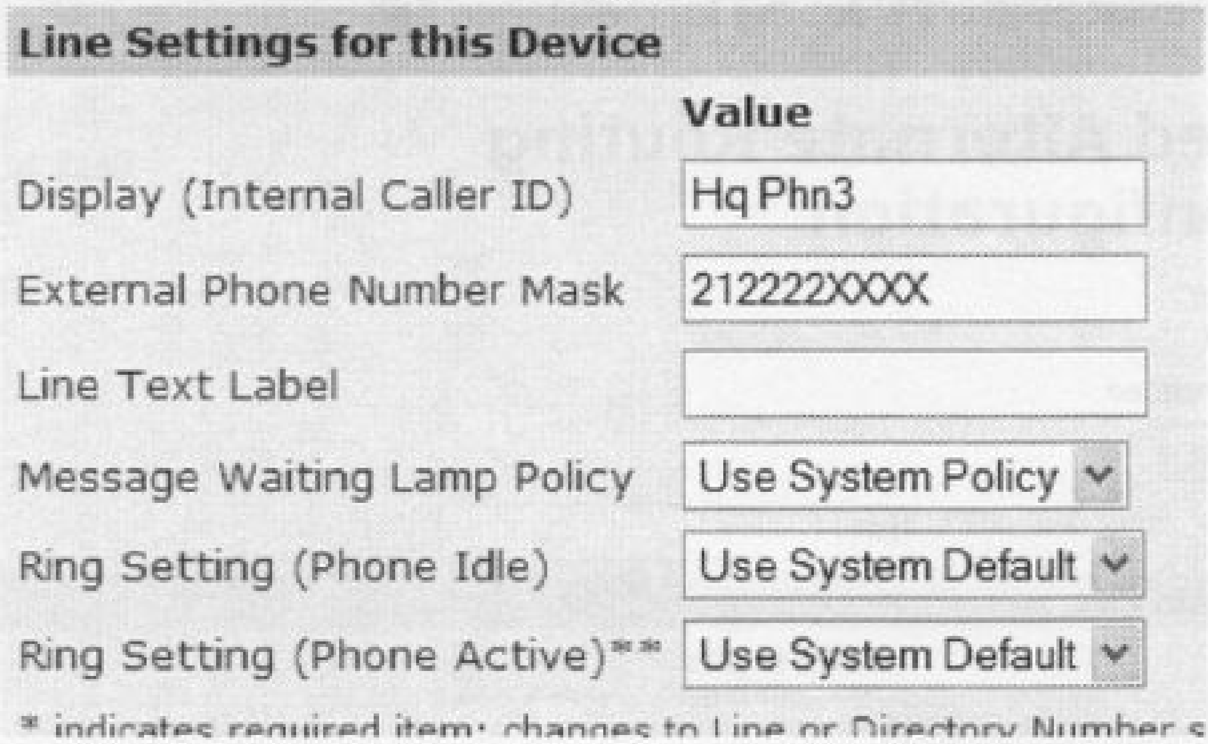


➔ **Configure two AAR groups – one for HQ and one for BR1. We are using 10 digit extension numbers on the LINE so to complete the transformation to match a valid route pattern we must prefix '91' for the long distance call.**



➔ **Assign the AAR Group to the HQ and BR1 phones.**

➔ **Also in the LINE ensure that External Number Mask is set correctly.**



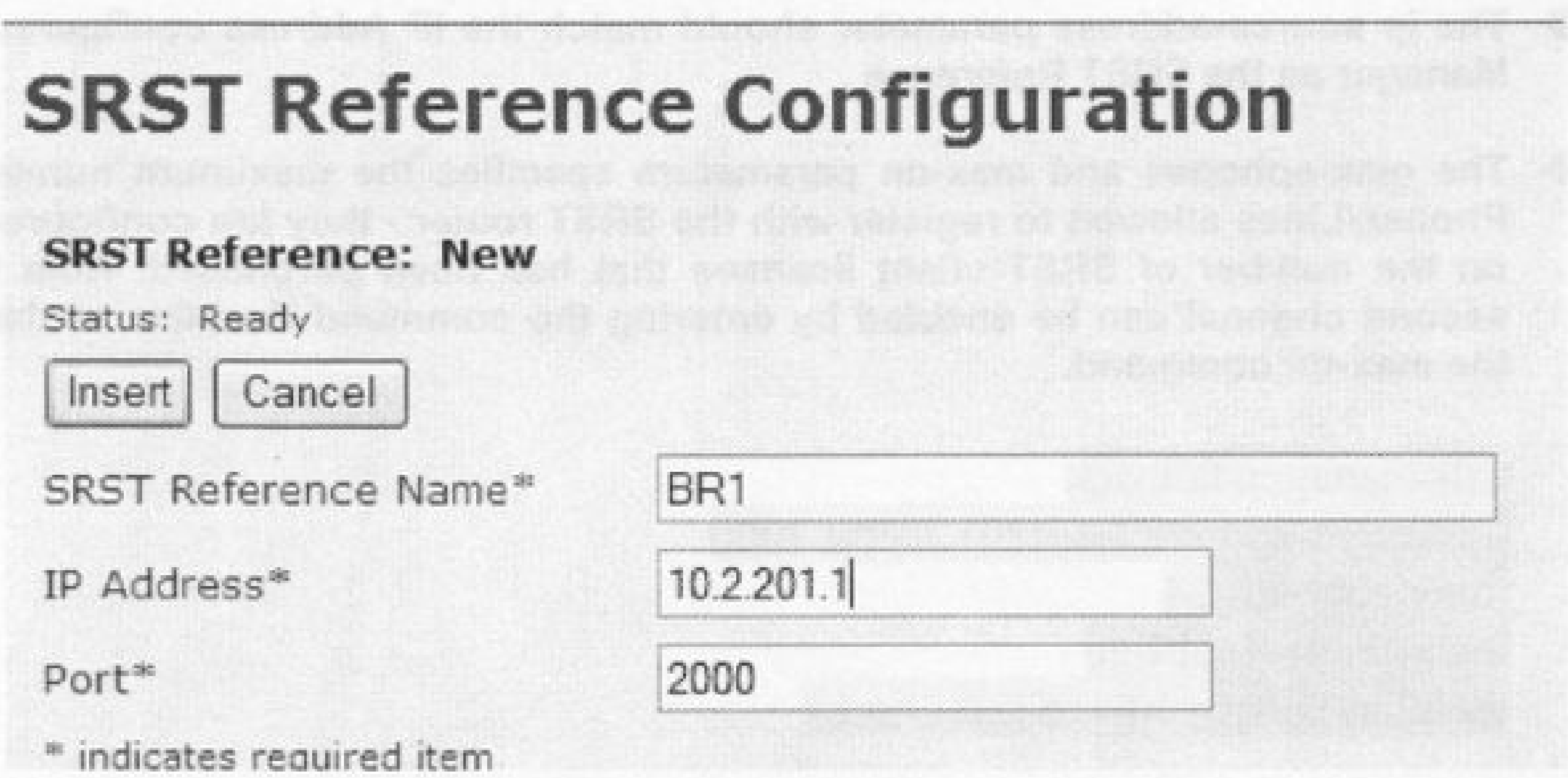
➔ **When in AAR mode, the device should be able to have visibility of the Long Distance partition otherwise AAR is useless. So assign the unrestricted CCS to AAR CSS even if the device CSS is restricted – the user can never knowingly activate the AAR CSS so we are not breaking the Calling Restriction we created earlier.**

➔ **Restart the CCM Service and bring the Location bandwidth down to 23Kbps. Call between sites and verify that AAR is working. On the Calling Device you will see the "Network Congestion Rerouting!!!" text appear as opposed to the "Not Enough Bandwidth" text that usually appears on the LCD when Locations CAC blocks a call.**

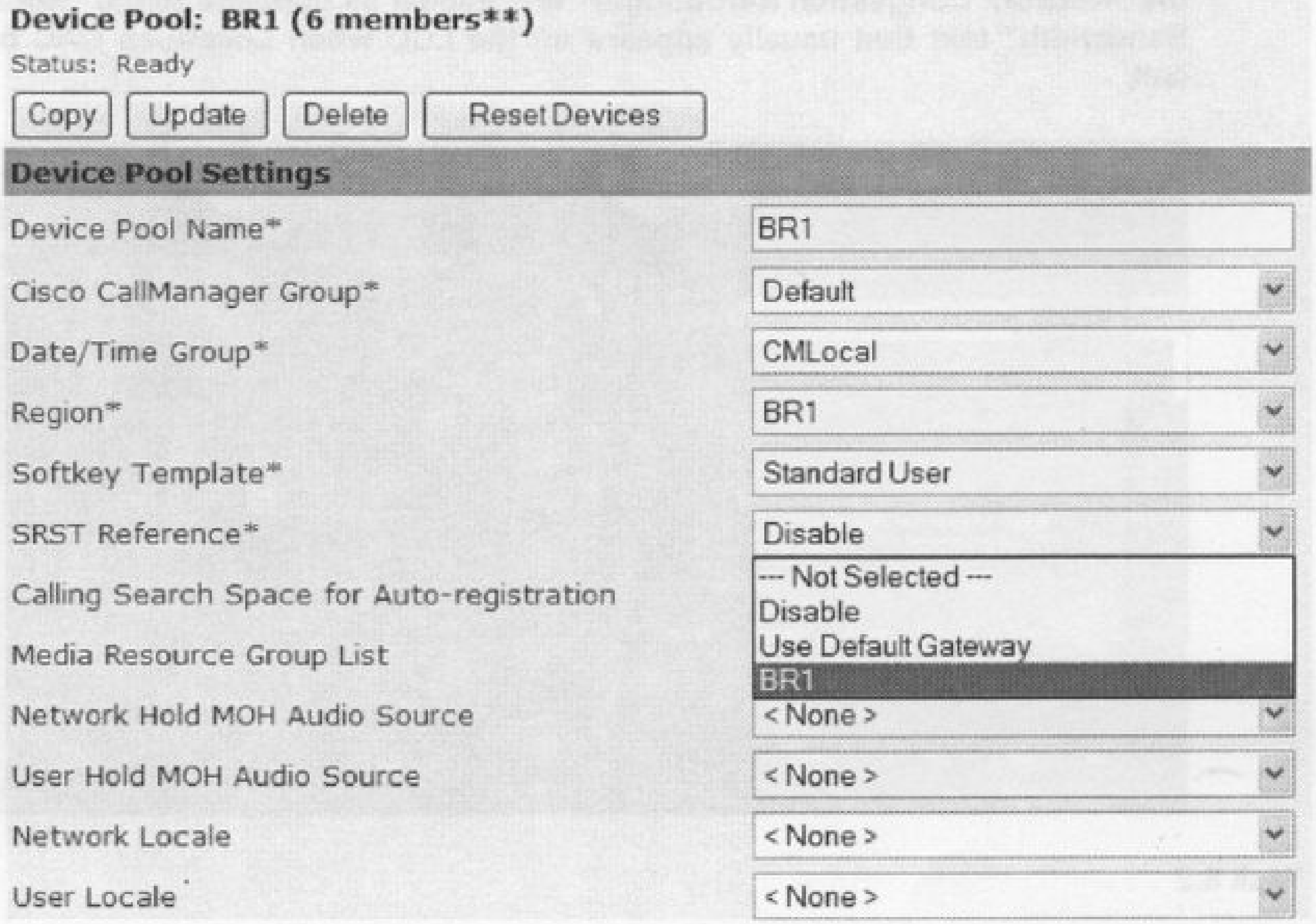
Task 8.2

Configure SRST at BR1 so that in the event of a WAN failure users can still make/receive calls from the PSTN. Use the voice sub-interface as the source address BUT assume that this is not the default gateway. All phones registered must have the second channel enabled on their lines.

➔ **Create a SRST Reference from the System menu.**



➔ **Assign the SRST Reference to the BR1 Device Pool and reset the BR1 devices.**



➔ **Now configure the IOS MGCP gateway for SRST. There are two separate type of fallback we want to enable (1) to allow the phones to register to the router via SCCP and (2) the MGCP gateway to become a temporary H323 gateway (since MGCP is a Master/Slave protocol the gateway is useless without the CCM).**

➔ **The ip source-address parameter should match the IP Address configured in Call Manager as the SRST Reference .**

➔ **The max-ephones and max-dn parameters specifies the maximum number of IP Phones/Lines allowed to register with the SRST router - they are configured based on the number of SRST client licenses that has been purchased. Note that the second channel can be enabled by entering the command dual-line at the end of the max-dn command.**

```
call-manager-fallback
 ip source-address 10.2.201.1 port 2000
 max-ephones 24
 max-dn 48 dual-line
dialplan-pattern 1 6175222… ext 4
```

➔ **For the router to fallback to the default application (H323), configure this command in global configuration mode. If the MGCP application is not available, the default application takes over.**

```
P2-BR1-RTR(config)#call application alternate default
```

➔ **Enable Call Manager Fallback.**

P2-BR1-RTR(config)#ccm-manager fallback-mgcp

➔ **To verify stop the CCM Service and check the status of the IOS gateway.**

P2-BR1-RTR#sh ephone summ

```
ephone-1 Mac:0011.93B6.EC51 TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
IP:10.2.201.120 Telecaster 7960 keepalive 6 1:1 CM Fallback

ephone-2 Mac:0011.BBE1.AD5F TCP socket:[2] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
IP:10.2.201.121 Telecaster 7940 keepalive 6 1:2 CM Fallback

Max 24, Registered 2, Unregistered 0, Deceased 0, Sockets 2
ephone_send_packet process switched 0
```

```
P2-BR1-RTR(config)#do sh ccm
MGCP Domain Name: P2-BR1-RTR
Priority        Status          Host
Primary         Down            10.2.200.21
First Backup    None
Second Backup   None

Current active Call Manager:    None
Backhaul/Redundant link port:   2428
Failover Interval:              30 seconds
Keepalive Interval:             15 seconds
Last keepalive sent:            14:10:11 UTC Sep 15 2005 (elapsed time: 00:00:20)
Last MGCP traffic time:         14:10:11 UTC Sep 15 2005 (elapsed time: 00:00:20)
Last failover time:             None
Last switchback time:           None
Switchback mode:                Graceful
MGCP Fallback mode:             Enabled/ON
Last MGCP Fallback start time:  14:09:55 UTC Sep 15 2005
Last MGCP Fallback end time:    14:10:11 UTC Sep 15 2005
MGCP Download Tones:            Disabled
```

Task 8.3

Configure the SCCP heartbeat timer to 20 seconds and ensure the clock displayed on the phone is using the 12 hour display. Also ensure that the inter-digit timeout is 7 seconds.

➔ **The keepalive command is applicable only after a Cisco IP phone has registered with the Cisco SRST-enabled router.**

```
P2-BR1-RTR(config)#call-manager-fallback
P2-BR1-RTR(config-cm-fallback)#keepalive 20
P2-BR1-RTR(config-cm-fallback)#timeouts interdigit 7
P2-BR1-RTR(config-cm-fallback)#time-format 12
```


Task 8.4

Configure SRST such that one 3-party conference is allowed.

P2-BR1-RTR(config-cm-fallback)#max-conferences 1

Task 8.5

Configure Music on Hold for all phones in SRST fallback.

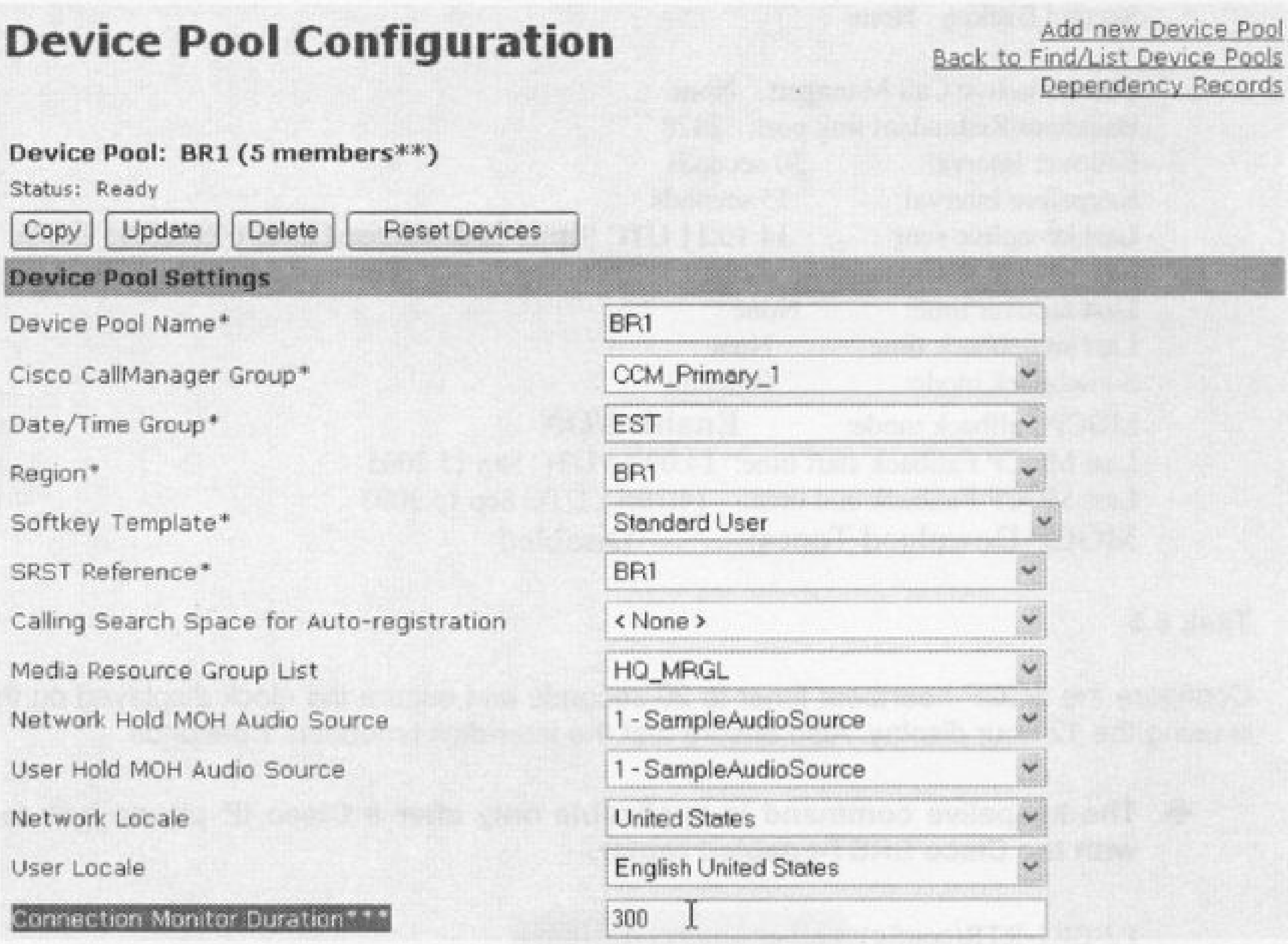
➔ **If the music-on-hold.au file does not exist, pull down with TFTP from the CCM.**

P2-BR1-RTR(config-cm-fallback)#moh music-on-hold.au

Task 8.6

Configure SRST such that the phones will only re-register back to Call Manager after normal service has been resumed for 5 minutes. (normal service is defined as the WAN is operational and Call Manager service is running).

➔ **In CCM configure the Connection Monitor Duration Timer in Device Pool. This setting defines the amount of time that the IP phone monitors its connection to Cisco CallManager before it unregisters from SRST and re-registers to Cisco CallManager.**



➔ **The default value, which specifies 120 seconds, resides in the Connection Monitor Duration enterprise parameter.**

➔ **Change this setting if you need to disable the connection monitor (by changing the value to zero) or if you want to extend the connection monitor time.**

Task 8.7

Calls to HQ and BR2 must be preserved using 4 digit dialing. You cannot use the 'prefix' command or translation rules to achieve this task.

➔ **Use the num-exp command - for configuration see Task 8.9.**

Task 8.8

Ensure that the same Class of restriction is preserved when phones are in SRST fallback.

➔ **Configure COR - for configuration see Task 8.9. For detailed explanation see Task 3.2.**

Task 8.9

Configure Class of Restriction such that no PSTN caller can dial BR1 phone 2.

➔ **The dial-peers defined in the CCME tasks of the dial-plan section can be re-used with one or two exceptions.**

```
num-exp 1... 12122221...
num-exp 3... 0113313223...

dial-peer cor custom
 name pt-911
 name pt-loc
 name pt-ld
 name pt-internl
!
!
dial-peer cor list css-911
 member pt-911
!
dial-peer cor list css-loc
 member pt-loc
!
dial-peer cor list css-ld
 member pt-ld
!
dial-peer cor list css-intnl
 member pt-internl
!
dial-peer cor list css-911-loc
 member pt-911
 member pt-loc
!
dial-peer cor list css-ALL
 member pt-911
 member pt-loc
 member pt-ld
 member pt-internl
```



```
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 2/0/0:23
!
dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 2/0/0:23
!
dial-peer voice 9911 pots
 corlist outgoing css-911
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 2/0/0:23
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......
 port 2/0/0:23
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 port 2/0/0:23
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 9011T
 port 2/0/0:23
 prefix 011
!
dial-peer voice 1001 pots
 destination-pattern 12122221...
 no digit-strip
 port 2/0/0:23
!
dial-peer voice 3001 pots
 destination-pattern 0113313223...
 no digit-strip
 port 2/0/0:23
!
dial-peer voice 2 pots
 corlist incoming css-911
 incoming called-number .
 direct-inward-dial
!
!
call-manager-fallback
 max-conferences 1
 timeouts interdigit 7
```

```
ip source-address 10.2.201.1 port 2000
max-ephones 24
max-dn 48 dual-line
dialplan-pattern 1 6175222... extension-length 4
keepalive 20
moh music-on-hold.au
cor incoming css-911-loc 1 2002 - 2003
cor incoming css-ALL 2 2002
cor outgoing css-intnl 3 2002
```

Task 8.10

Use the TCL script already in IOS Flash to provide an IVR Auto-attendant in the case of a WAN down – SRST situation. The pilot DN for CallManager in a non-SRST event is 2000. The pilot DN for the SRST event should also be 2000. If no extension can be reached all calls should ring 2001.

➔ **The old style (pre 12.4) of inputting Call Applications and parameters is shown below**

```
call application voice srstaa flash:its_Cisco.2.0.1.0.tcl
call application voice srstaa language 1 en
call application voice srstaa aa-pilot 6175222000
call application voice srstaa cm-pilot 2000
call application voice srstaa operator 2001
call application voice srstaa set-location en 0 flash:
!
!
dial-peer voice 2000 pots
 incoming called-number 6175222000
 application srstaa
```

➔ **These can actually still be used if you want or are more familiar with – and when entered you will receive a number of these messages:**

```
Warning: This command has been deprecated and will be automatically
converted to the following:
```


➔ **And everything will be automatically configured for you as follows:**

```
application
 service srstaa flash:its_Cisco.2.0.1.0.tcl
  param operator 2001
  paramspace english language en
  paramspace english index 1
  paramspace english location flash:
  param cm-pilot 2000
  paramspace english prefix en
  param aa-pilot 6175222000
!
dial-peer voice 2000 pots
 incoming called-number 6175222000
 service srstaa
```

➔ **Also note that the only difference between the CME and the SRST version of this script is the parameter 'cm-pilot'.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 9: Unity

Estimated Time to Complete: 4 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 9 Unity

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab Section 1 and the basics within the CCM and CCME sections must be completed.

Section 9 Configuration Tasks

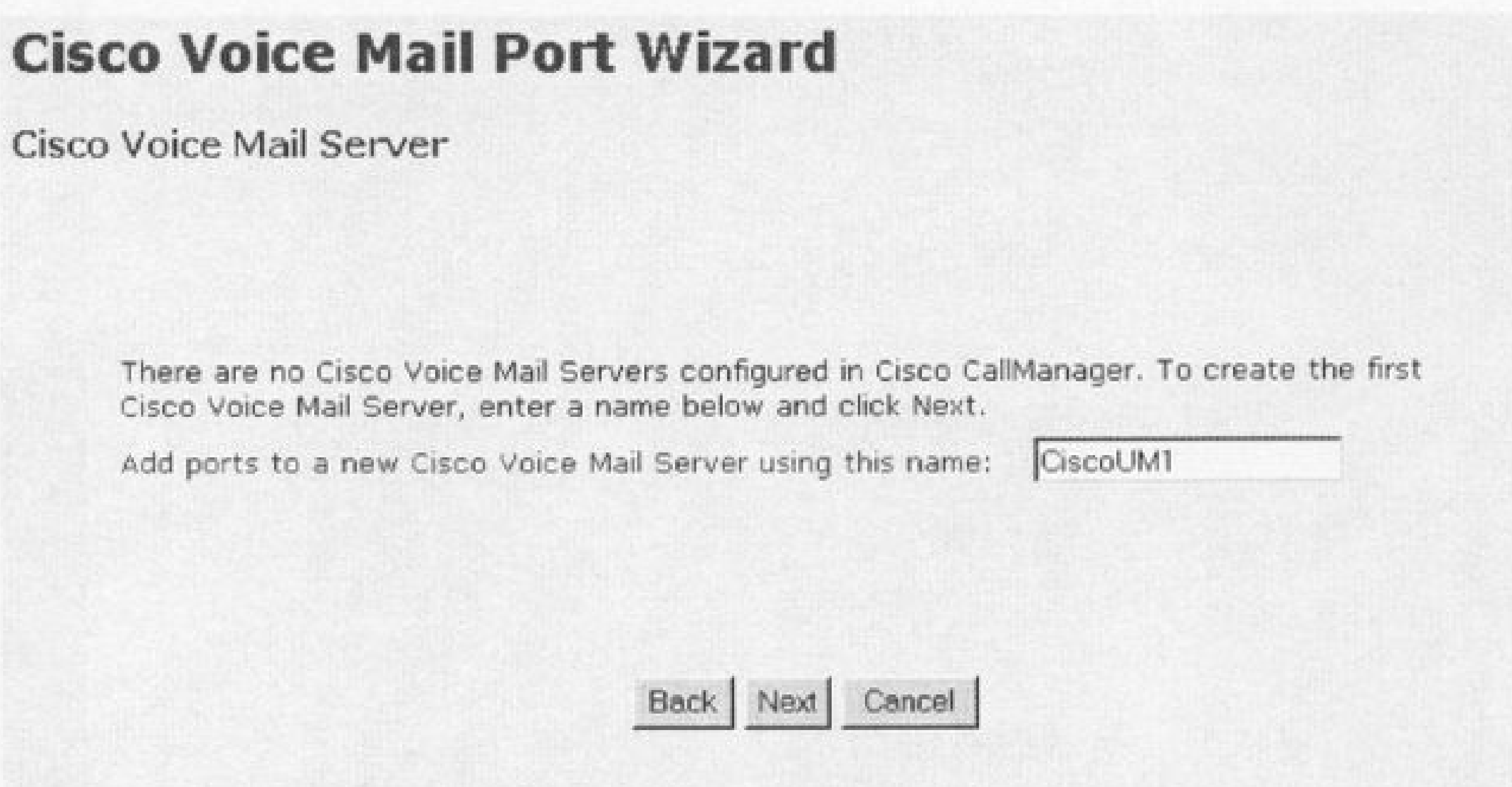
Task 9.1

Integrate Call Manager with Unity with the following information:

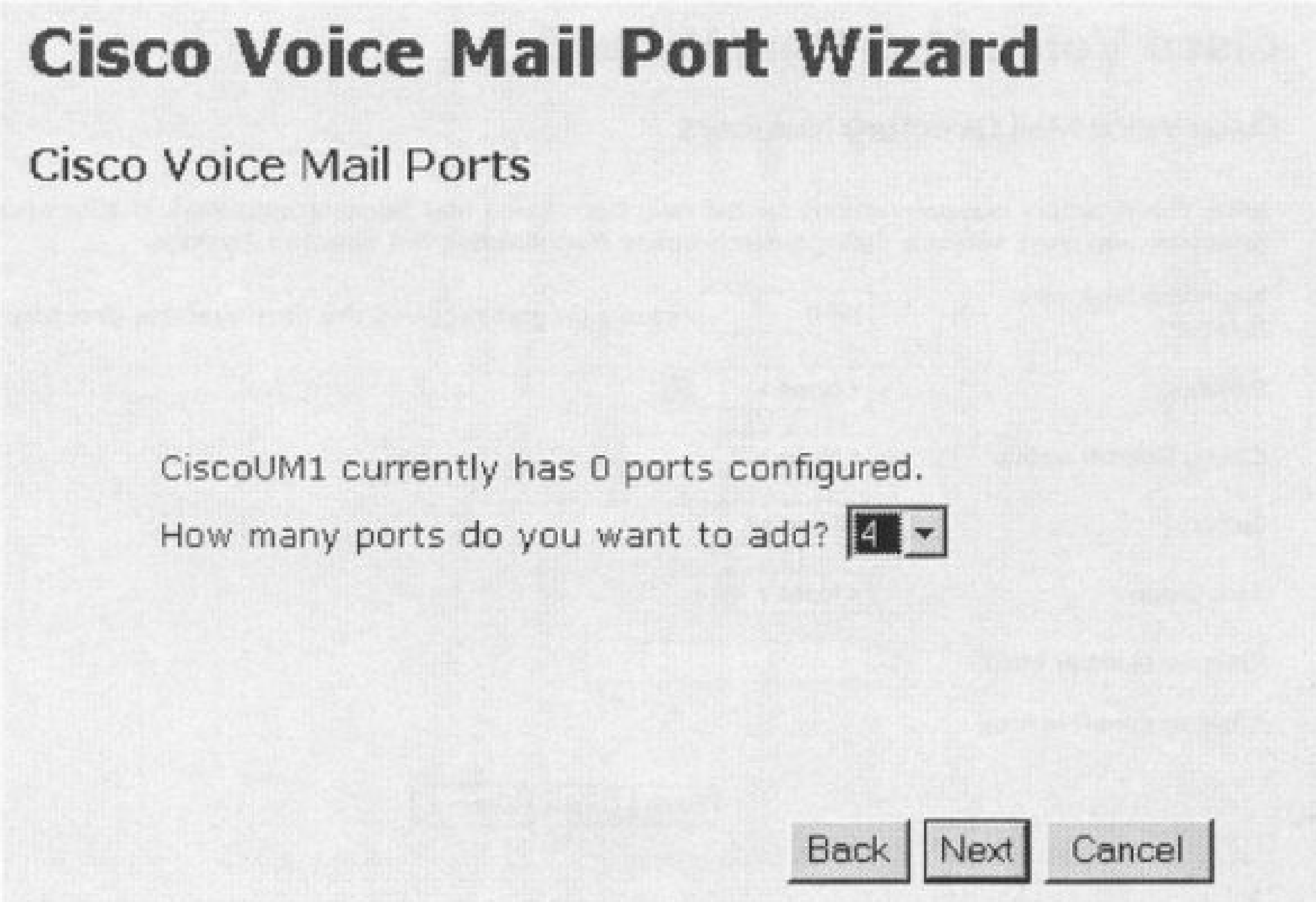
- Voice Mail Pilot = 1600
- Voice Mail Ports = 1601-1604
- MWI On/Off = 1999/1998

➔ **Run the voicemail port wizard from the Call Manager Administration web page click on Feature-Voice Mail-Cisco Voice Mail Port Wizard. Remember what the wizard doesn't do – you will need to configure MWI, Pilot and Profile.**

➔ **Leave the name of the port-prefix as the default.**

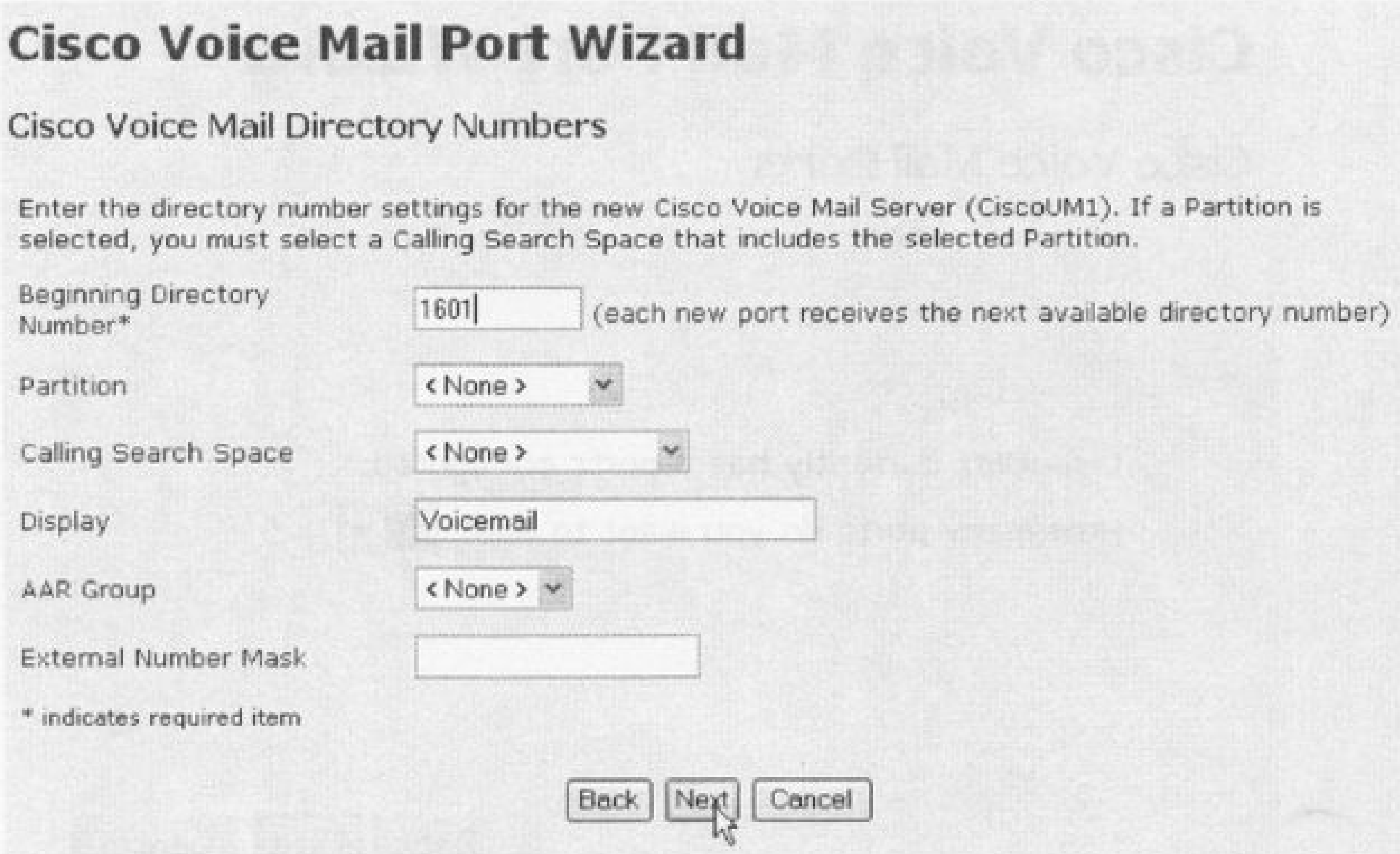


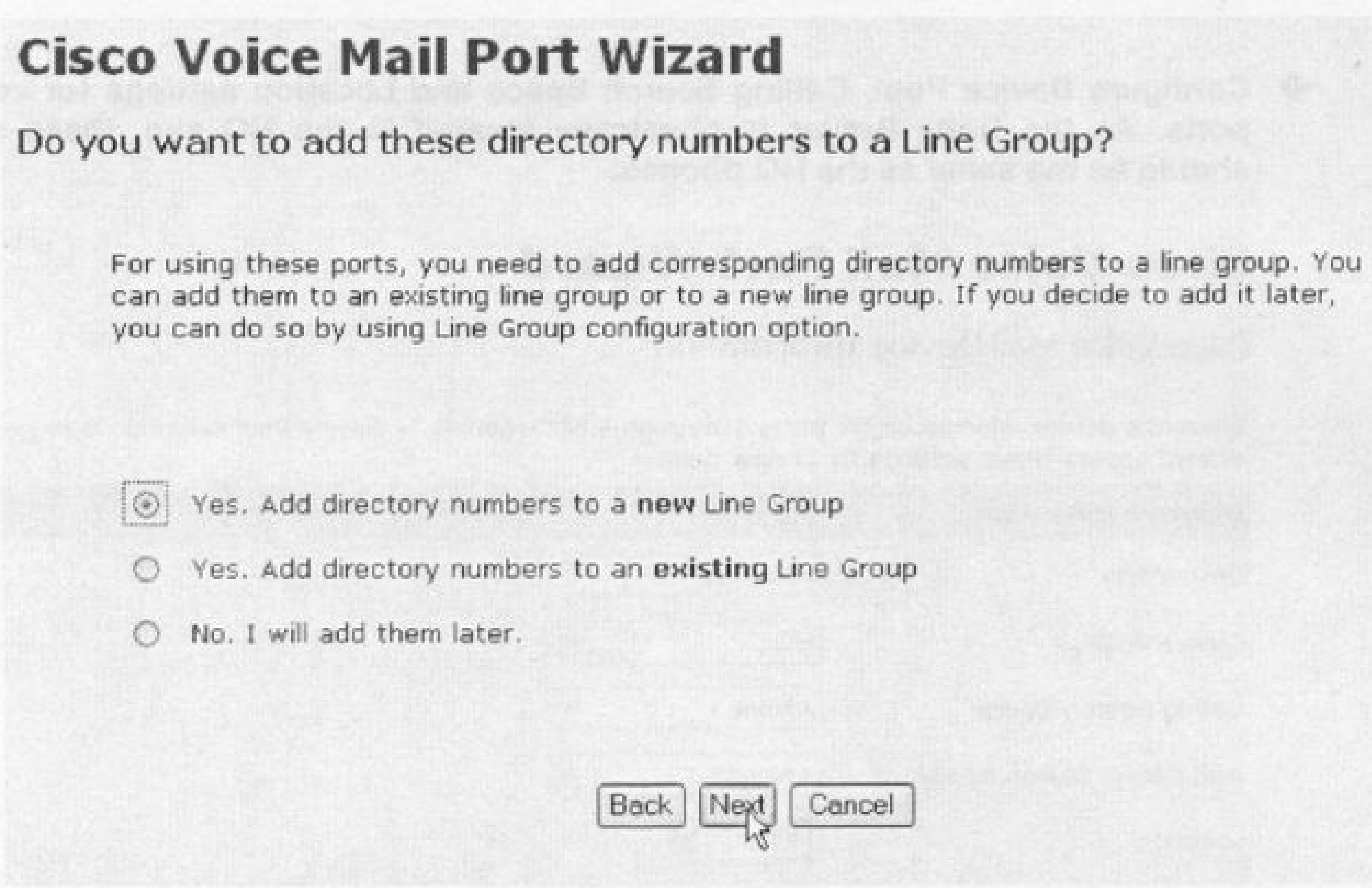
➔ **Select the number of ports you wish to configure - this is based on how many are licensed.**

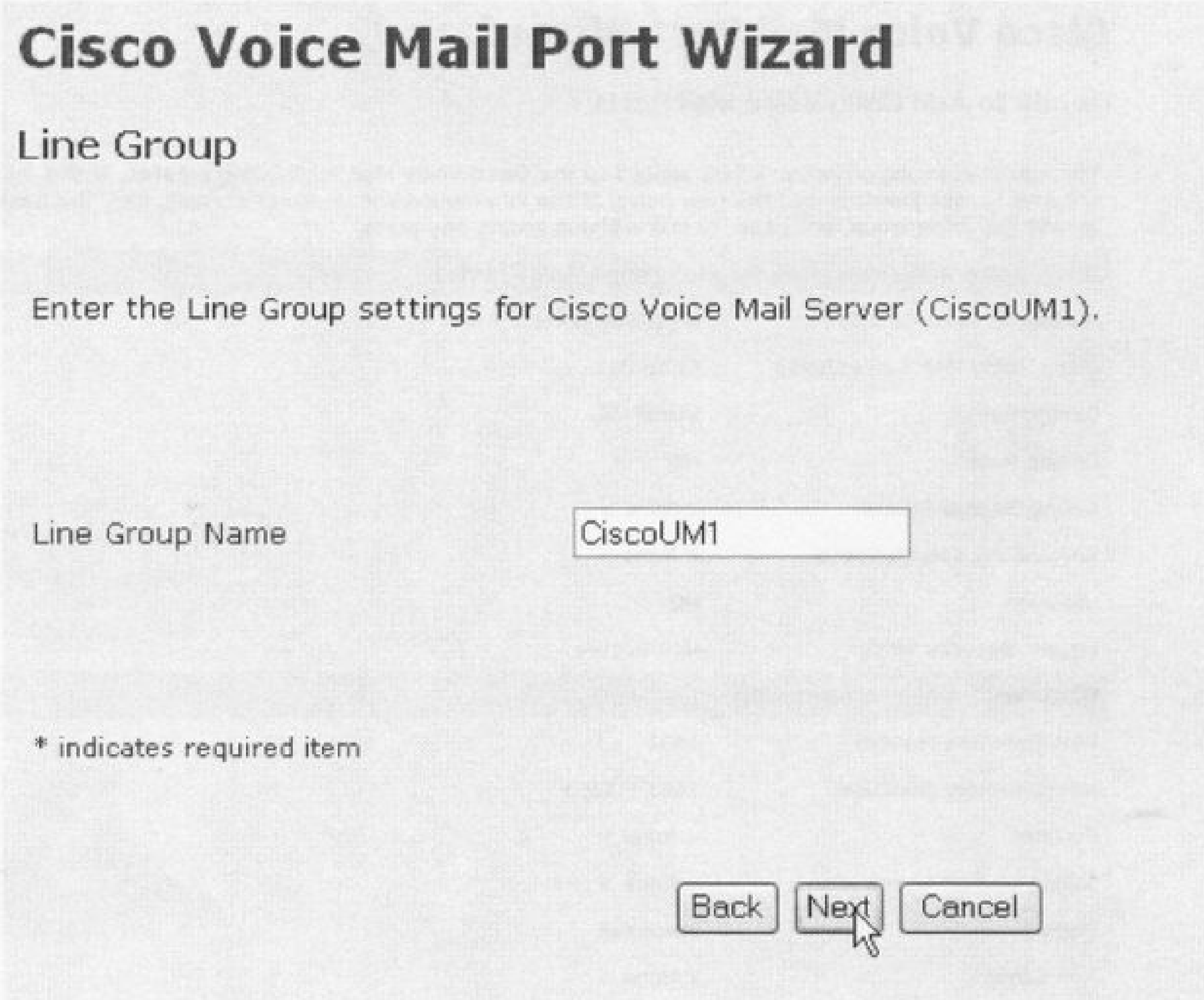


➔ **Configure Device Pool, Calling Search Space and Location settings for voicemail ports. As the Unity Server is physically located in the HQ site, these settings should be the same as the HQ phones.**

➔ **On the next page enter the DN of the Pilot Number and configure Partition and CSS - use the same as the phones you have configured on your system.**






Cisco Voice Mail Port Wizard
Line Group
Enter the Line Group settings for Cisco Voice Mail Server (CiscoUM1).
Line Group Name
CiscoUM1
* indicates required item
Back
Next
Cancel

Cisco Voice Mail Port Wizard

Ready to Add Cisco Voice Mail Ports

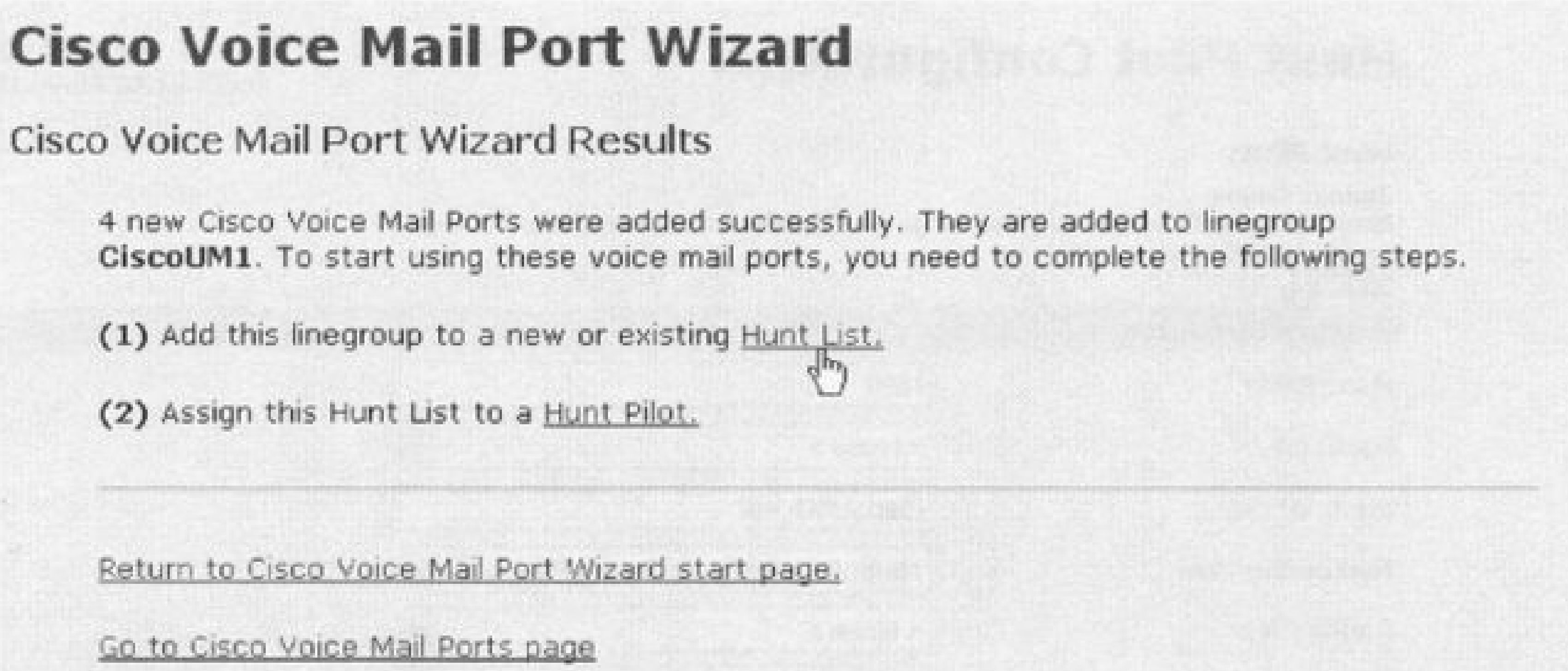
The information shown below will be applied to the Cisco Voice Mail Ports being created. If this information is correct, click Finish to add the new ports. If the information shown is not correct, click the Back button to edit the information, or Cancel to quit without adding any ports.

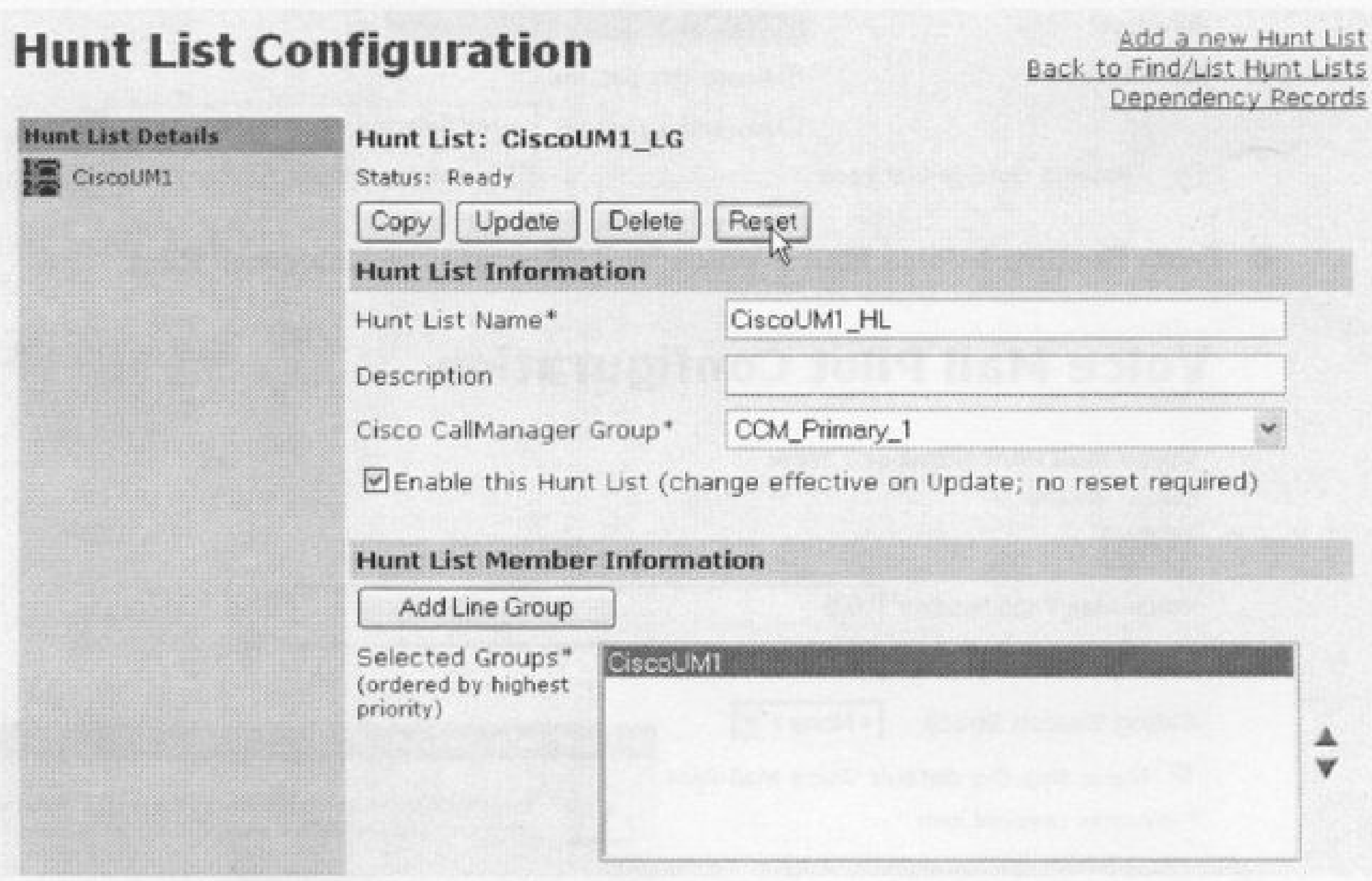
Cisco Voice Mail Device Information (apply to all ports)	
Number of Ports to Add	4 (adding ports 1 - 4)
Cisco Voice Mail Server Name	CiscoUM1
Description	Voicemail
Device Pool	HQ
Calling Search Space	< None >
AAR Calling Search Space	< None >
Location	HQ
Device Security Mode	Non Secure

Directory Number Information	
Pilot Directory Number	1601
New Directory Numbers	1601 - 1604
Partition	< None >
Calling Search Space	< None >
Display	Voicemail
AAR Group	< None >
External Number Mask	< None >
Line Group	CiscoUM1

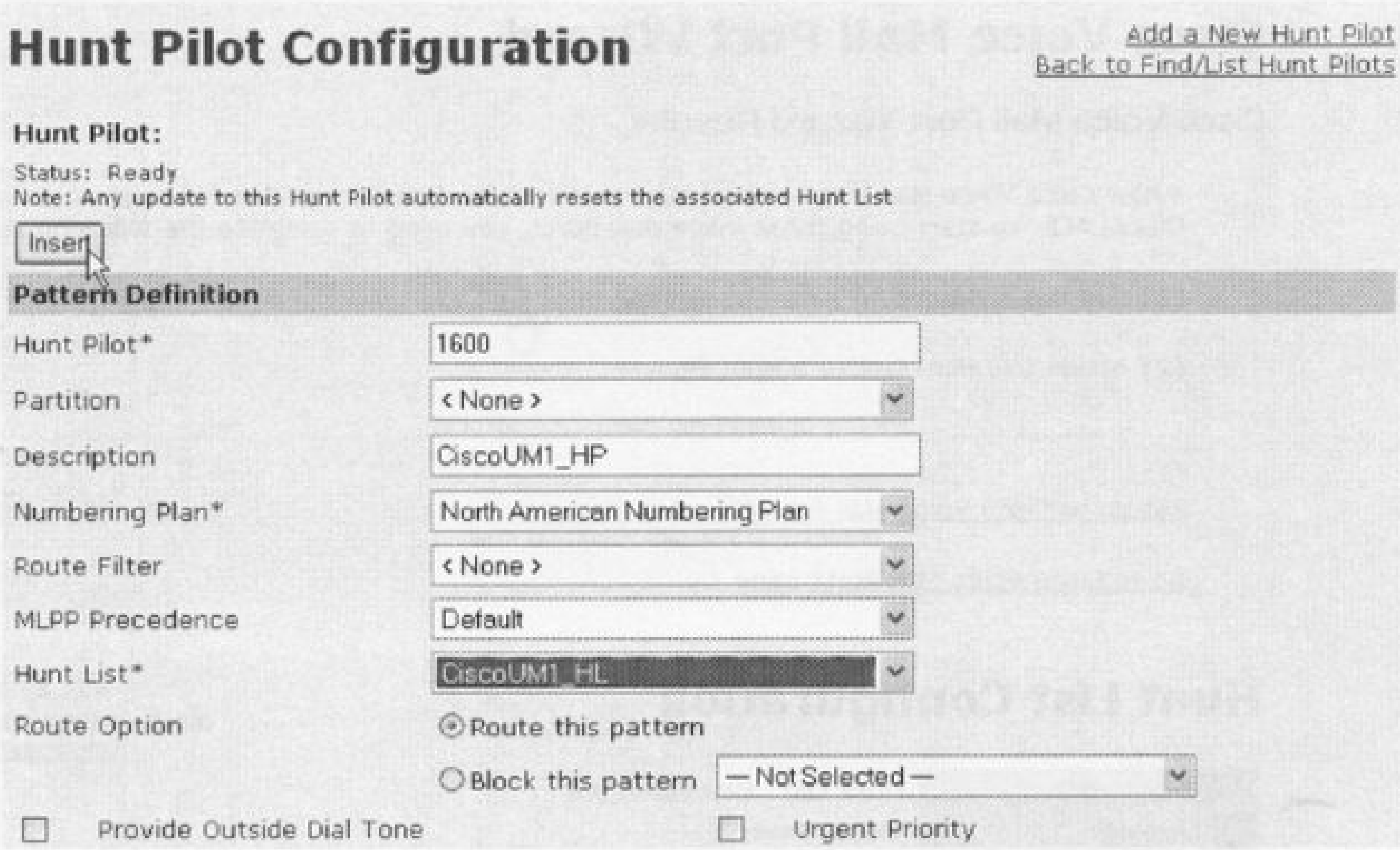
Back | Finish | Cancel

➔ **Departing from CCM 3.3, we need to add these which have been placed in a Line Group – into a Hunt List.**

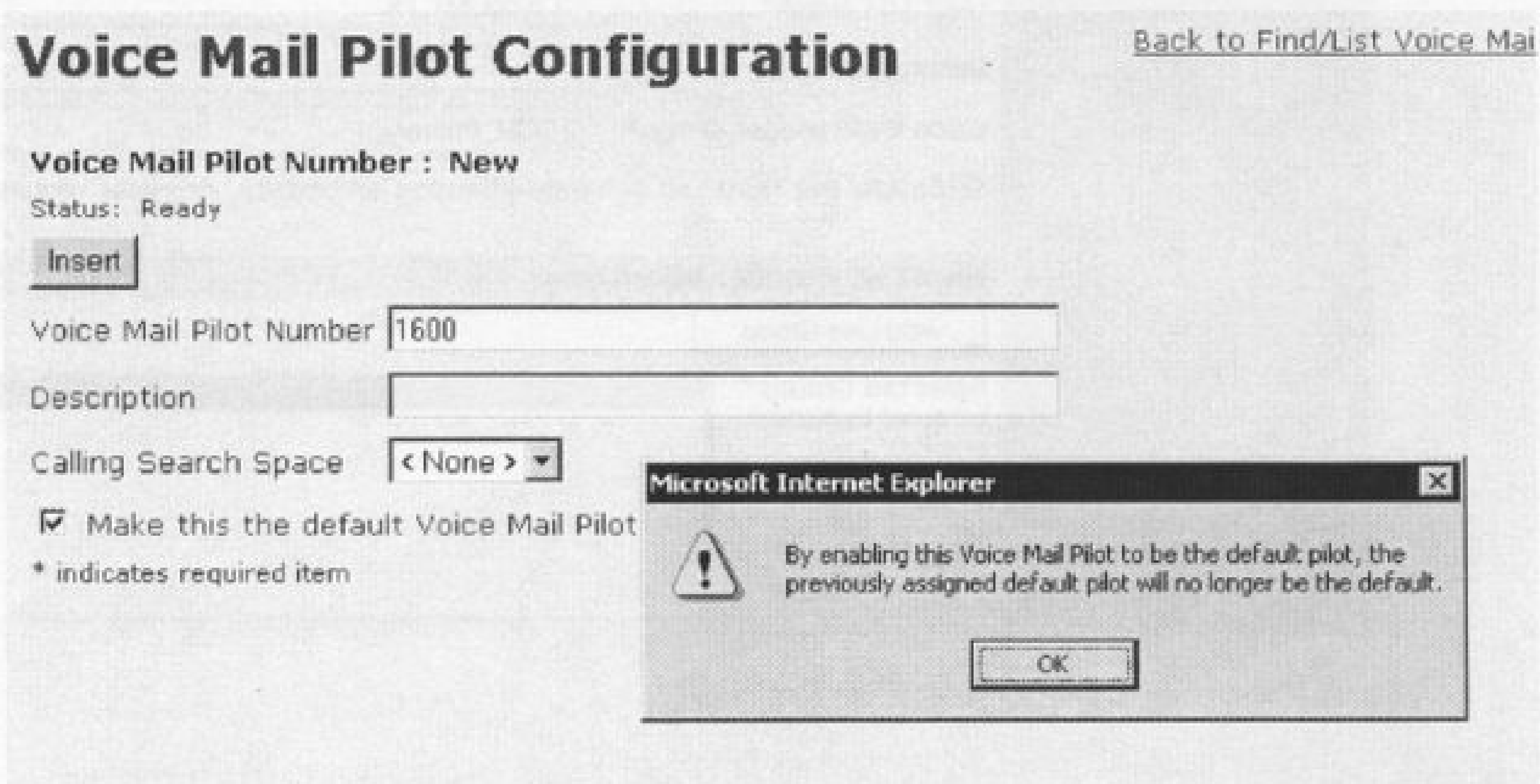




➔ **Now we must create a Hunt Pilot to reach the List and ultimately the Line Group of Voicemail Ports.**

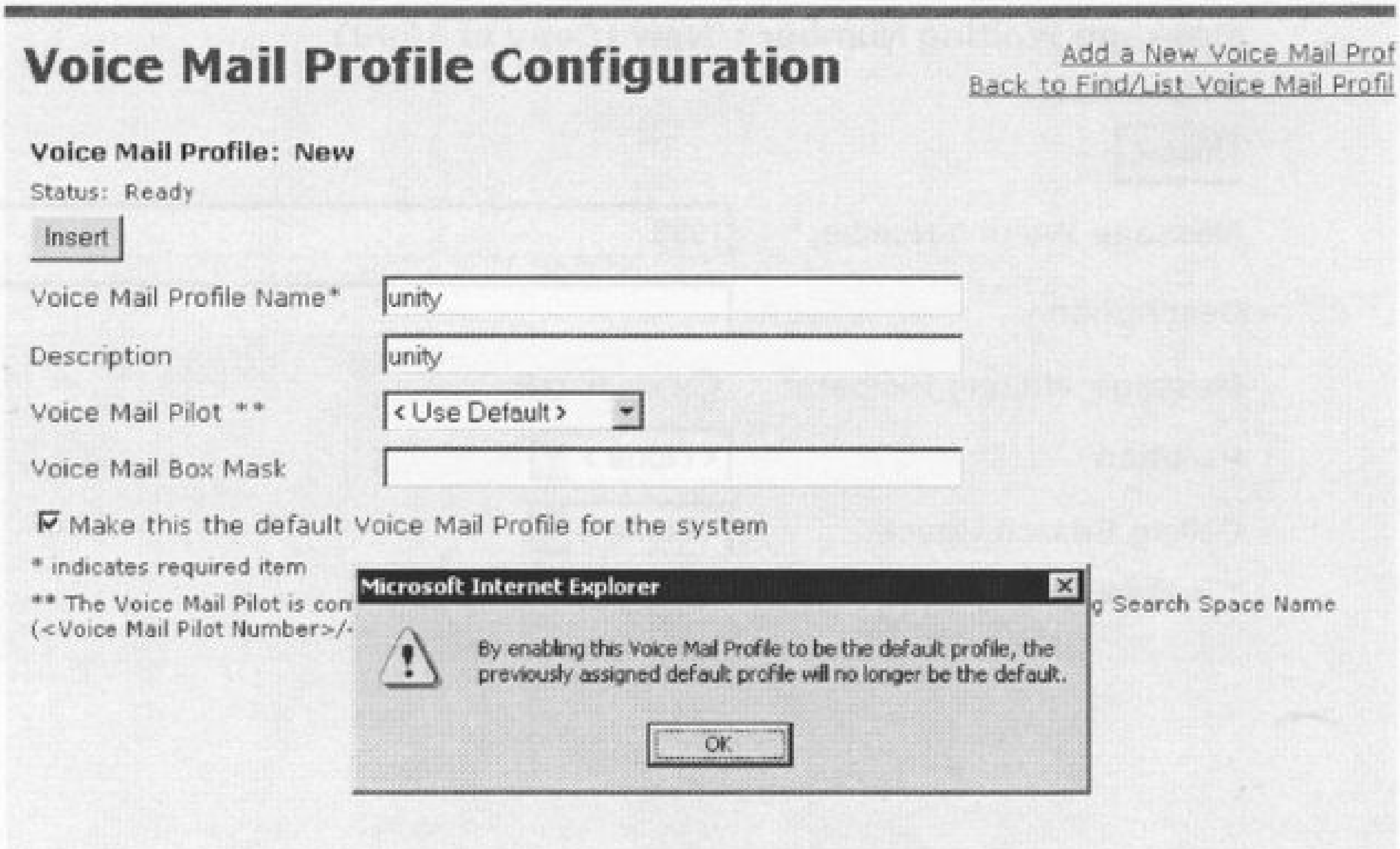


➔ **From Feature➔Voice Mail➔ Voice Mail Pilot add the Voicemail Pilot.**

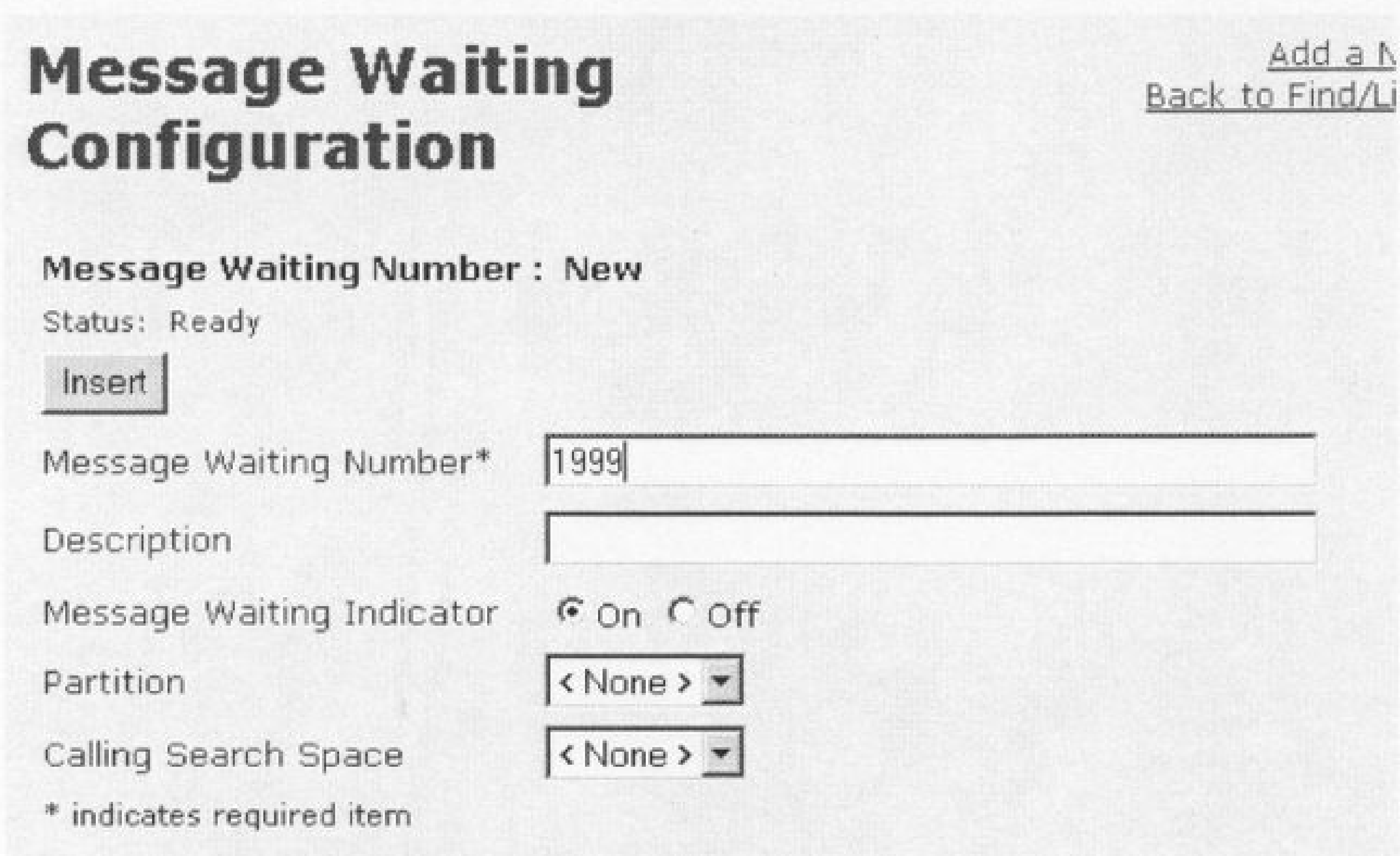


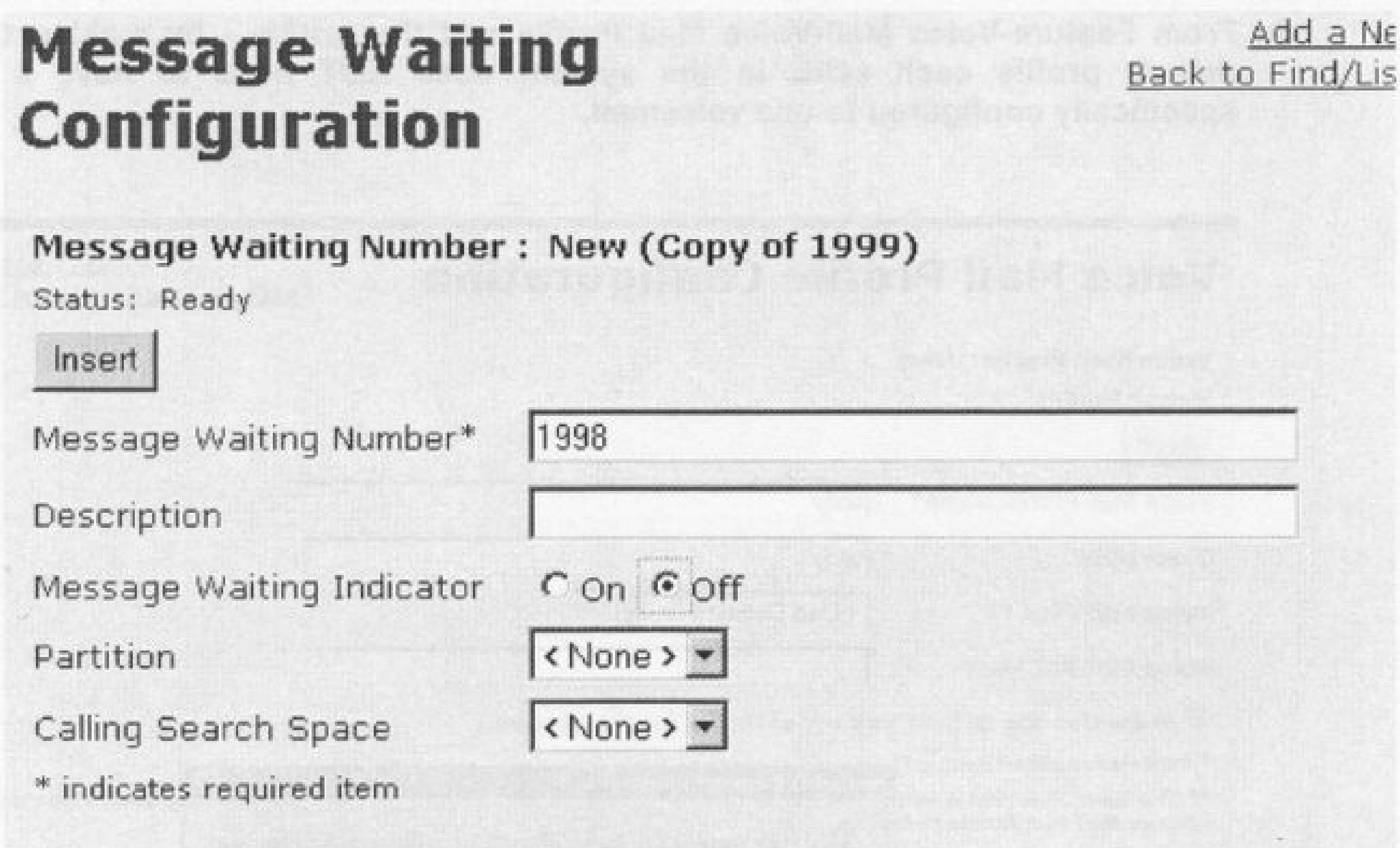
➔ **Configure the Pilot DN and ensure that the CSS can see the phone partitions.**

➔ **From Feature-Voice Mail-Voice Mail Profile add the profile - by making this the default profile each LINE in the system does NOT need to have a profile specifically configured to use voicemail.**



➔ **Configure Message Waiting Indicator from Feature-Voice Mail-Message Waiting. Enter the DN that will be used to turn on and off the MWI light.**





Message Waiting Configuration

Add a Ne
Back to Find/Lis

Message Waiting Number : New (Copy of 1999)

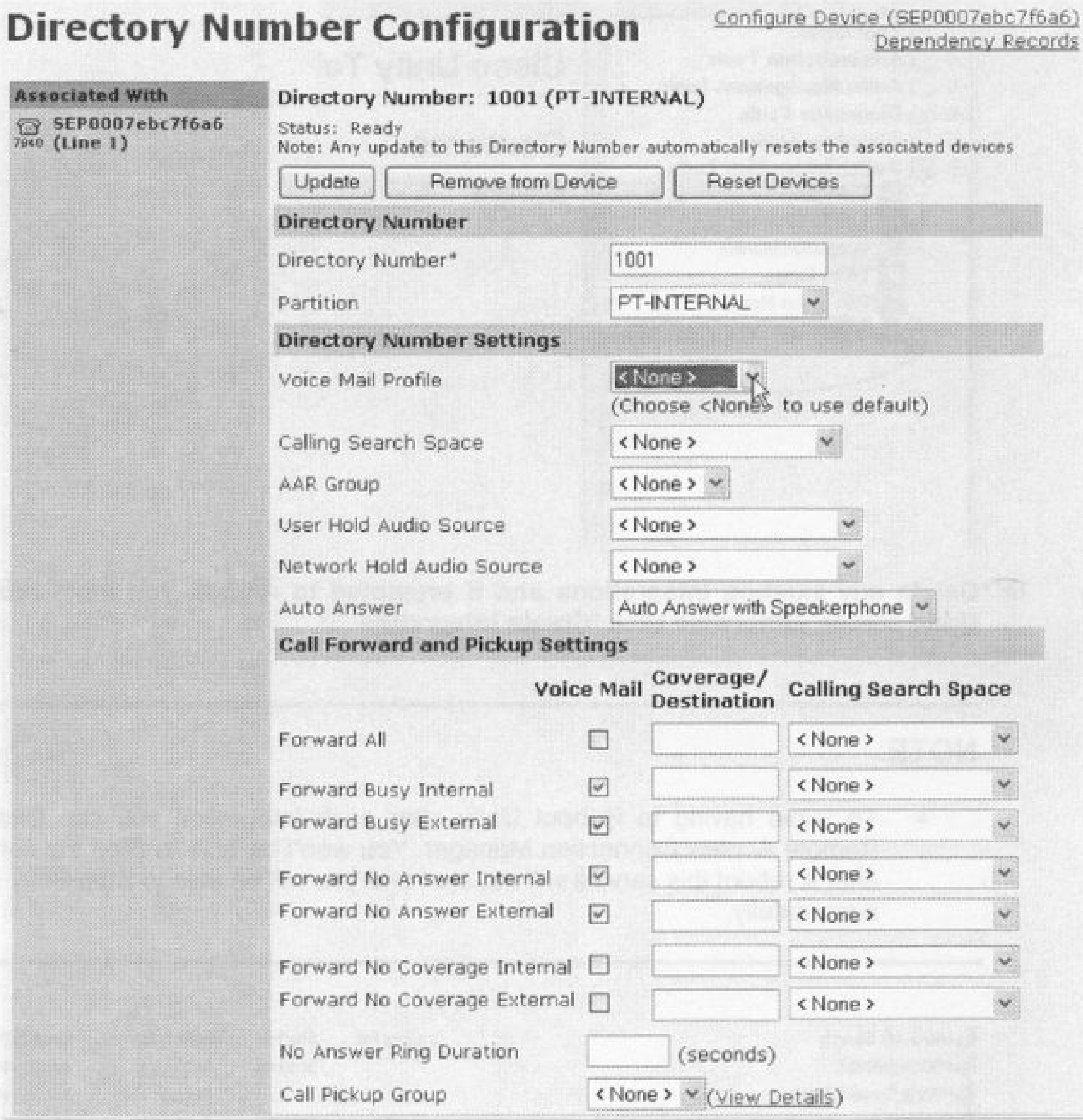
Status: Ready

Insert

Message Waiting Number*	1998
Description	
Message Waiting Indicator	○ On ◉ Off
Partition	< None >
Calling Search Space	< None >

* indicates required item

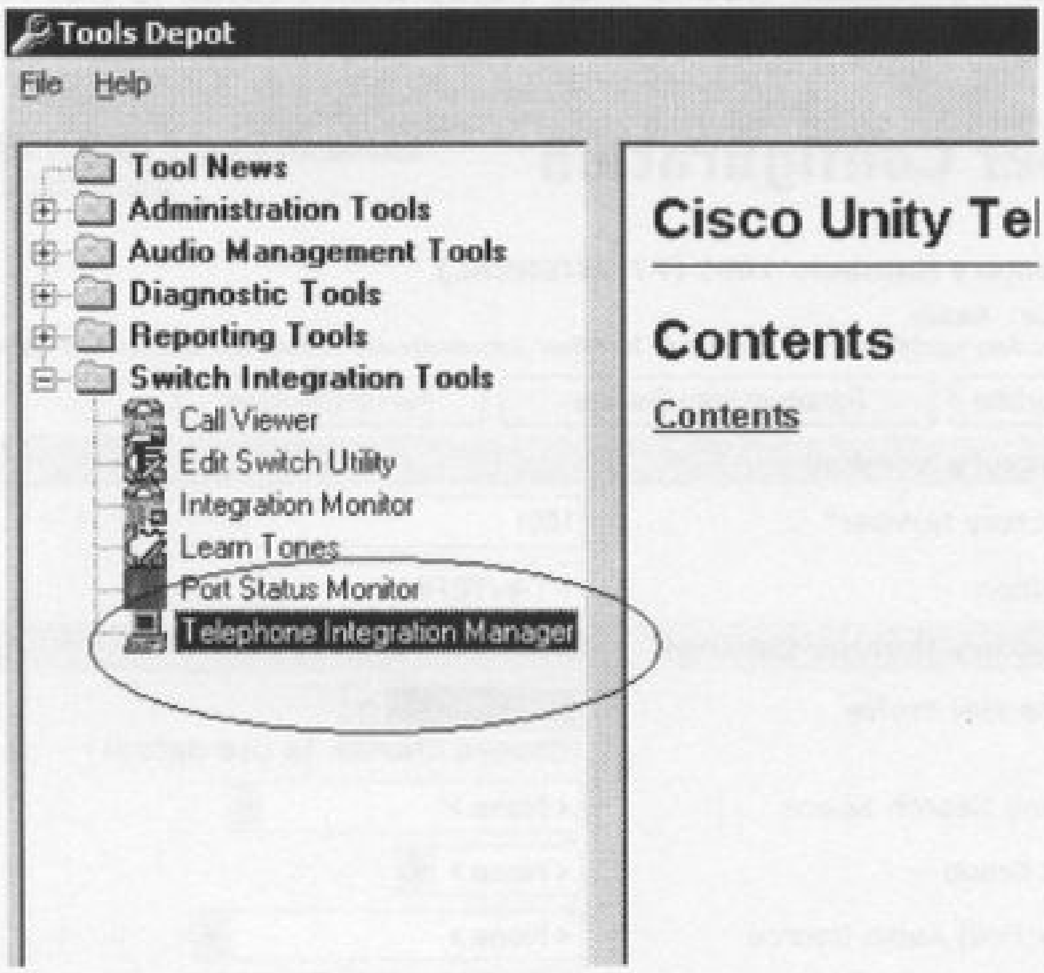
➔ **For all LINES in the system, you will have to configure Call Forward No Answer and Call Forward Busy to VoiceMail. Notice that Voice Mail Profile is not required since we configured the Profile we created as the default.**



➔ **At this stage Call Manager configuration for voicemail is now complete. The Unity Server now needs to be configured to communicate with Call Manager.**

➔ **Launch Unity Tools Depot via the Desktop or from the Windows Start menu, click Programs > Cisco Unity Tools Depot.**

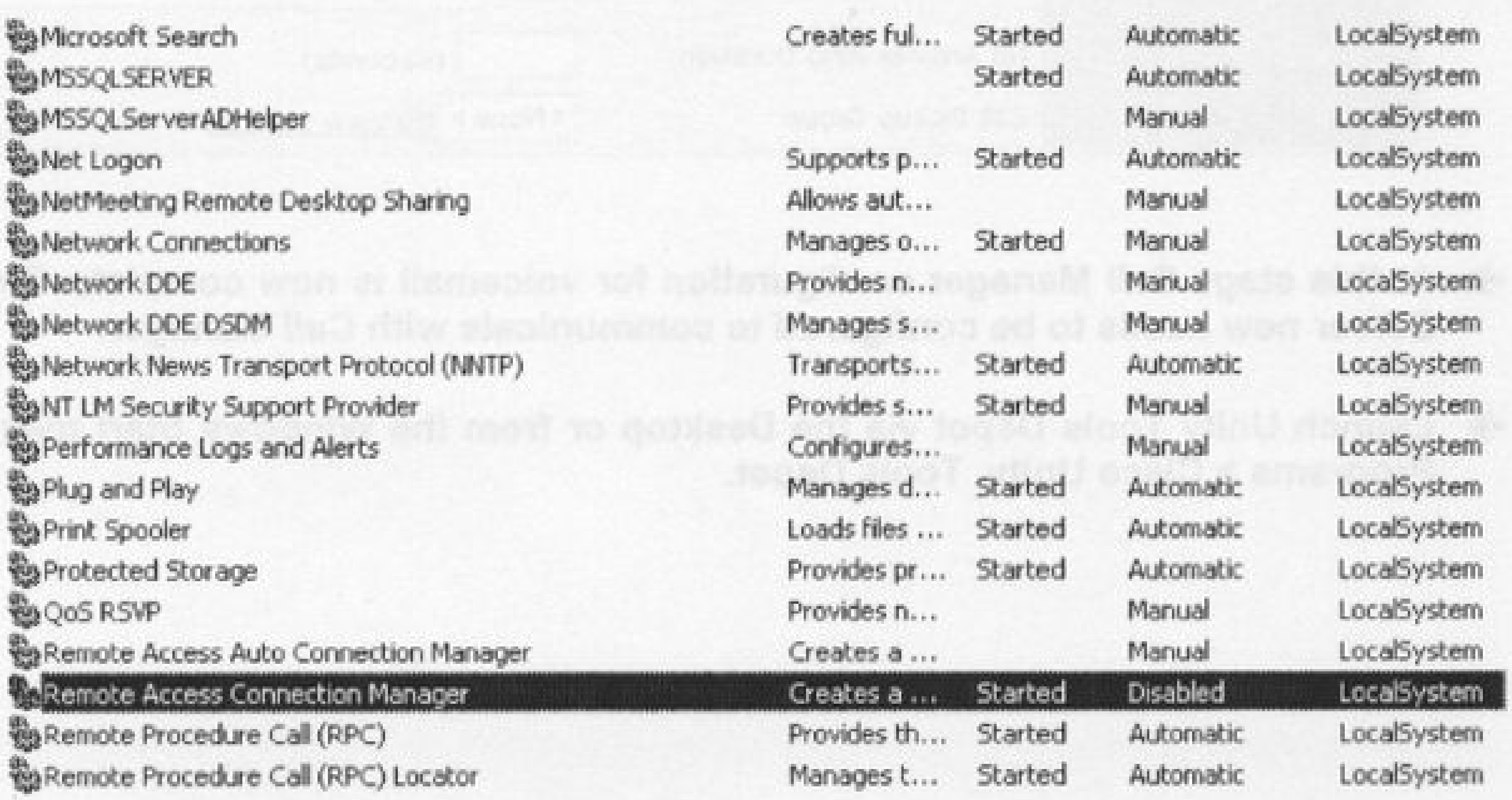
➔ **Launch The Telephone Integration Manager (UTIM) from Switch Integration.**



➔ **Delete any existing Integrations and if prompted to reboot, you must reboot the Unity server. Otherwise click 'Create Integration'.**

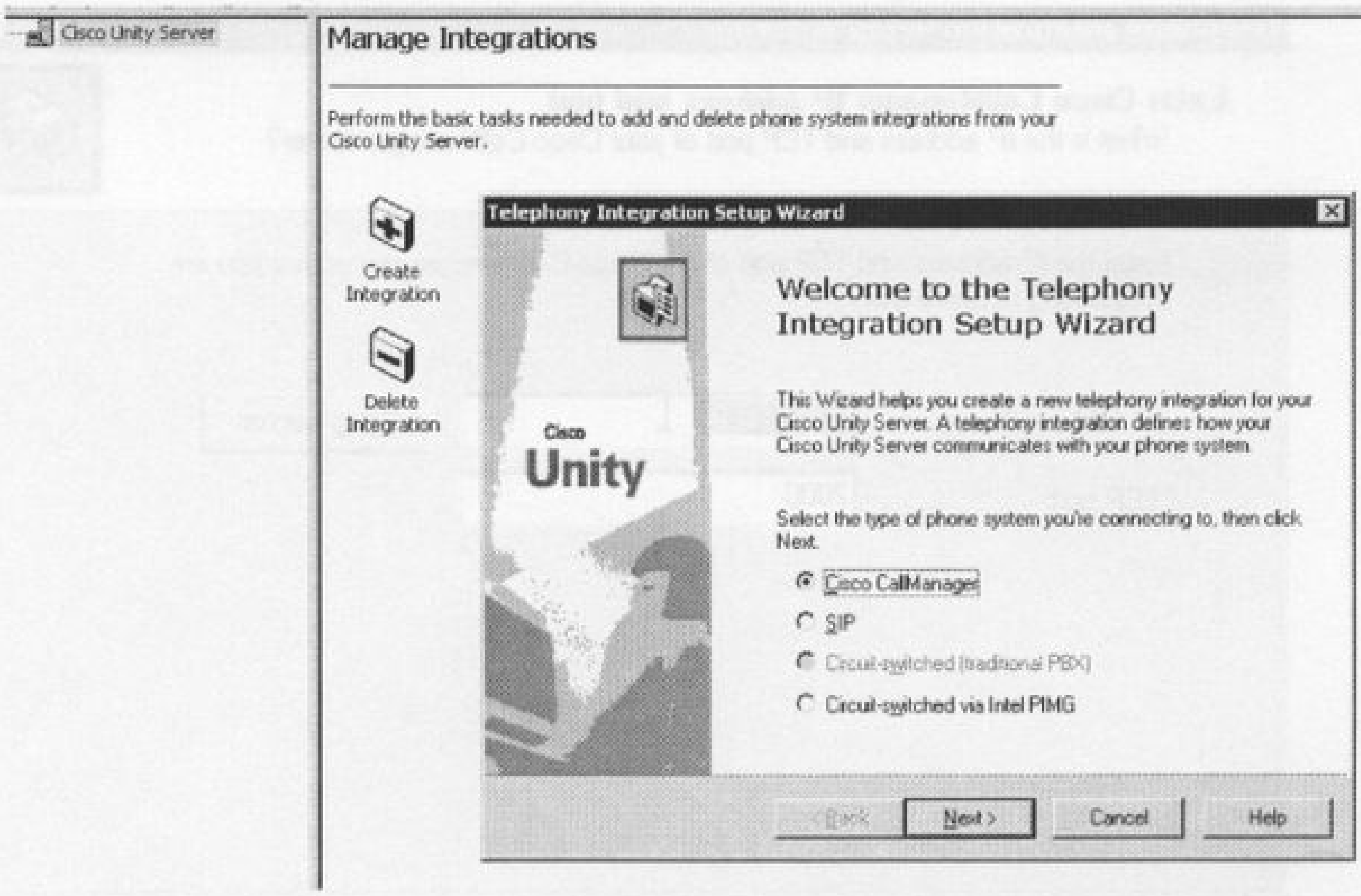
NOTE:

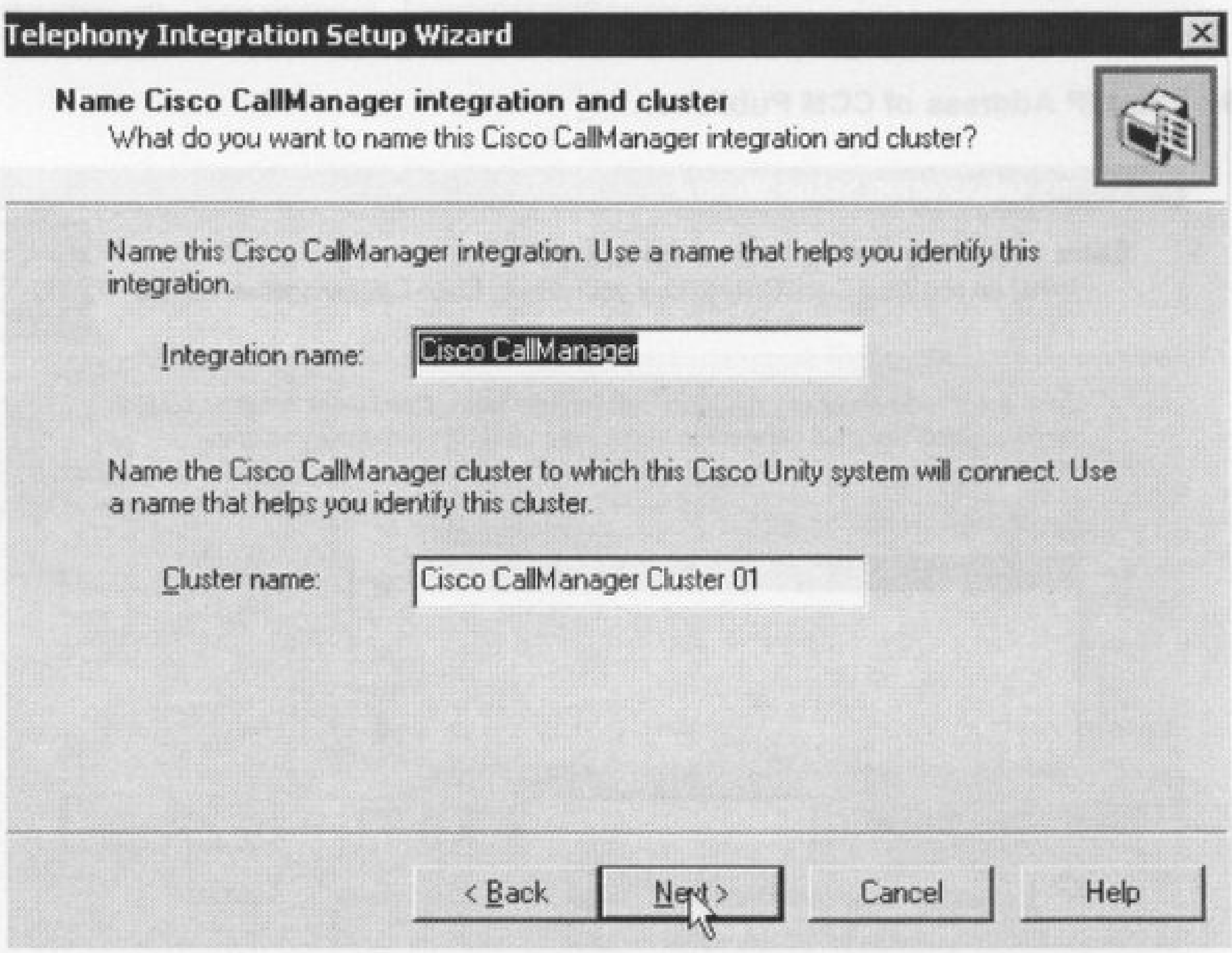
- To avoid having to Reboot Unity after each Integration you can Disable the Remote Access Connection Manager. You won't be able to Stop the service but after a reboot this service will not start and you will be able to Stop Unity services successfully.



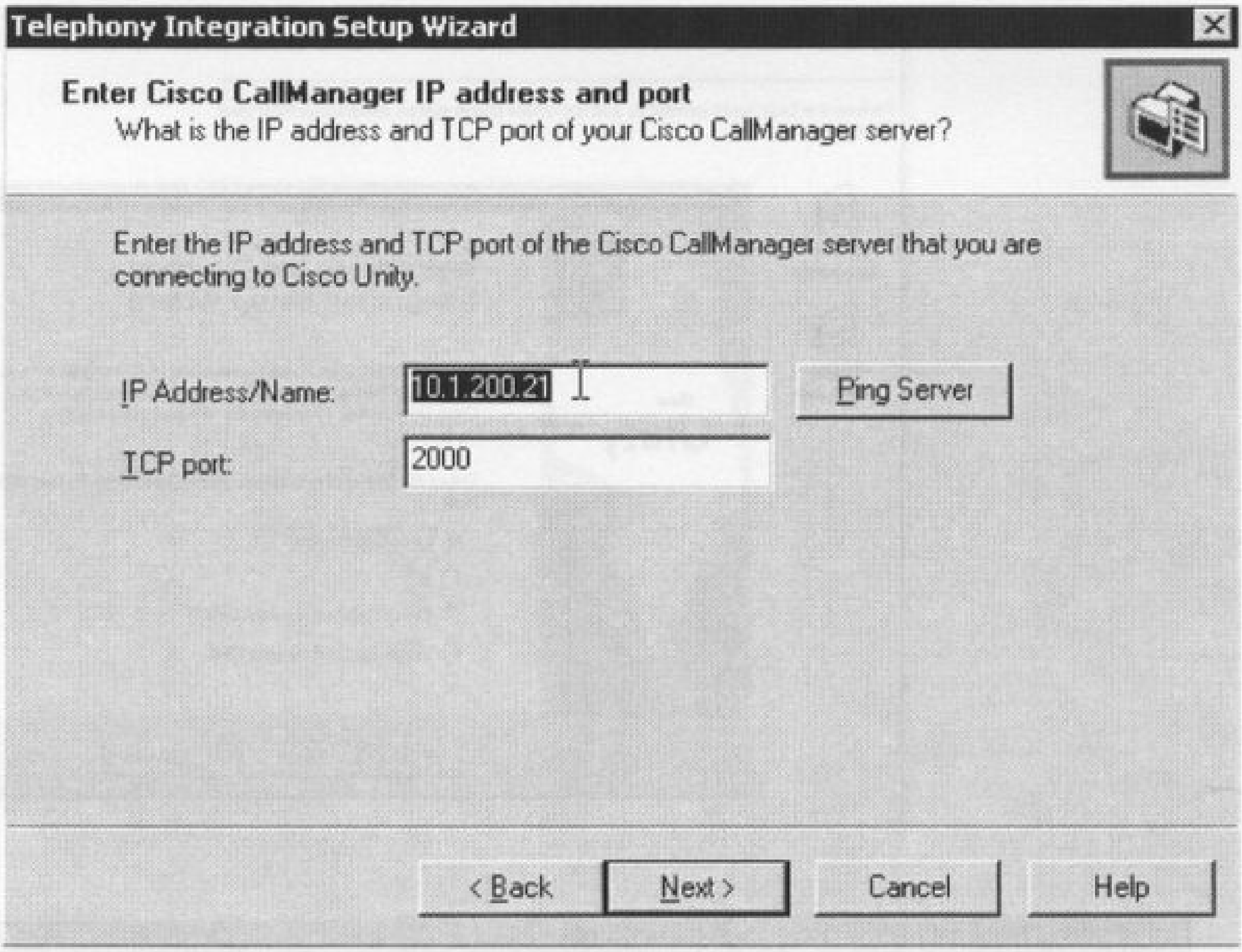
Microsoft Search	Creates ful...	Started	Automatic	LocalSystem
MSSQLSERVER		Started	Automatic	LocalSystem
MSSQLServerADHelper			Manual	LocalSystem
Net Logon	Supports p...	Started	Automatic	LocalSystem
NetMeeting Remote Desktop Sharing	Allows aut...		Manual	LocalSystem
Network Connections	Manages o...	Started	Manual	LocalSystem
Network DDE	Provides n...		Manual	LocalSystem
Network DDE DSDM	Manages s...		Manual	LocalSystem
Network News Transport Protocol (NNTP)	Transports...	Started	Automatic	LocalSystem
NT LM Security Support Provider	Provides s...	Started	Manual	LocalSystem
Performance Logs and Alerts	Configures...		Manual	LocalSystem
Plug and Play	Manages d...	Started	Automatic	LocalSystem
Print Spooler	Loads files ...	Started	Automatic	LocalSystem
Protected Storage	Provides pr...	Started	Automatic	LocalSystem
QoS RSVP	Provides n...		Manual	LocalSystem
Remote Access Auto Connection Manager	Creates a ...		Manual	LocalSystem
Remote Access Connection Manager	Creates a ...	Started	Disabled	LocalSystem
Remote Procedure Call (RPC)	Provides th...	Started	Automatic	LocalSystem
Remote Procedure Call (RPC) Locator	Manages t...	Started	Automatic	LocalSystem

➔ **In UTIM - choose the Call Manager option.**

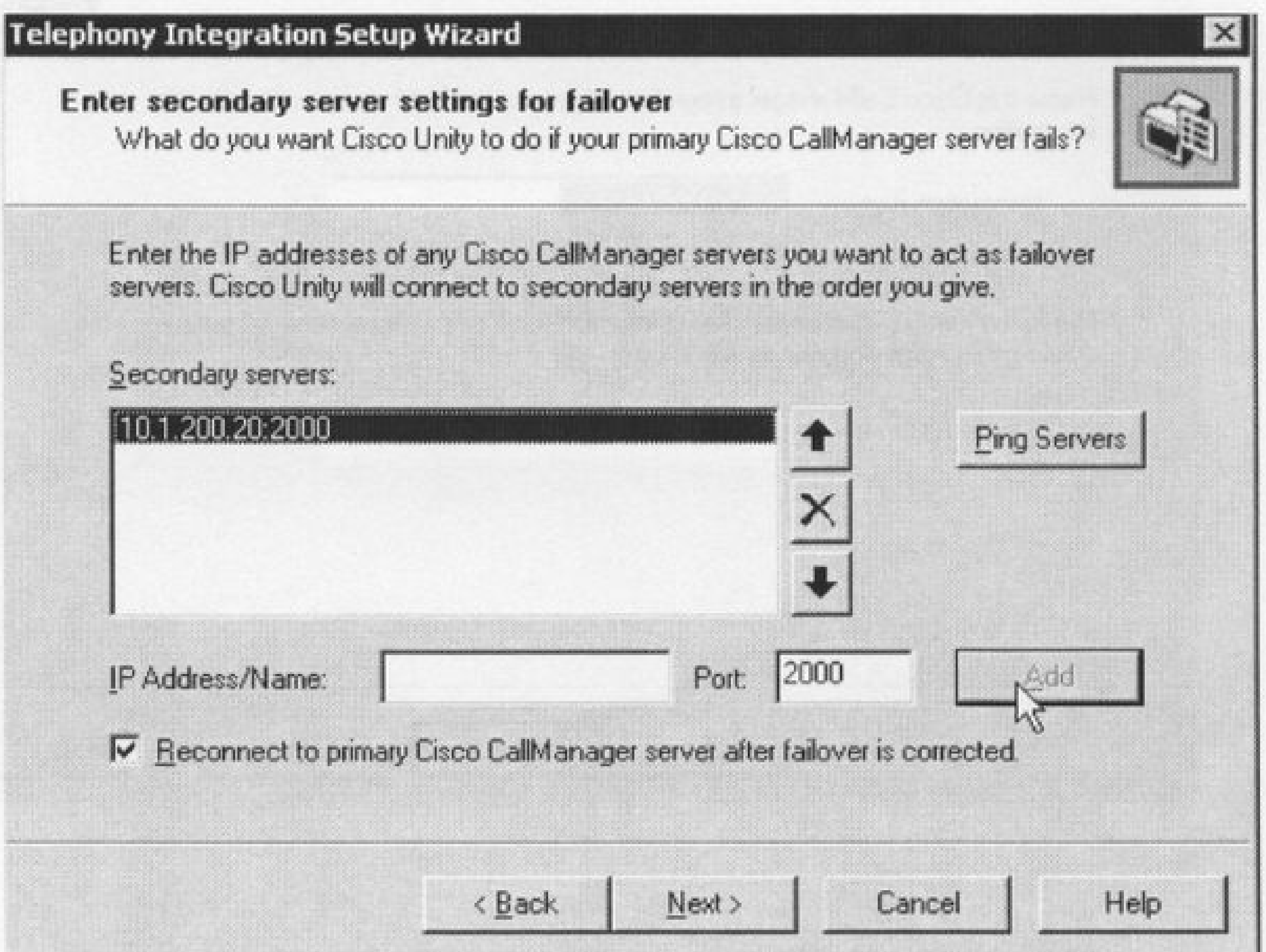




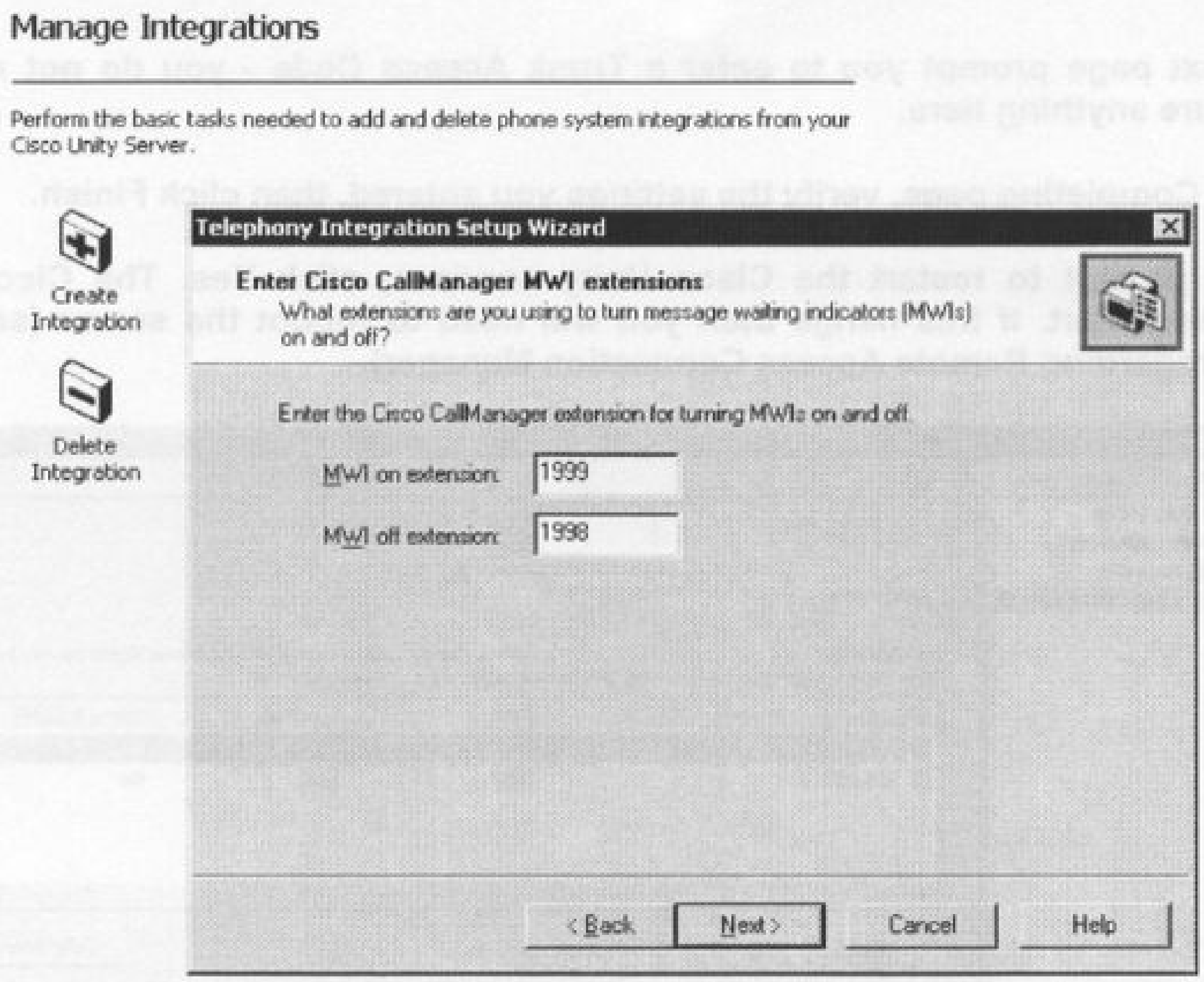
➔ **Enter IP Address of CCM Subscriber.**

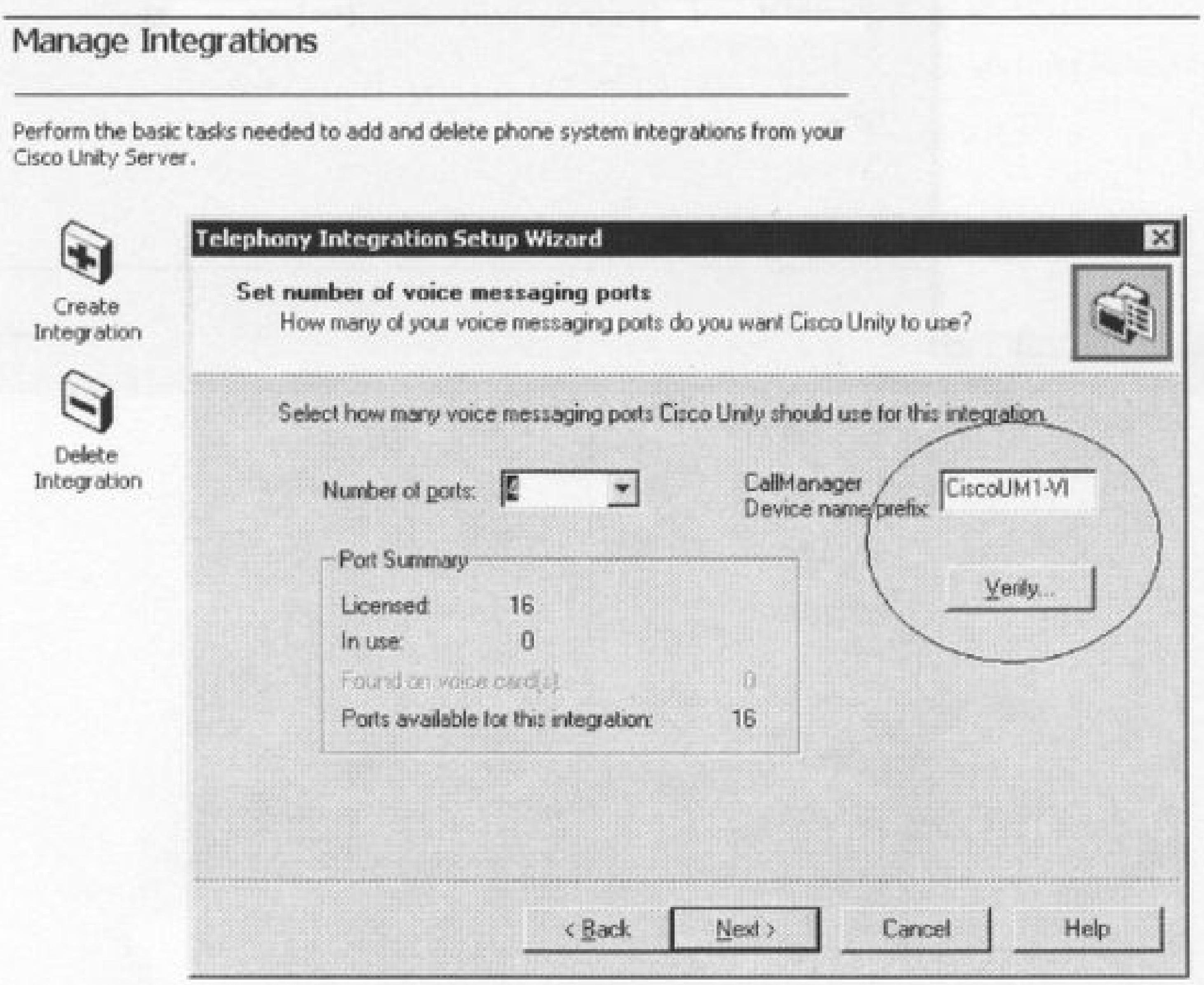


➔ **Enter IP Address of CCM Publisher.**



→ **Enter MWI On/Off DNs.**



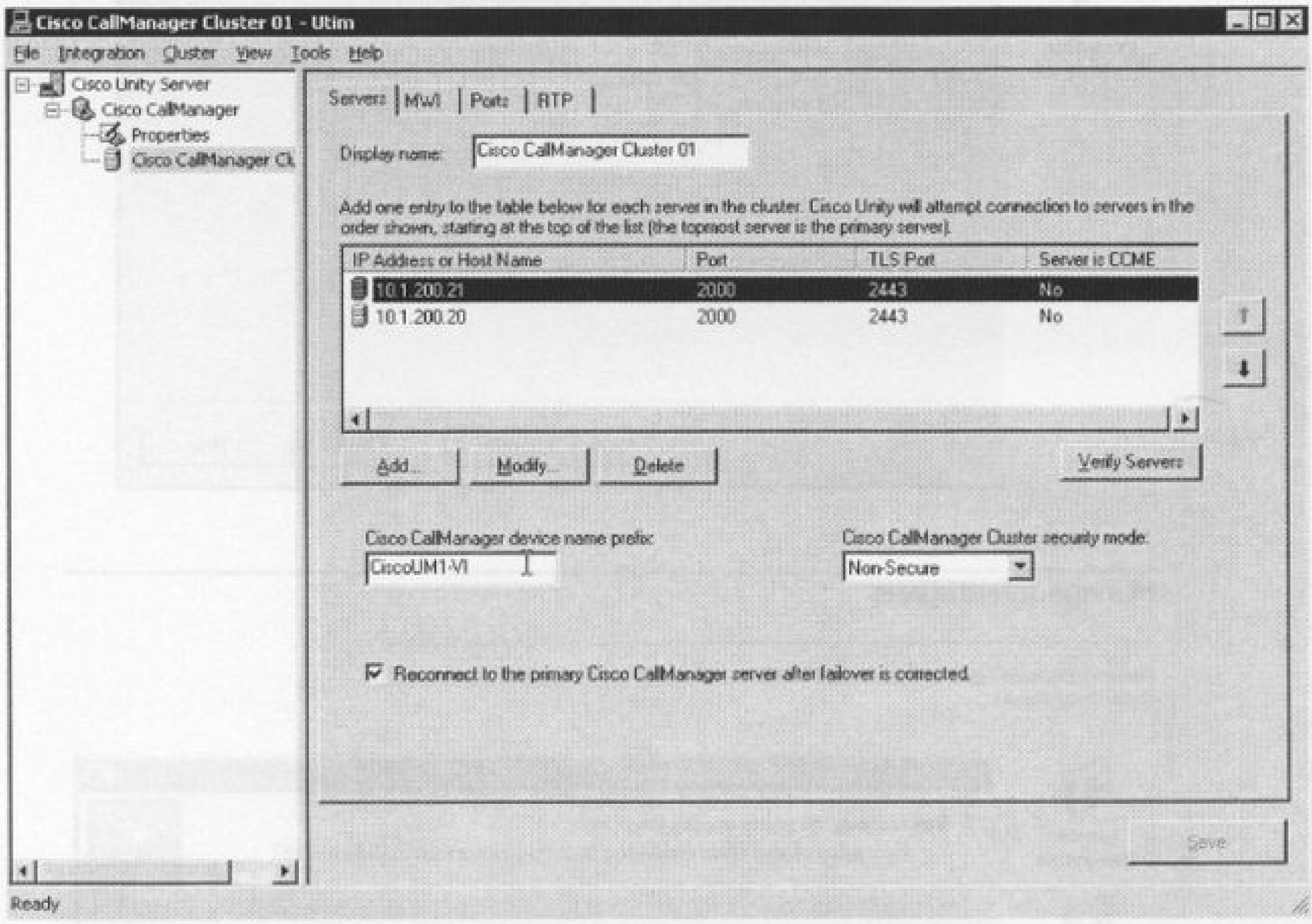


➔ **You can click Verify to confirm that the CallManager device name prefix is correct - the name is resolved via NETBIOS.**

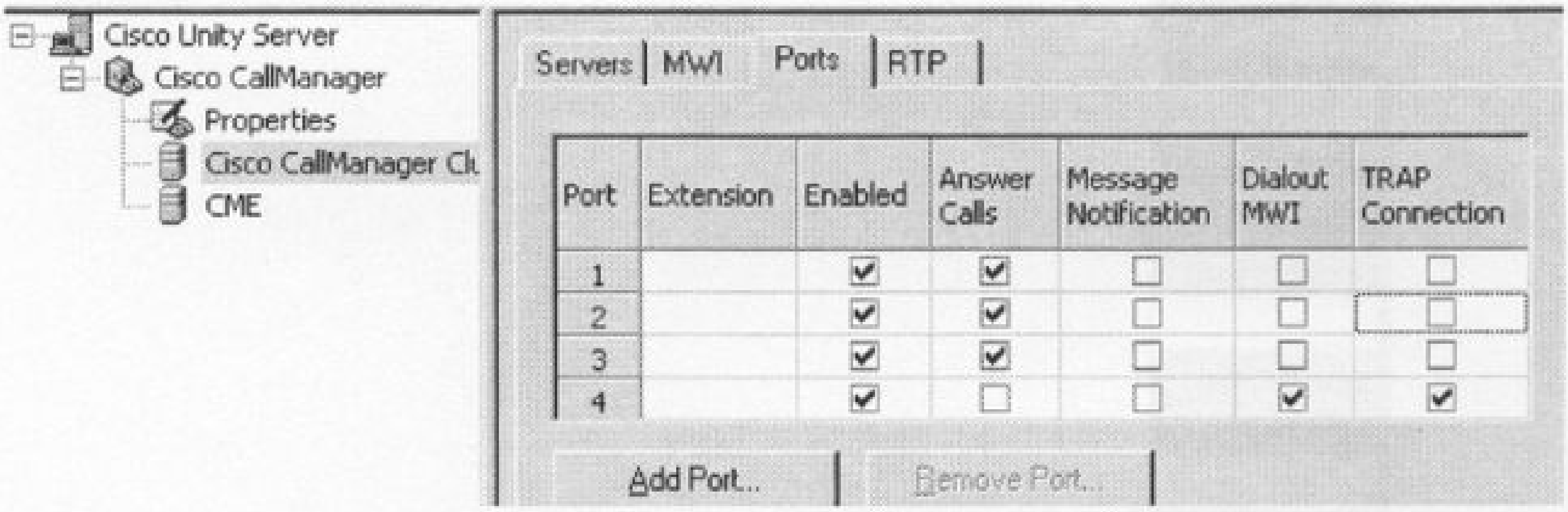
➔ **The next page prompt you to enter a Trunk Access Code - you do not need to configure anything here.**

➔ **On the Completing page, verify the settings you entered, then click Finish.**

➔ **At the prompt to restart the Cisco Unity services, click Yes. The Cisco Unity services restart. If this hangs then you will need to reboot the server (see Note above regarding Remote Access Connection Manager).**



➔ **When the Unity services have restarted (or Unity has been rebooted), you must configure the voicemail ports from the Telephone Integration page from UTIM. Looking ahead to the next section we require the 4th port to be dedicated to MWI so we will disable Dialout MWI for the first 3 ports. Message Notification to pagers or emails is not required and should be disabled on all ports. TRAP Connection (Telephony Record and Playback) which is used for Media Master should only be enabled on one cluster in the Integration - in this example TRAP is enabled on one port in the CCM cluster. The first 3 ports are used to retrieve/leave voice messages.**



Task 9.2

Integrate CME into Unity with the following information:

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998

➔ **Unity Ports will have a Skinny registration to the CME in the same way as Unity ports register to the Call Manager. Note that calls to voicemail from CME do NOT require PSTN connectivity.**

➔ **It is very important to complete the CME IOS configuration before configuring the Unity server to communicate with CME. Otherwise there is a chance that the Unity ports will register in no particular order (auto assign).**

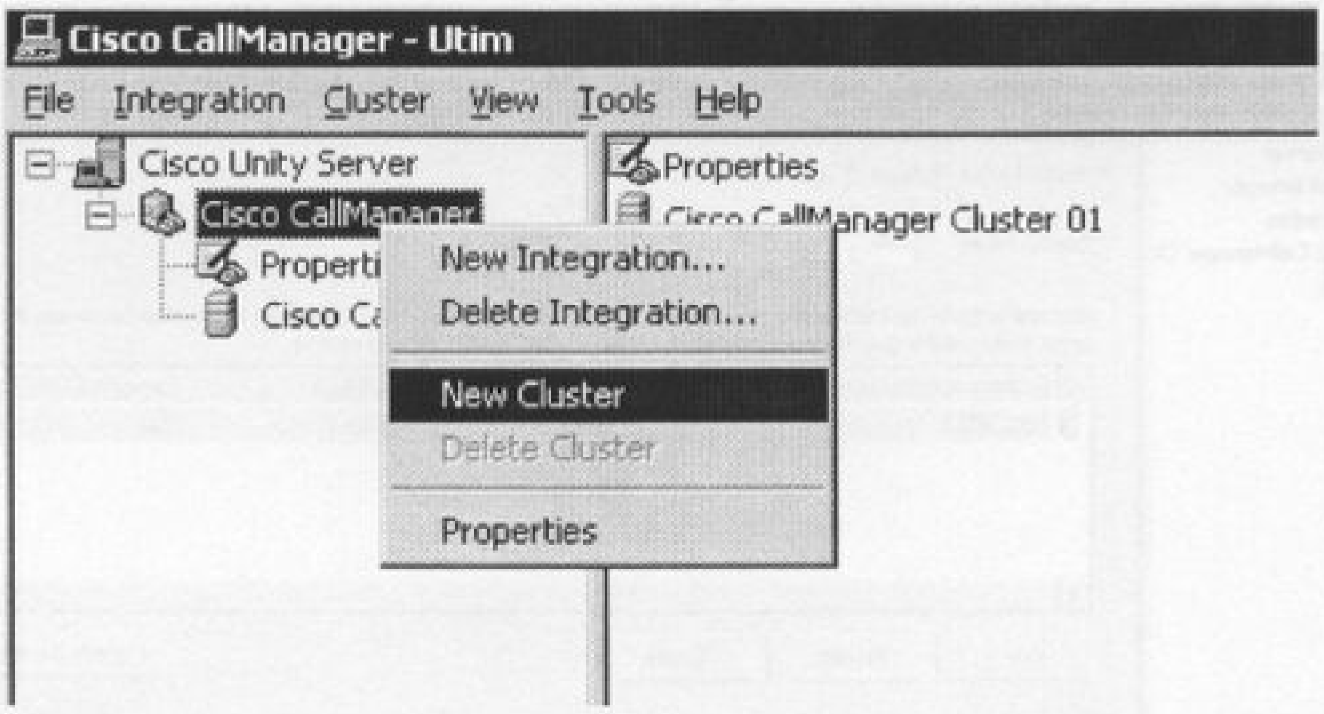
➔ **On the CME increase the maximum number of phones and DNs.**

```
P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)#max-ephone 7
P2-BR2-RTR(config-telephony)#max-dn 10
P2-BR2-RTR(config-telephony)#voicemail 3600
```

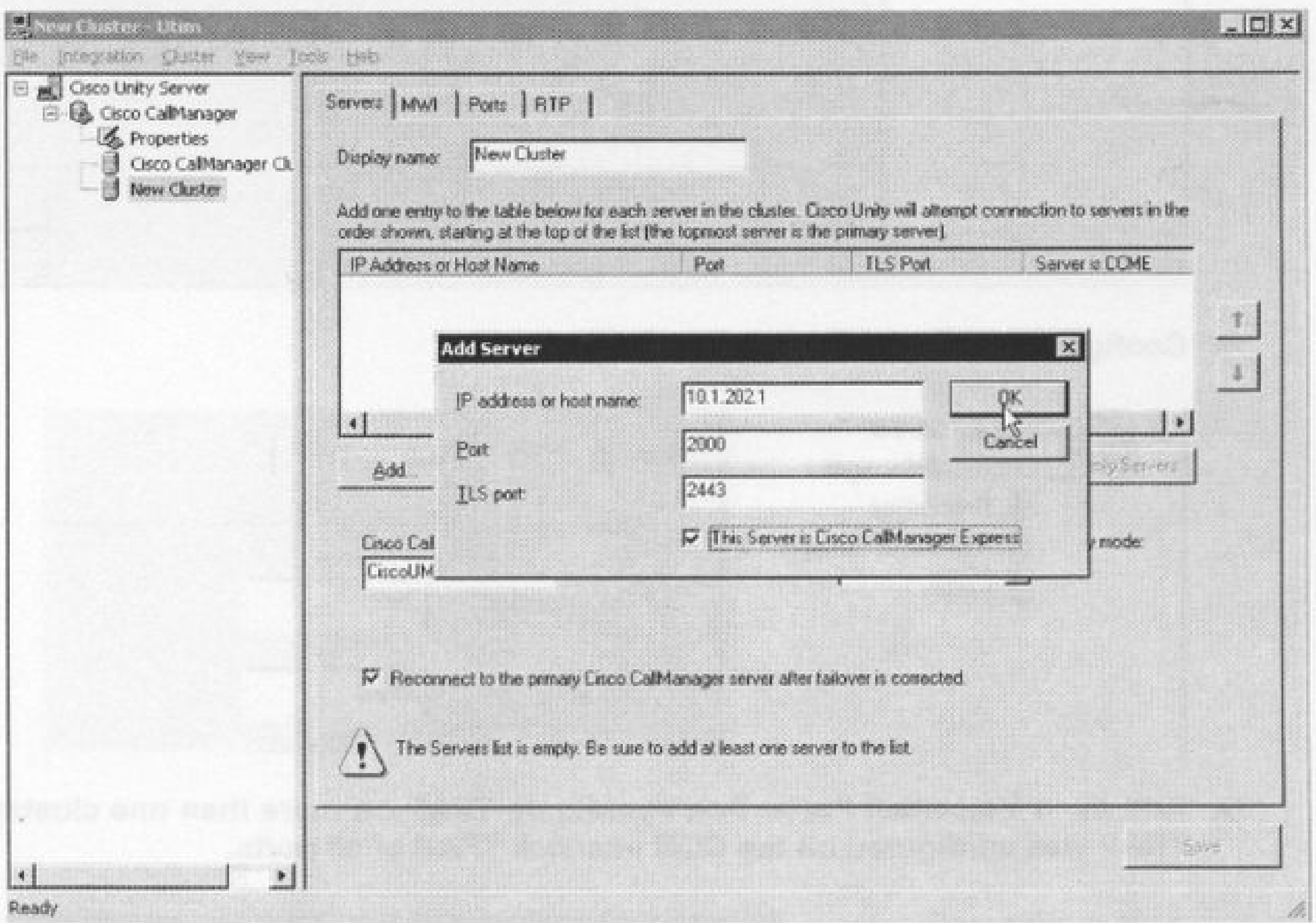
➔ **Add Unity ports and MWI DNs.**

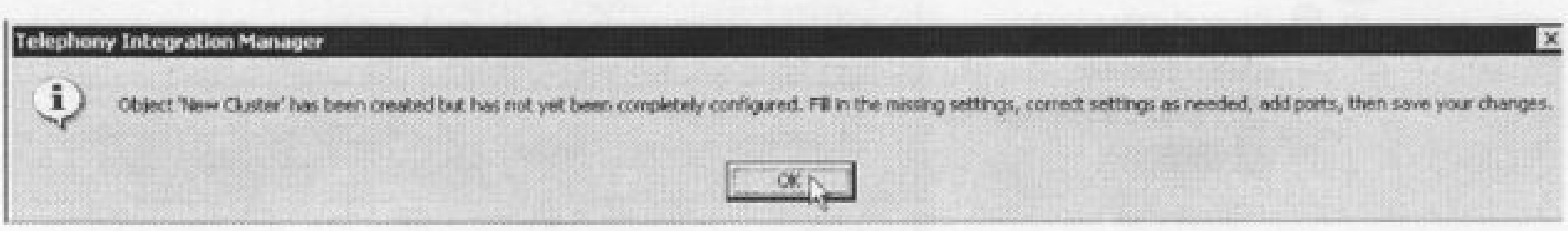
```
ephone-dn  6
 number 3600
 no huntstop
!
ephone-dn  7
 number 3600
 preference 1
 no huntstop
!
ephone-dn  8
 number 3600
 preference 2
!
ephone-dn  9
 number A01
!
ephone-dn  10
 number 3999 secondary 3998
 mwi on-off
!
ephone  4
 vm-device-id CiscoUM2-VI1
 button  1:6
!
ephone  5
 vm-device-id CiscoUM2-VI2
 button  1:7
!
ephone  6
 vm-device-id CiscoUM2-VI3
 button  1:8
!
ephone  7
 vm-device-id CiscoUM2-VI4
 button  1:9
```

➔ **CME can be integrated into Unity - from UTIM add the CME as a New cluster.**

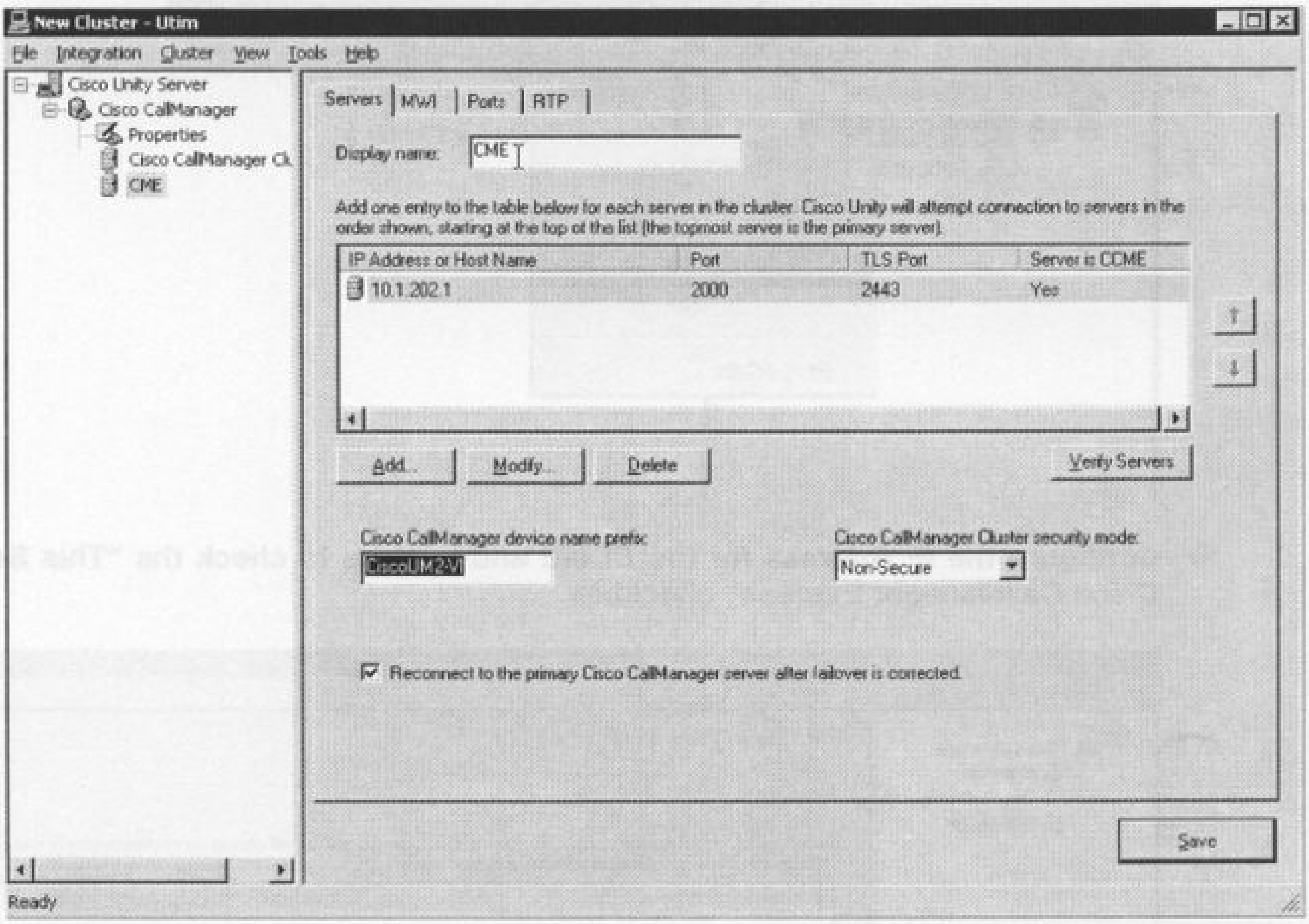


➔ **Configure the IP Address for the CCME and be sure to check the "This Server is Cisco CallManager Express" checkbox.**

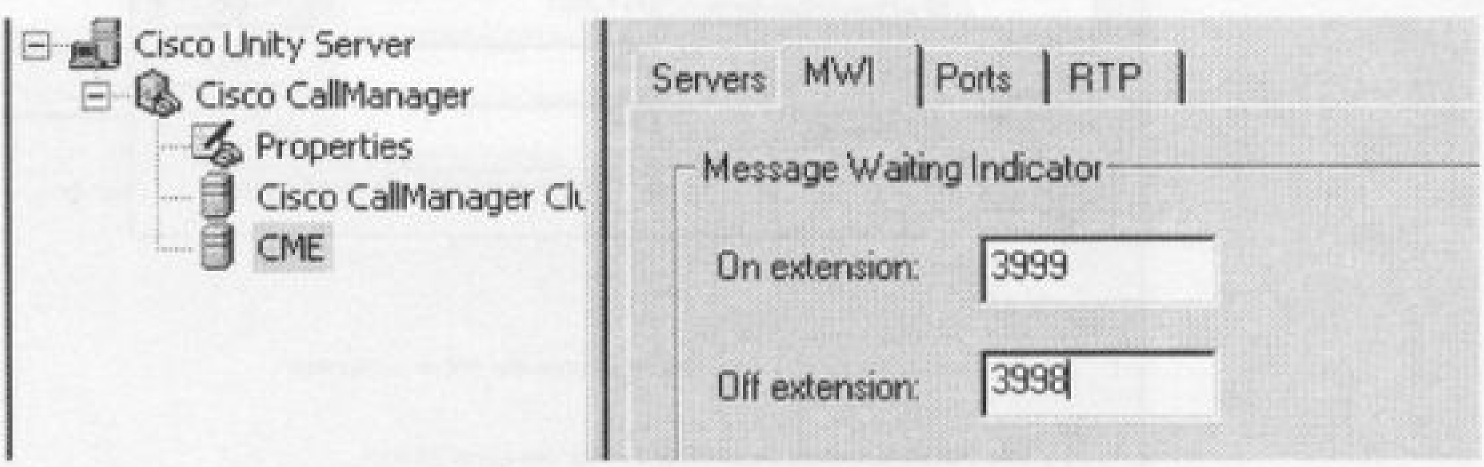




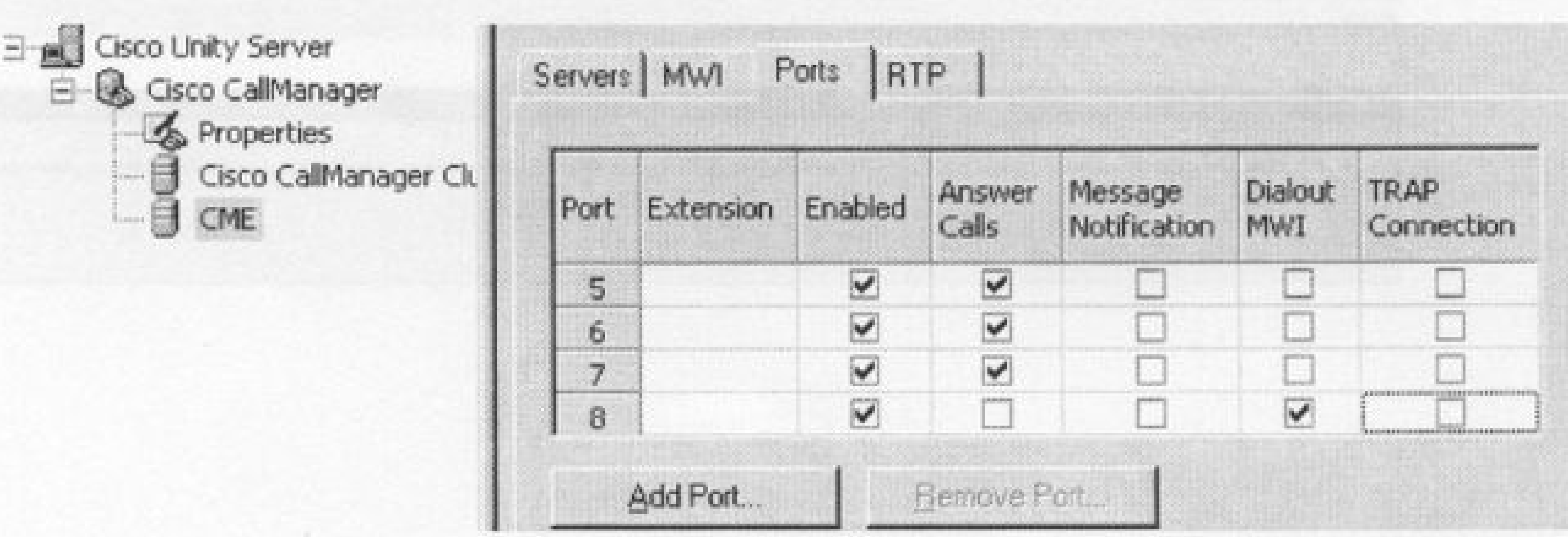
➔ **Be sure to change the Unity Prefix so that it is not the same as your CallManager installation – otherwise you will have big problems.**



➔ **Configure MWI DNs.**



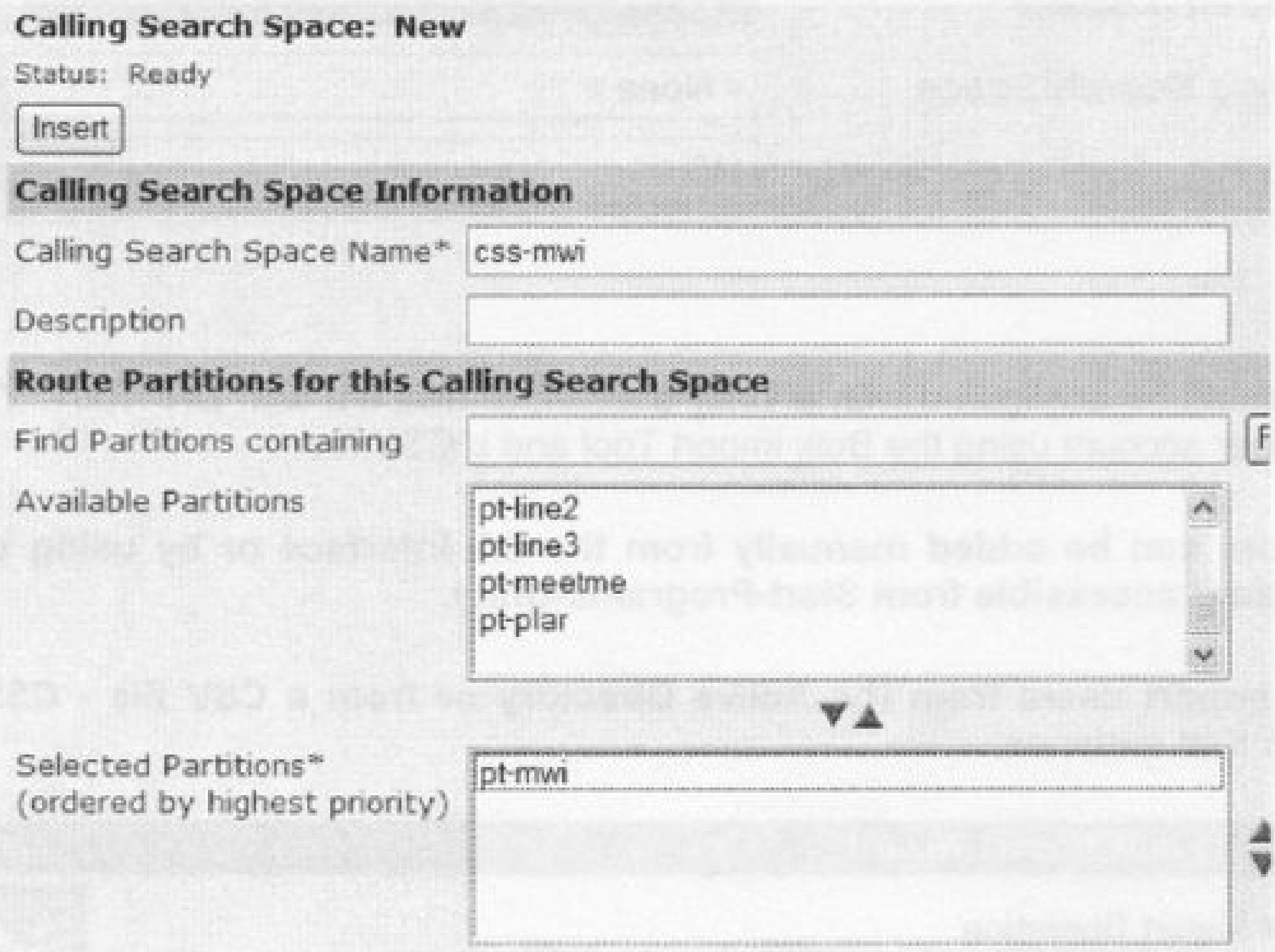
➔ **Add the 4 Voicemail Ports. Don't configure TRAP on more than one cluster. Since TRAP was configured on the CCM uncheck TRAP of all ports.**

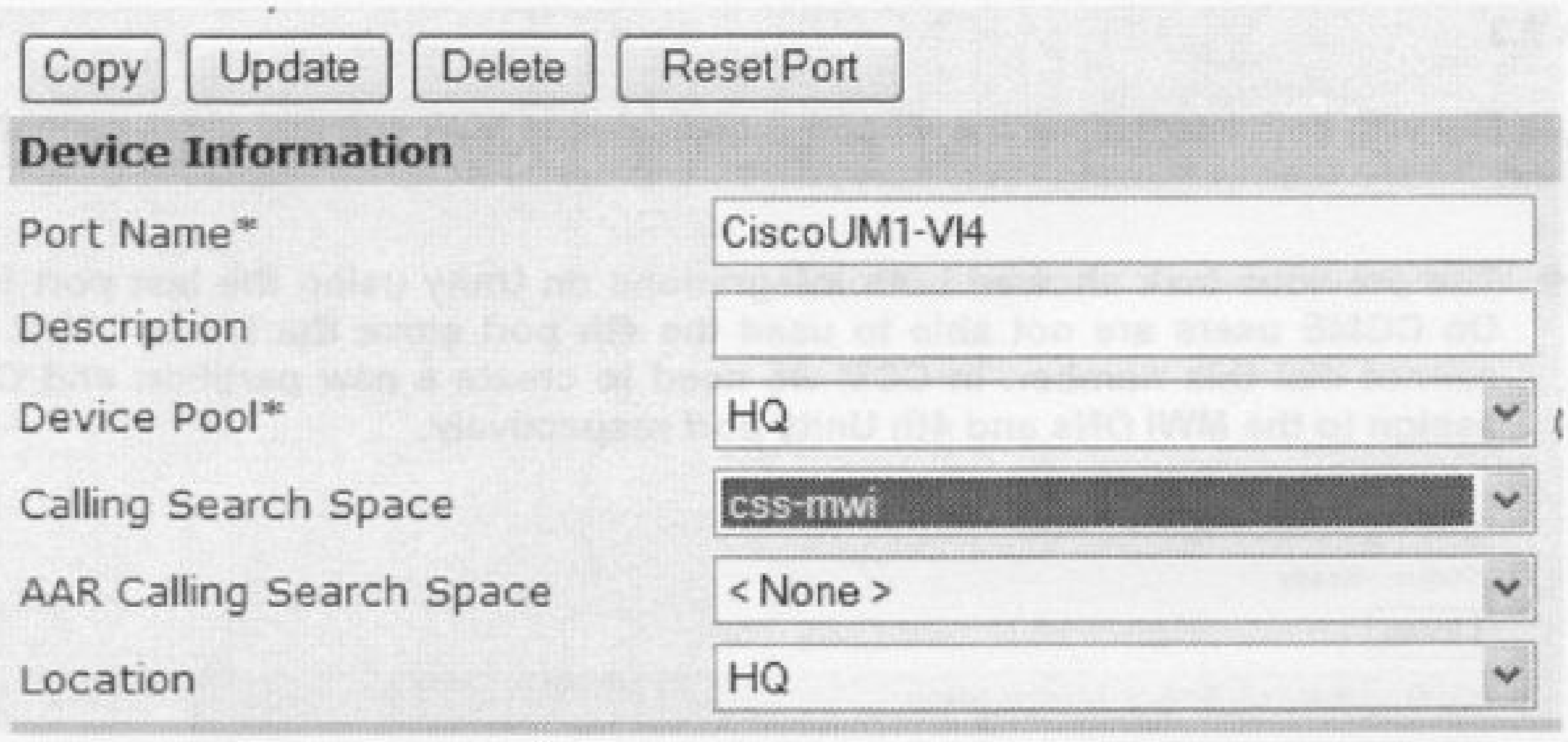


Task 9.3

Ensure that with both integrations the 4th port is dedicated to MWI and that users cannot dial the MWI ext.

➔ **The previous task showed both integrations on Unity using the last port for MWI. On CCME users are not able to used the 4th port since the DN is "A01" - users cannot dial this number. In CCM we need to create a new partition and CSS and assign to the MWI DNs and 4th Unity port respectively.**



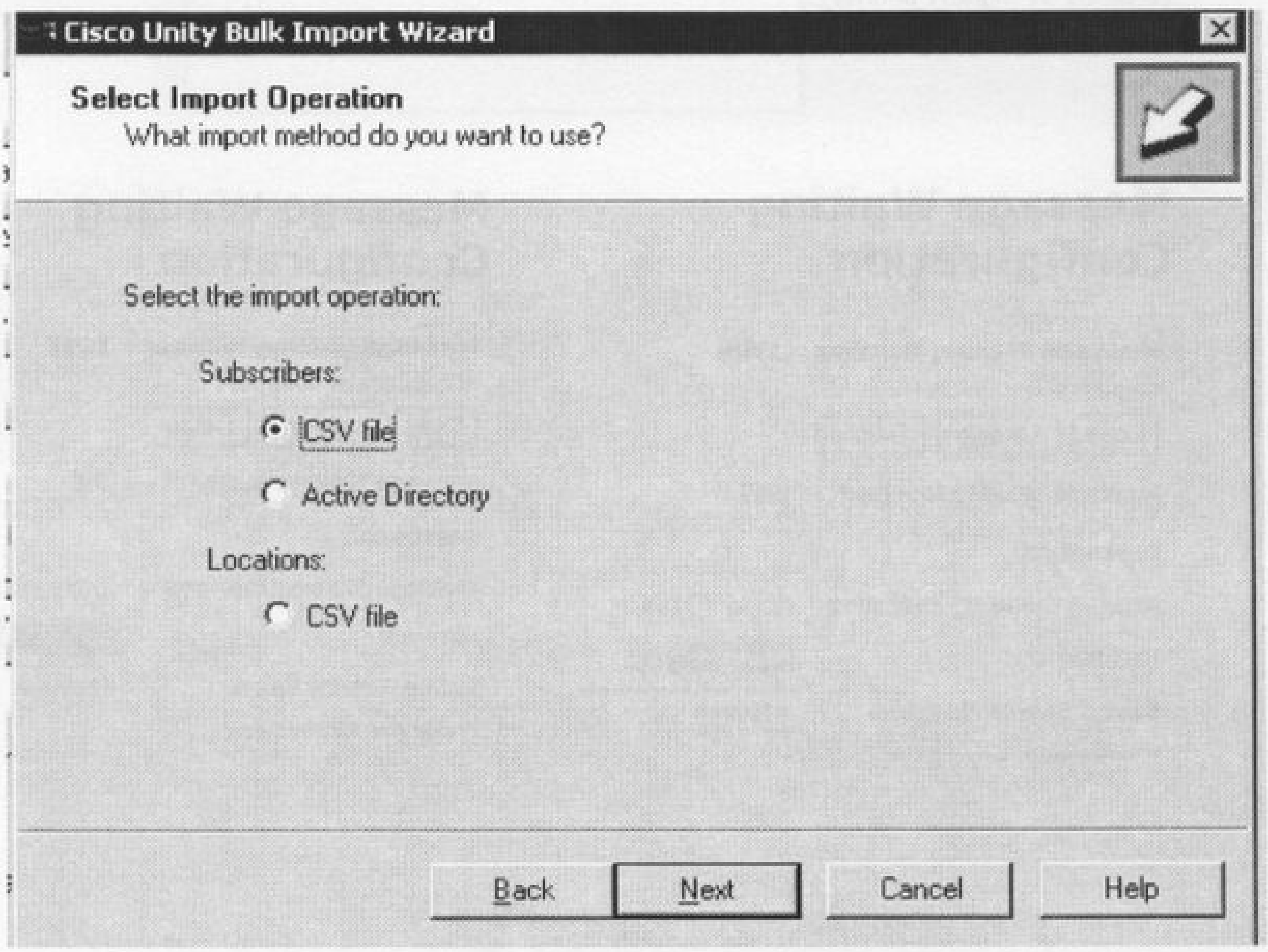


Task 9.4

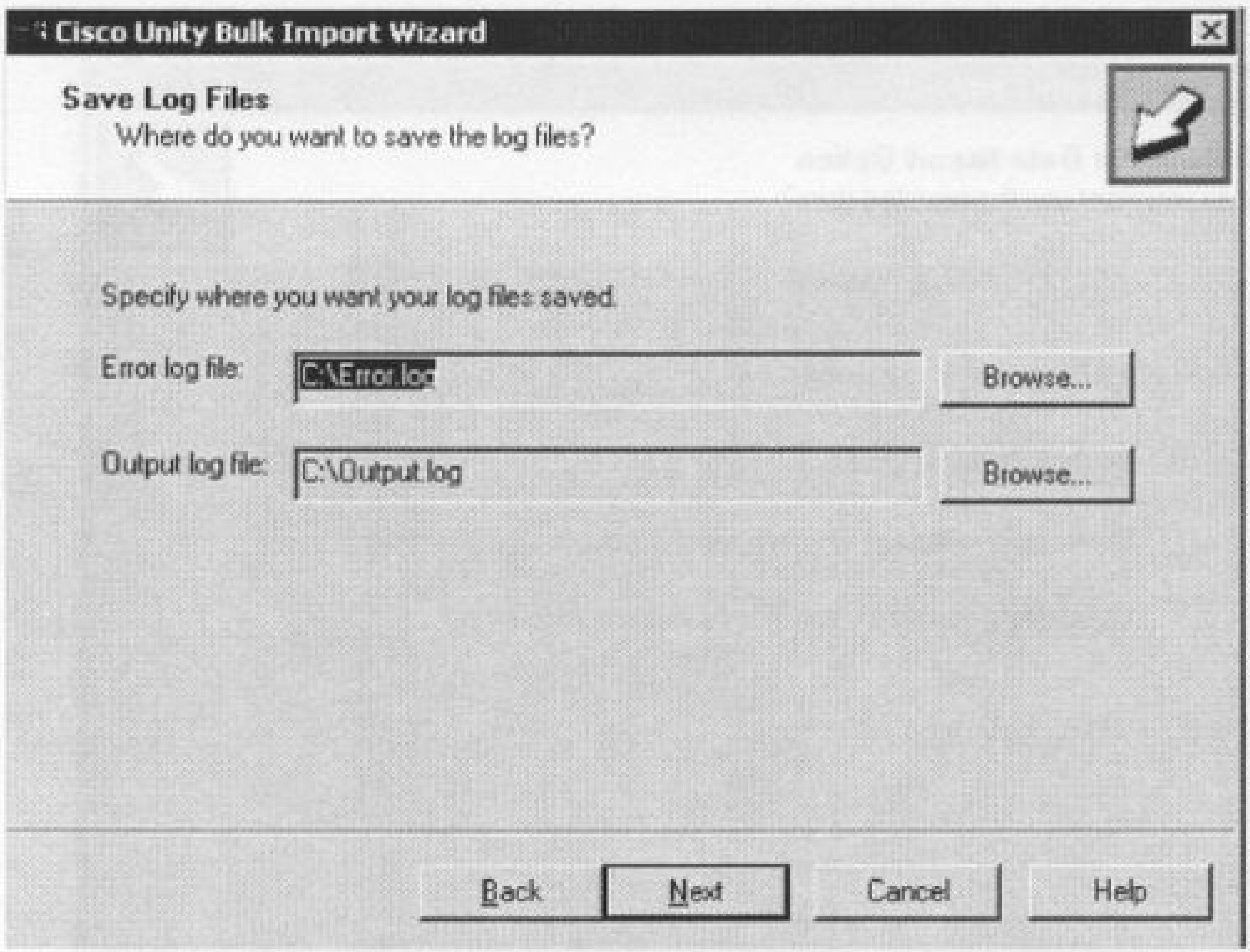
Phone 1 at HQ should be configured with a Unity subscriber account with DN=1001. You must create this subscriber account using the Bulk Import Tool and a CSV file.

→ **Subscribers can be added manually from the SA interface or by using the bulk import wizard accessible from Start-Programs-Unity.**

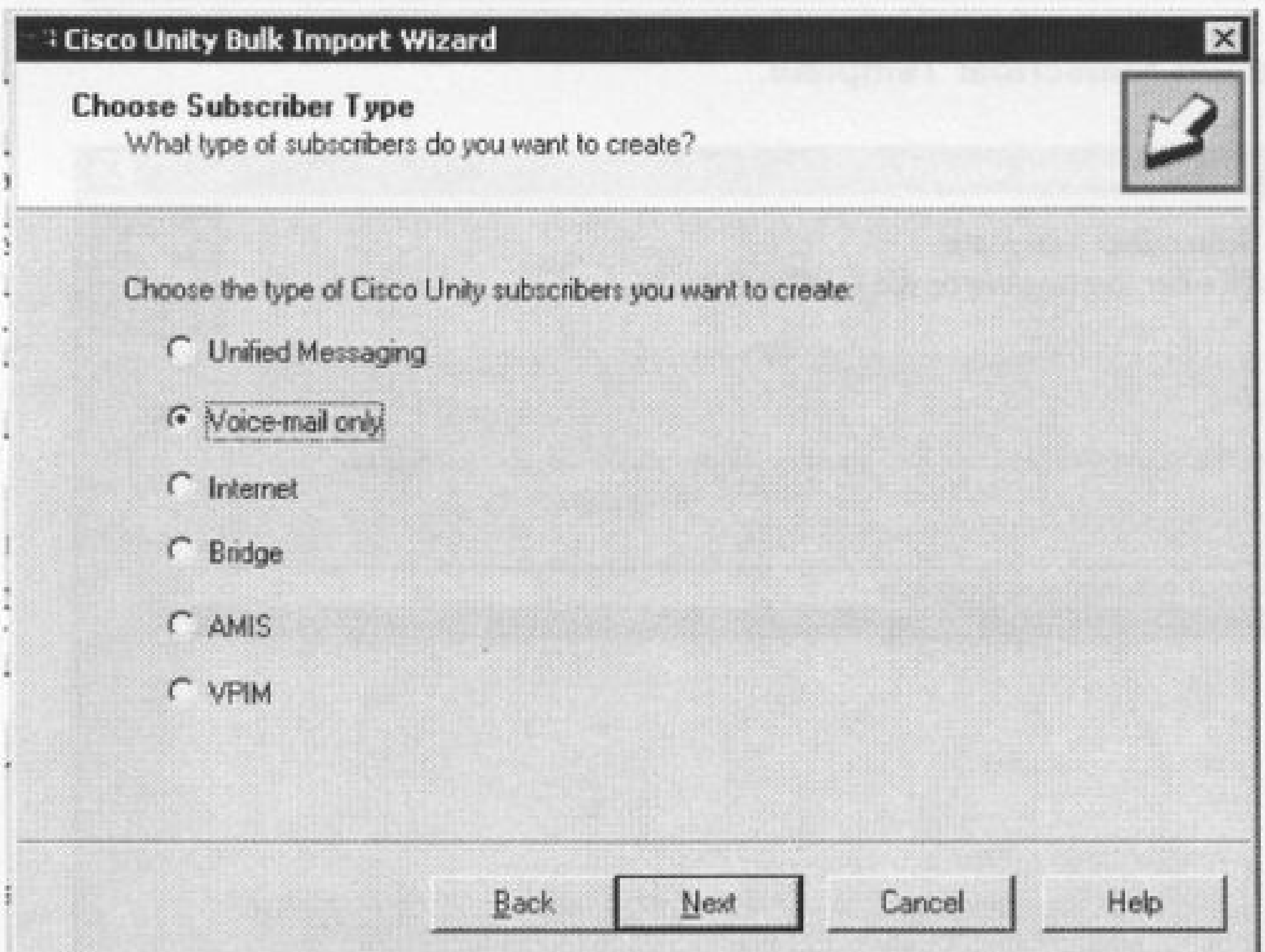
→ **You can import users from the Active Directory or from a CSV file - CSV file is quicker in this instance.**



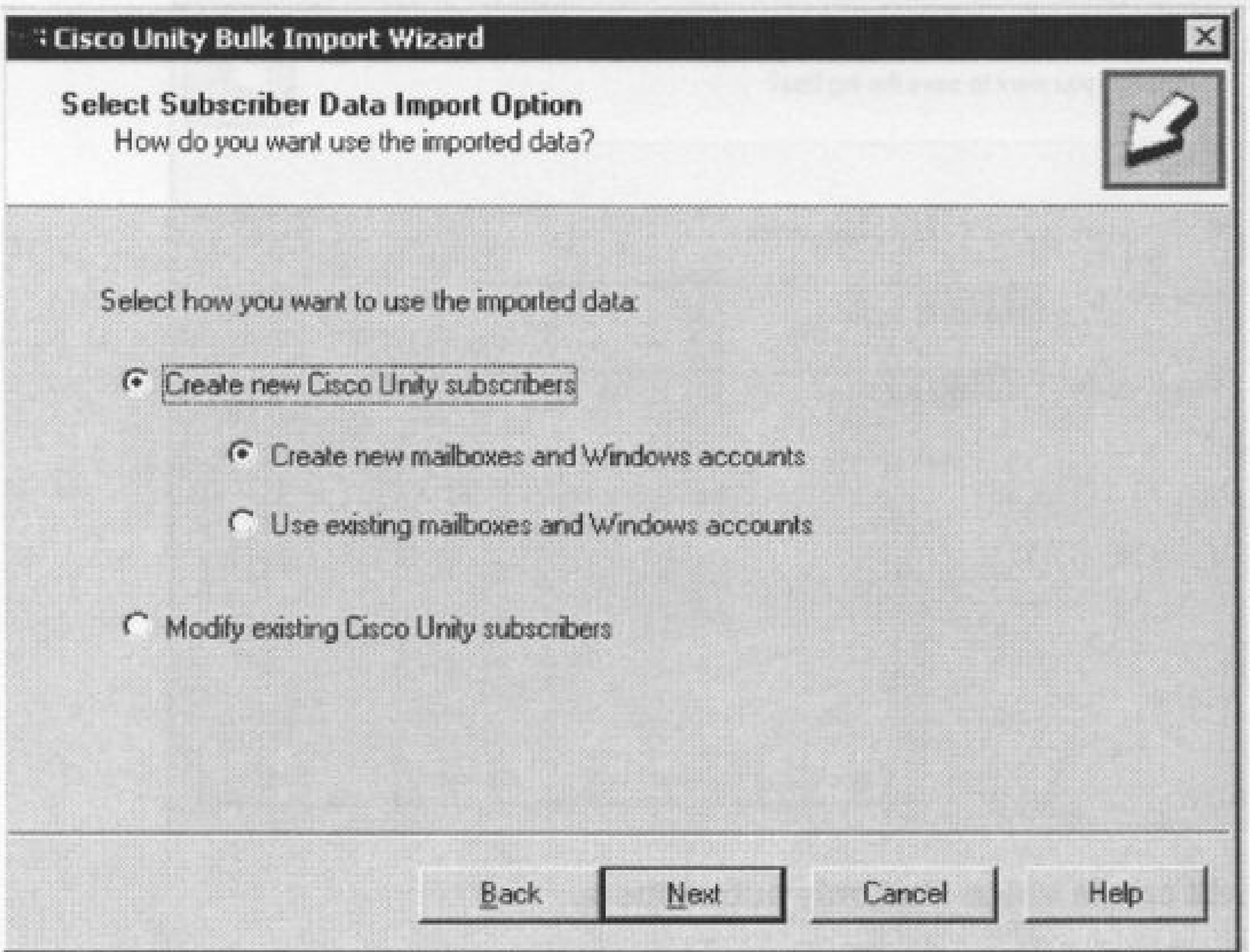
➔ **Leave the location of where the log files are stored to the default locations.**



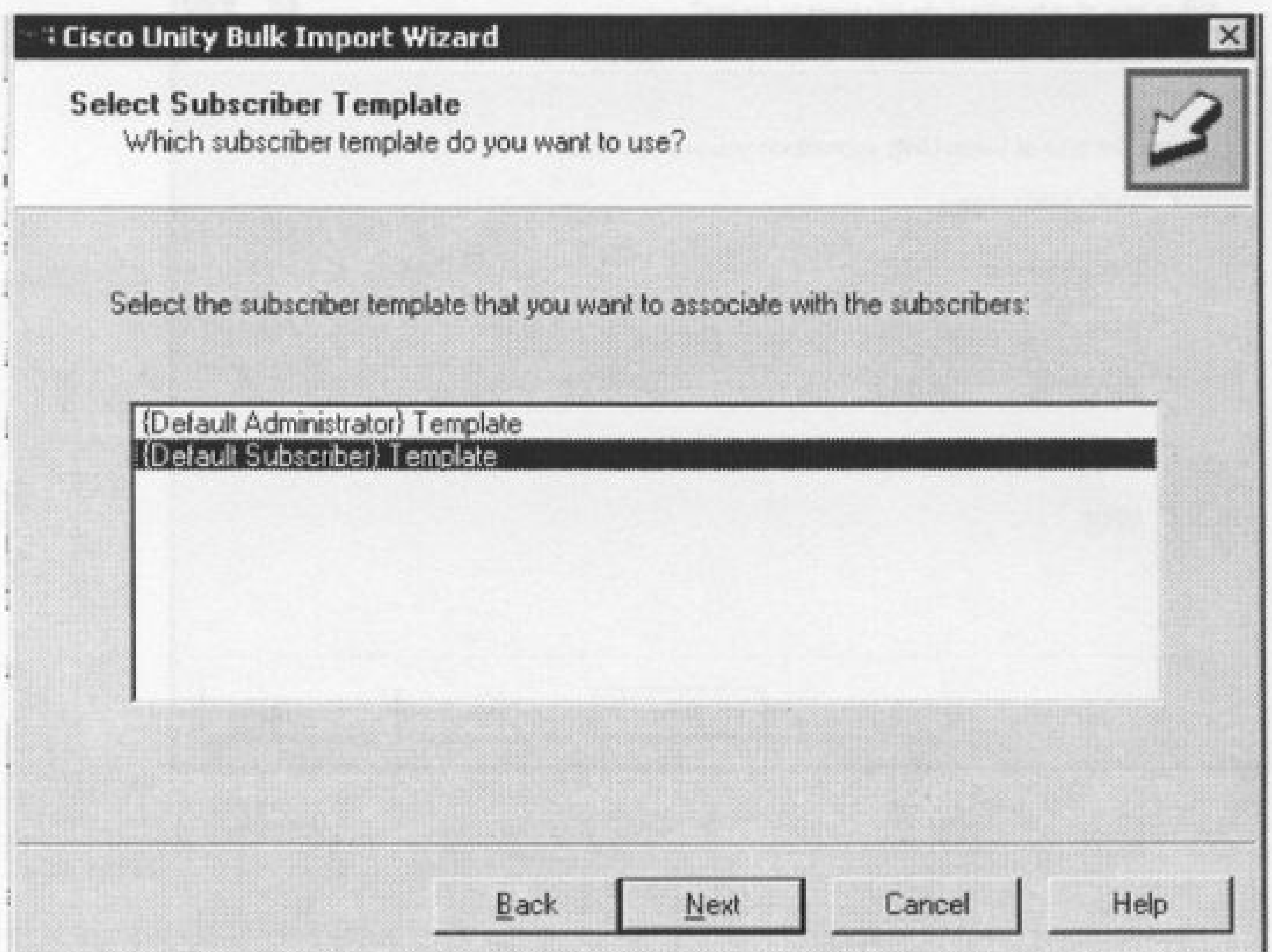
➔ **We will create Voice-Mail only subscribers.**



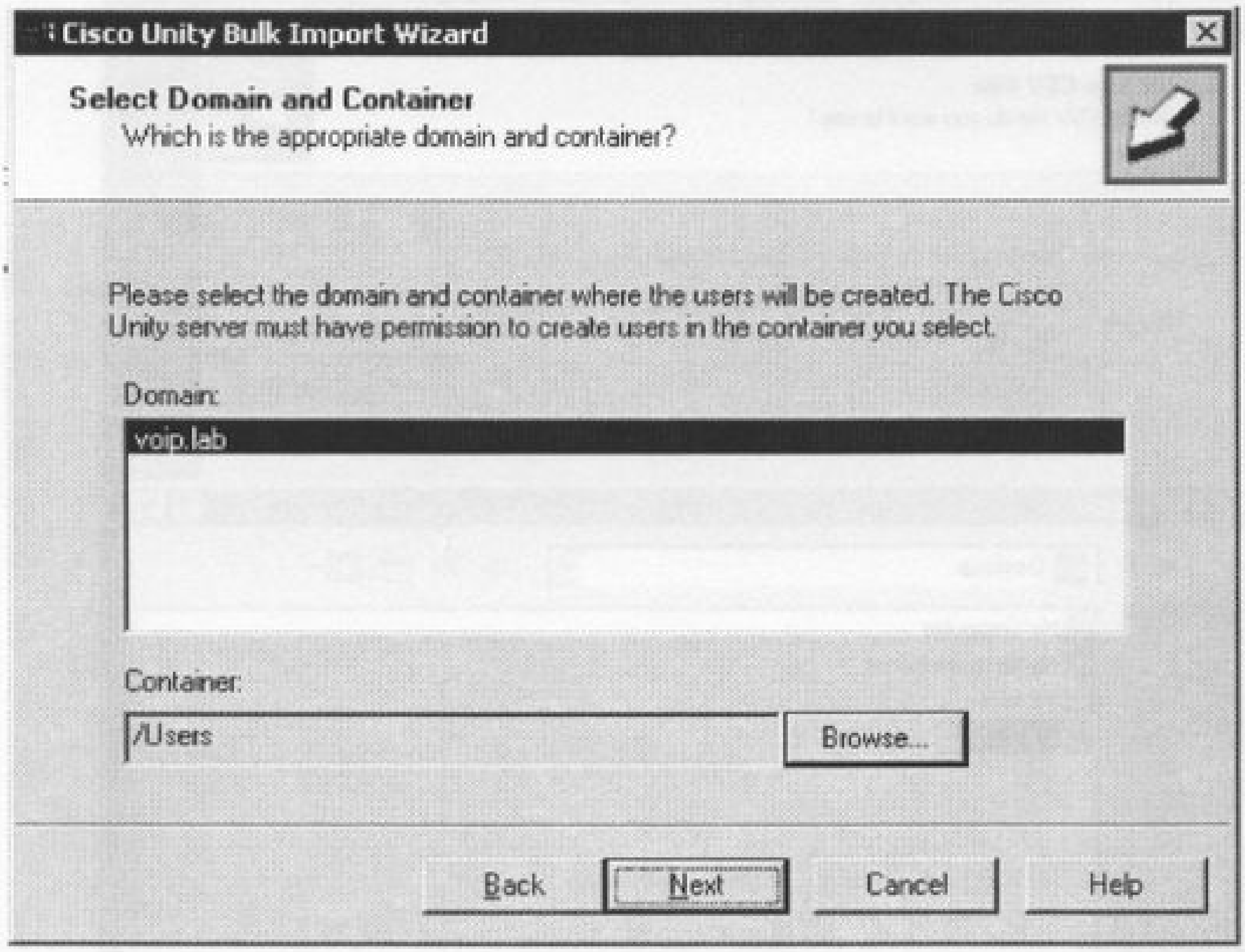
➔ **Since the Exchange and Windows accounts do not exist we will create them at this stage as well.**



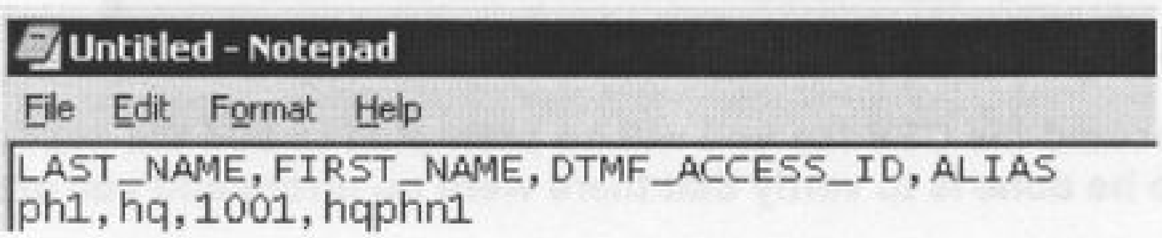
➔ **Select Default Subscriber Template.**



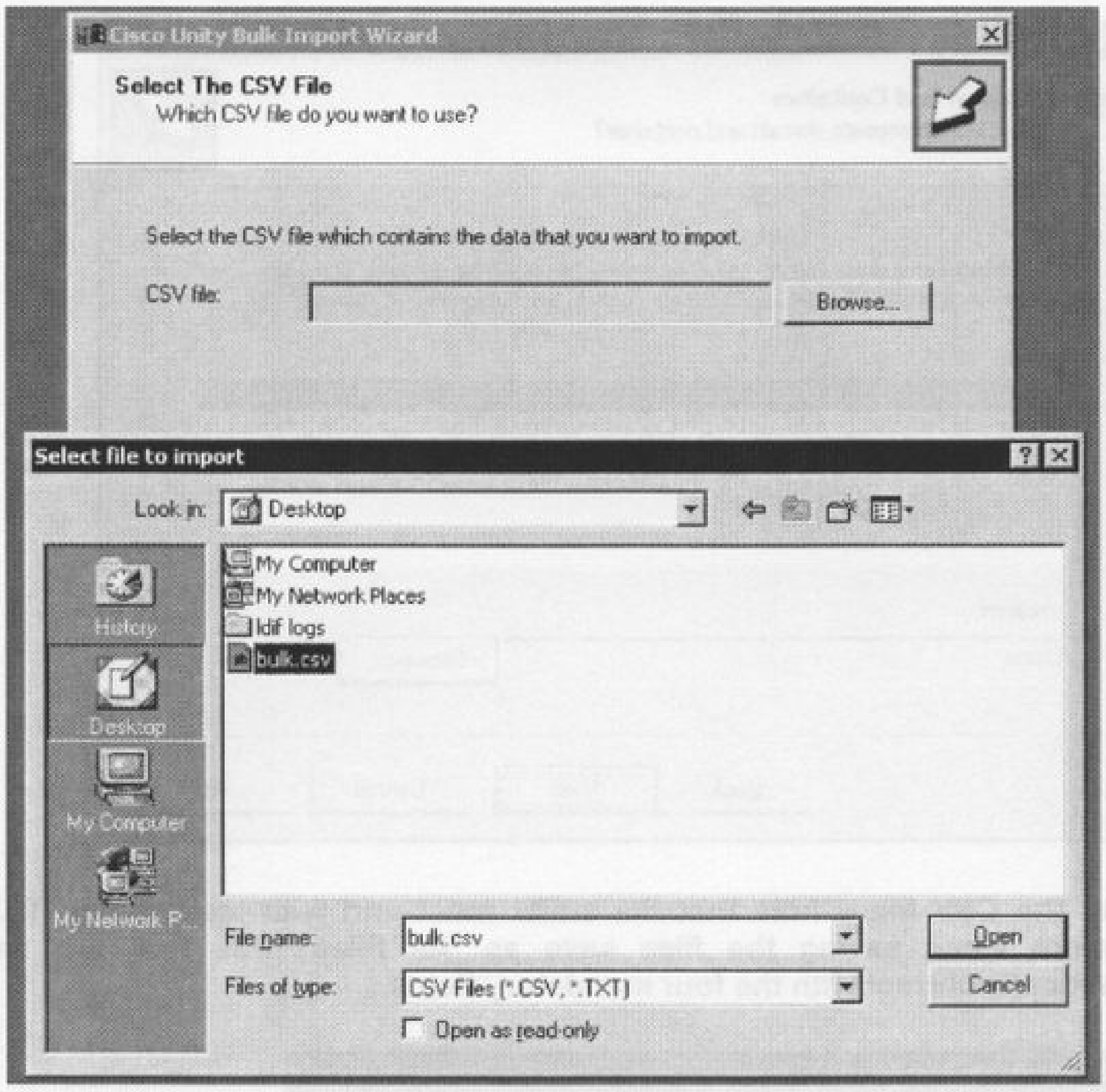
➔ **Select the Domain and Container (leave as default).**



➔ **Create the CSV file – note that the suffix must end with .csv and NOT .csv.txt. Therefore when saving the files save as 'All Files'. The first line must be syntactically correct with the four mandatory fields.**



➔ **Find the CSV file you have created.**

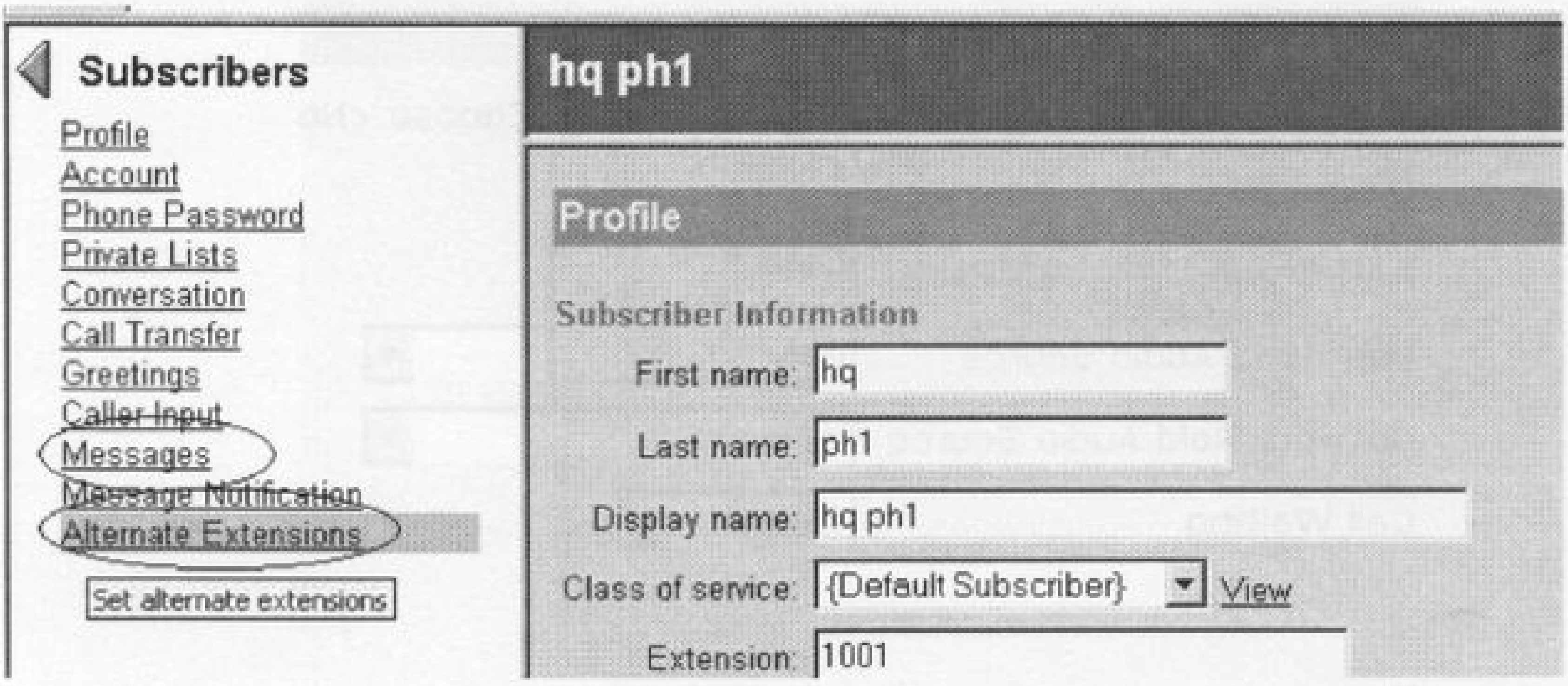


➔ **Once you have located the CSV file you will be prompted to add the subscribers – all that remains to be done is to verify that there were no errors and you are done!**

Task 9.5

Phone 3 at HQ should use the corresponding subscriber account of Phone 1. For example ext '1003' will use the voicemail account for '1001'. Ensure the Phone 1 subscriber greeting is heard when Phone 3 is forwarded to voicemail and that MWI lights up both phones.

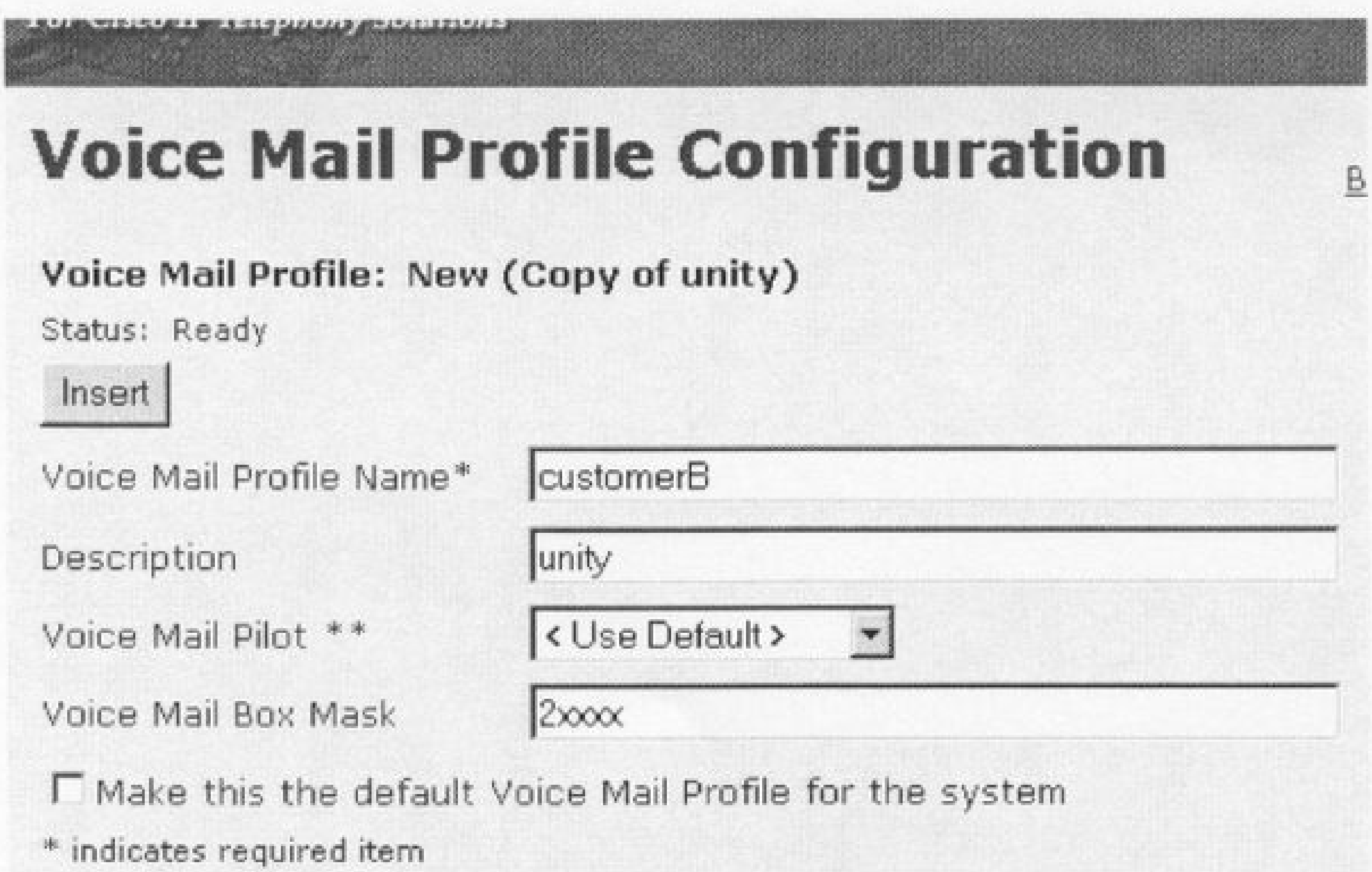
➔ **For the subscriber created in the previous task create an Alternate Extension and Alternate MWI with DN=1003.**



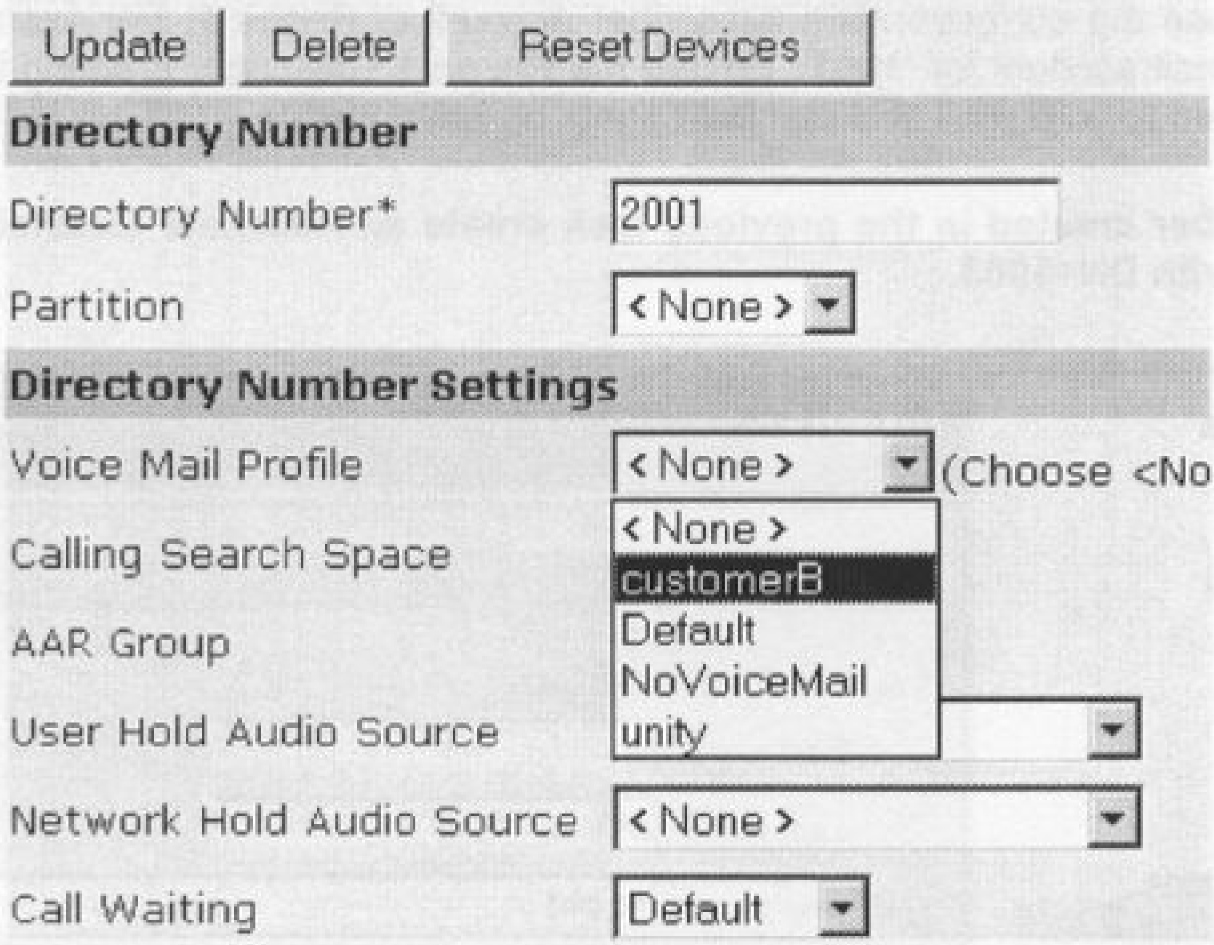
Task 9.6

Create a Unity subscriber account for BR1 phone 1 with DN = 22001. Ensure that the correct subscriber greeting is heard and that MWI is working correctly. You may NOT use Alternate Extension or Alternate MWI to achieve this task.

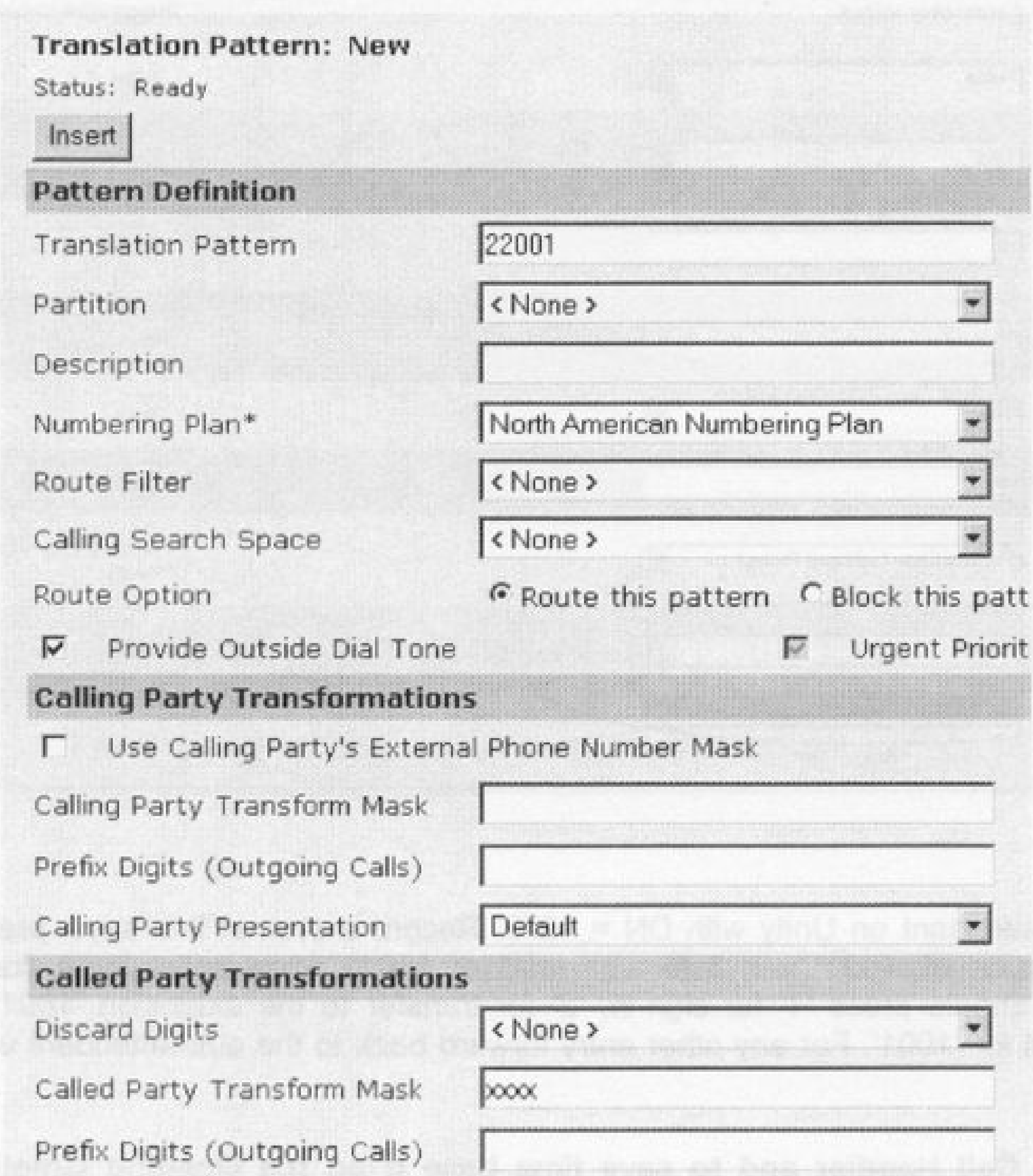
➔ **Create a new Voicemail profile and add a leading '2' in the mask.**



➔ **This profile needs to be assigned to the relevant Line.**

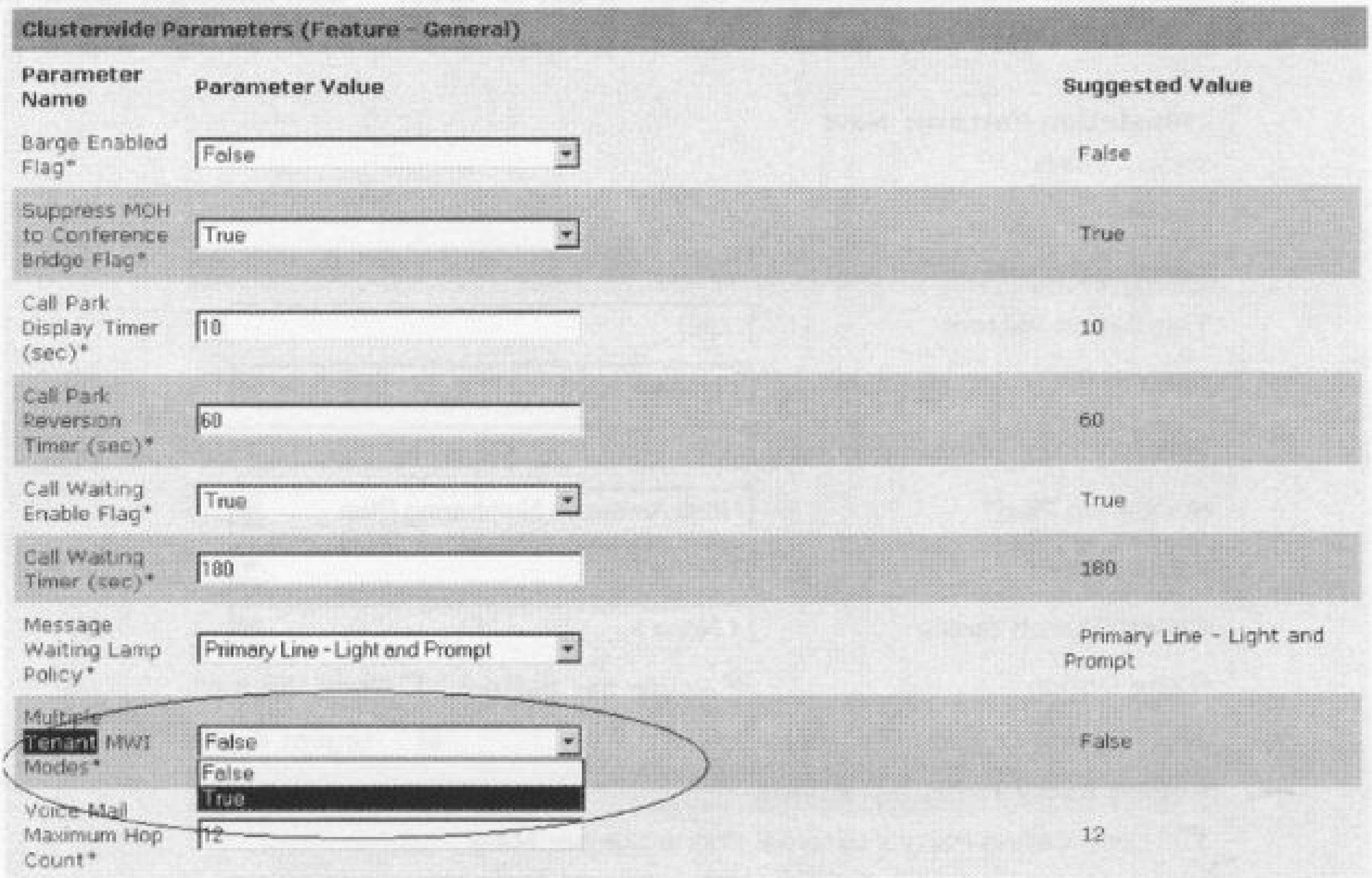


➔ **The problem of MWI is solved using Translation Patterns - in the customer B partition we will transform '22001' to '2001'. A Translation Pattern with DN=22001 is created with 'Called Transform Mask' is set to 'xxxx' – Call Manager looks only at 4 digits right justified.**



➔ **In order to use transformation masks with MWI a CCM Service Parameter need to be edited. The 'Multiple Tenant MWI modes' needs to be set to 'True' in order for MWI to be able to work with Translation Patterns.**

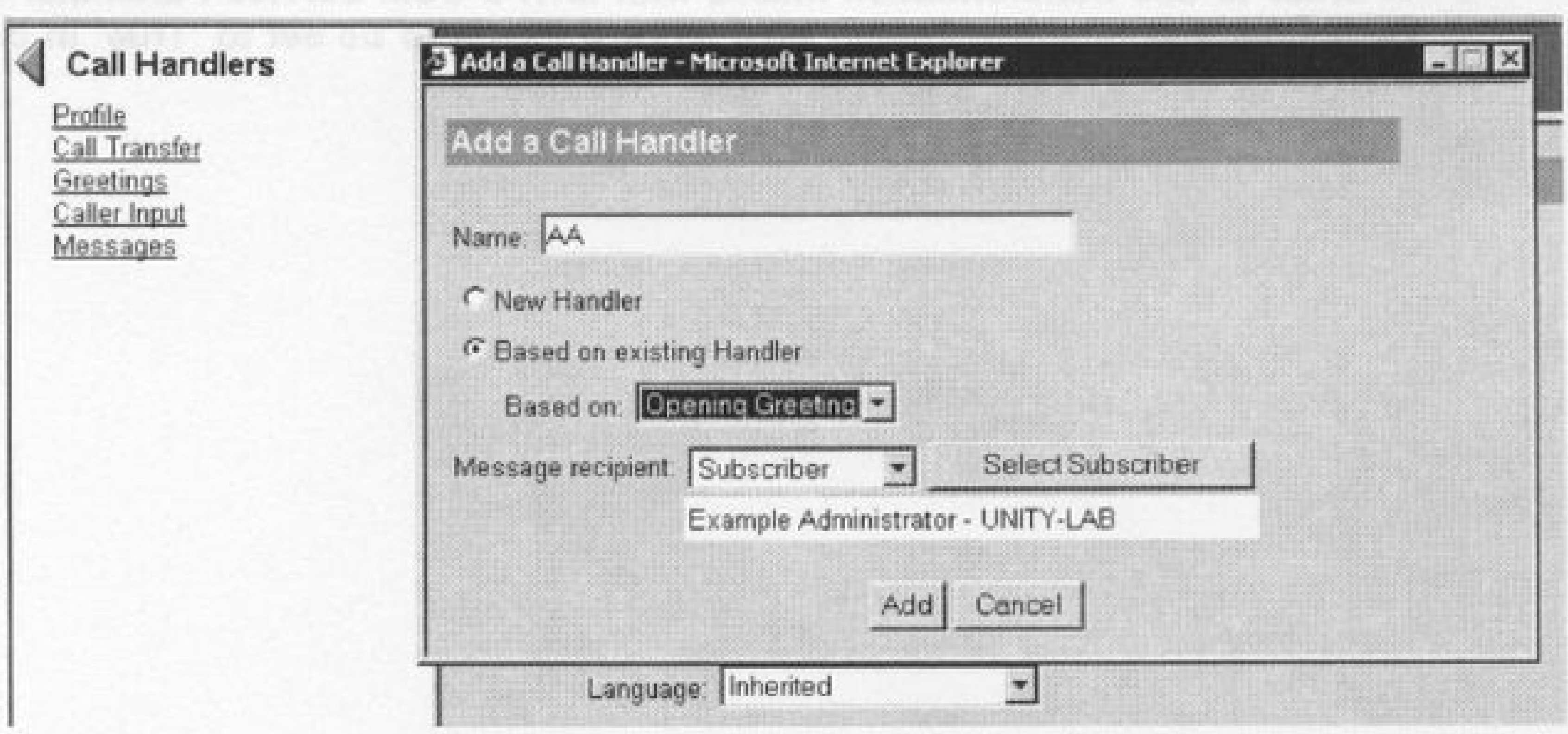
➔ **Once this has been changed don't forget to restart the Call Manager service from Control Center.**



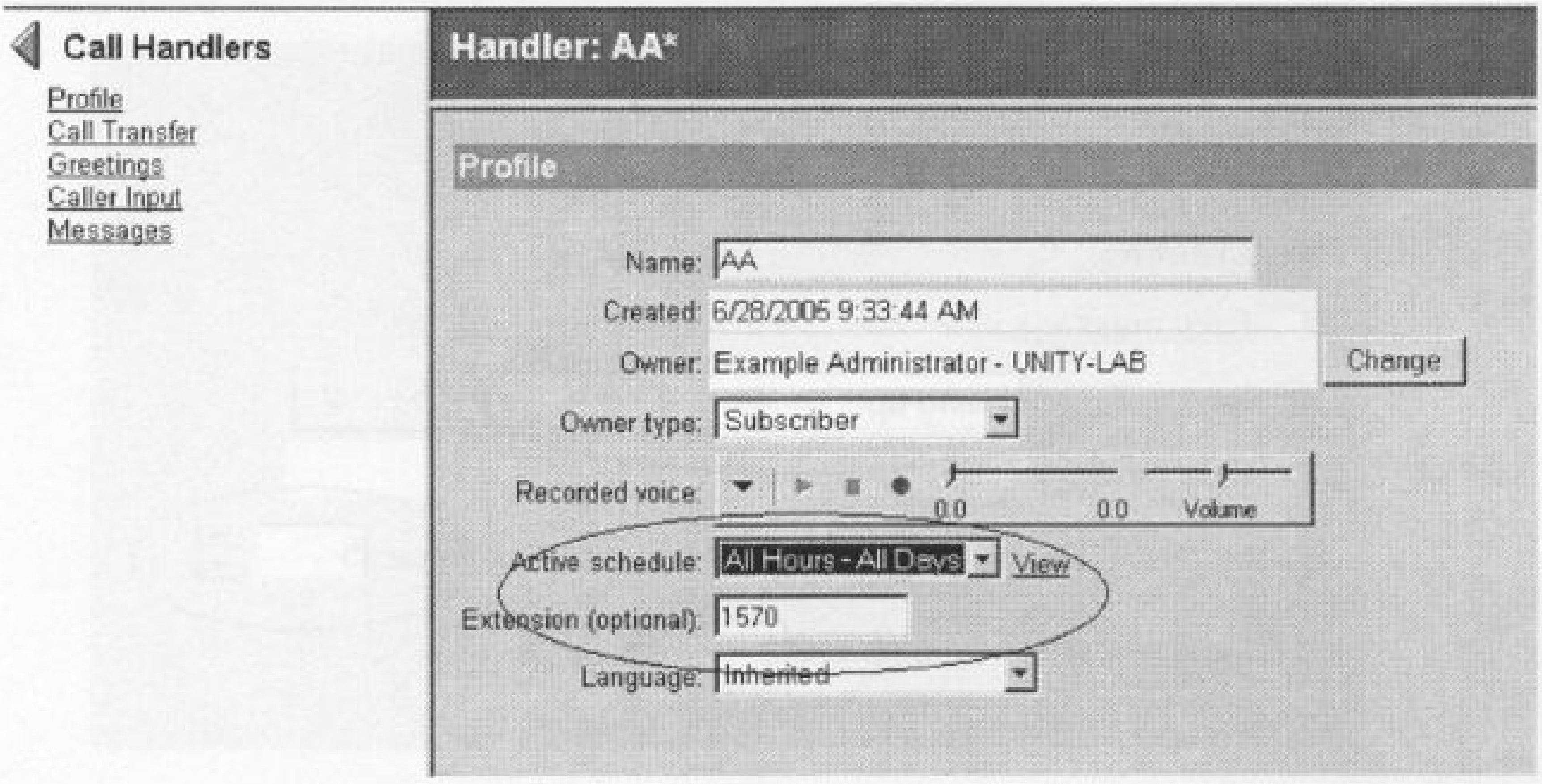
Task 9.7

Configure an auto-attendant on Unity with DN = 1570. Record a prompt that says 'press 1 for sign-in, 2 for extension of '1001' and 3 for voicemail of 1001'. Allow caller input during this greeting. The user should press '1' for sign-in, '2' for transfer to the extension '1001', '3' for transfer to voicemail for '1001'. For any other entry forward back to the auto-attendant using the error greeting.

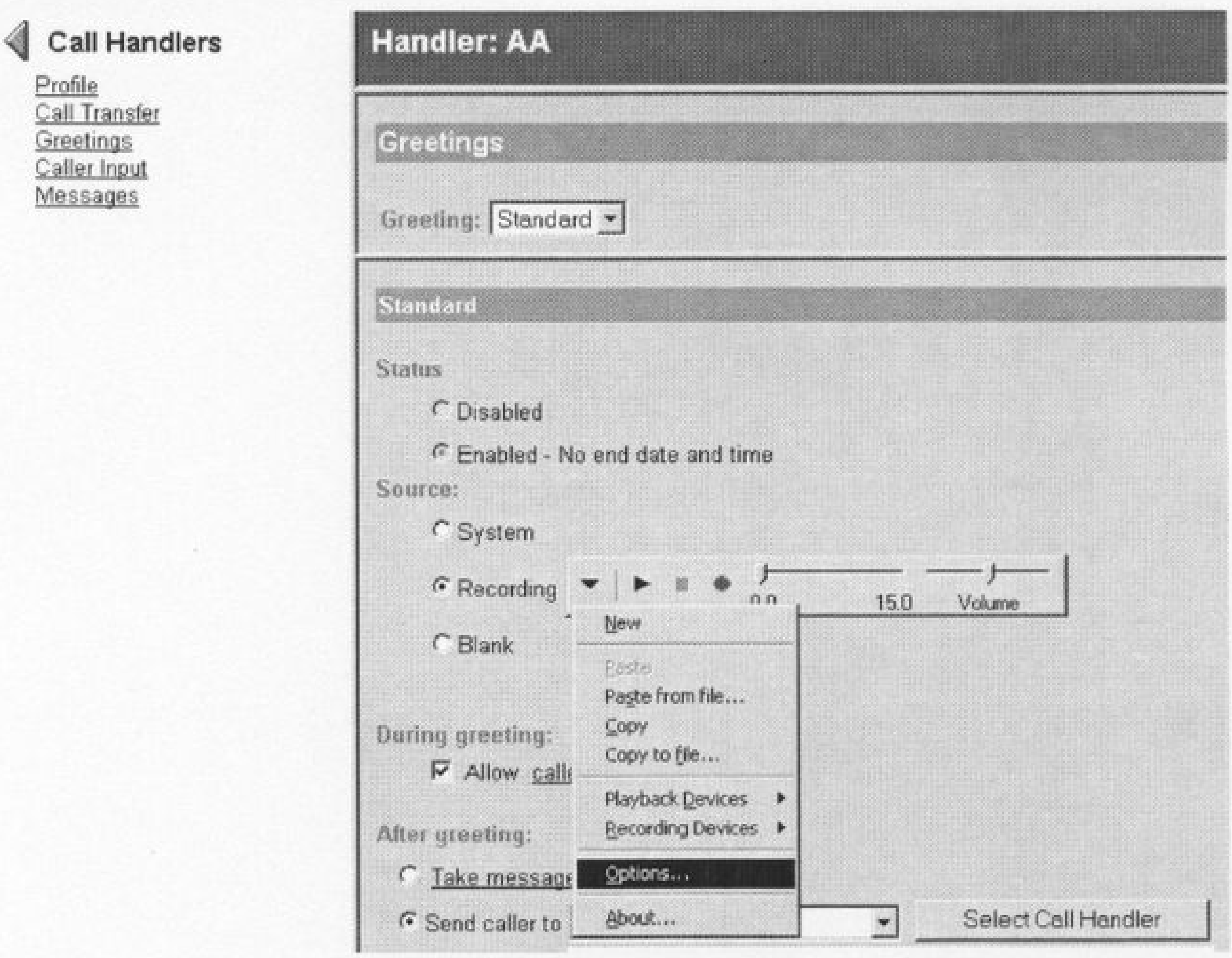
➔ **Create the Call Handler and to save time base it on the Opening Greeting call handler.**



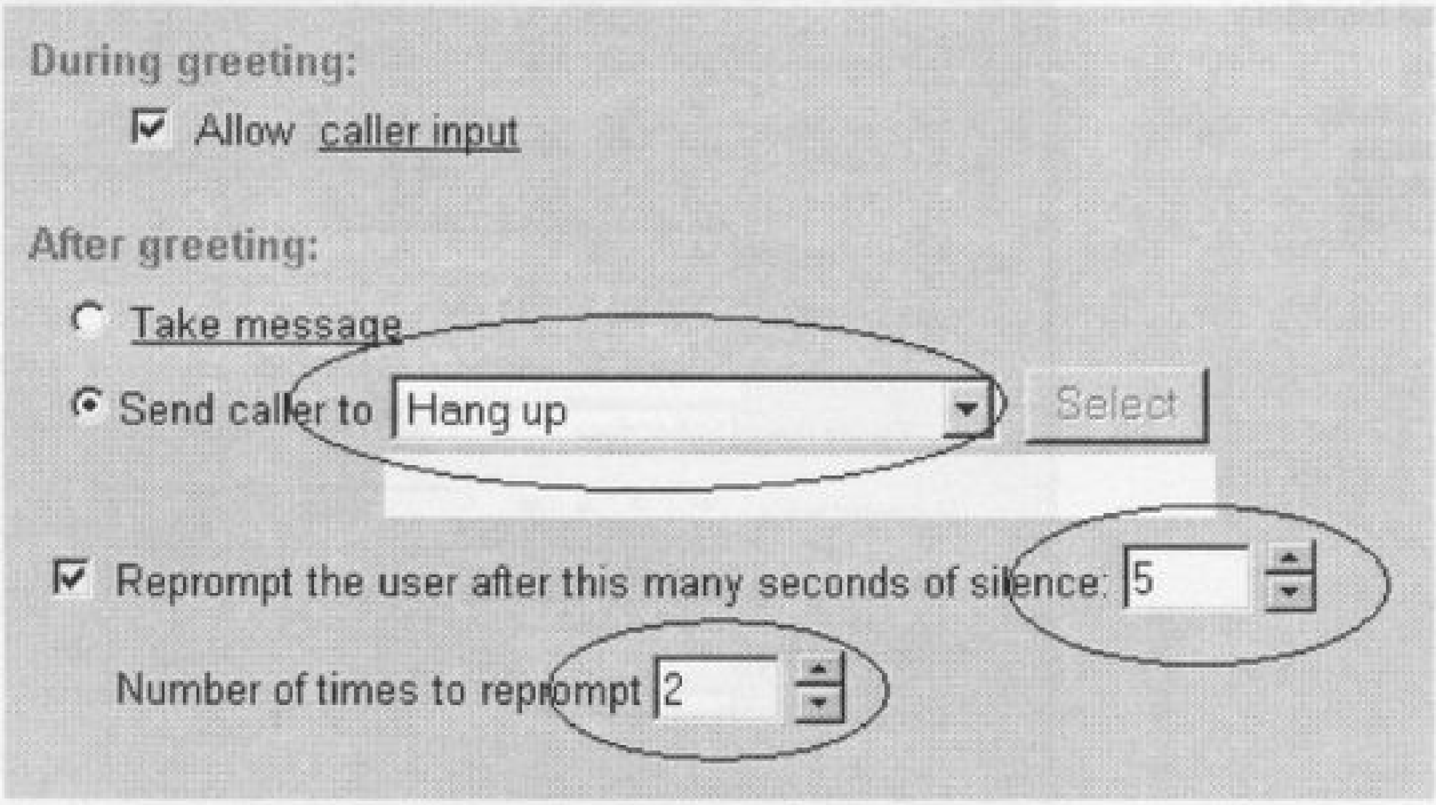
➔ **Change the Active Schedule so the 'Closed' greeting is not used out of business hours. Also assign the appropriate DN to the Call Handler.**



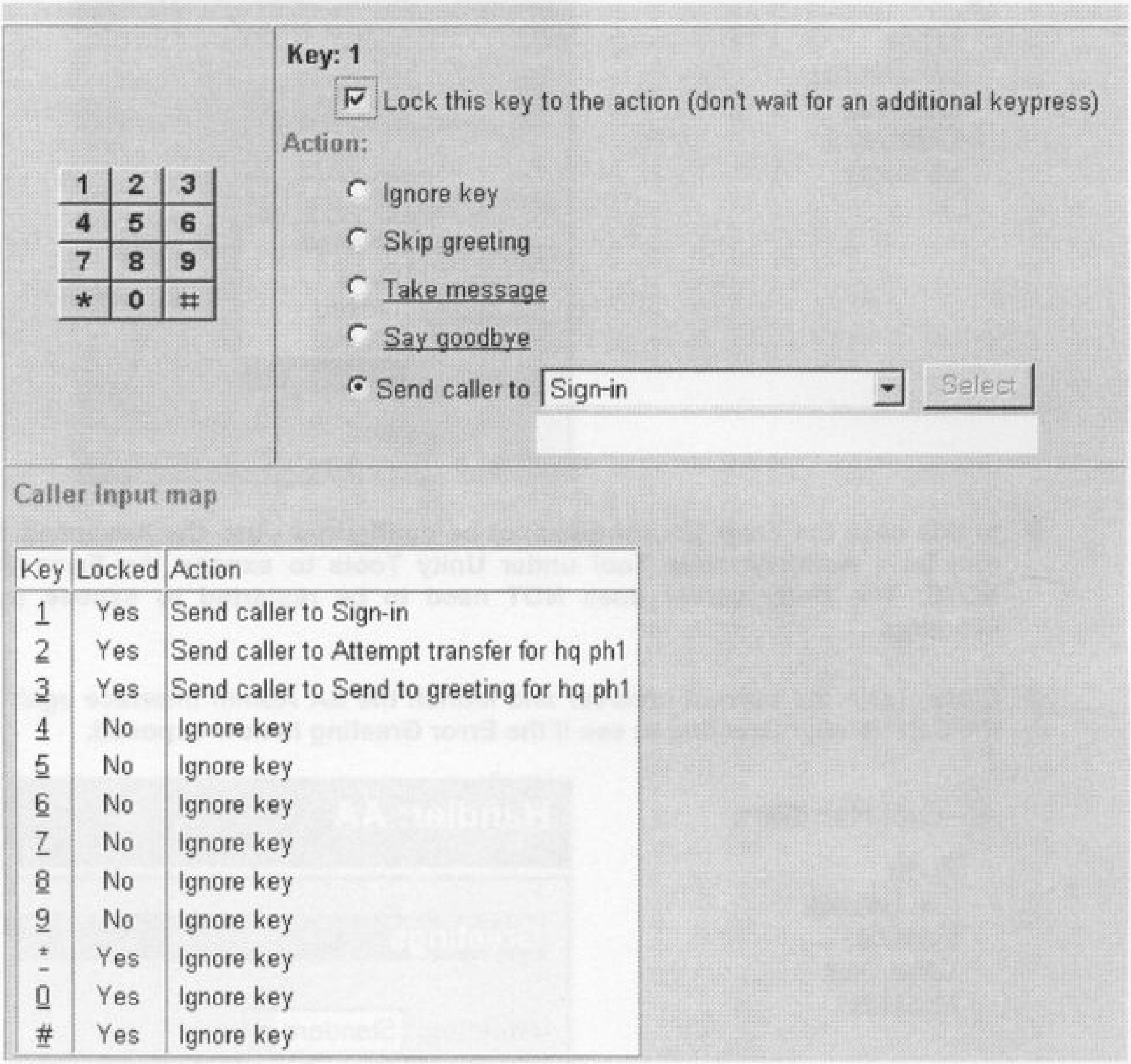
➔ **From the 'Greetings' page go to options and specify the Unity Server and Extension Number of the phone which will be used with Media Master to record the Call Handler Greeting (Welcome to PODX, press '1' to sign in, '2' for HQ phone 1, '3' for voicemail of HQ Phone 1).**



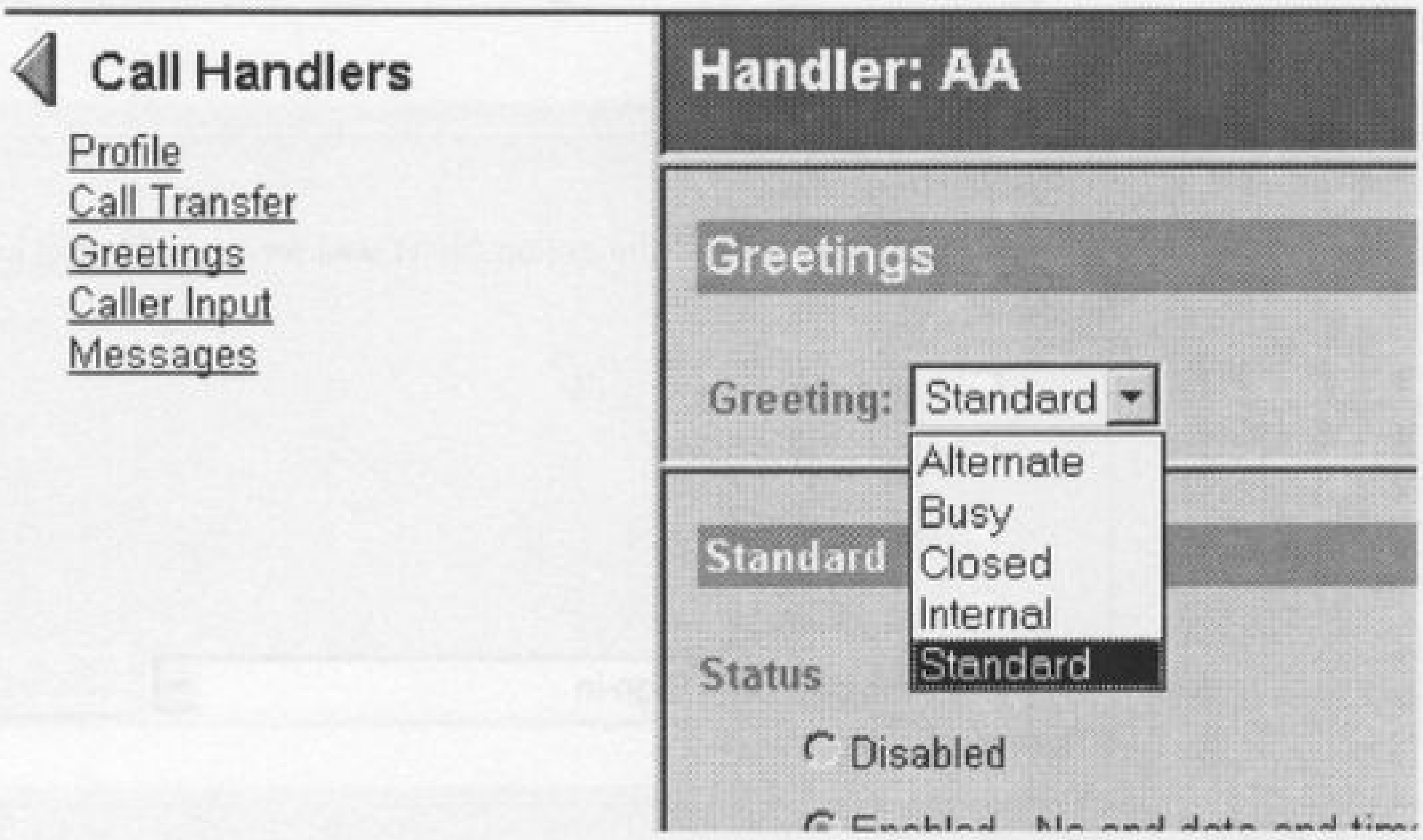
➔ **On the same page specify that the caller is allowed to enter digits during the greeting. After 5 seconds of silence Unity will play the prompt again (twice) before ending the call.**



➔ **From the 'Caller Input' specify the actions required on relevant key presses. By locking keys Unity proceed to the desired action without waiting for the inter-digit timeout. All unused keys should be set to 'Ignore' - this will invoke the Error Greeting.**

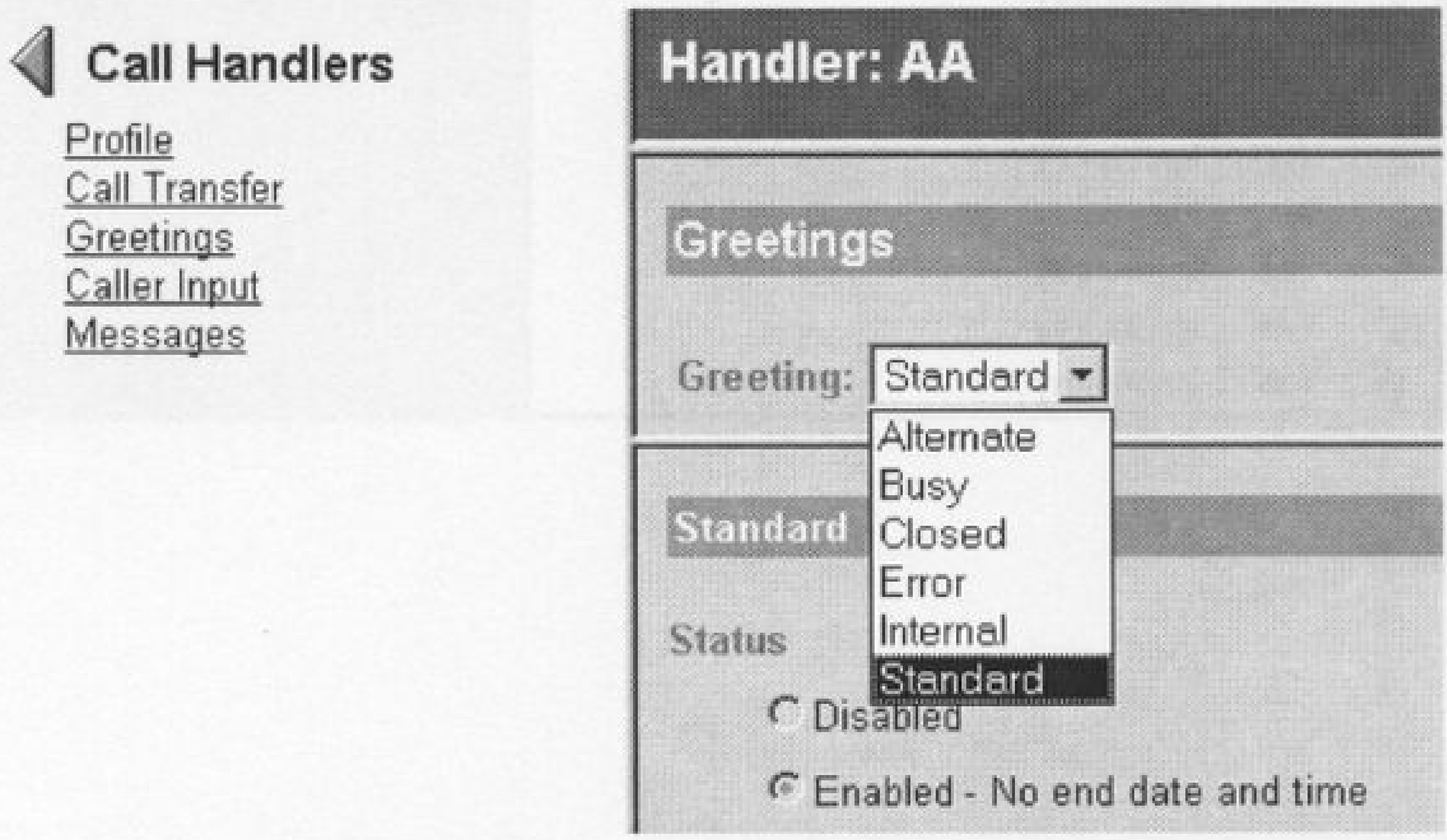


➔ **Go to the Call Handler Greeting and check if the Error Greeting is allowed to be configured.**

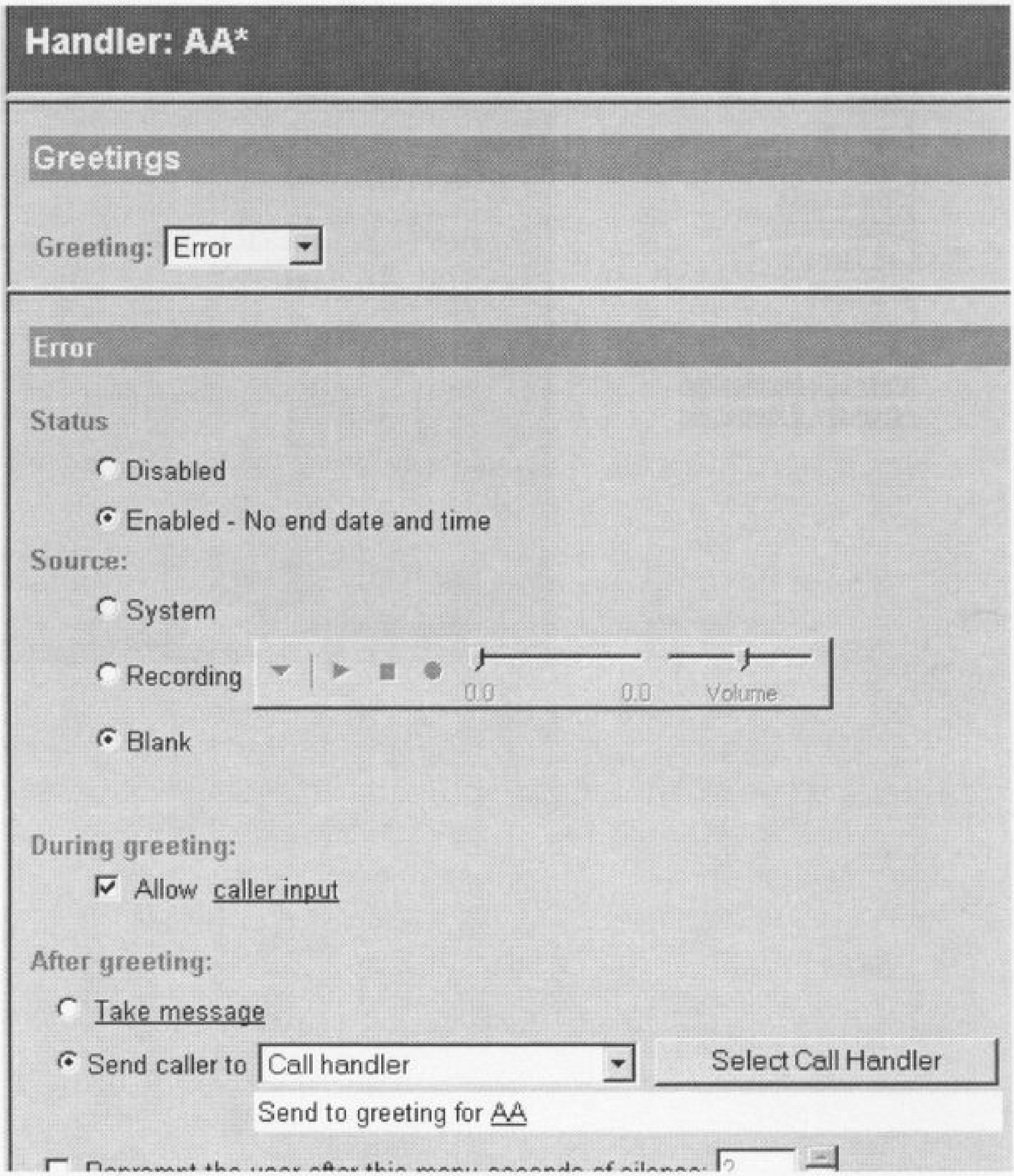


➔ **In this case the Error Greeting cannot be configured - use the Advanced Settings tool from Administrative Tool under Unity Tools to expose the Error Greeting. NOTE: The Unity server does NOT need to be restarted to expose the Error Greeting.**

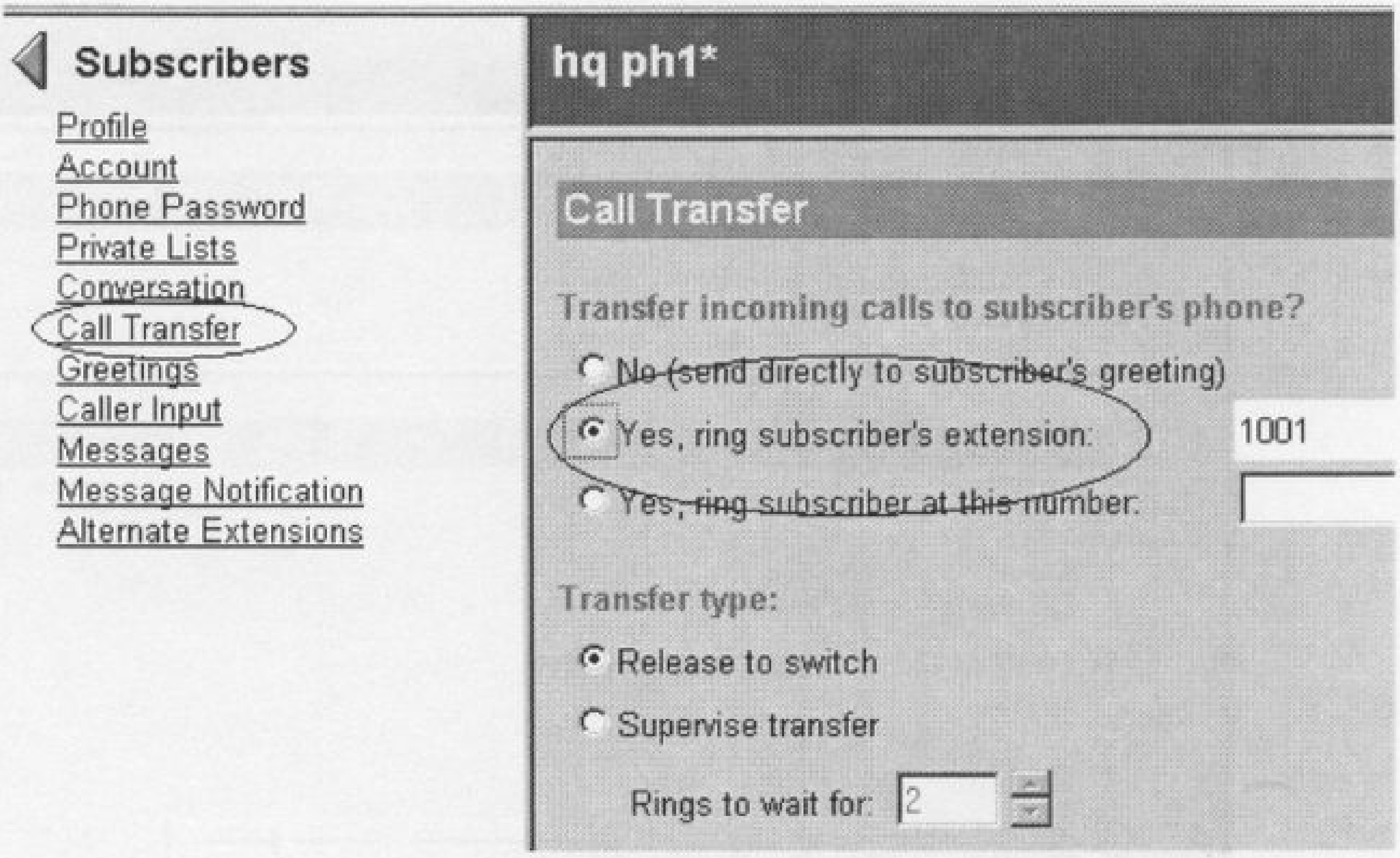
➔ **Close down the current browser and launch the SA Admin Interface again. Check the Call Handler Greeting to see if the Error Greeting is now exposed.**



➔ **Configure the Error Greeting - play a blank greeting and send to the Greeting of the Auto-Attendant.**



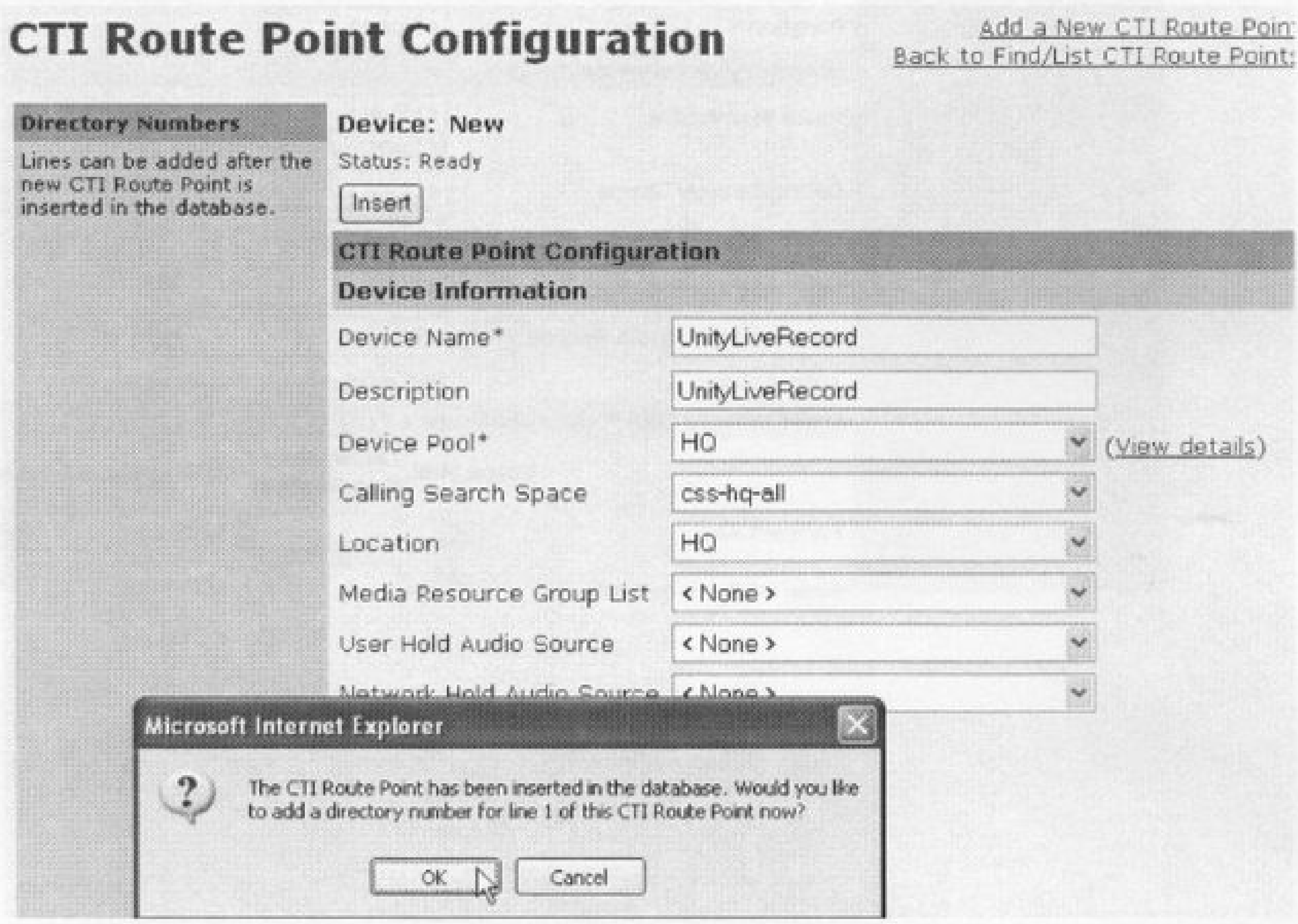
➔ **One last vital step: configure the subscriber's Call Transfer options to permit dialing the extension.**

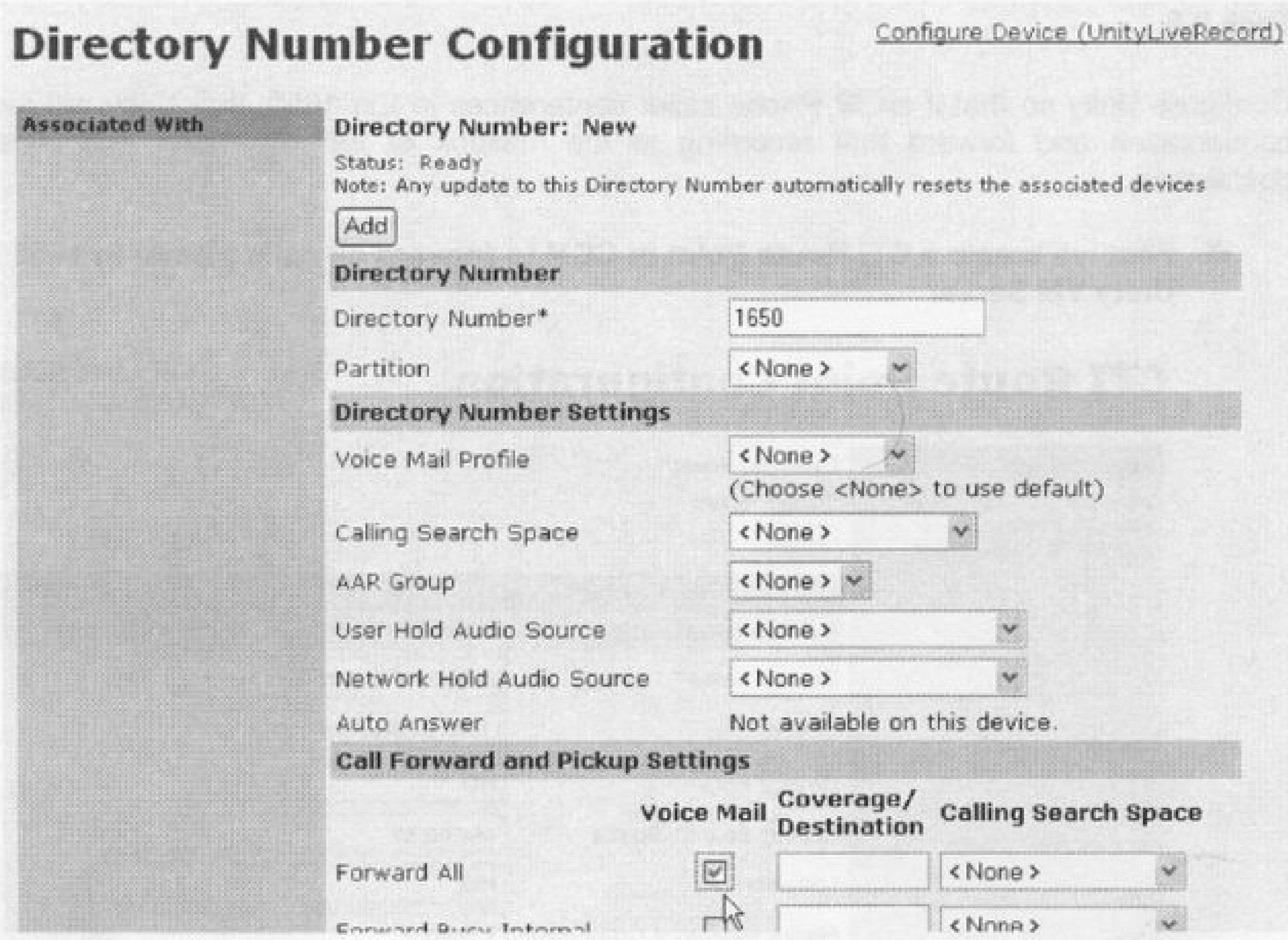


Task 9.8

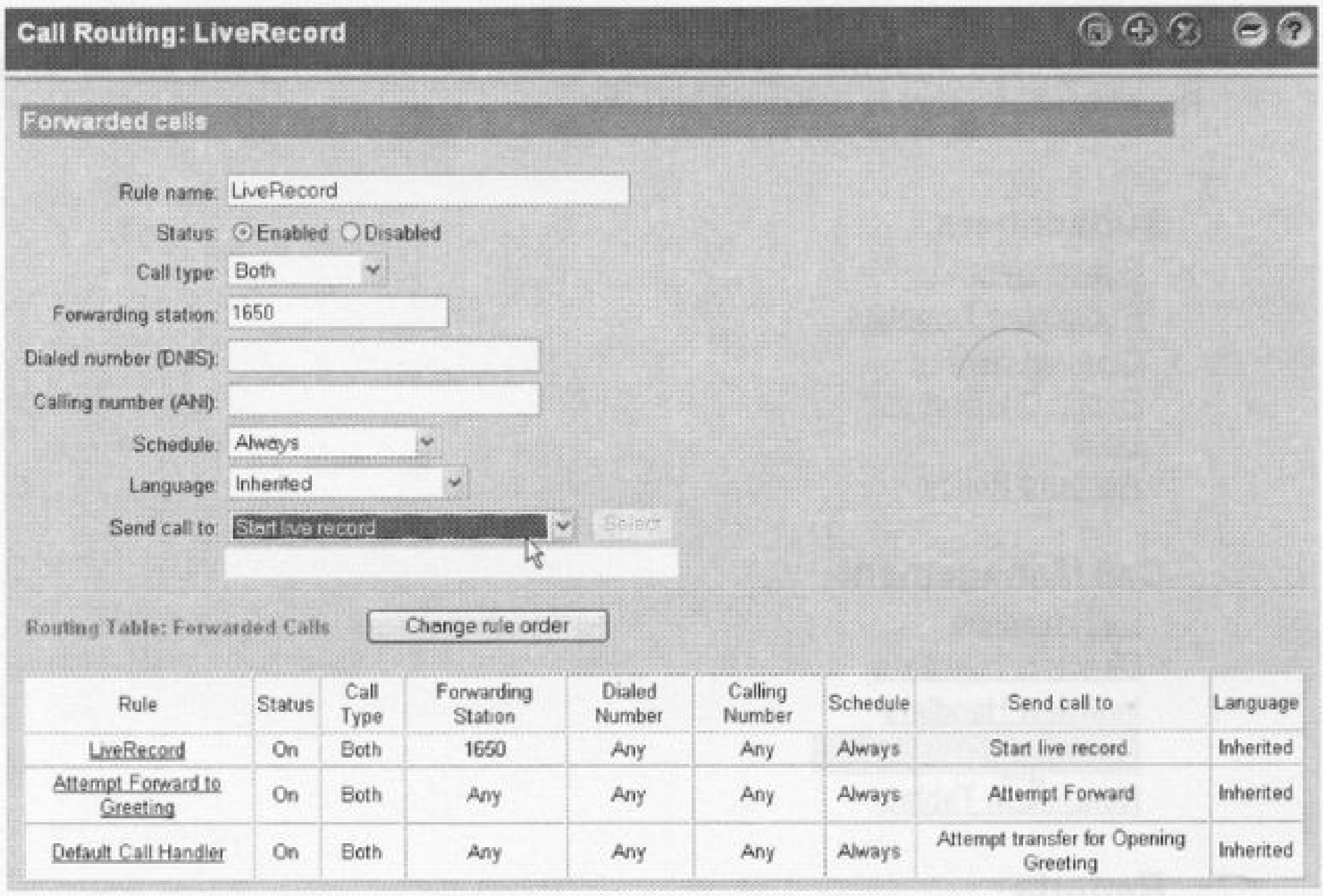
Configure Unity so that if an IP Phone caller conferences in Ext 1650, that Unity will record the conversation and forward that recording to the mailbox of the IP Phone that initiated the conference.

➔ **First we create a CTI Route Point in CCM to forward all calls placed to 1650 into the Unity VM Server**




Directory Number Configuration
Configure Device (UnityLiveRecord)
Associated With
Directory Number: New
Status: Ready
Note: Any update to this Directory Number automatically resets the associated devices
Add
Directory Number
Directory Number*
1650
Partition
< None >
Directory Number Settings
Voice Mail Profile
< None >
(Choose <None> to use default)
Calling Search Space
< None >
AAR Group
< None >
User Hold Audio Source
< None >
Network Hold Audio Source
< None >
Auto Answer
Not available on this device.
Call Forward and Pickup Settings
Voice Mail
Coverage/ Destination
Calling Search Space
Forward All
< None >

➔ **Now in Unity we need to Create a new Routing Rule for 'Forwarded Calls' to match incoming calls from the 'Forwarding Station' of 1650 and 'Send call to' to the Live Record feature that is included in Unity.**



➔ **Finally to test place a call into 1650 and start talking – when you hang up, the live recording should be a new message in the mailbox from the extension you dialed in from.**

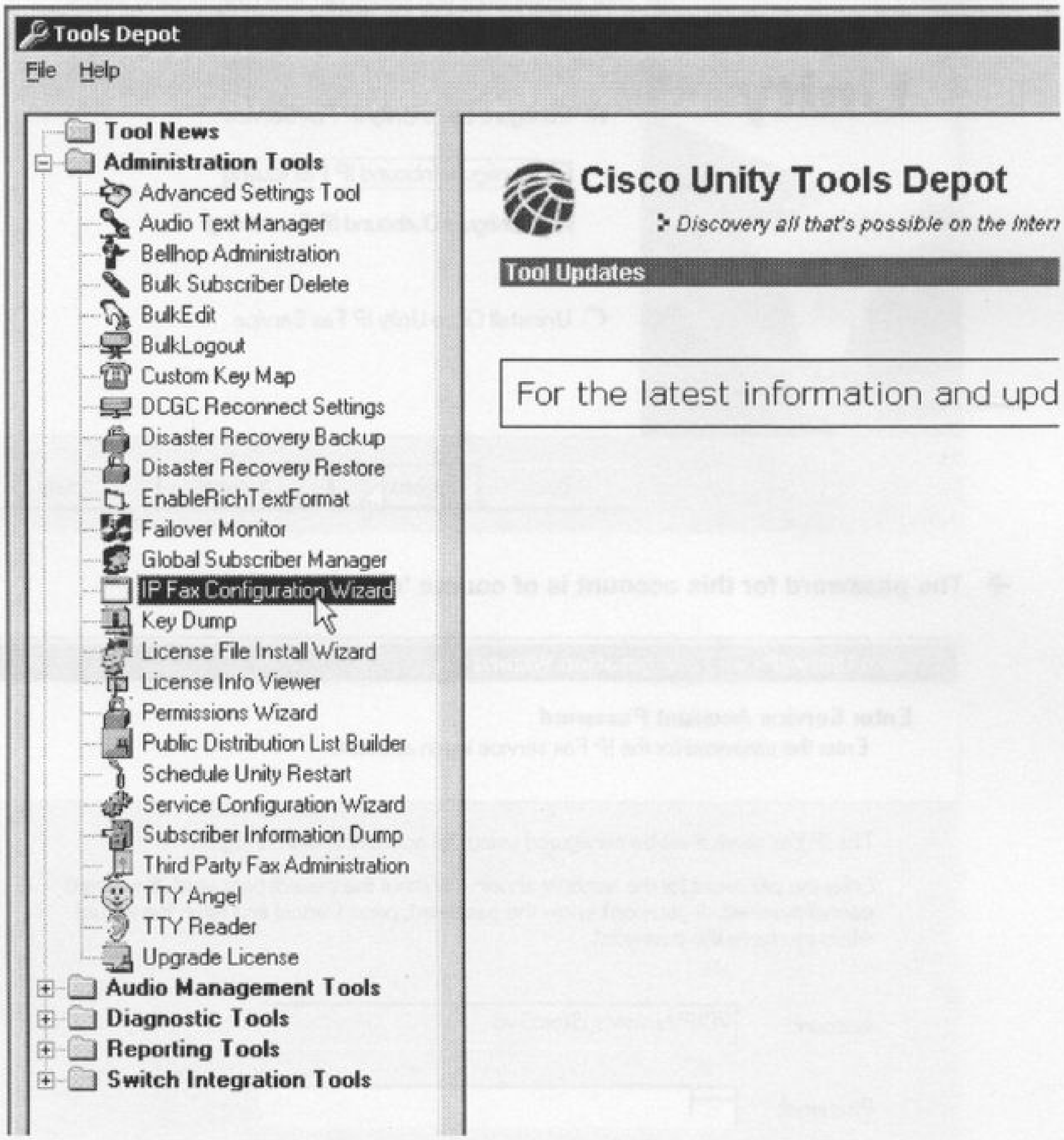
➔ **You may also be on a call to another phone and conference in 1650 – and whichever phone dialed the 1650 conference will be where the bi-directional stream of audio is recorded and sent to its mailbox.**

Task 9.9

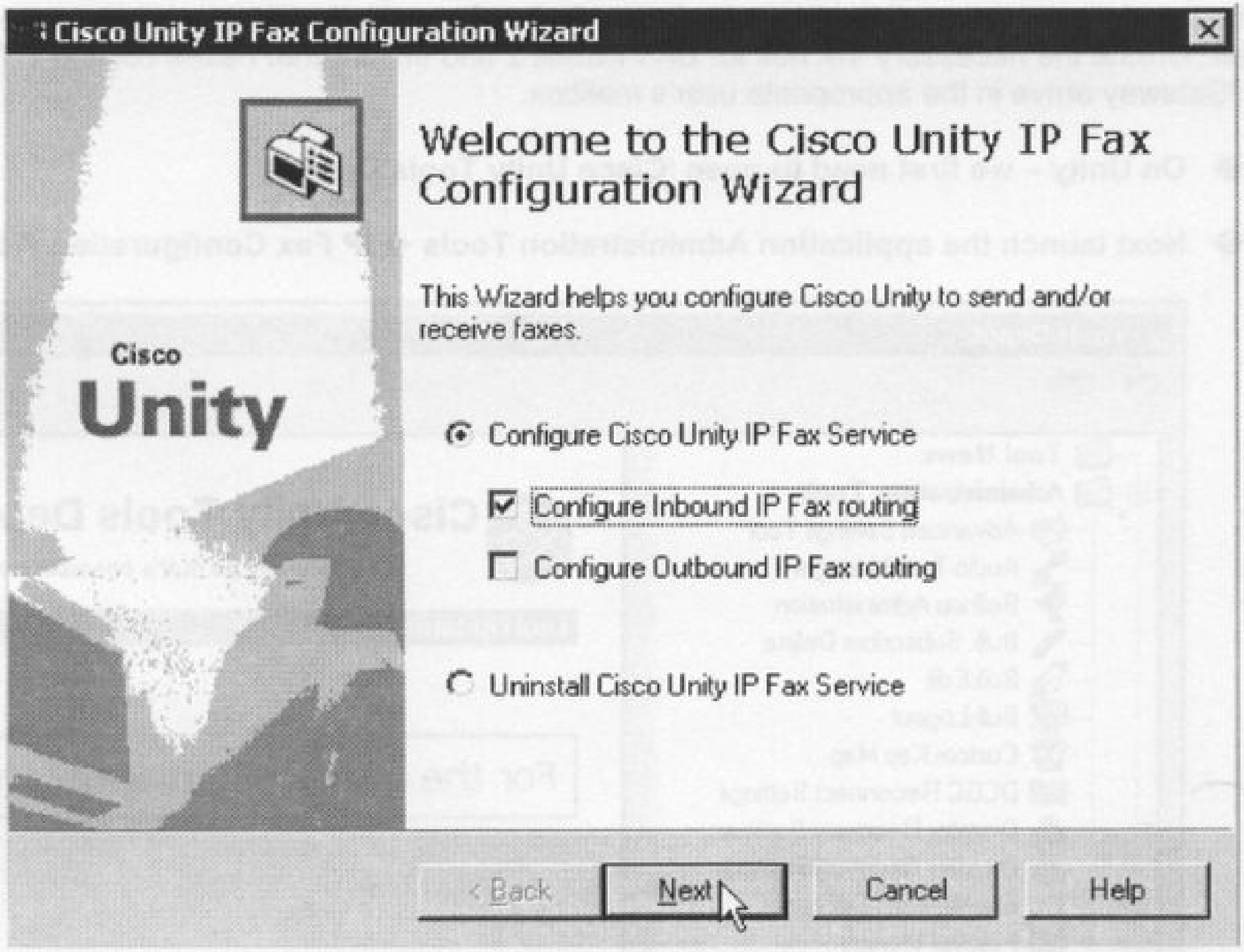
Continuing from question 4.8 and using Table 5; Configure Unity to be an Inbound only Fax Server. Create the necessary VM box for BR1 Phone 2 and ensure that Faxes coming in from the BR1 Gateway arrive in the appropriate user's mailbox.

→ **On Unity – we first need to open 'Cisco Unity Tools Depot'**

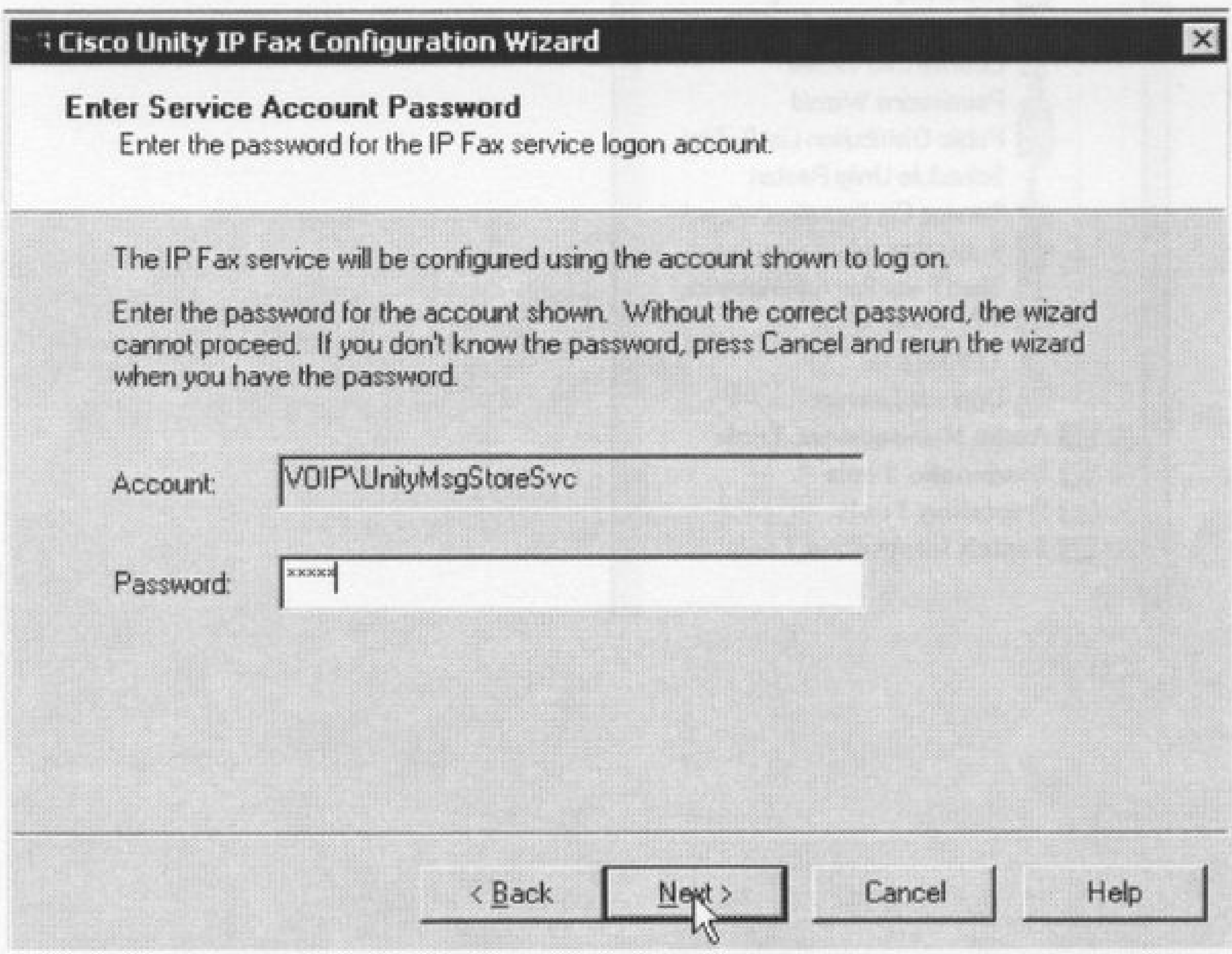
→ **Next launch the application Administration Tools → IP Fax Configuration Wizard**



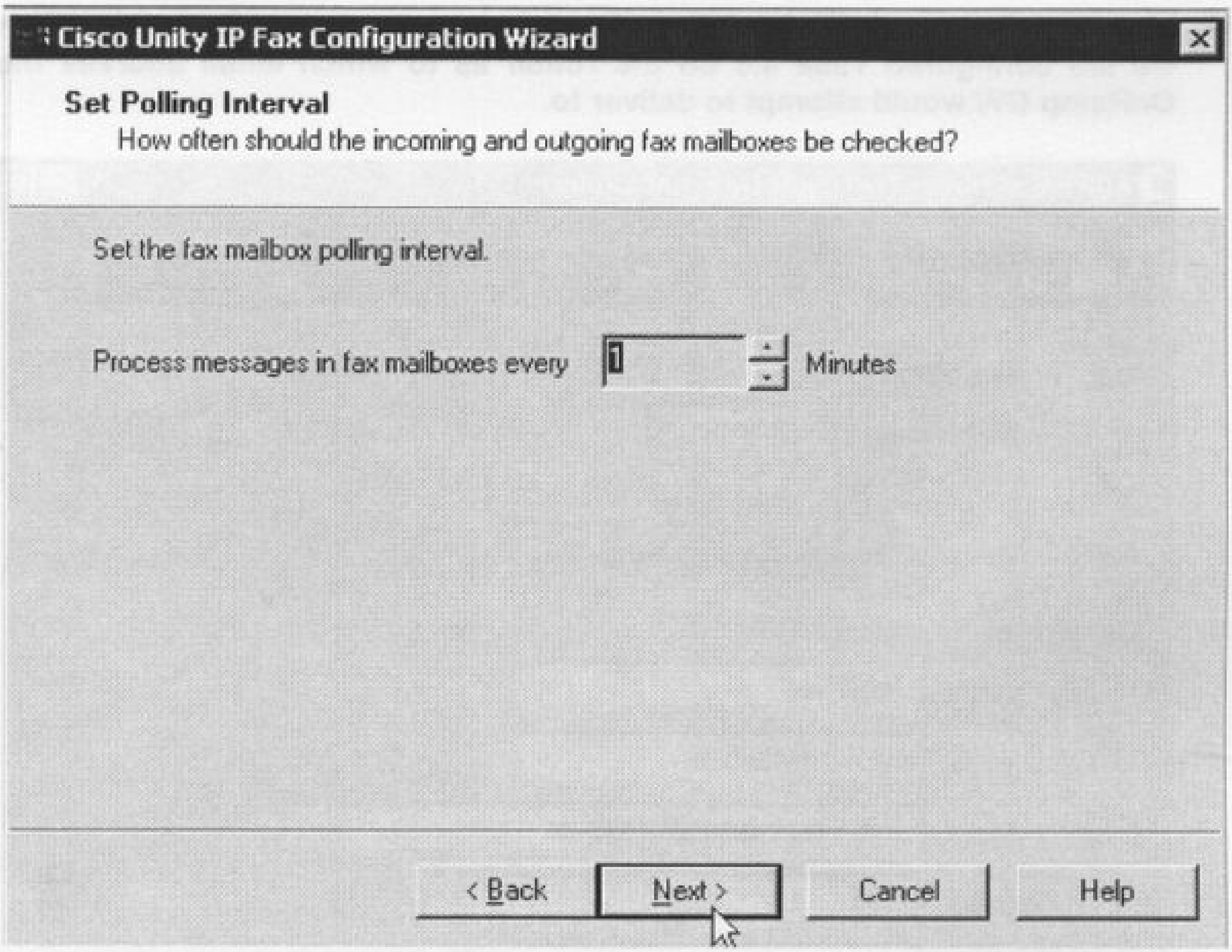
➔ **At this time we will be configuring Inbound IP Fax routing only.**



➔ **The password for this account is of course 'cisco'.**

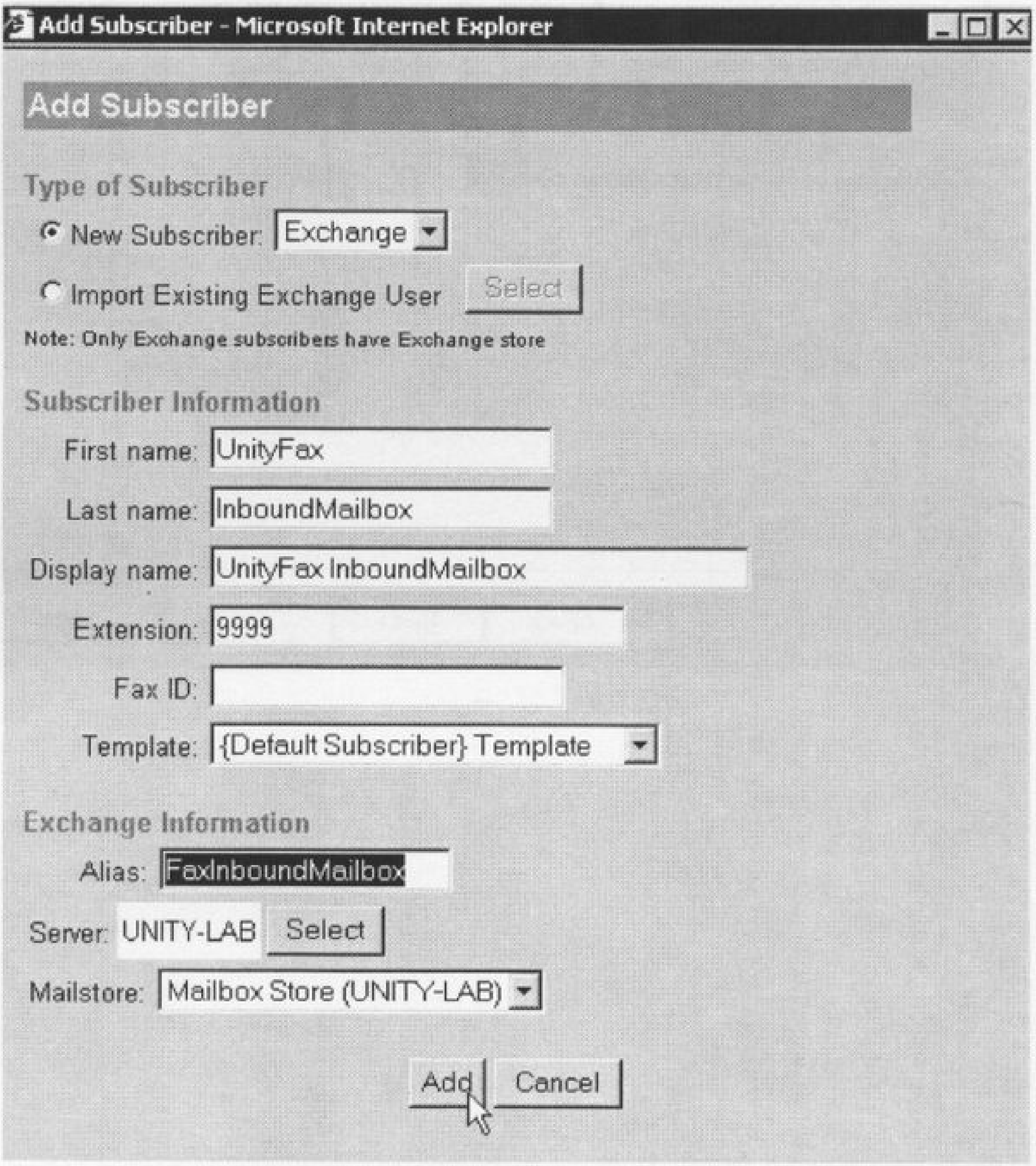


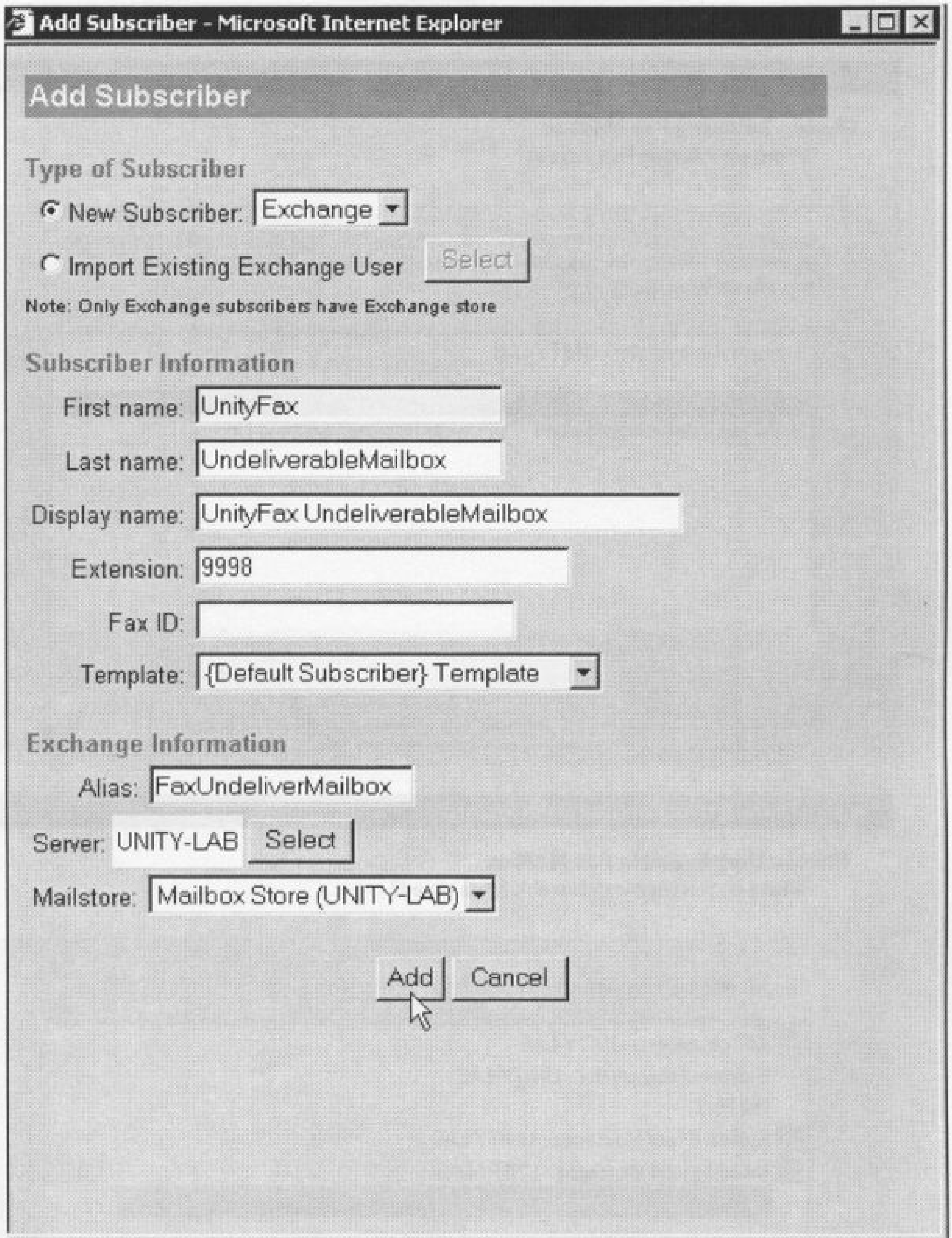
➔ **A 1 minute polling interval is recommended for the lab so we don't have to wait to see if our config works or not when testing.**



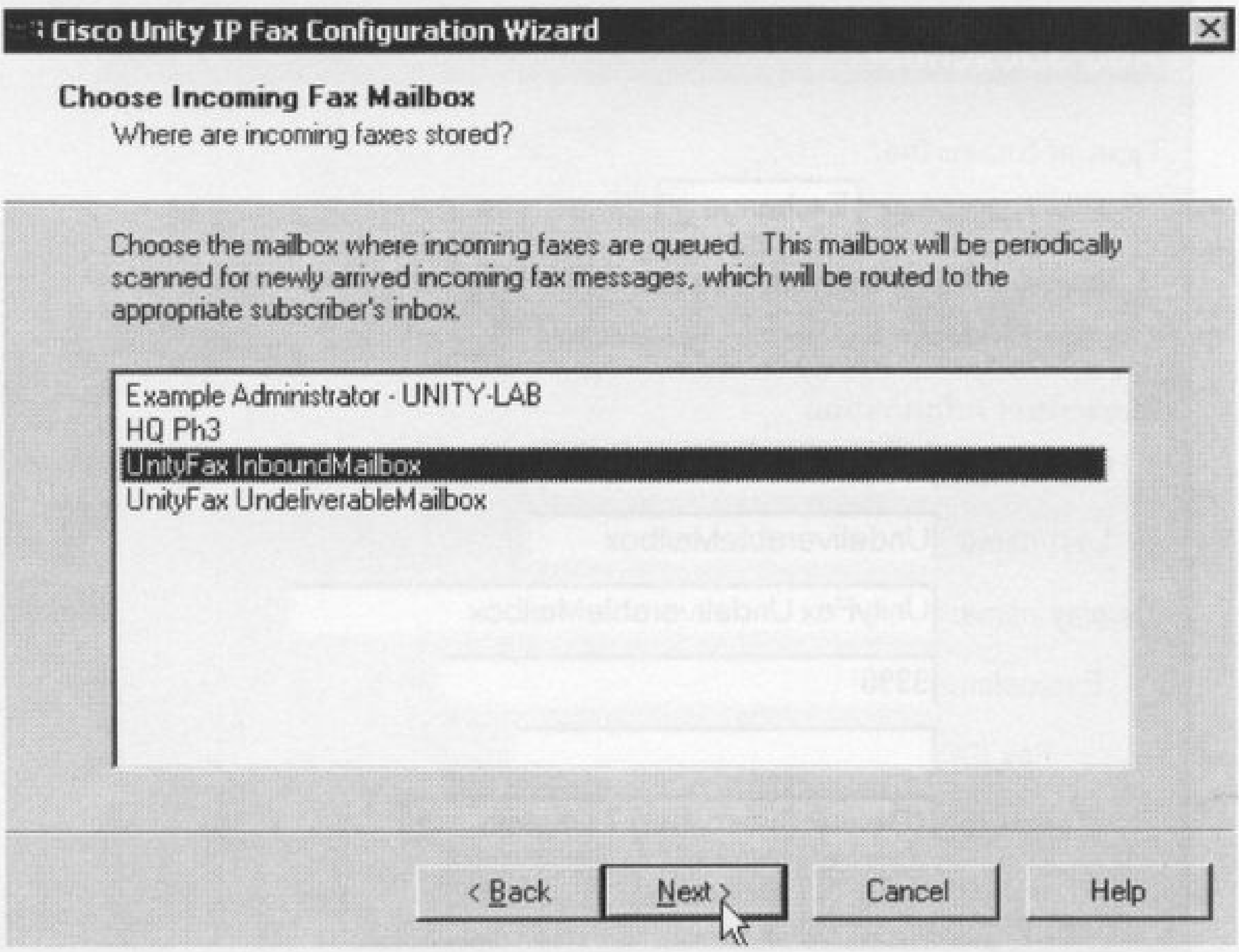
➔ **Now we need to create 2 Exchange mailboxes to store 'Incoming' and 'Undeliverable' Faxes – and we can do this quickly from the Unity SAWeb interface.**

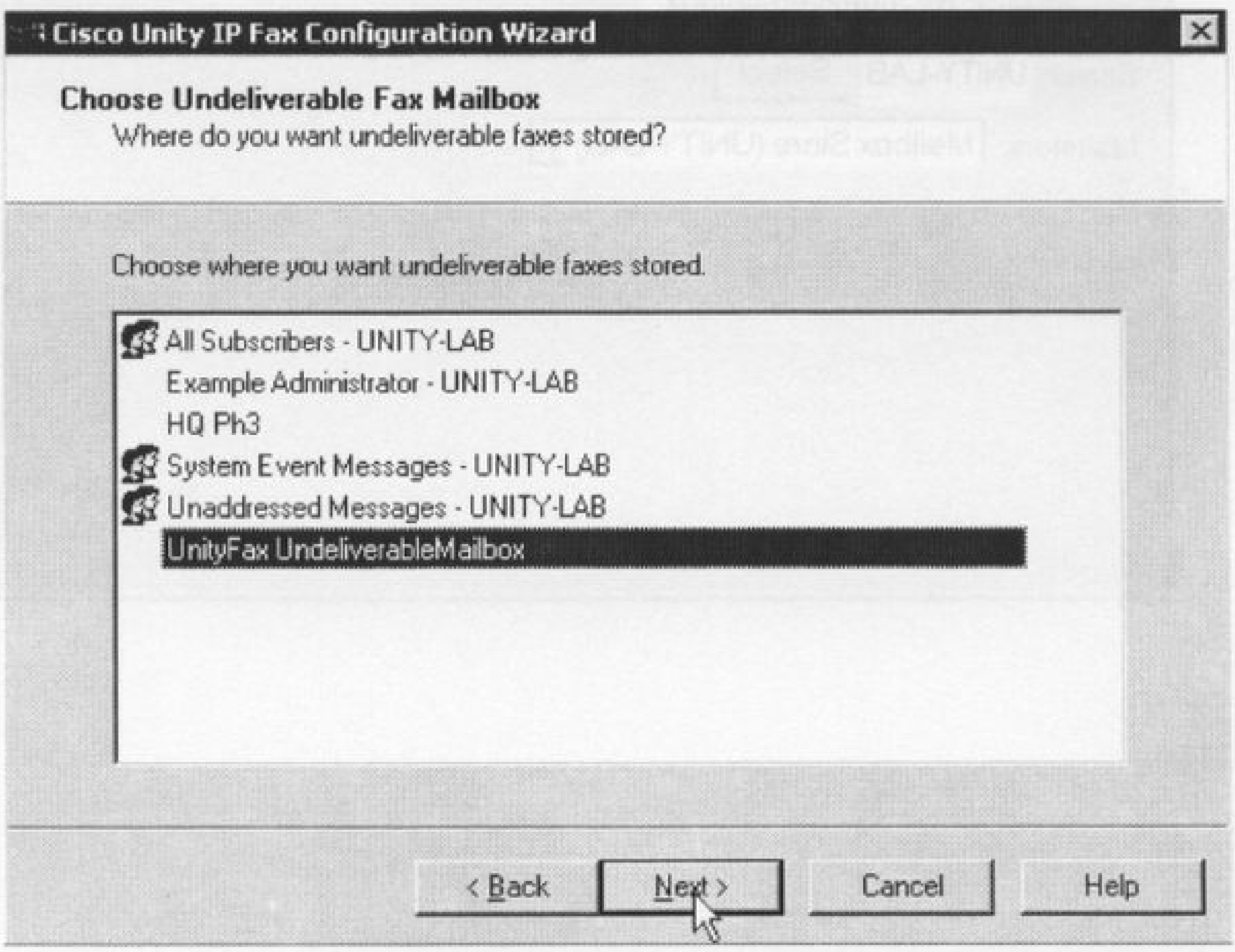
➔ ***Remember that our Inbound Fax Alias needs to be the same exact name as when we did configured Task 4.8 on the router as to which email address the router OnRamp GW would attempt to deliver to.**




Add Subscriber - Microsoft Internet Explorer
Add Subscriber
Type of Subscriber
New Subscriber: Exchange
Import Existing Exchange User Select
Note: Only Exchange subscribers have Exchange store
Subscriber Information
First name: UnityFax
Last name: UndeliverableMailbox
Display name: UnityFax UndeliverableMailbox
Extension: 9998
Fax ID:
Template: {Default Subscriber} Template
Exchange Information
Alias: FaxUndeliverMailbox
Server: UNITY-LAB Select
Mailstore: Mailbox Store (UNITY-LAB)
Add Cancel

➔ **Next we need to specify in back the wizard – those boxes.**

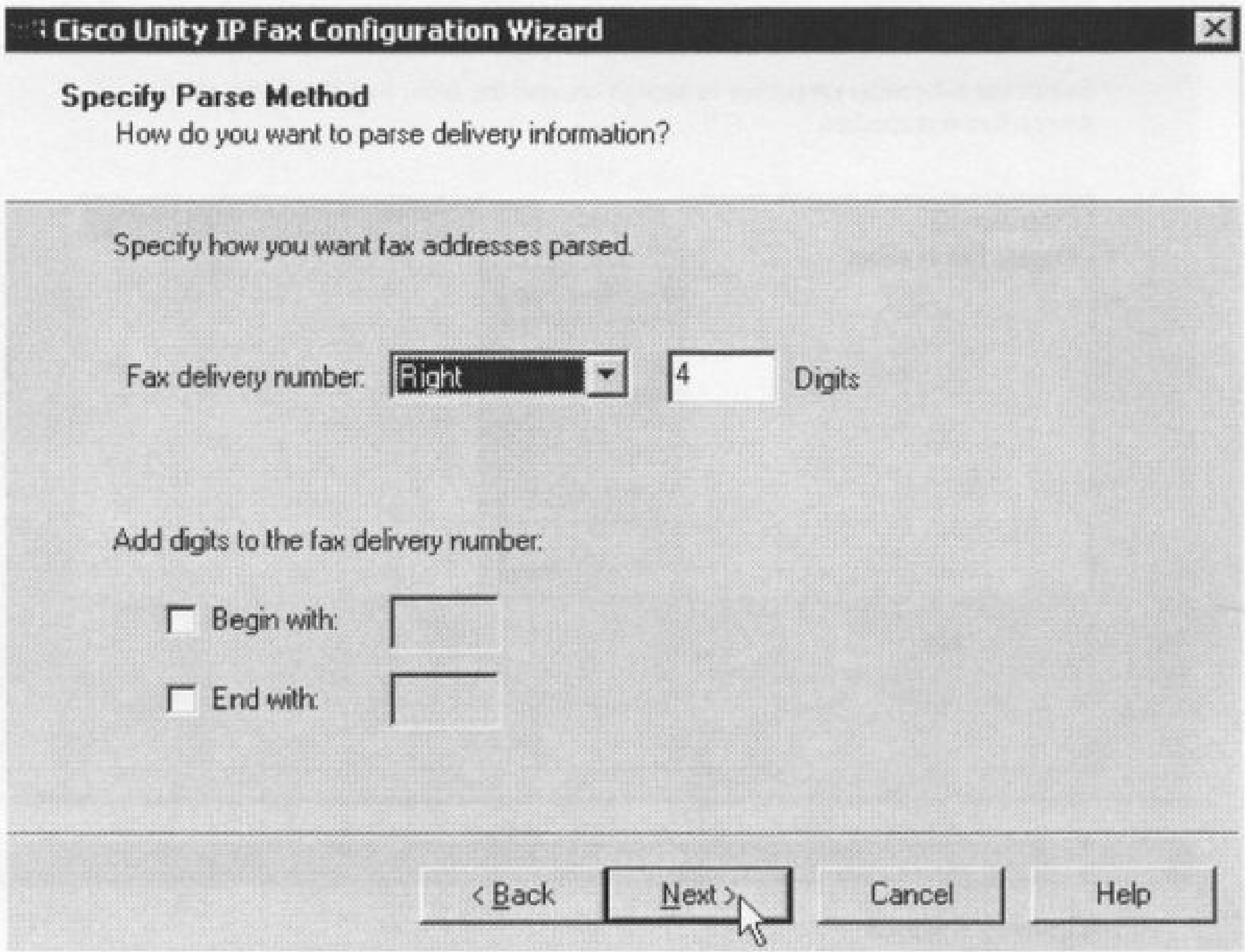




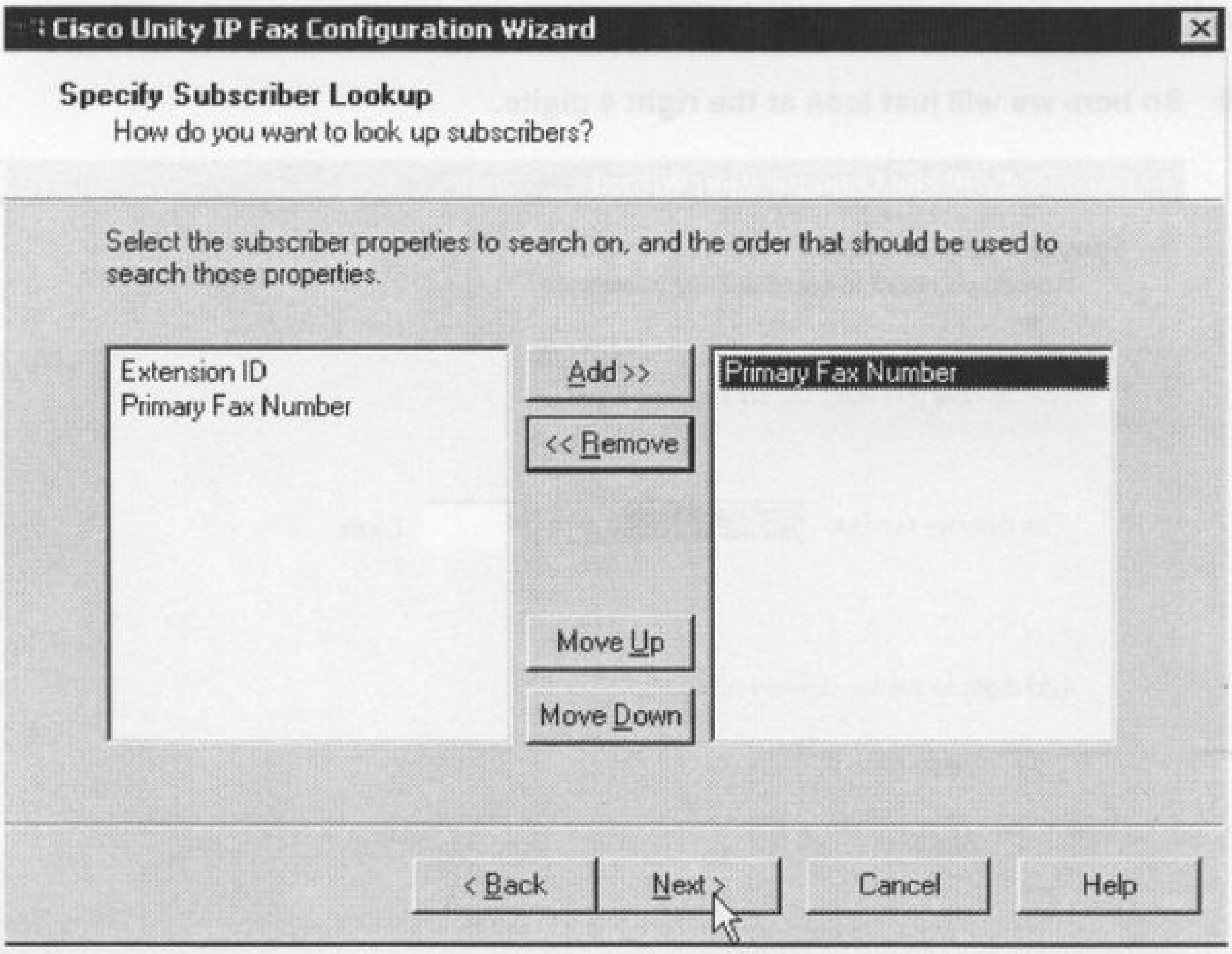
➔ **Now we need to decide – of the 10 digit E164 DNIS – how many digits we want to view and use as criteria for sending to the users' VM box?**

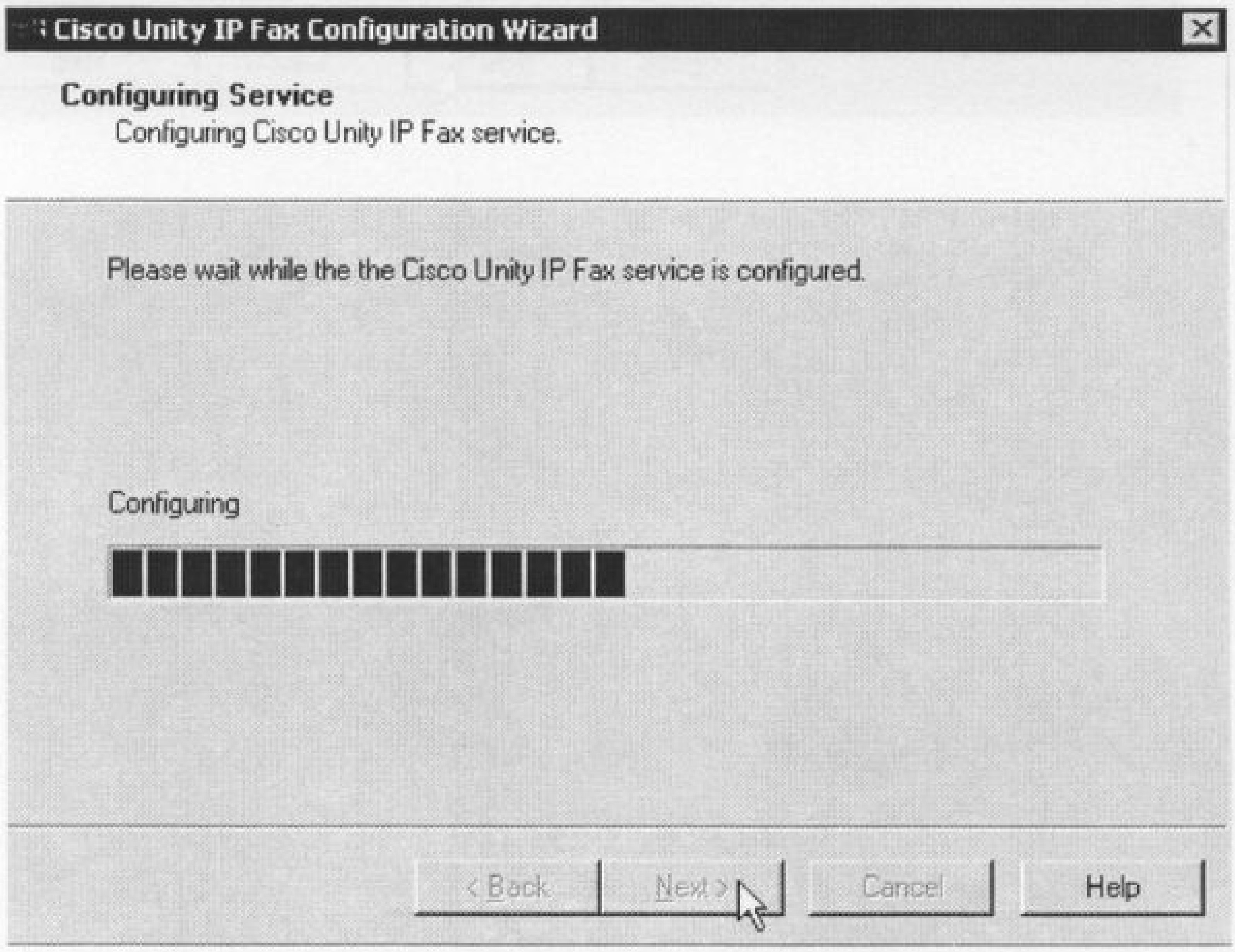
➔ **Later we will go into the SAWeb interface to add a FaxID to Ph's 2 and 3.**

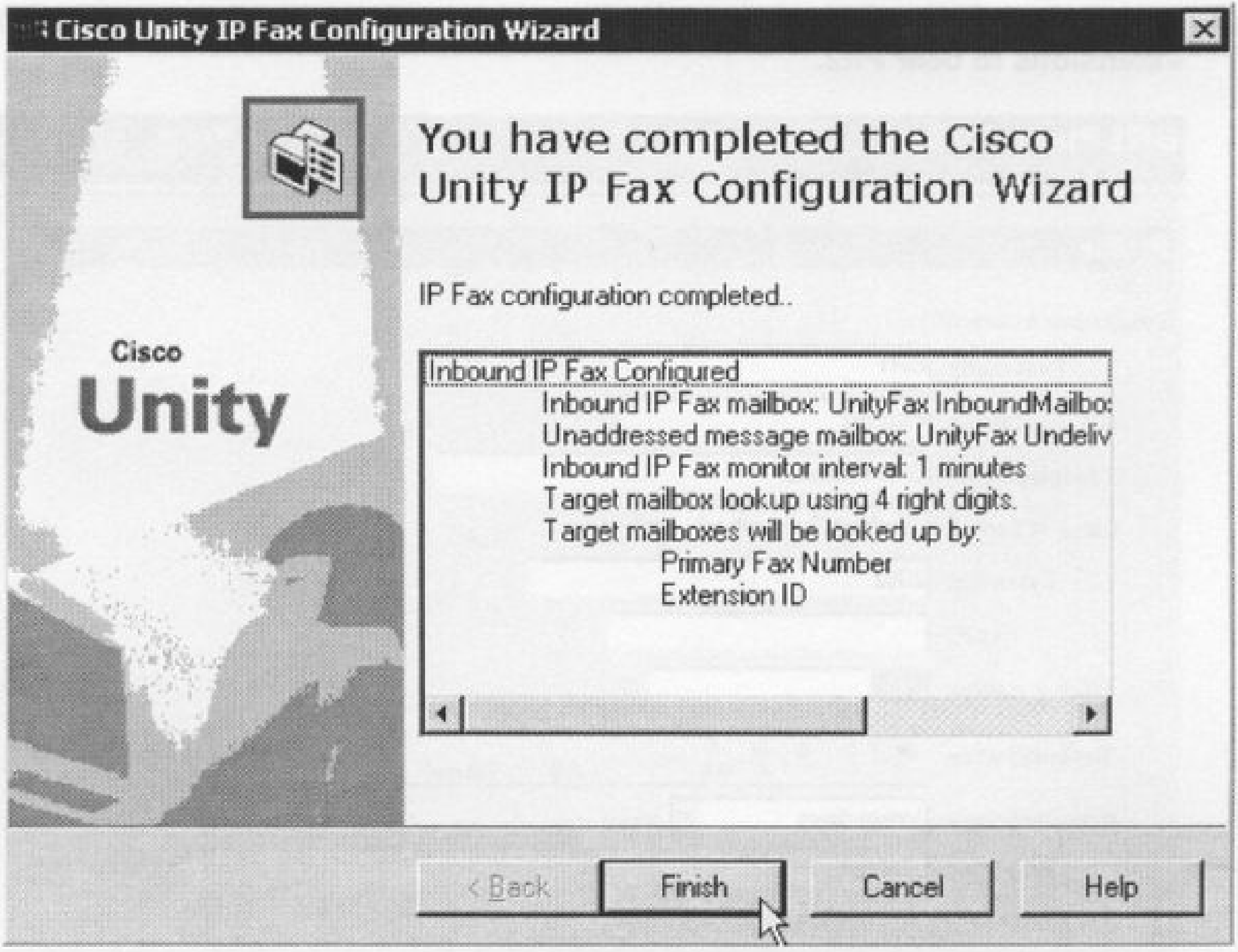
➔ **So here we will just look at the right 4 digits.**



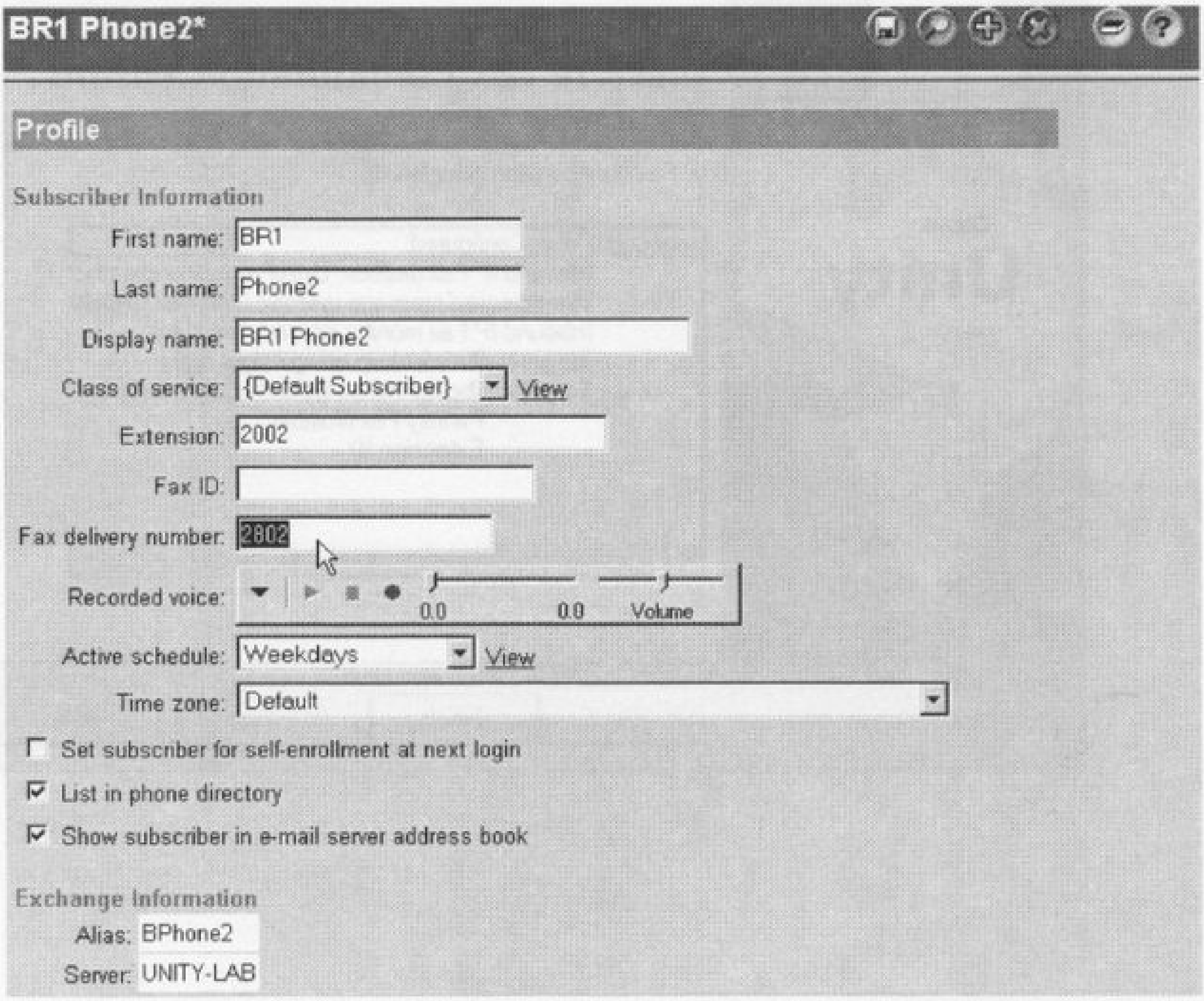
➔ **Now we will tell the wizard that we are going to look first at the Primary Fax Number in the Users table in the DB to determine where to deliver the fax.**



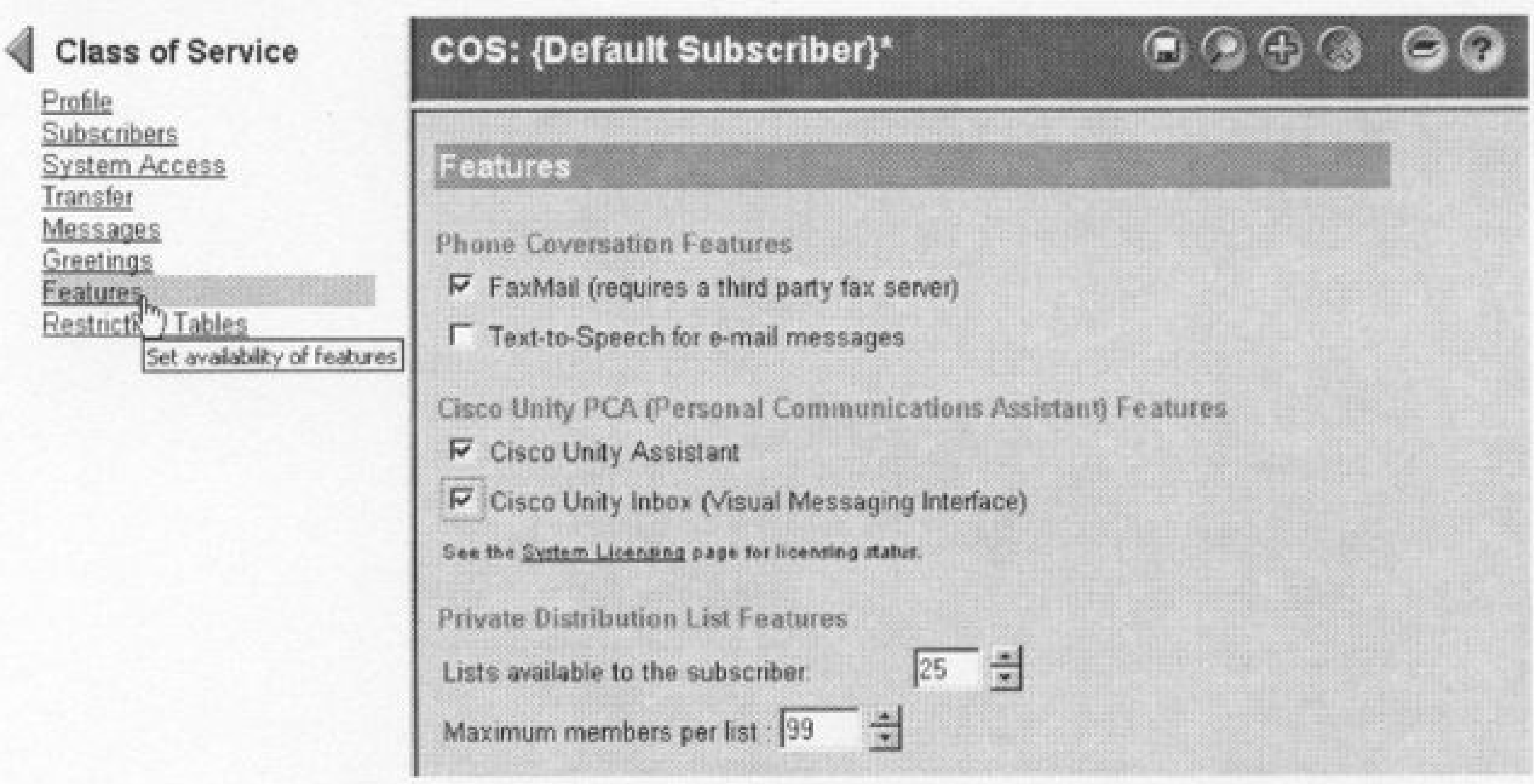



Cisco Unity IP Fax Configuration Wizard
You have completed the Cisco Unity IP Fax Configuration Wizard
Cisco
Unity
IP Fax configuration completed..
Inbound IP Fax Configured
Inbound IP Fax mailbox: UnityFax InboundMailbo
Unaddressed message mailbox: UnityFax Undeliv
Inbound IP Fax monitor interval: 1 minutes
Target mailbox lookup using 4 right digits.
Target mailboxes will be looked up by:
Primary Fax Number
Extension ID
< Back
Finish
Cancel
Help

➔ **Now back on the Unity SAWeb interface – we need to assign the 2802 Fax extensions to user Ph2.**



➔ **We also need to go to Class of Service ➔ Features for the CoS that is assigned to the Subscriber receiving the Faxes and ensure that "FaxMail" and "Cisco Unity Inbox" are checked.**



➔ **Now let's place a fax inbound (see the web interface of ProctorLabs.com for the "Send fax to BR1 GW" button) and watch some debugs on the BR1 router to see our fax come in through our Pots DP 10 and go out through our MMOIP DP 20.**

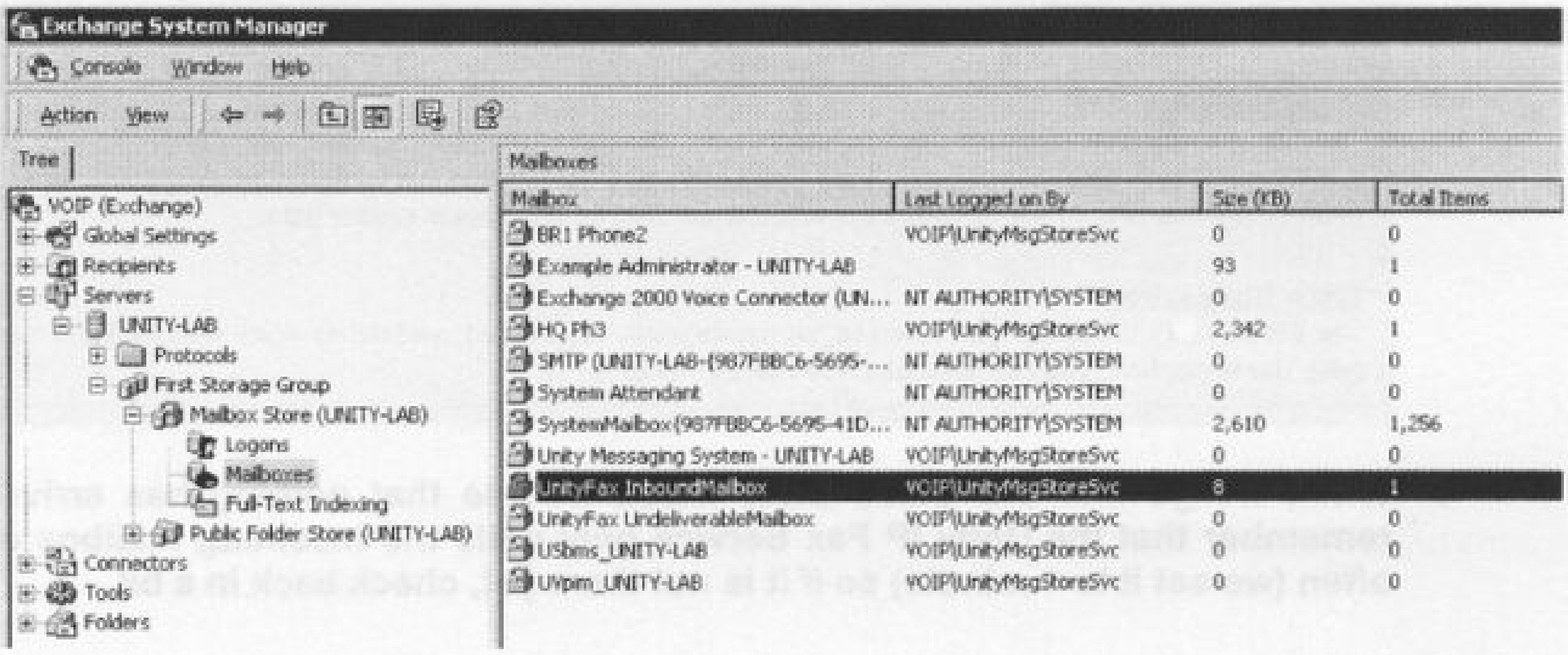
➔ ***NOTE: Remember from earlier that when testing Faxing – you will need to create an ACL to block MGCP traffic from get to the CCM or stop the CCM service all together (it might also be a good time to test SRST) – this way the PRI will be handed back over to the Default Application away from MGCP so that the Fax application can intercept the specific call.**

```
P1-BR1-RTR# debug isdn q931
P1-BR1-RTR# debug fax mspi all
P1-BR1-RTR#
*Apr 29 00:04:22.562: ISDN Se2/0/0:23 Q931: RX <- SETUP pd = 8  callref = 0x0015
        Bearer Capability i = 0x8090A2
                Standard = CCITT
                Transfer Capability = Speech
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0xA98381
                Exclusive, Channel 1
        Calling Party Number i = 0x2181, '3935551212'
                Plan:ISDN, Type:National
        Called Party Number i = 0xA1, '6175212802'
                Plan:ISDN, Type:National
*Apr 29 00:04:22.578: ISDN Se2/0/0:23 Q931: TX -> CALL_PROC pd = 8  callref = 0x8015
        Channel ID i = 0xA98381
                Exclusive, Channel 1
*Apr 29 00:04:22.578: ISDN Se2/0/0:23 Q931: TX -> CONNECT pd = 8  callref = 0x8015
*Apr 29 00:04:22.586: ISDN Se2/0/0:23 Q931: RX <- CONNECT_ACK pd = 8  callref = 0x0015
P1-BR1-RTR#
*Apr 29 00:04:22.586: %ISDN-6-CONNECT: Interface Serial2/0/0:0 is now connected to
3935551212 N/A
P1-BR1-RTR#
P1-BR1-RTR#
*Apr 29 00:04:36.706: //52/8C00A96B8011/MSPI_ON/mspi_call_setup_request:
    Outgoing Peer Tag=20
    Envelope From=FAX=3935551212@P1-BR1-RTR.voip.lab
    Envelope To=FaxInboundMailbox@voip.lab
    Mime Outer Type=2
 *Apr 29 00:04:37.706: //52/8C00A96B8011/MSPI_ON/mspi_check_connect:
    MMccb(Count=0)
 *Apr 29 00:04:37.706: //52/8C00A96B8011/MSPI_ON/mspi_check_connect:
    SMTP Connected To The Server !
 *Apr 29 00:04:37.706: //52/8C00A96B8011/MSPI/mspi_bridge:
    MMccb(State=CONNECTED, Type=Onramp), Destination Call Id=53
P1-BR1-RTR#
P1-BR1-RTR#
P1-BR1-RTR#
 *Apr 29 00:04:51.254: //52/8C00A96B8011/MSPI_ON/mspi_xmit:
    MMccb(State=CONFERENCED, Type=Onramp, Buffer Count=0),
    Source Call Id=53
 *Apr 29 00:04:51.254: //52/8C00A96B8011/MSPI_ON/mspi_xmit:
    MMccb(State=CONFERENCED, Type=Onramp, Buffer Count=1),
```



```
P1-BR1-RTR#
*Apr 29 00:04:57.226: //-1/xxxxxxxxxxxx/MSPI/mspi_free_ccb:
  Total Allocated MMccbs=1, Total Inserted MMccbs=0
P1-BR1-RTR#
```

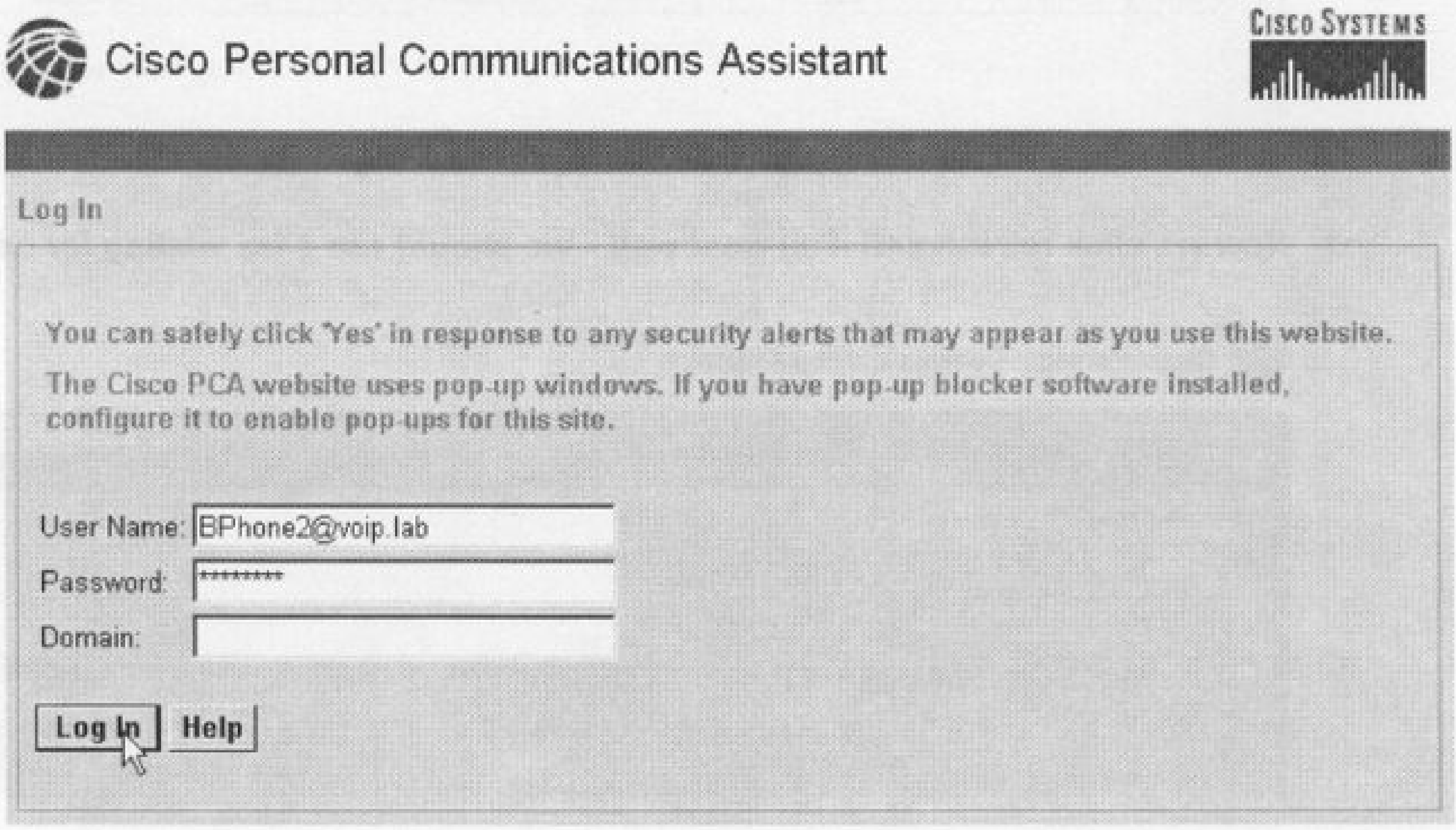
➔ **Over on the Unity server in the Exchange System Manager – we can see that the mail has hit the appropriate mailbox and is awaiting processing.**

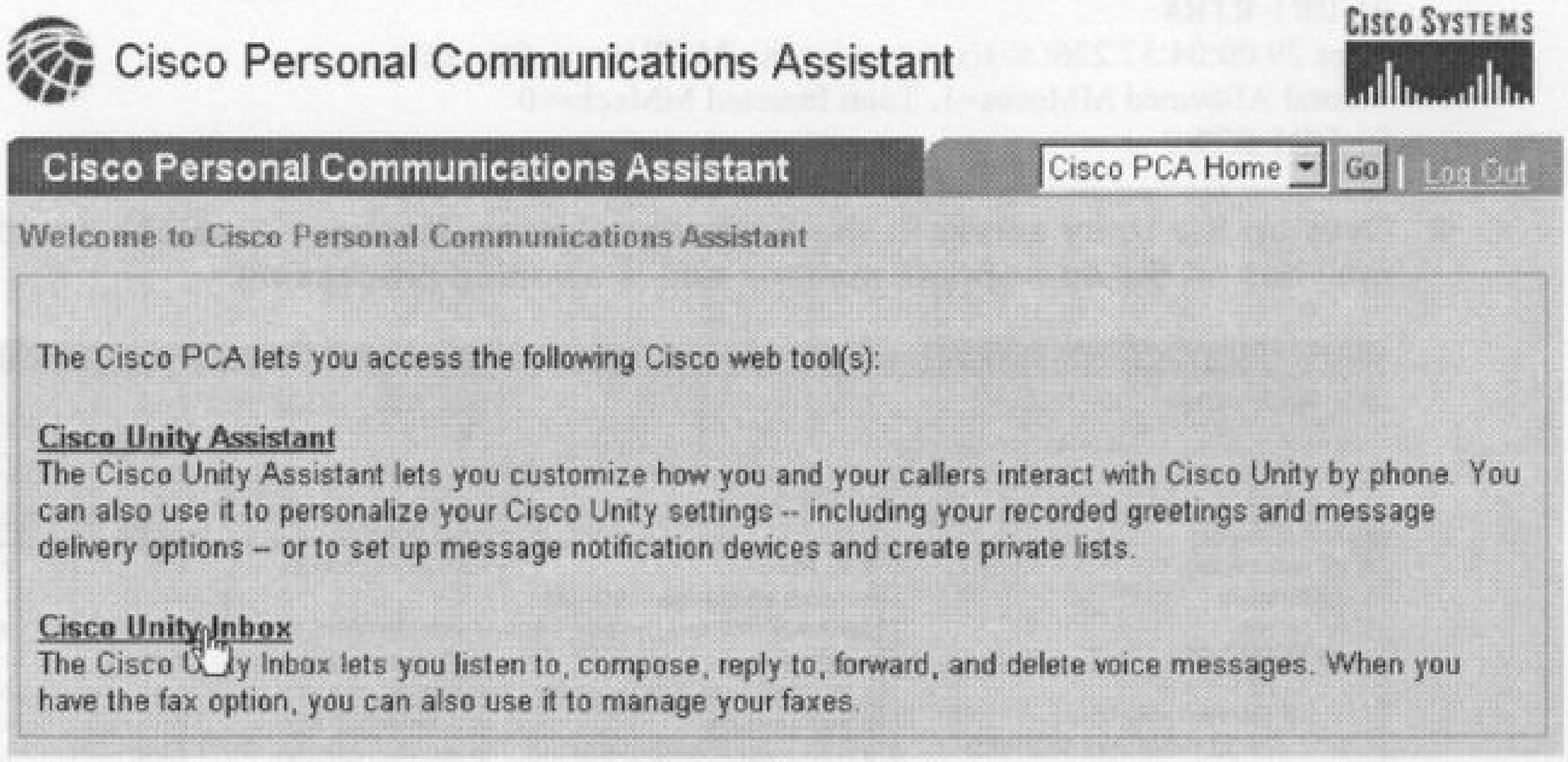


➔ **Now it is about time to login to the Cisco Unity Inbox for the BR1 Phone 3 Subscriber and of course we do that through IE at the address:**

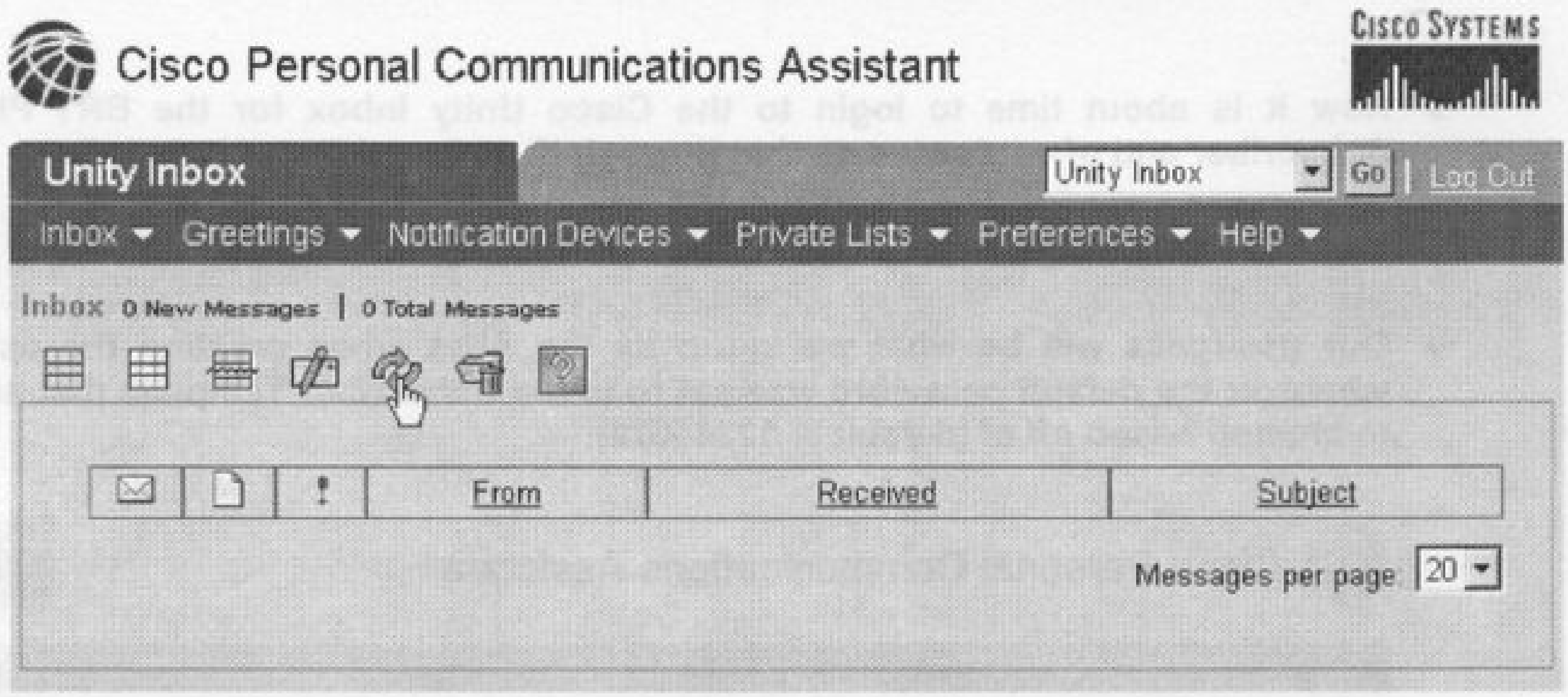
http://10.X.200.22/ciscopca

➔ **Our user/pass will be what we setup as the Alias when creating the user and whatever the default password was set to in the Subscriber Template that we used to created based off of (default is 12345678).**

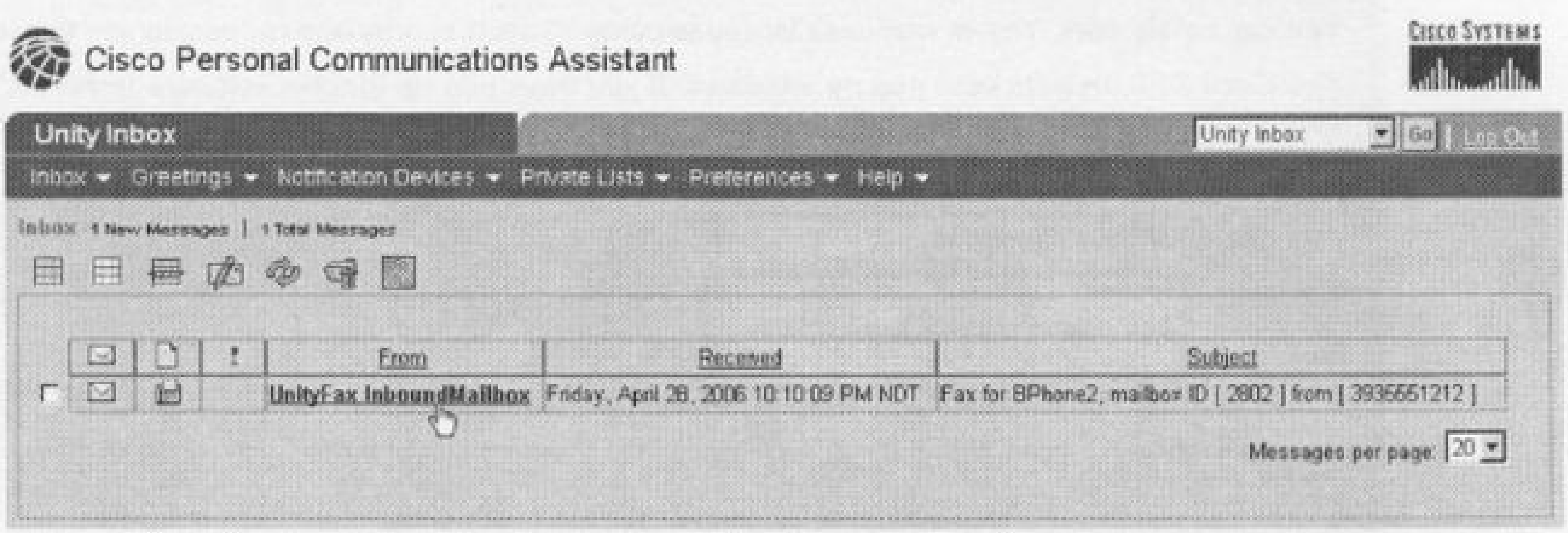


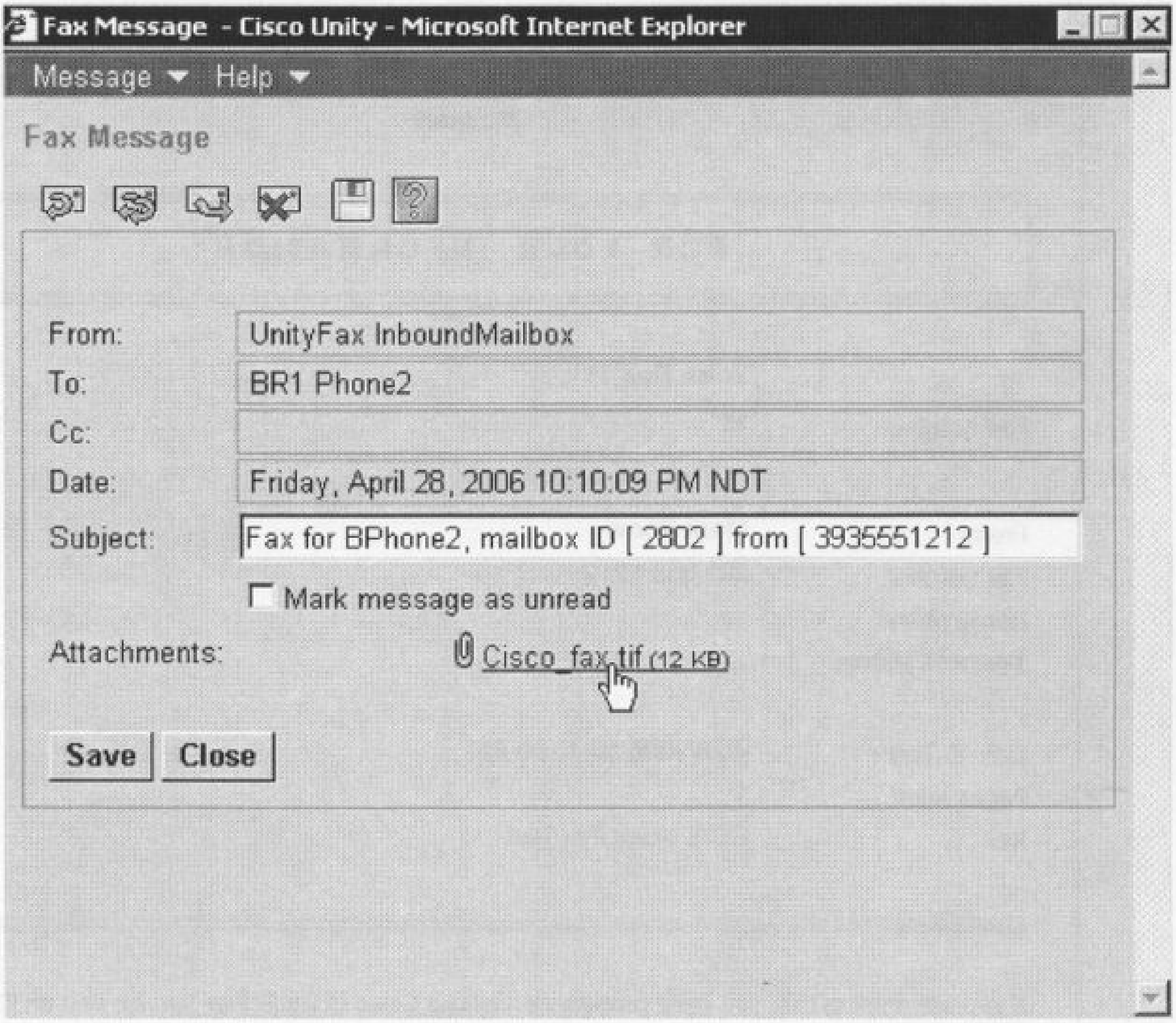


➔ **When we go into our Cisco Unity Inbox we see that nothing has arrived yet – remember that the Unity IP Fax Service only polls the Incoming mailbox every so often (we set it to 1 minute) so if it is not there yet, check back in a bit.**



➔ **Now we click refresh and if all went well – we should see a fax waiting for us!**




Fax Message - Cisco Unity - Microsoft Internet Explorer
Message
Help
Fax Message
From:
UnityFax InboundMailbox
To:
BR1 Phone2
Cc:
Date:
Friday, April 28, 2006 10:10:09 PM NDT
Subject:
Fax for BPhone2, mailbox ID [2802] from [3935551212]
Mark message as unread
Attachments:
Cisco_fax.tif (12 KB)
Save
Close

➔ **And here is our Fax!**

IPexpert

FOR YOUR INFORMATION

To:	**Voice Pod 11**
Fax number:	11
From:	**Mark Snow**
Fax number:	393.555.1212
Home phone:	
Business phone:	
Date & Time:	4/28/2006 10:40:00 PM
Pages sent:	1
Re:	CCIE Voice Fax Test

If you are reading this, you have properly configured Cisco Unity IP Fax Service and an IOS OnRamp GW!

➔ ***NOTE: While this is the correct solution – sometimes your mileage may vary – and your fax may fail – after all we are doing Fax Passthrough not Relay (ATA limitation per pod in the PSTN) – so the CED tones must travel inbound inside the codec. If you happen to meet with such uncertainty, try waiting until the debug shows that the line is clear and try sending your fax again once or twice.**

➔ **If your fax fails more than 3 times – you most likely have a configuration error.**

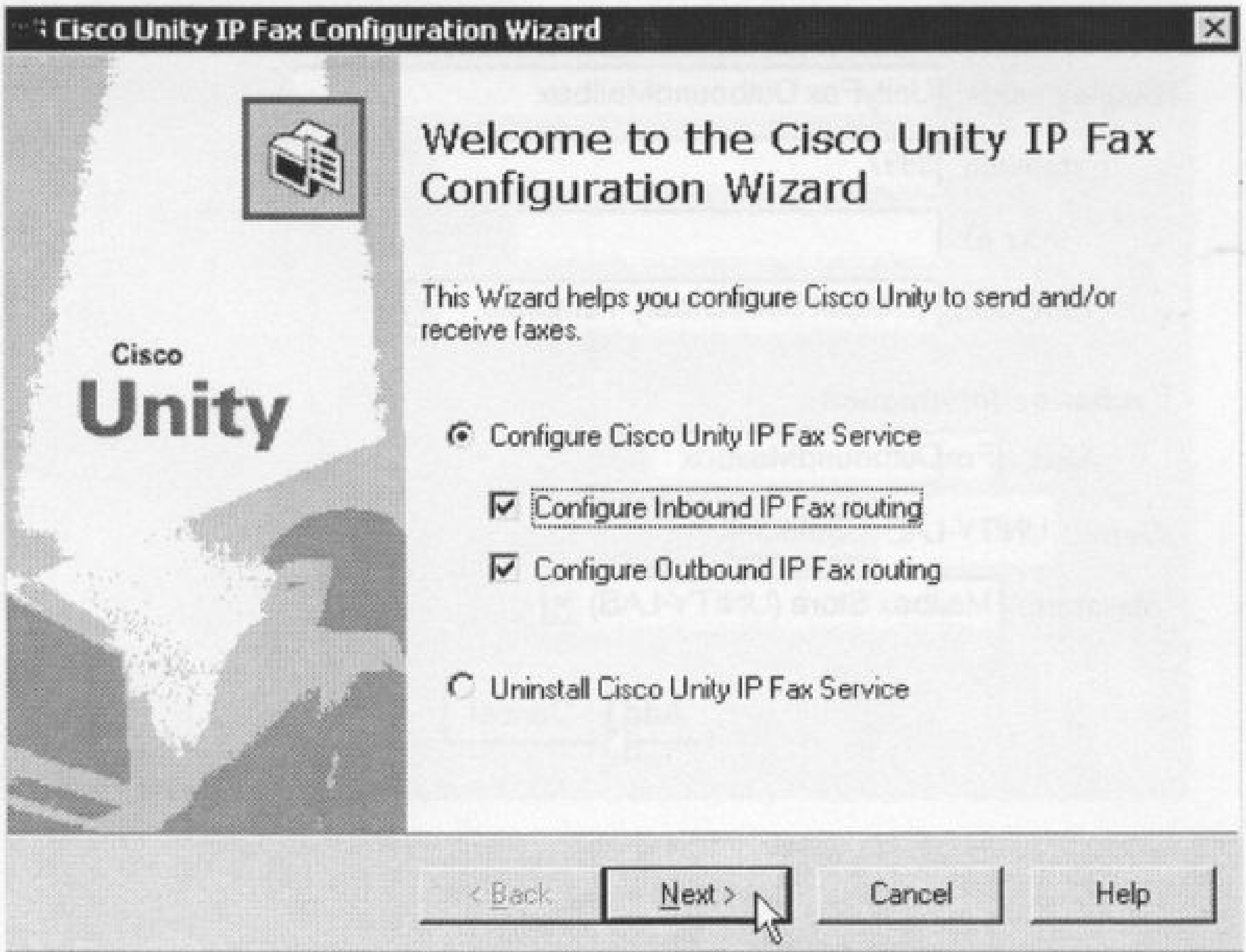
Task 9.10

Continuing from question 4.10; Configure Unity to be an Outbound (and Inbound) Fax Server. Ensure that Faxes going out to the PSTN number in Table 6 from the BR1 Gateway arrive and are viewable.

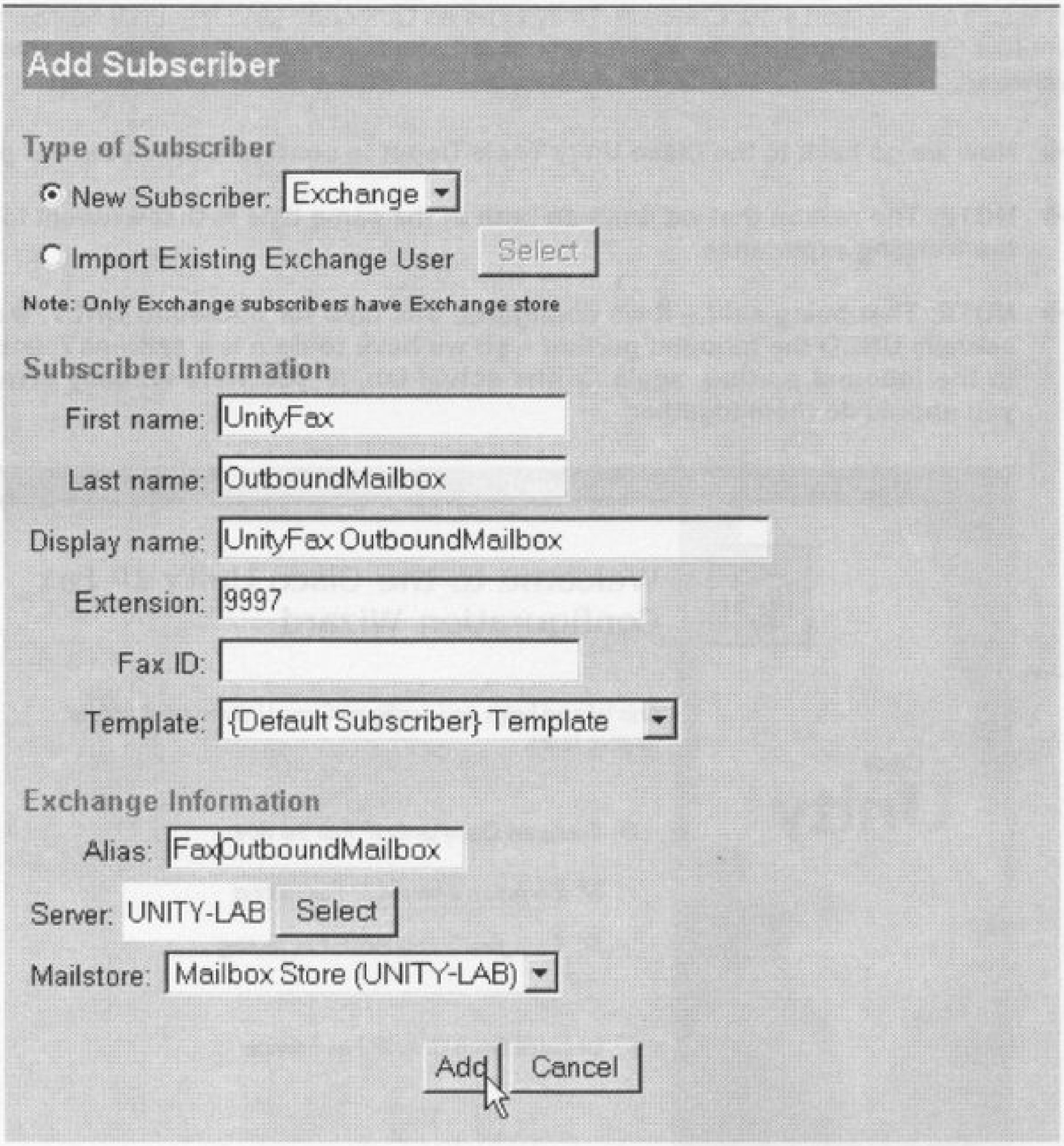
➔ **Now we go back to the Cisco Unity Tools Depot to configure the outbound portion.**

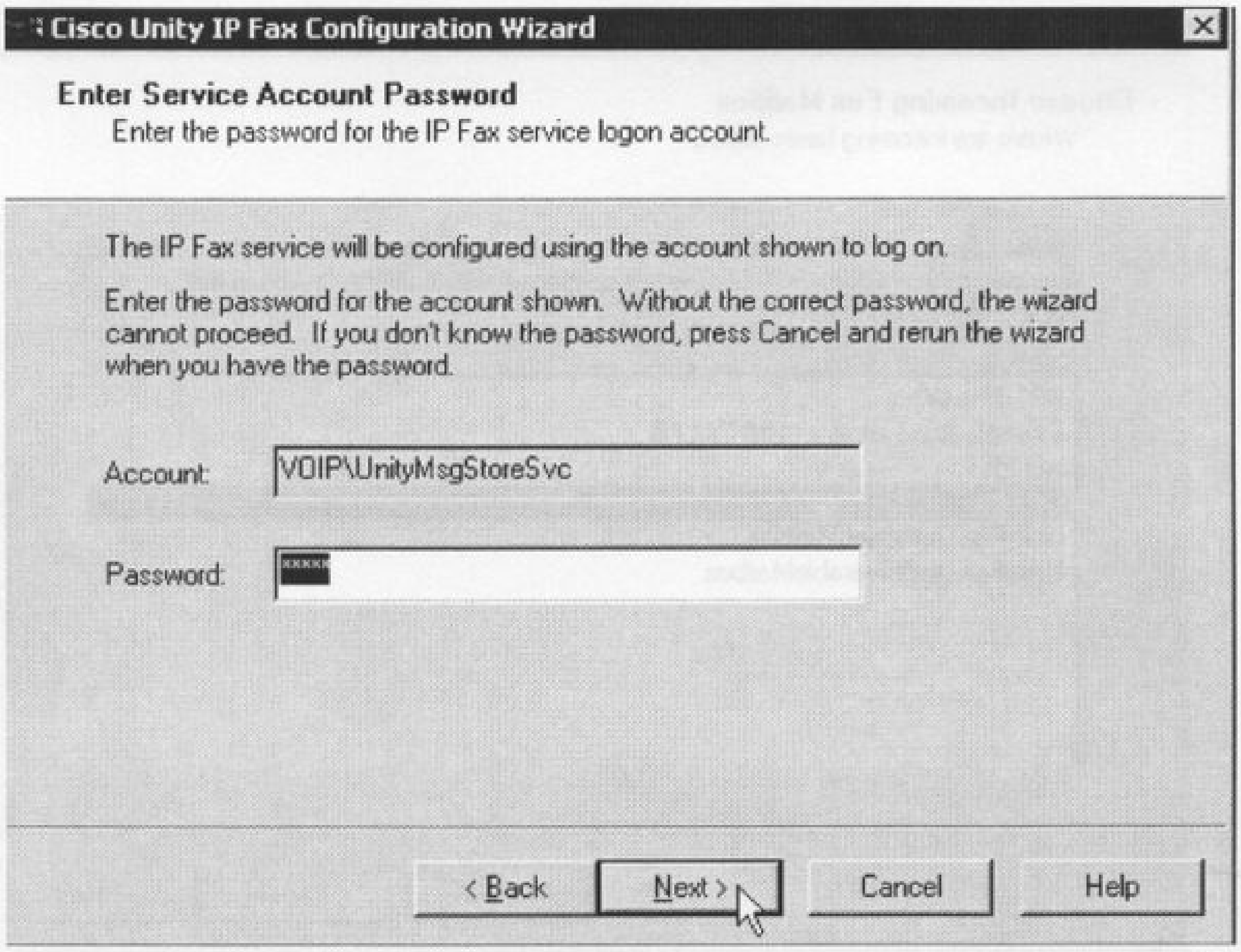
➔ **NOTE: The reason that we don't do both at the same time is that we want to isolate the learning experience.**

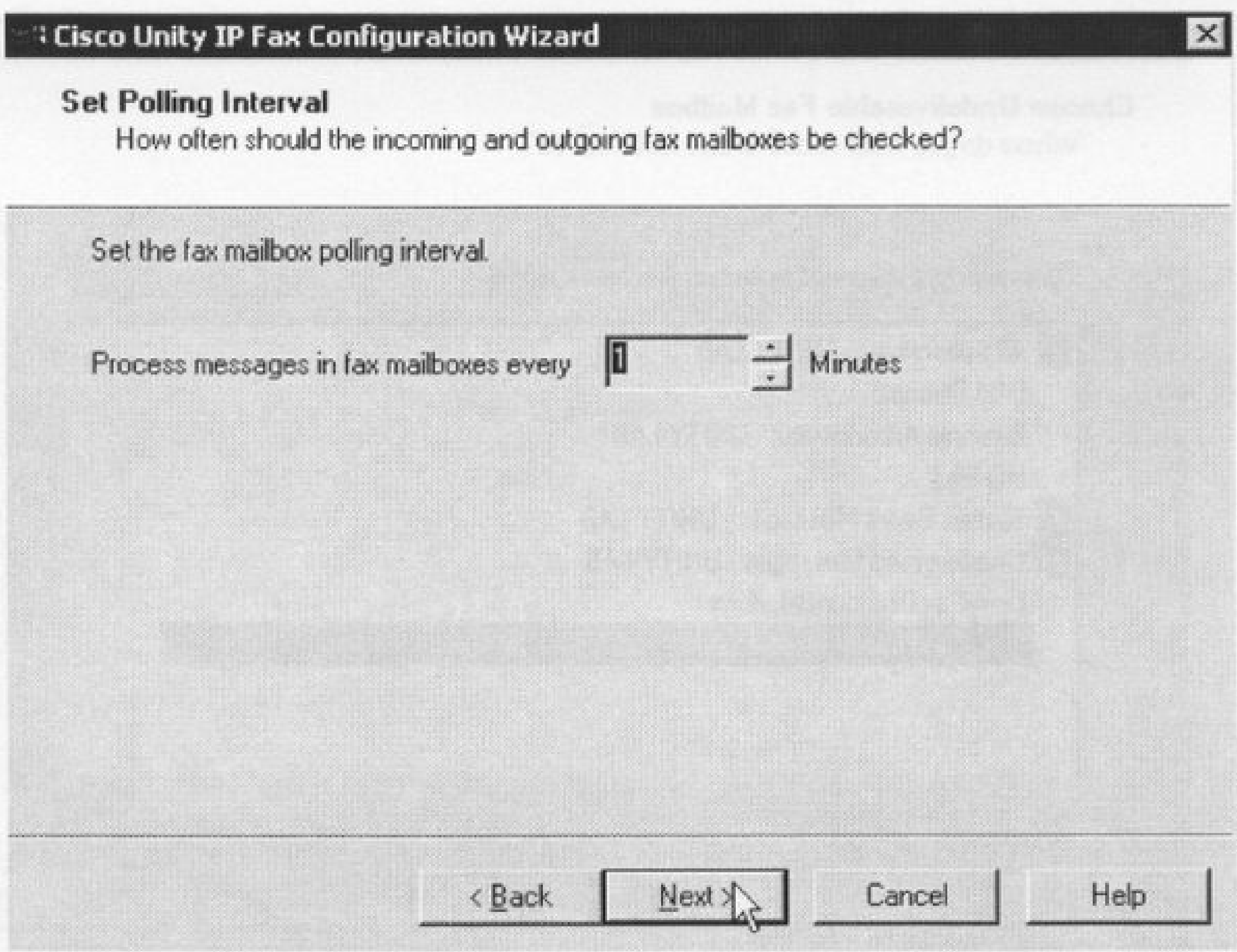
➔ **NOTE: That being said – if we configured this time for outbound ONLY, we would actually UNDO the Inbound portion – so we have to do a few screens relating only to the inbound portion, again. In the actual lab, IF you were actually given both, you should do them together.**

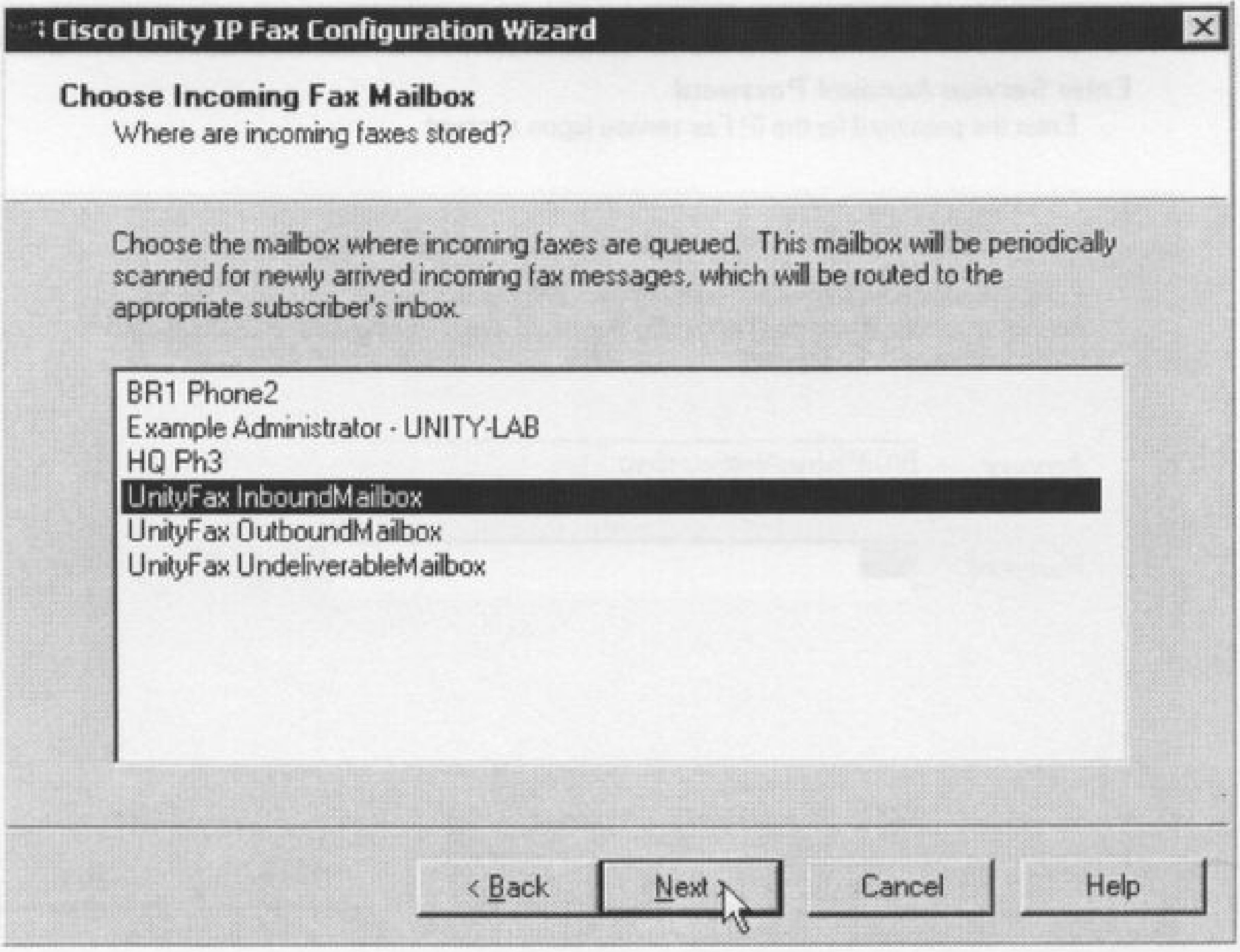


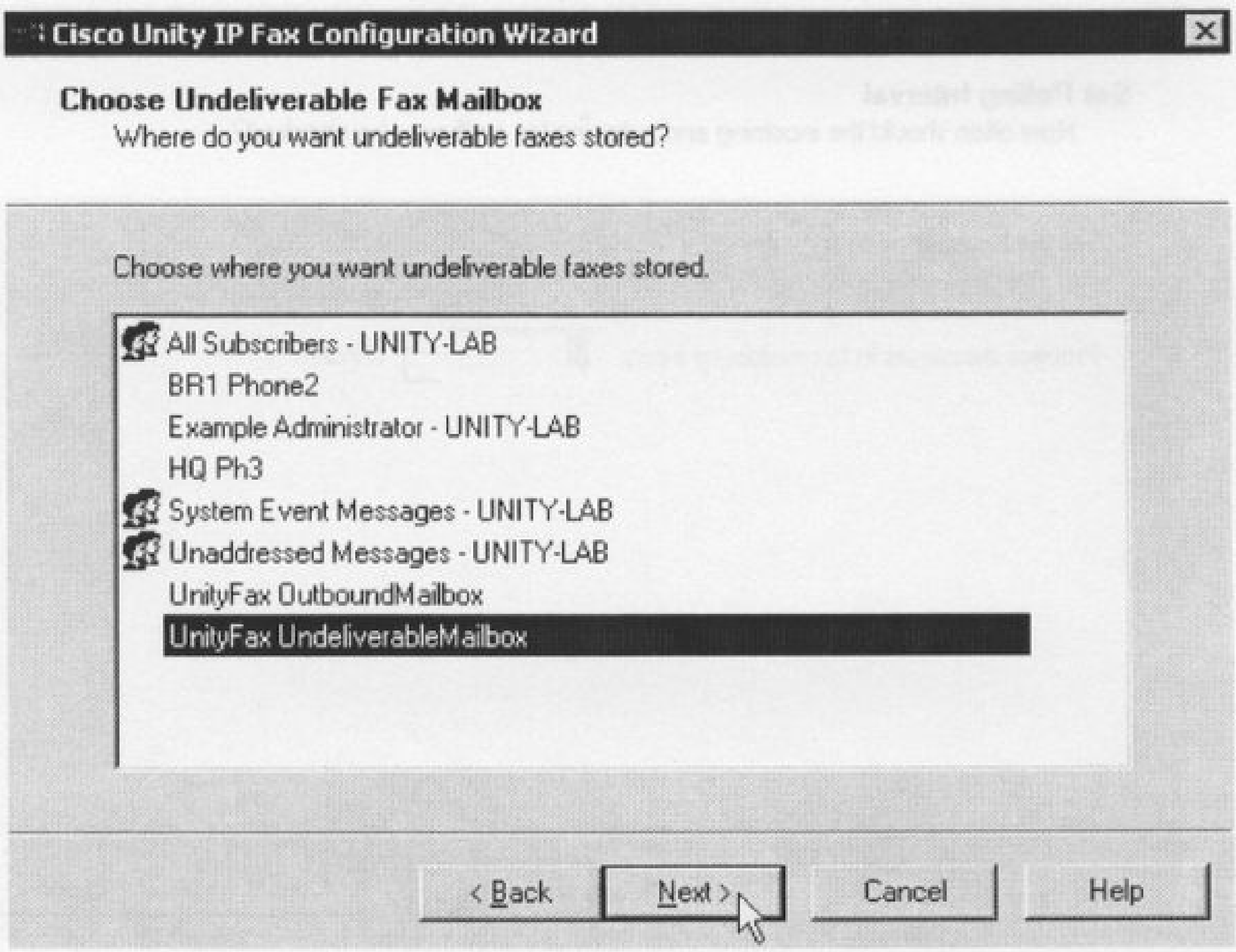
➔ **We will need to create 1 more mailbox to serve outgoing faxes.**

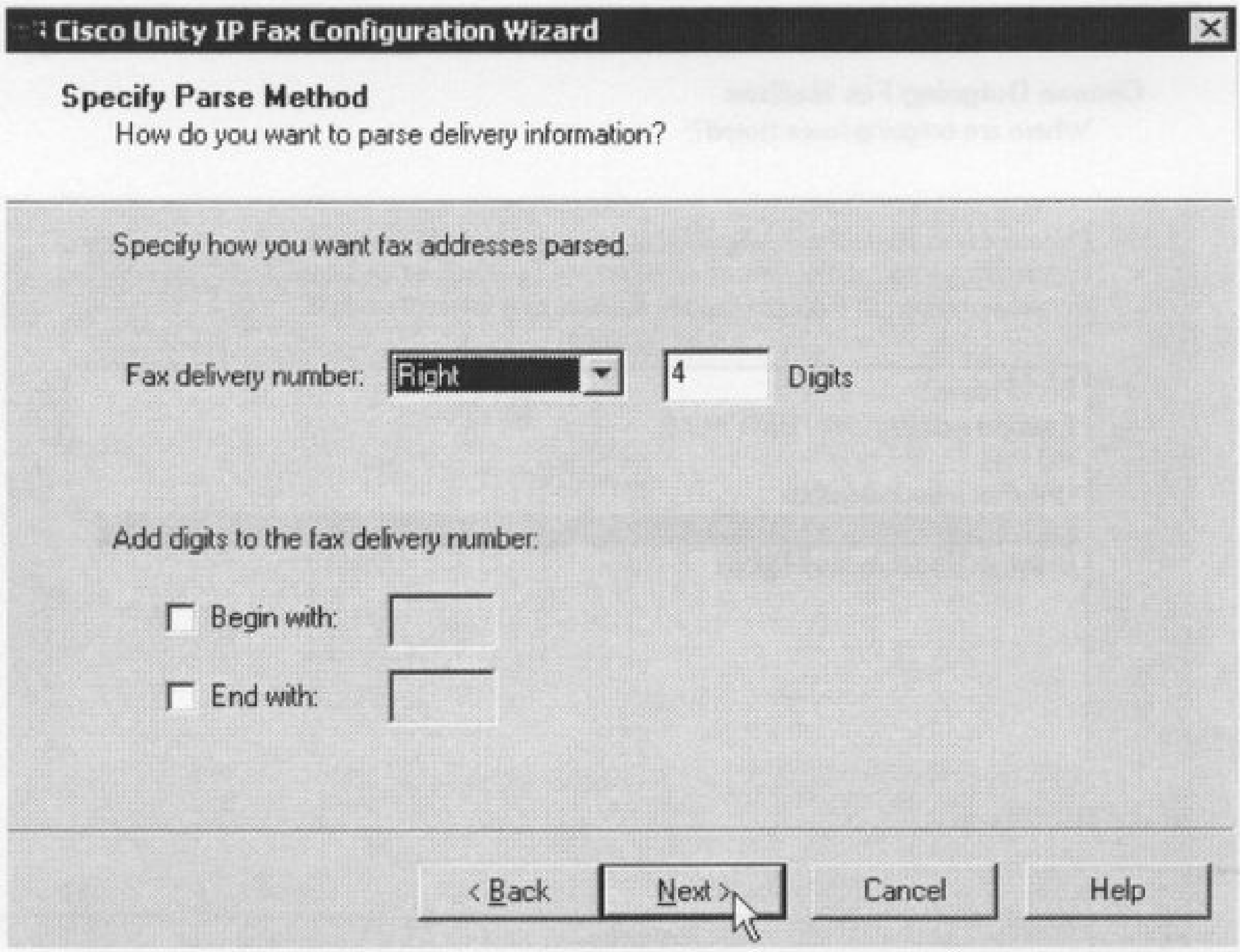


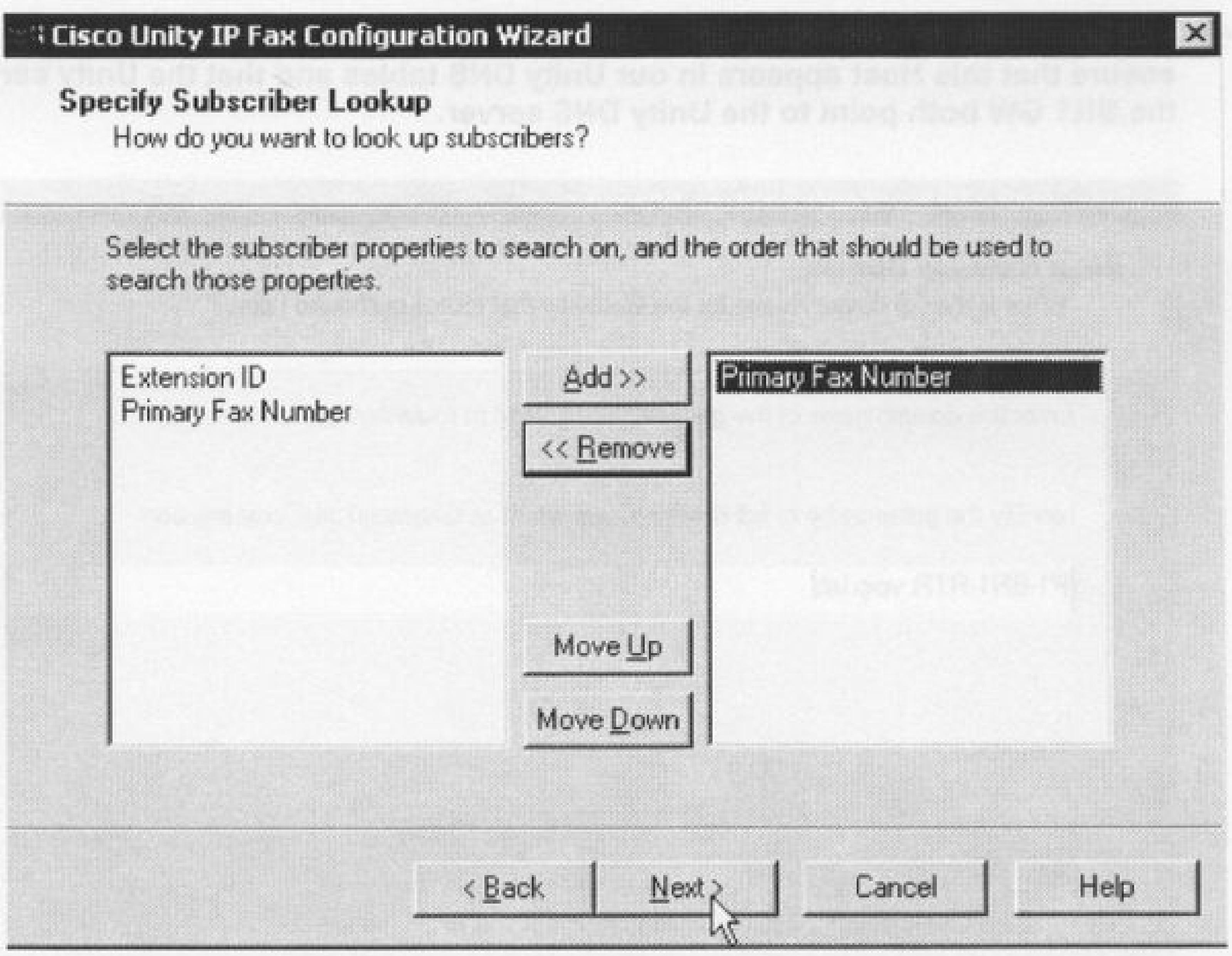

Cisco Unity IP Fax Configuration Wizard
Enter Service Account Password
Enter the password for the IP Fax service logon account.
The IP Fax service will be configured using the account shown to log on.
Enter the password for the account shown. Without the correct password, the wizard cannot proceed. If you don't know the password, press Cancel and rerun the wizard when you have the password.
Account: VOIP\UnityMsgStoreSvc
Password:
< Back
Next >
Cancel
Help

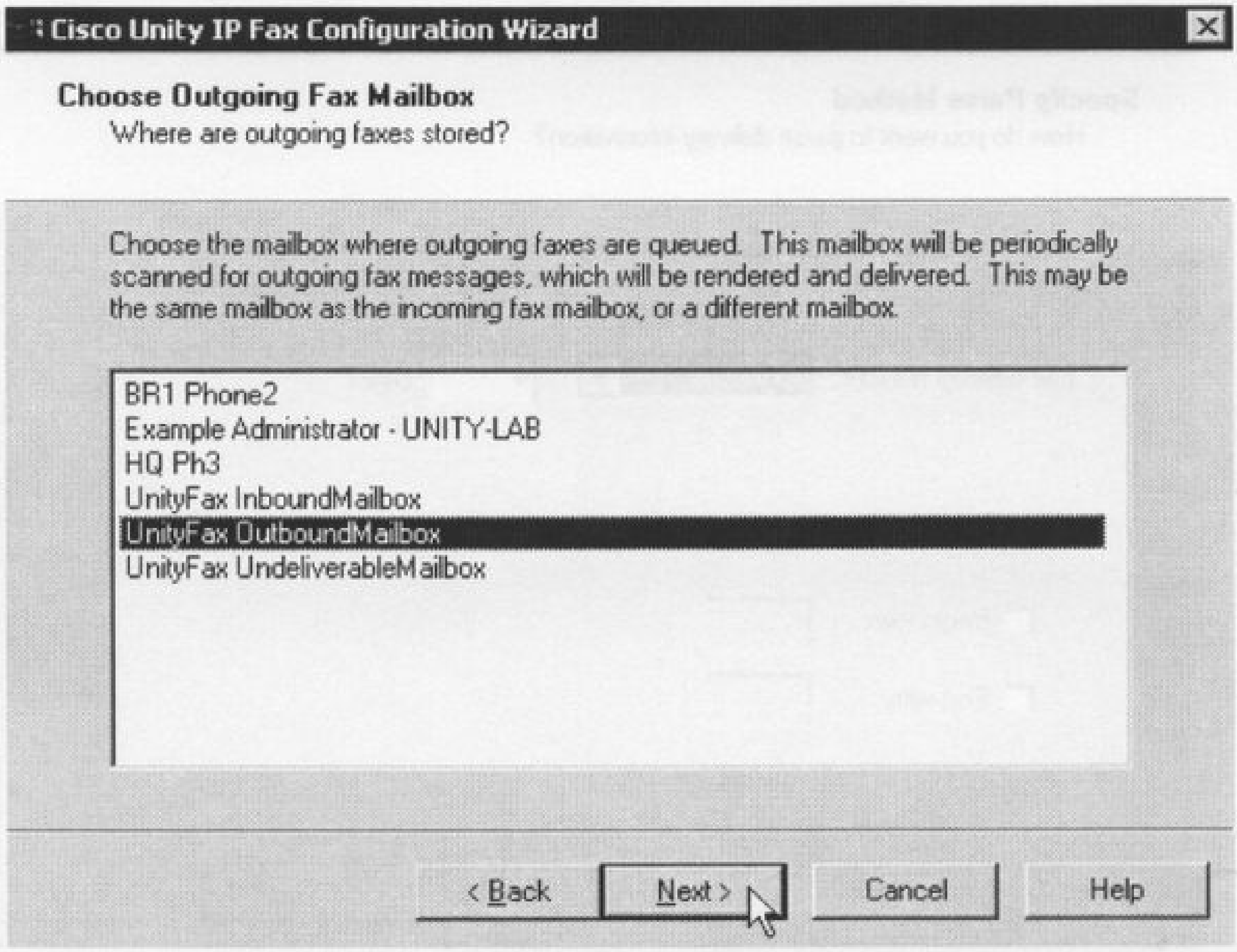

Cisco Unity IP Fax Configuration Wizard
Set Polling Interval
How often should the incoming and outgoing fax mailboxes be checked?
Set the fax mailbox polling interval.
Process messages in fax mailboxes every 1 Minutes
< Back
Next >
Cancel
Help


Cisco Unity IP Fax Configuration Wizard
Choose Incoming Fax Mailbox
Where are incoming faxes stored?
Choose the mailbox where incoming faxes are queued. This mailbox will be periodically scanned for newly arrived incoming fax messages, which will be routed to the appropriate subscriber's inbox.
BR1 Phone2
Example Administrator - UNITY-LAB
HQ Ph3
UnityFax InboundMailbox
UnityFax OutboundMailbox
UnityFax UndeliverableMailbox
< Back
Next >
Cancel
Help

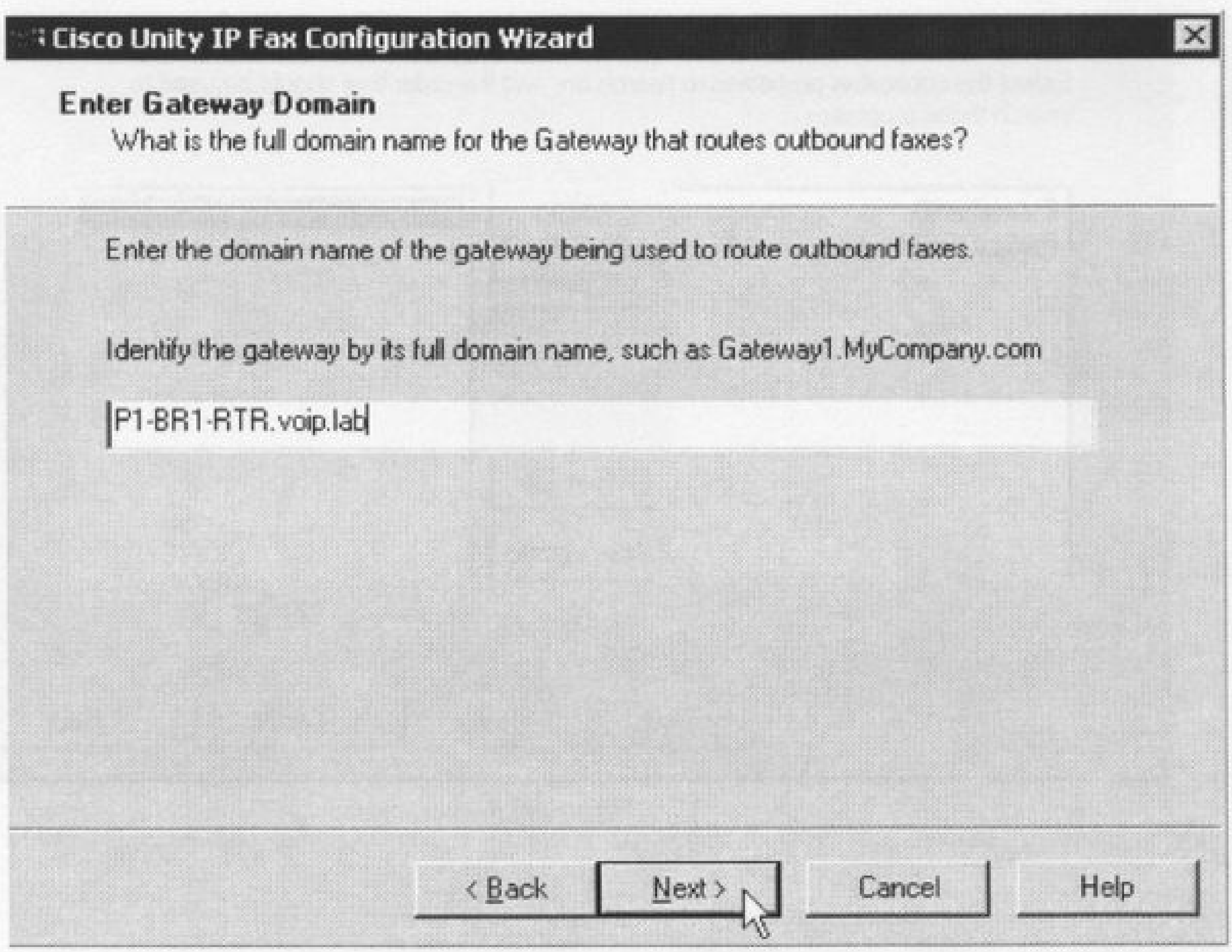

Cisco Unity IP Fax Configuration Wizard
Choose Undeliverable Fax Mailbox
Where do you want undeliverable faxes stored?
Choose where you want undeliverable faxes stored.
All Subscribers - UNITY-LAB
BR1 Phone2
Example Administrator - UNITY-LAB
HQ Ph3
System Event Messages - UNITY-LAB
Unaddressed Messages - UNITY-LAB
UnityFax OutboundMailbox
UnityFax UndeliverableMailbox
< Back
Next >
Cancel
Help

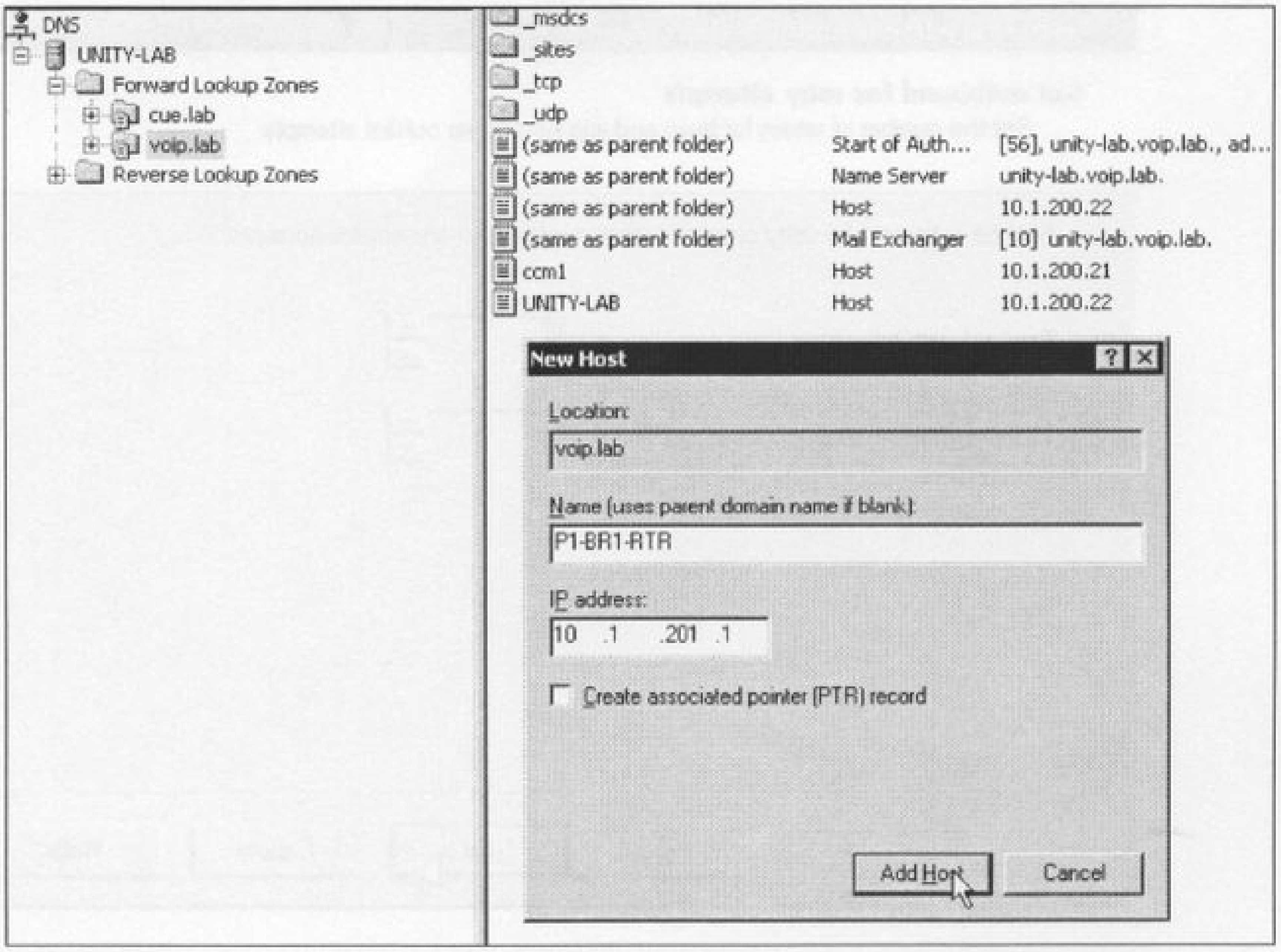

Cisco Unity IP Fax Configuration Wizard
Specify Parse Method
How do you want to parse delivery information?
Specify how you want fax addresses parsed.
Fax delivery number:
Right
4
Digits
Add digits to the fax delivery number:
Begin with:
End with:
< Back
Next >
Cancel
Help

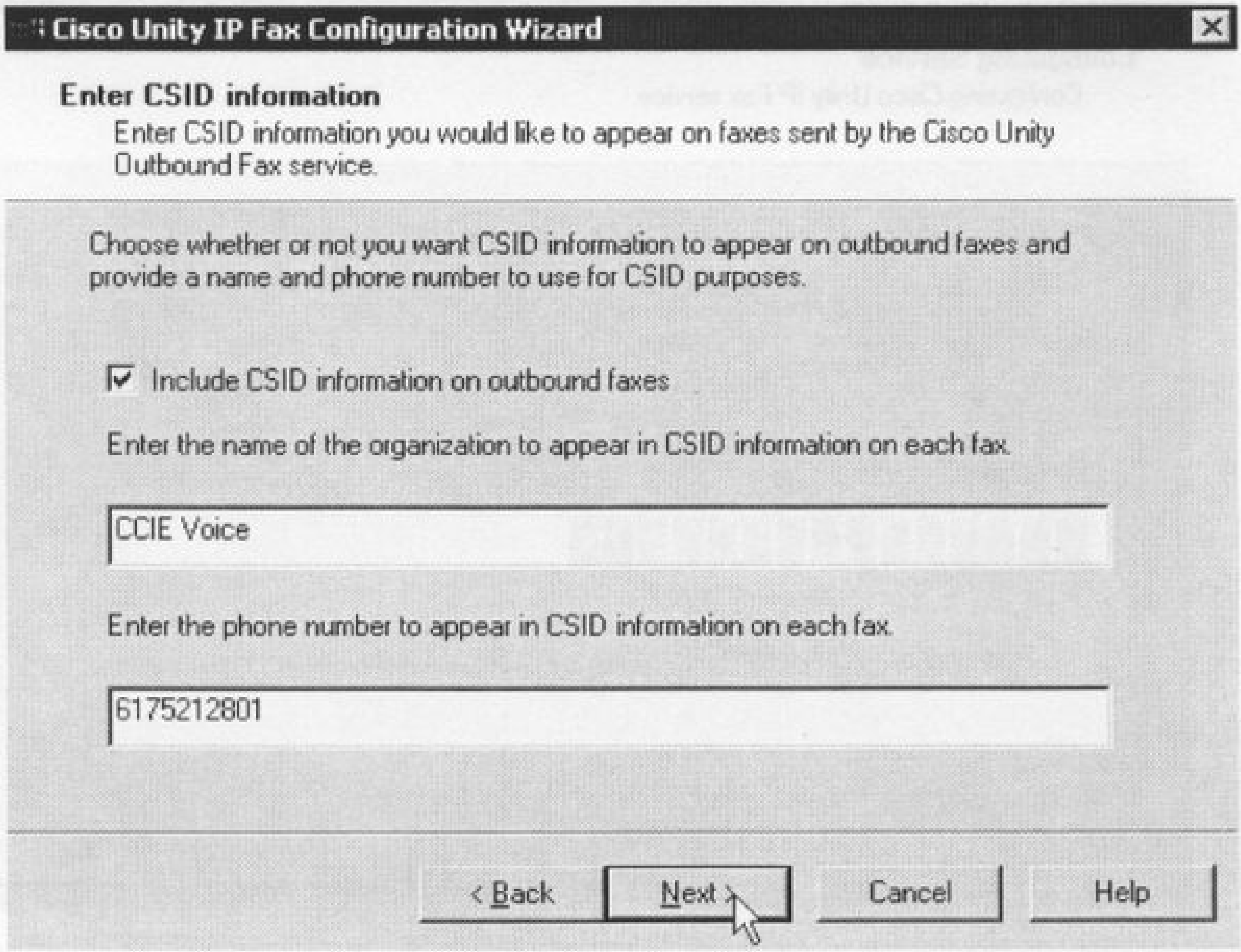

Cisco Unity IP Fax Configuration Wizard
Specify Subscriber Lookup
How do you want to look up subscribers?
Select the subscriber properties to search on, and the order that should be used to search those properties.
Extension ID
Primary Fax Number
Add >>
<< Remove
Primary Fax Number
Move Up
Move Down
< Back
Next >
Cancel
Help

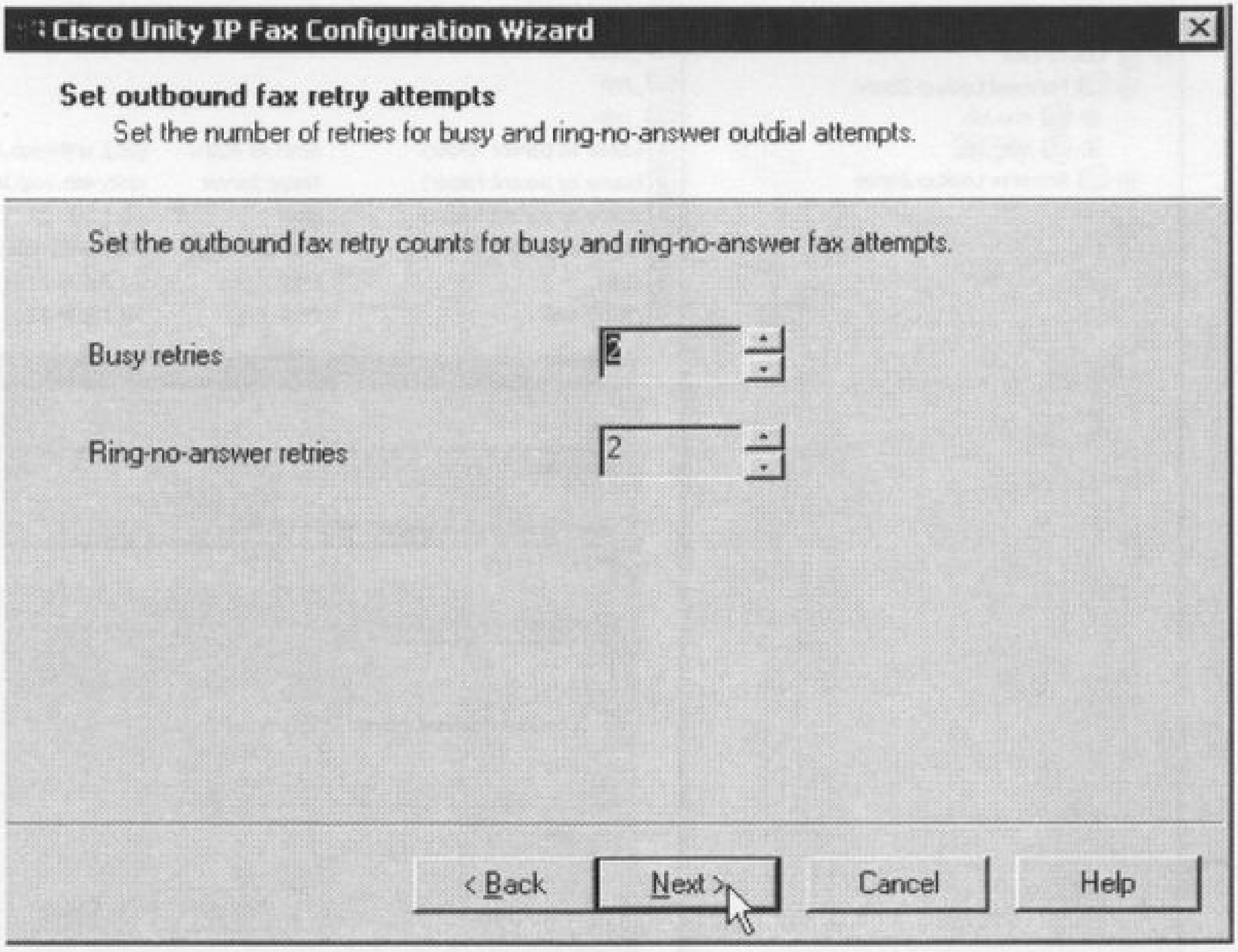


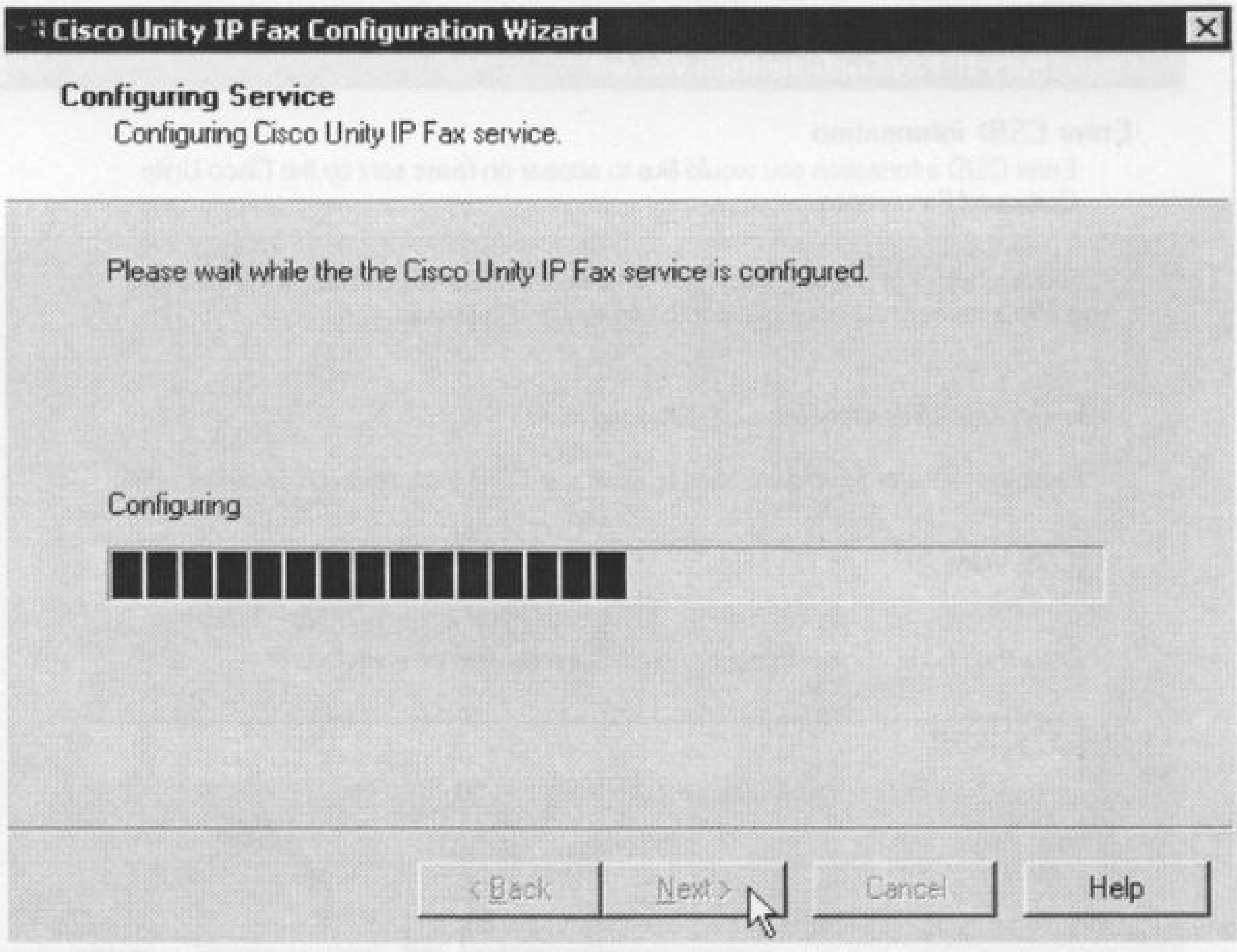
➔ **Now we need to identify the Fax OffRamp GW by its FQDN so we will also need to ensure that this Host appears in our Unity DNS tables and that the Unity server and the BR1 GW both point to the Unity DNS server.**

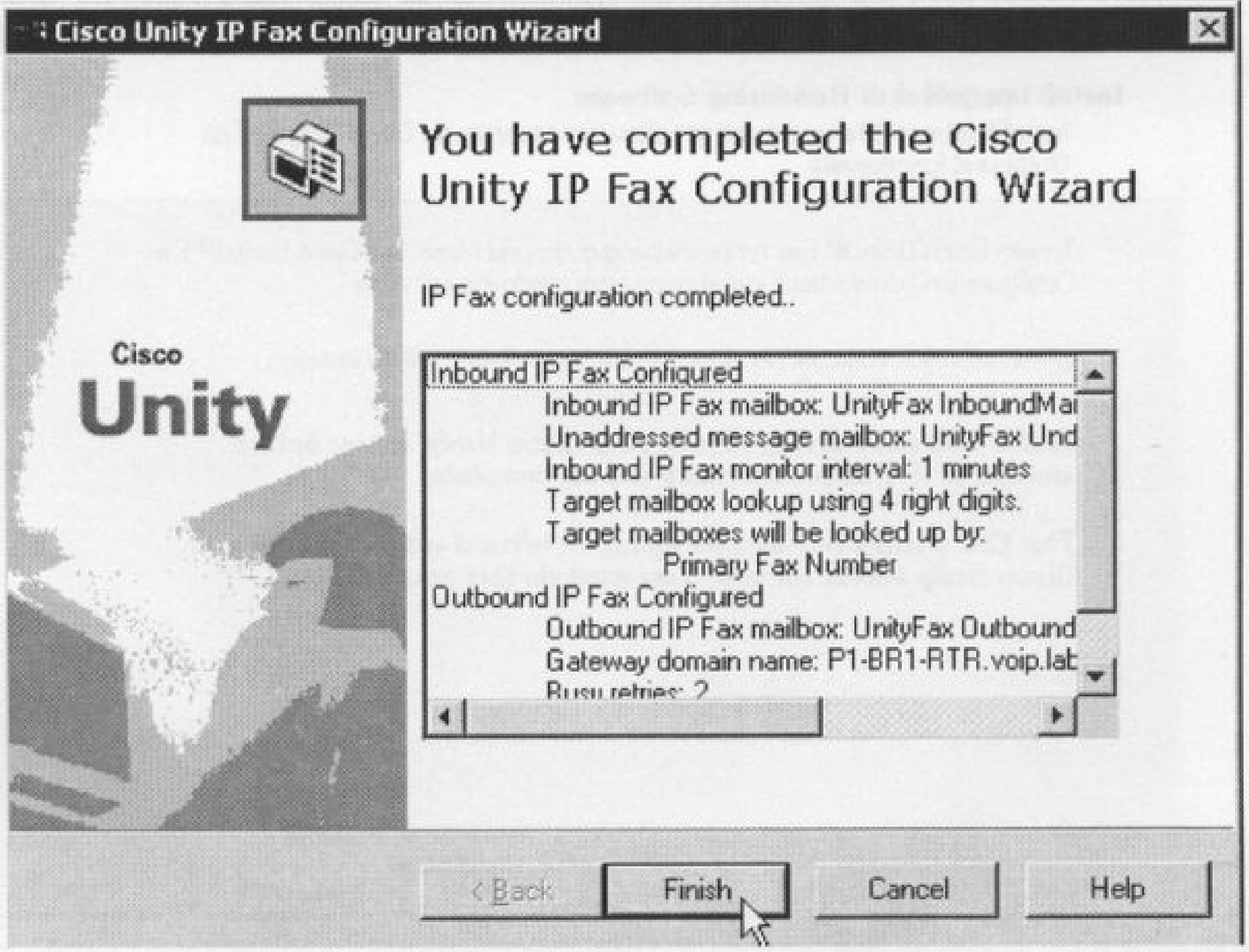



DNS
UNITY-LAB
Forward Lookup Zones
cue.lab
voip.lab
Reverse Lookup Zones
_msdcs
_sites
_tcp
_udp
(same as parent folder) Start of Auth... [56], unity-lab.voip.lab., ad...
(same as parent folder) Name Server unity-lab.voip.lab.
(same as parent folder) Host 10.1.200.22
(same as parent folder) Mail Exchanger [10] unity-lab.voip.lab.
ccm1 Host 10.1.200.21
UNITY-LAB Host 10.1.200.22
New Host
Location:
voip.lab
Name (uses parent domain name if blank):
P1-BR1-RTR
IP address:
10 .1 .201 .1
Create associated pointer (PTR) record
Add Host
Cancel


Cisco Unity IP Fax Configuration Wizard
Enter CSID information
Enter CSID information you would like to appear on faxes sent by the Cisco Unity Outbound Fax service.
Choose whether or not you want CSID information to appear on outbound faxes and provide a name and phone number to use for CSID purposes.
Include CSID information on outbound faxes
Enter the name of the organization to appear in CSID information on each fax.
CCIE Voice
Enter the phone number to appear in CSID information on each fax.
6175212801
< Back
Next >
Cancel
Help

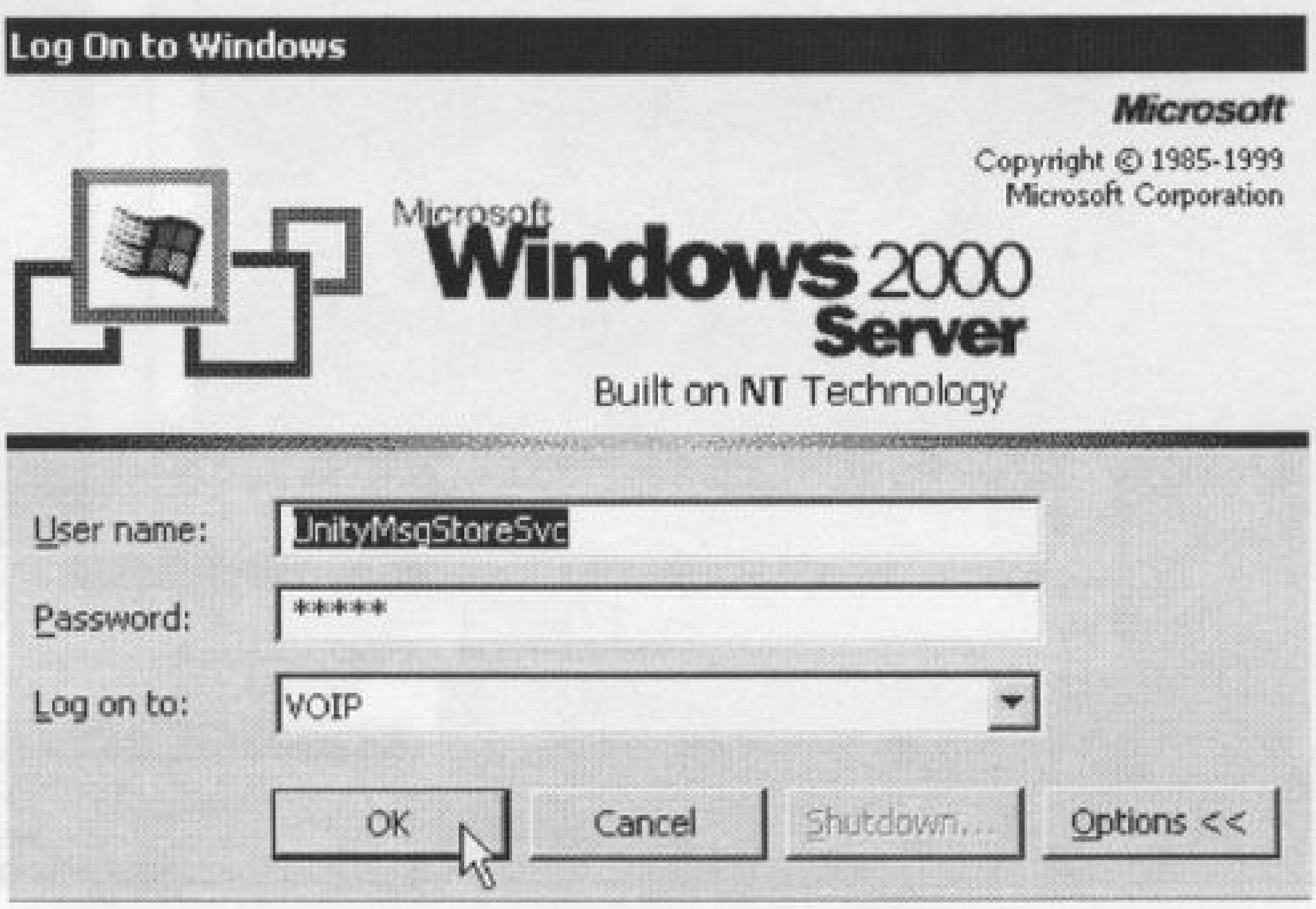

Cisco Unity IP Fax Configuration Wizard
Set outbound fax retry attempts
Set the number of retries for busy and ring-no-answer outdial attempts.
Set the outbound fax retry counts for busy and ring-no-answer fax attempts.
Busy retries
2
Ring-no-answer retries
2
< Back
Next >
Cancel
Help


Cisco Unity IP Fax Configuration Wizard
Configuring Service
Configuring Cisco Unity IP Fax service.
Please wait while the the Cisco Unity IP Fax service is configured.
Configuring
< Back
Next >
Cancel
Help

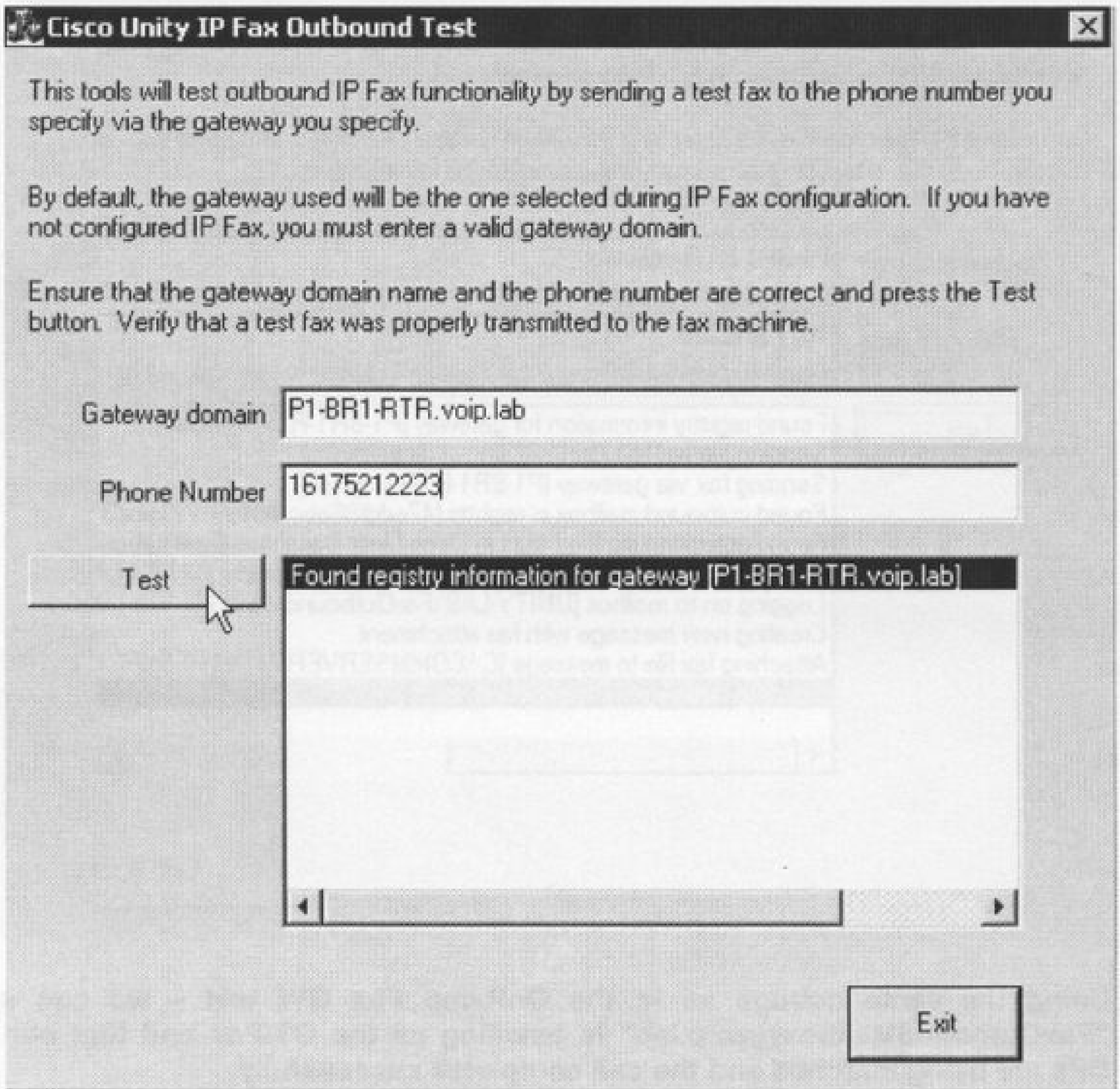


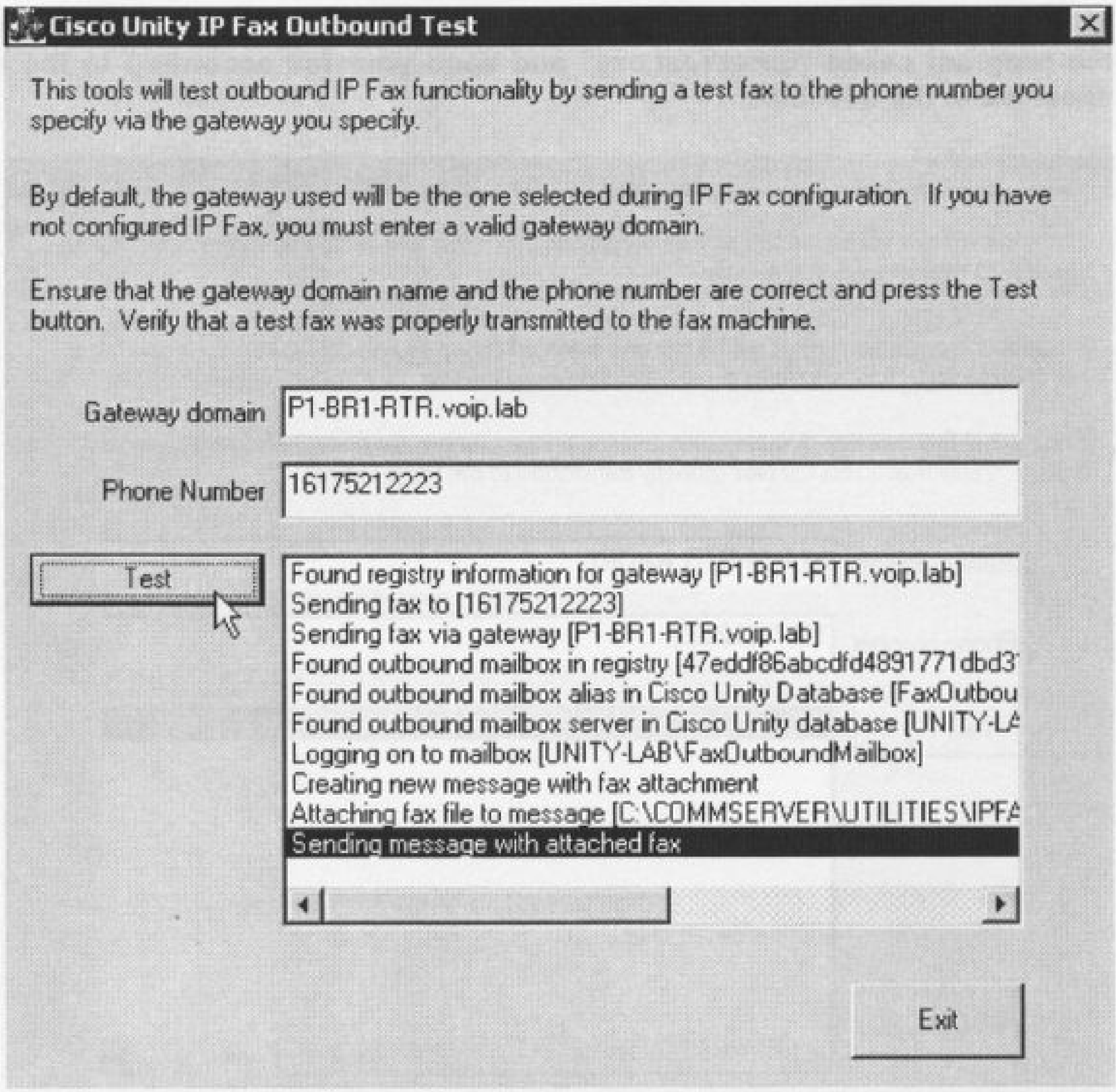
➔ **Reboot the Unity Server!**

➔ **Now we need to login to Unity with the UnityMsgStoreSvc account in order to be able to run the Fax Test program.**



➔ **Now browse to the C:\CommServer\Utilities\IPFaxConfigWizard directory and run the program called "IpFaxTest.exe" and send your fax according to the number specified in the question.**





➔ **Using the same debugs as in the OnRamp Fax GW test – we can see that "FaxOutboundMailbox@voip.lab" is emailing us the G3 Fax and that our correct DPs are being matched and the call completes successfully.**

```
P1-PSTN-WAN#
*Apr 29 03:48:25.217: //-1/xxxxxxxxxxxx/MSPI_OFF/mspi_offramp_tel_num_trans:
  Mail From=FaxOutboundMailbox@voip.lab, Phone Number In=fax=16175212223, Phone
Number Dial=
*Apr 29 03:48:25.217: //-1/xxxxxxxxxxxx/MSPI_OFF/mspi_offramp_tel_num_trans:
  Incoming Dial-peer(Tag=100, Matched Digits=11, Destination Pattern=16175212223)
*Apr 29 03:48:25.217: //-1/xxxxxxxxxxxx/MSPI_OFF/mspi_offramp_match_digits:
  Outgoing Peer(Tag=110, Destination Pattern=16175212223, Strip Enable=TRUE)
*Apr 29 03:48:25.217: //-1/xxxxxxxxxxxx/MSPI_OFF/mspi_offramp_tel_num_trans:
  Incoming Dial-peer(Tag=100), Outgoing Dial-peer(Tag=110), Cover Page=FALSEexit

*Apr 29 03:48:25.217: //-1/xxxxxxxxxxxx/MSPI_OFF/mspi_offramp_new_rcpt:
  Envelope To=fax=16175212223@P1-BR1-RTR.voip.lab, Length=35,
  MMccb(Incoming Dial-peer=100, Outgoing Dial-peer=110,
  Telephone Number Dial=16175212223, Sub Address=, Cover Page=FALSE
*Apr 29 03:48:25.217: //-1/xxxxxxxxxxxx/MSPI_OFF/mspi_offramp_new_rcpt:exit@1127
*Apr 29 03:48:26.261: //-1/D91258CC8062/MSPI_OFF/mspi_get_ani:
  in_str="UnityFax OutboundMailbox" <FaxOutboundMailbox@voip.lab>
*Apr 29 03:48:26.261: //-1/D91258CC8062/MSPI_OFF/mspi_get_ani:
  in_str=FaxOutboundMailbox@voip.lab
```



```
*Apr 29 03:48:26.261: //87/D91258CC8062/MSPI_OFF/mspi_offramp_rfc822_header:
  Envelope From=FaxOutboundMailbox@voip.lab, Size=28

Subject=00000000EF0535A5228848468D754C057ECE82B707008DCEF15B9A5FF34782453B
DC13CB53AE0000000 1927600008DCEF15B9A5FF34782453BDC13CB53AE000000019B3300
00
  From Personal Name=UnityFax OutboundMailbox
  From="UnityFax OutboundMailbox" <FaxOutboundMailbox@voip.lab>
  To=<fax=1617
[Connection to 10.1.200.2 closed by foreign host]
P1-BR1-RTR#5212223@P1-BR1-RTR.voip.lab>
   Notification Type=0
*Apr 29 03:48:26.261: //87/D91258CC8062/MSPI_OFF/mspi_offramp_rfc822_header:
  MMccb(Called Number=16175212223, Calling Number=, Incoming Dial-peer=100)
*Apr 29 03:48:26.265: ISDN Se2/0/0:23 Q931: pak_private_number: Invalid type/plan 0x0 0x1
may be overriden; sw-type 13
*Apr 29 03:48:26.265: ISDN Se2/0/0:23 Q931: Applying typeplan for sw-type 0xD is 0x0 0x0,
Called num 16175212223
*Apr 29 03:48:26.265: ISDN Se2/0/0:23 Q931: TX -> SETUP pd = 8  callref = 0x0081
     Bearer Capability i = 0x8090A2
          Standard = CCITT
          Transfer Capability = Speech
          Transfer Mode = Circuit
          Transfer Rate = 64 kbit/s
     Channel ID i = 0xA98383
          Exclusive, Channel 3
     Calling Party Number i = 0x0081, N/A
          Plan:Unknown, Type:Unknown
     Called Party Number i = 0x80, '16175212223'
          Plan:Unknown, Type:Unknown
*Apr 29 03:48:26.285: ISDN Se2/0/0:23 Q931: RX <- CALL_PROC pd = 8  callref = 0x8081
     Channel ID i = 0xA98383
          Exclusive, Channel 3
*Apr 29 03:48:26.297: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONNECTING)
*Apr 29 03:48:26.297: //87/D91258CC8062/MSPI_OFF/moff_save_buffer:
  MIME Type=12, Buffer Length=1536
*Apr 29 03:48:26.333: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONNECTING)
*Apr 29 03:48:26.333: //87/D91258CC8062/MSPI_OFF/moff_save_buffer:
  MIME Type=12, Buffer Length=1536
*Apr 29 03:48:26.369: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONNECTING)
*Apr 29 03:48:26.369: //87/D91258CC8062/MSPI_OFF/moff_save_buffer:
  MIME Type=12, Buffer Length=1536
*Apr 29 03:48:26.409: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONNECTING)
*Apr 29 03:48:26.409: //87/D91258CC8062/MSPI_OFF/moff_save_buffer:
  MIME Type=12, Buffer Length=1536
*Apr 29 03:48:26.445: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONNECTING)
*Apr 29 03:48:26.445: //87/D91258CC8062/MSPI_OFF/moff_save_buffer:
  MIME Type=12, Buffer Length=1536
*Apr 29 03:48:26.481: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONNECTING)
*Apr 29 03:48:26.481: //87/D91258CC8062/MSPI_OFF/moff_save_buffer:
```



```
  MIME Type=12, Buffer Length=1536
*Apr 29 03:48:26.481: //87/D91258CC8062/MSPI_OFF/moff_save_buffer:
  Disabled Receiving!
*Apr 29 03:48:26.521: ISDN Se2/0/0:23 Q931: RX <- ALERTING pd = 8  callref = 0x8081
P1-BR1-RTR#
P1-BR1-RTR#
*Apr 29 03:48:37.641: ISDN Se2/0/0:23 Q931: RX <- CONNECT pd = 8  callref = 0x8081
*Apr 29 03:48:37.641: %ISDN-6-CONNECT: Interface Serial2/0/0:2 is now connected to
16175212223 N/A
P1-BR1-RTR#
*Apr 29 03:48:37.641: ISDN Se2/0/0:23 Q931: TX -> CONNECT_ACK pd = 8  callref = 0x0081
P1-BR1-RTR#
*Apr 29 03:48:44.781: //87/D91258CC8062/MSPI/mspi_bridge:
  MMccb(State=CONNECTING, Type=Offramp), Destination Call Id=90
*Apr 29 03:48:44.781: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:44.785: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:44.785: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:44.785: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:44.785: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:44.785: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
P1-BR1-RTR#
*Apr 29 03:48:44.785: //87/D91258CC8062/MSPI/mspi_bridge:
  Offramp Rcpt Enabled
P1-BR1-RTR#
*Apr 29 03:48:56.481: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONFERENCED)
*Apr 29 03:48:56.481: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:56.481: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=1536, MMccb(Info Type=10, State=CONFERENCED)
*Apr 29 03:48:56.481: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:56.497: //87/D91258CC8062/MSPI_OFF/mspi_offramp_put_buffer:
  Mime Type=12, Buffer Length=596, MMccb(Info Type=10, State=CONFERENCED)
P1-BR1-RTR#
*Apr 29 03:48:56.497: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  Mime Type=12
*Apr 29 03:48:56.497: //87/D91258CC8062/MSPI_OFF/mspi_offramp_send_buffer:
  BUFF_LAST
P1-BR1-RTR#
*Apr 29 03:49:03.585: //87/D91258CC8062/MSPI/mspi_bridge_drop:
  MMccb(State=DESTROYING, Type=Offramp), Destination Call Id=90
*Apr 29 03:49:03.593: %ISDN-6-DISCONNECT: Interface Serial2/0/0:2  disconnected from
16175212223 , call lasted 25 seconds
*Apr 29 03:49:03.593: ISDN Se2/0/0:23 Q931: TX -> DISCONNECT pd = 8  callref = 0x0081
        Cause i = 0x8090 - Normal call clearing
*Apr 29 03:49:03.601: ISDN Se2/0/0:23 Q931: RX <- RELEASE pd = 8  callref = 0x8081
*Apr 29 03:49:03.601: ISDN Se2/0/0:23 Q931: TX -> RELEASE_COMP pd = 8  callref =
0x0081
*Apr 29 03:49:03.605: //87/D91258CC8062/MSPI/mspi_call_disconnect:
```



```
  Cause Value=normal call clearing (16),
  MMccb(State=DISCONNECTING, Type=Offramp)
*Apr 29 03:49:03.605: //87/D91258CC8062/MSPI/mspi_offramp_call_history:
  MMccb(Disconnect Cause=normal call clearing (16) 16)
*Apr 29 03:49:03.605: //87/D91258CC8062/MSPI_OFF/mspi_call_get_offramp:
P1-BR1-RTR#
*Apr 29 03:49:03.605: //87/D91258CC8062/MSPI_OFF/mspi_call_get_offramp:exit@2527
*Apr 29 03:49:03.605: //87/D91258CC8062/MSPI_OFF/mspi_offramp_call_history:exit@2399
P1-BR1-RTR#
*Apr 29 03:49:11.949: //87/D91258CC8062/MSPI_OFF/mspi_offramp_dispose_context:
  MMccb(State=DISCONNECT_DONE)
*Apr 29 03:49:11.949: //-1/xxxxxxxxxxxx/MSPI/mspi_free_ccb:
  Total Allocated MMccbs=1, Total Inserted MMccbs=0
P1-BR1-RTR#
```

➔ **Finally, check the Proctor Labs page for your PSTN fax!**

Cisco Unity IP Fax Outbound Test

This test fax was sent by Cisco Unity IP Fax.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 10: IPCC Express

Estimated Time to Complete: 4 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 10 IPCC Express

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab Section 1 and the basics within the CCM section must be completed.

Section 10 Configuration Tasks

Task 10.1

Configure Auto-attendant and ICD with the following information:

- AA Route Point = 1710
- Script = aa.aef
- CTI Ports = 1711, 1712

- ICD Route Point = 1700
- Script = icd.aef
- CTI Ports = 1701, 1702

Create the following users that will be used in this task:

- "**jtapi**" to be used for the JTAPI Subsystem.
- "**rmjtapi**" to be used for the ICD Subsystem.
- "**telecaster**" to be used for the ICD Subsystem and enterprise data.
- "**crsadmin**" which must be the designated administrator for IPCC Express.
- **agent1** [assigned device HQ Phone 3 with ICD ext="1003"].
- **agent2** [assigned device BR Phone 2 with ICD ext="2003"]

[all passwords must be 'cisco' and PIN numbers set to '12345' except of course 'telecaster']

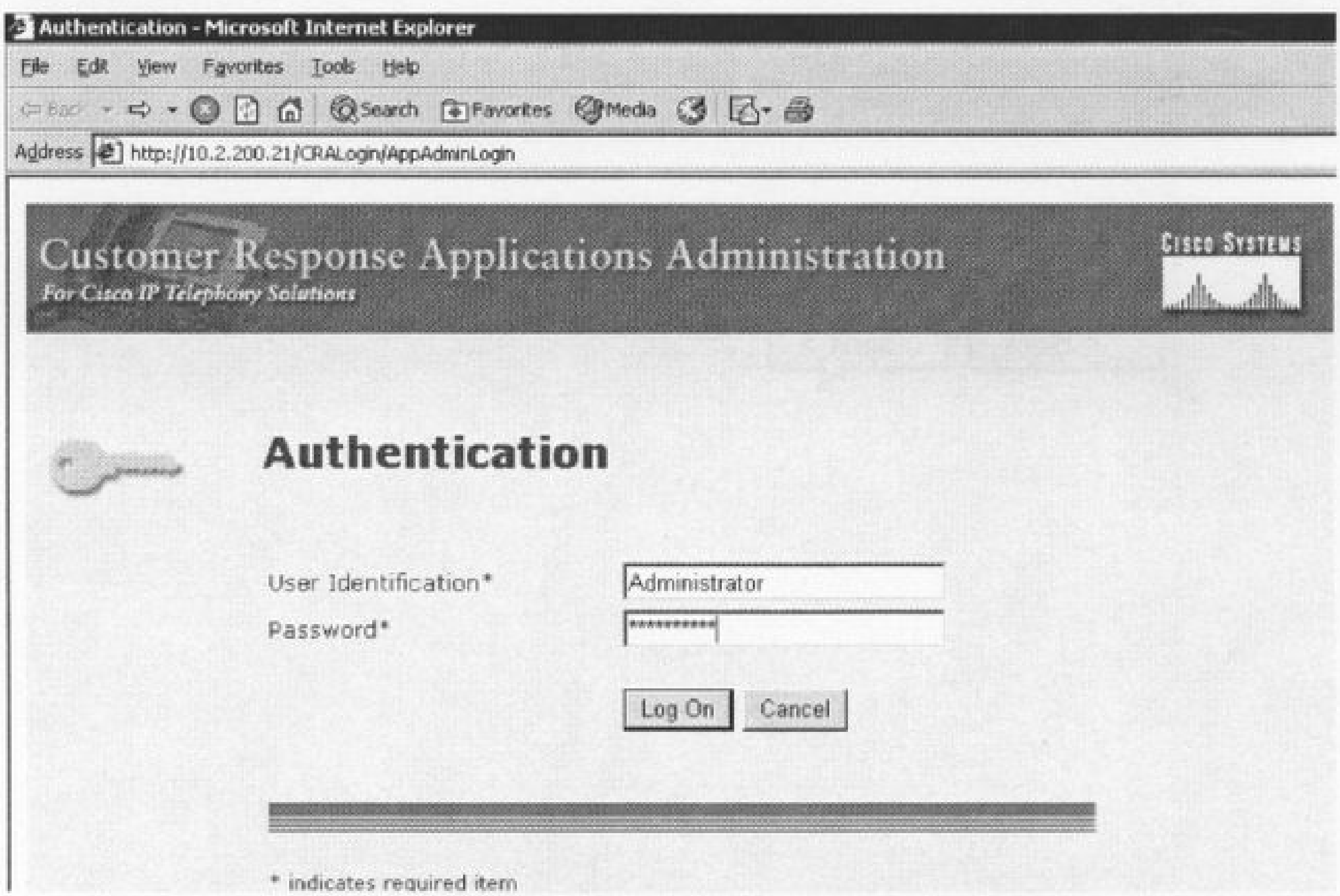
For the ICD application you must use skills based routing with the following information:

- CSQ: "GeneralQ"
- Skills: "sales" & "support"
- 'agent1' shall have the skill of 'support' at a proficiency level of 9 and the skill of 'sales' at a proficiency level of 10
- 'agent2' shall have the skill of 'support' at a proficiency level of 10 and the skill of 'sales' at a proficiency level of 9
- The CSQ 'GeneralQ' should have both skills assigned to it with a proficiency level of at least 5 or better for each
- With this stated, the engine should always choose agent1 over agent2 if agent1 is available (you may use whatever method you wish to accomplish this in the engine)
- The engine should also send every agent into a automatic state of 'Work' for 30 seconds before then automatically returning them to a state of 'Ready' (this should happen regardless of whether the call is routed to a specific agent or through the GeneralQ)

➔ **These will be the names of the Users that will be created in the LDAP Directory and assigned to their respective devices by the IPCC Engine – You will need to create the first 4 users, however, DO NOT configure the last two users before you setup the engine – IPCCX will take care of that for you.**

UserID	CTI App Required	Device Association	ICD Ext required
crsadmin	N	None – Used to Auth CRS Web	N
agent1	Y	Agent1 Device	Y
agent2	Y	Agent2 Device	Y
telecaster	Y	All Agent Devices including EM UDProfiles if any	N
jtapi	Y	CTI Route Points and CTI Ports	N
rmjtapi	Y	All Agent Devices including EM UDProfiles if any	N

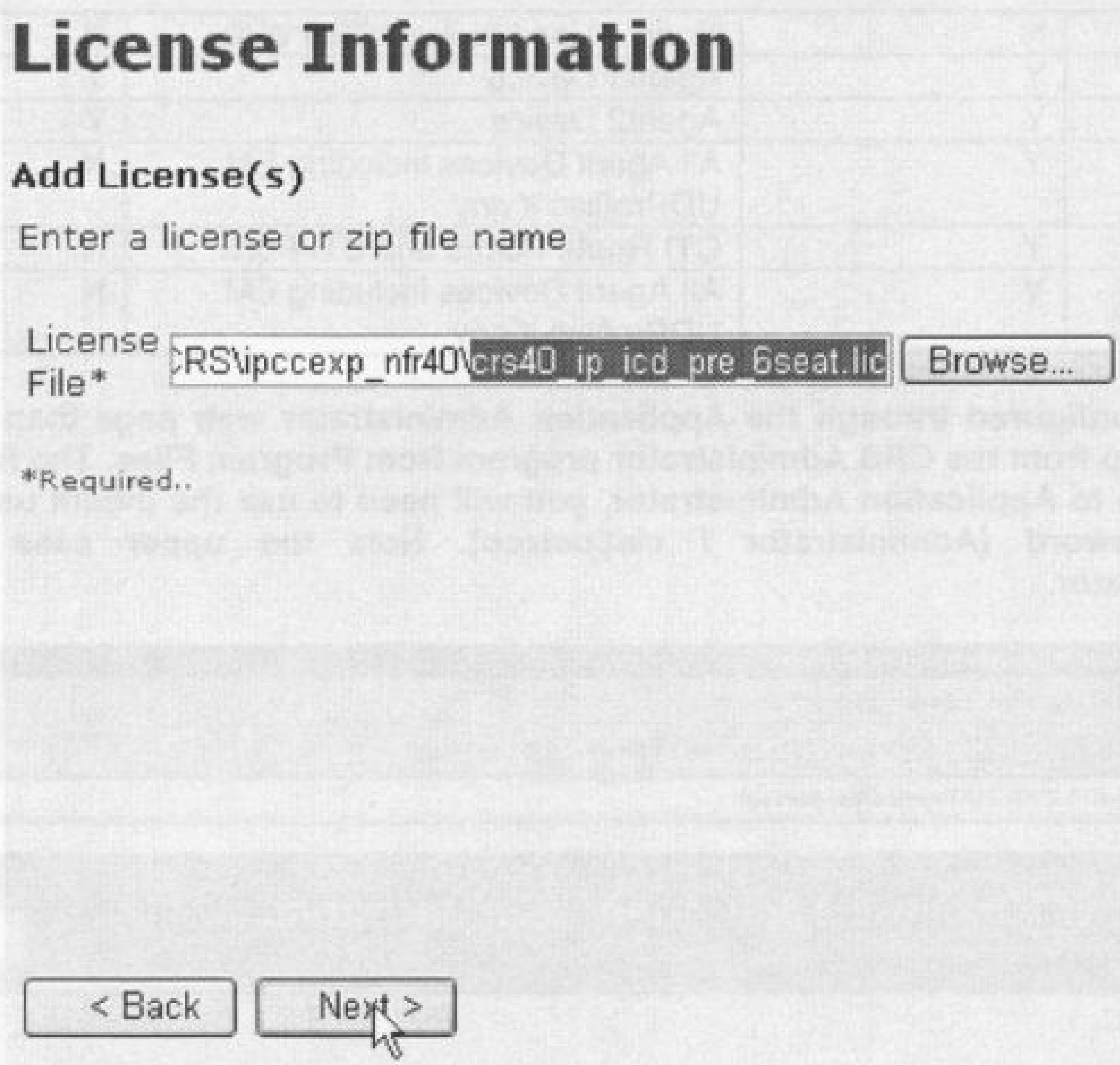
➔ **CRS is configured through the Application Administrator web page than can be brought up from the CRS Administrator program from Program Files. The first time you logon to Application Administrator, you will need to use the inbuilt username and password (Administrator / ciscocisco). Note the upper case 'A' in Administrator.**



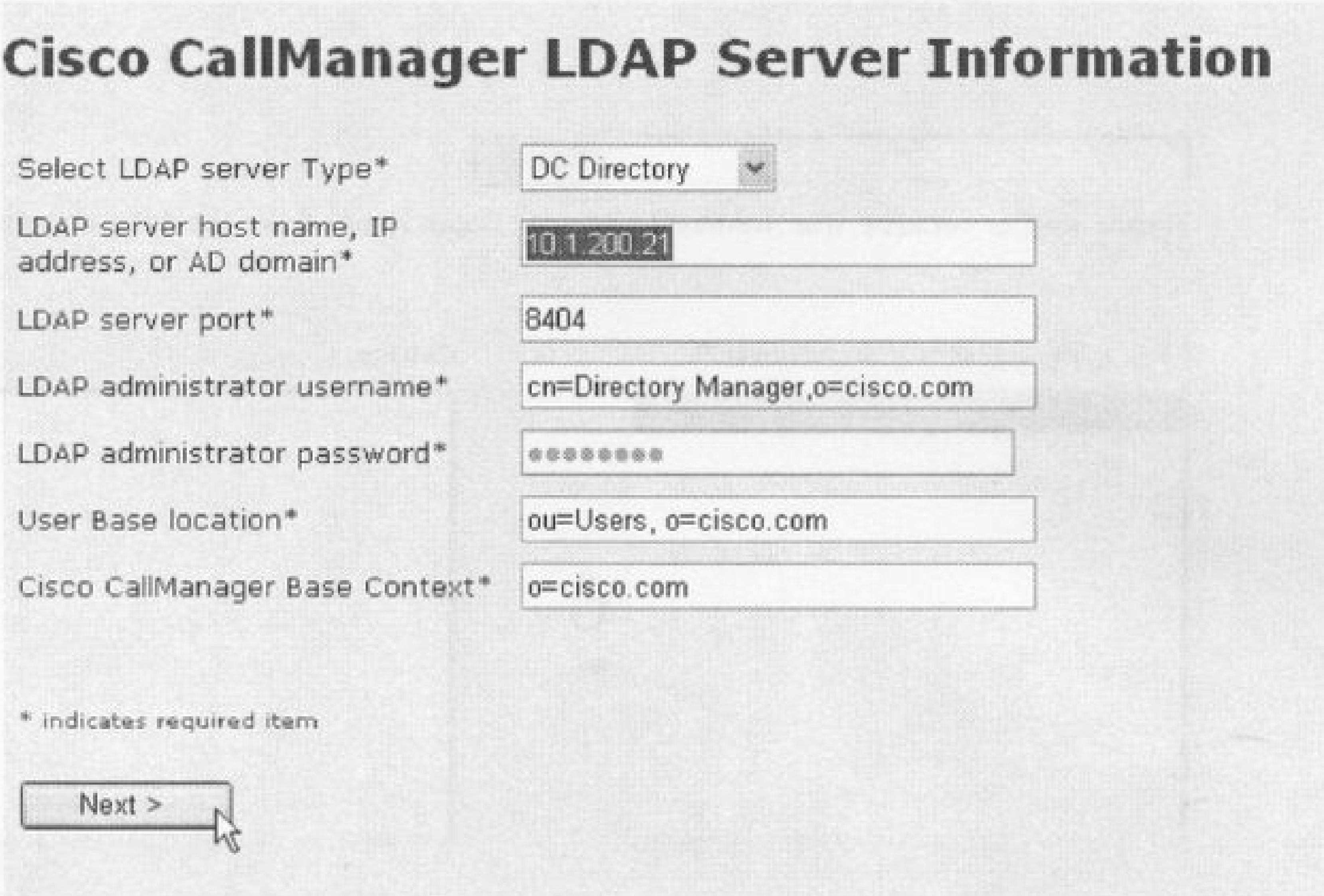
➔ **It is important to do this next step from within RDP or VNC in order to pull the license from the correct location.**

➔ **The license you will use is:**

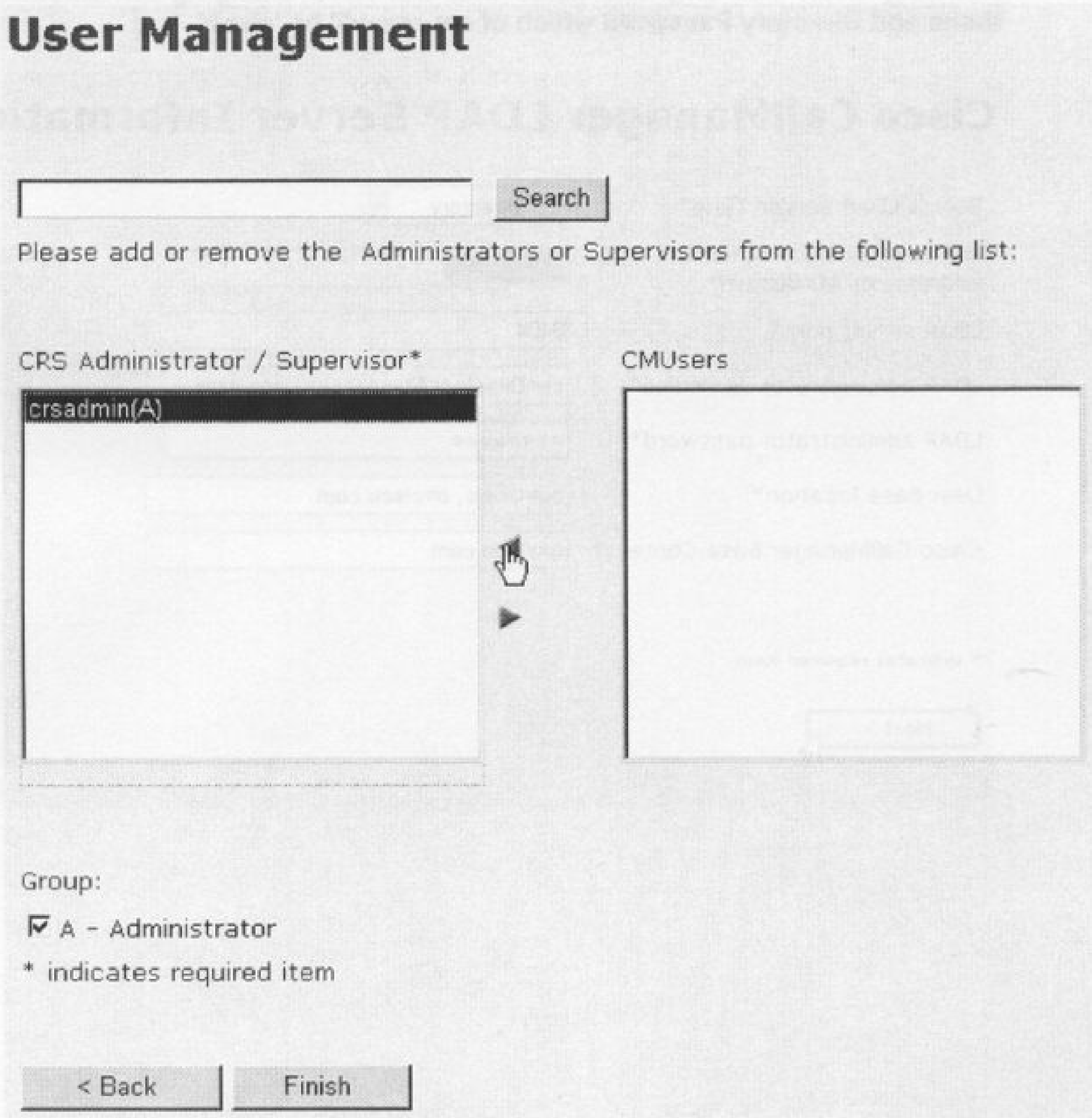
C:\AAA_ProctorLabs_Student\licenses\crs40_ip_icd_pre_6seat.lic



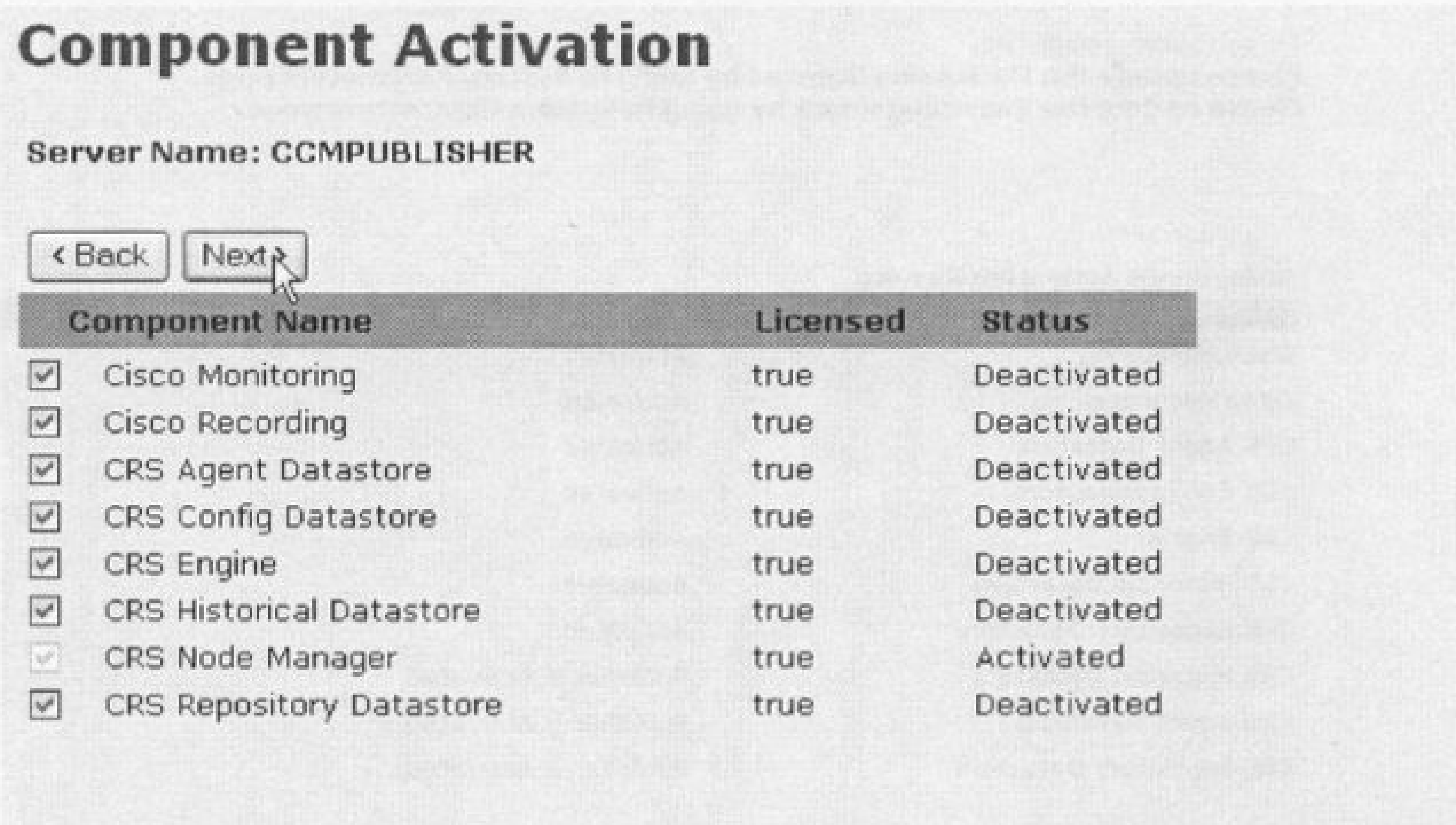
➔ **Once logged in, you will be prompted to enter the ip address and password of the Directory user. The only two fields that will need changing are Directory Host Name and Directory Password which of course will be 'cisco'.**

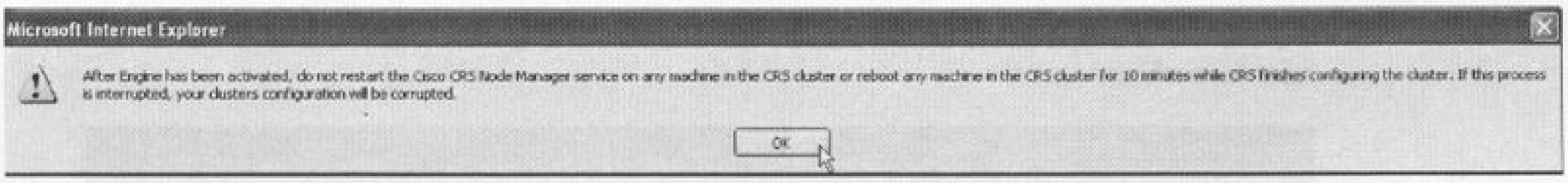


➔ **Now we need to assign a new Admin user from the LDAP.**

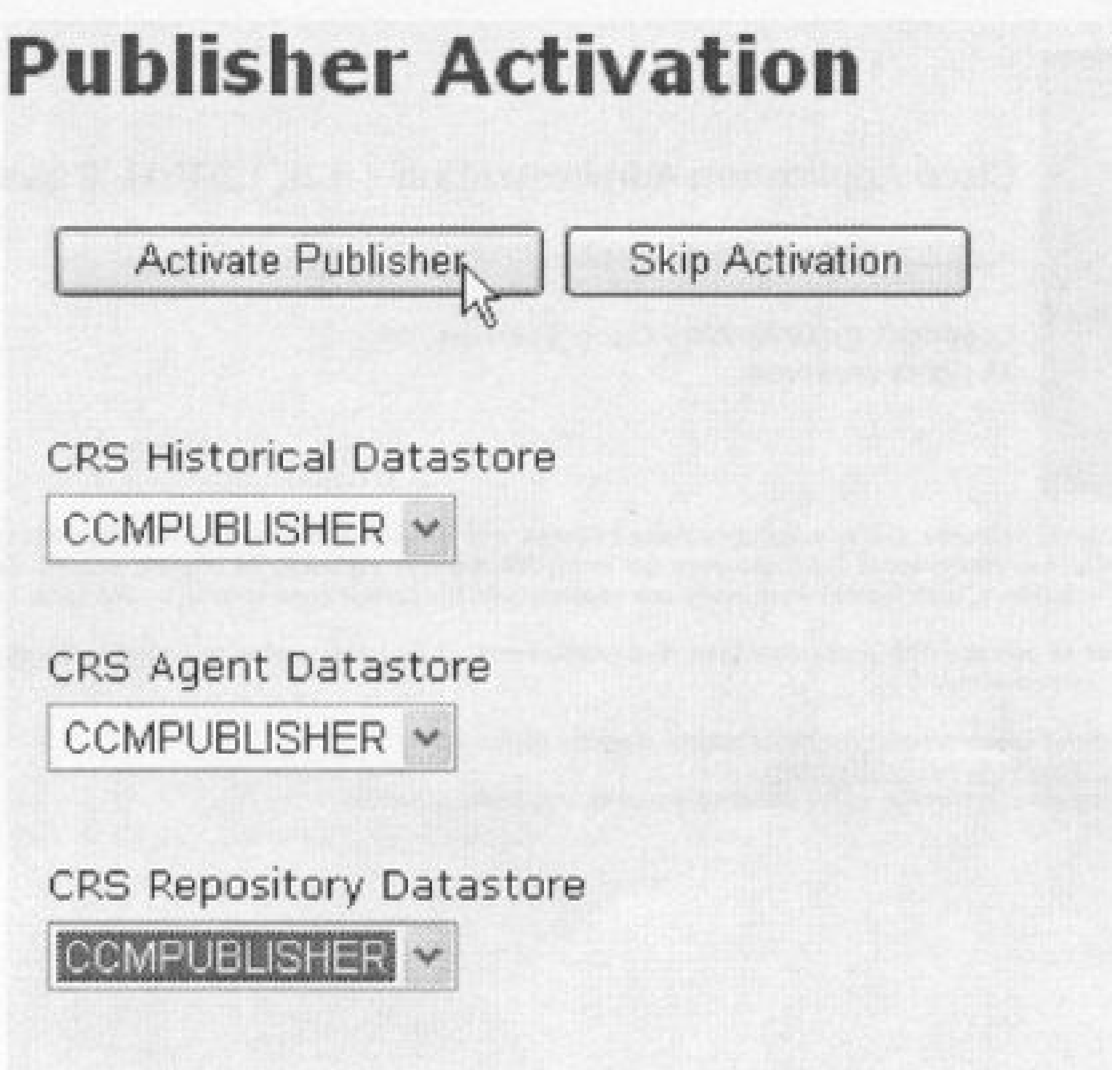


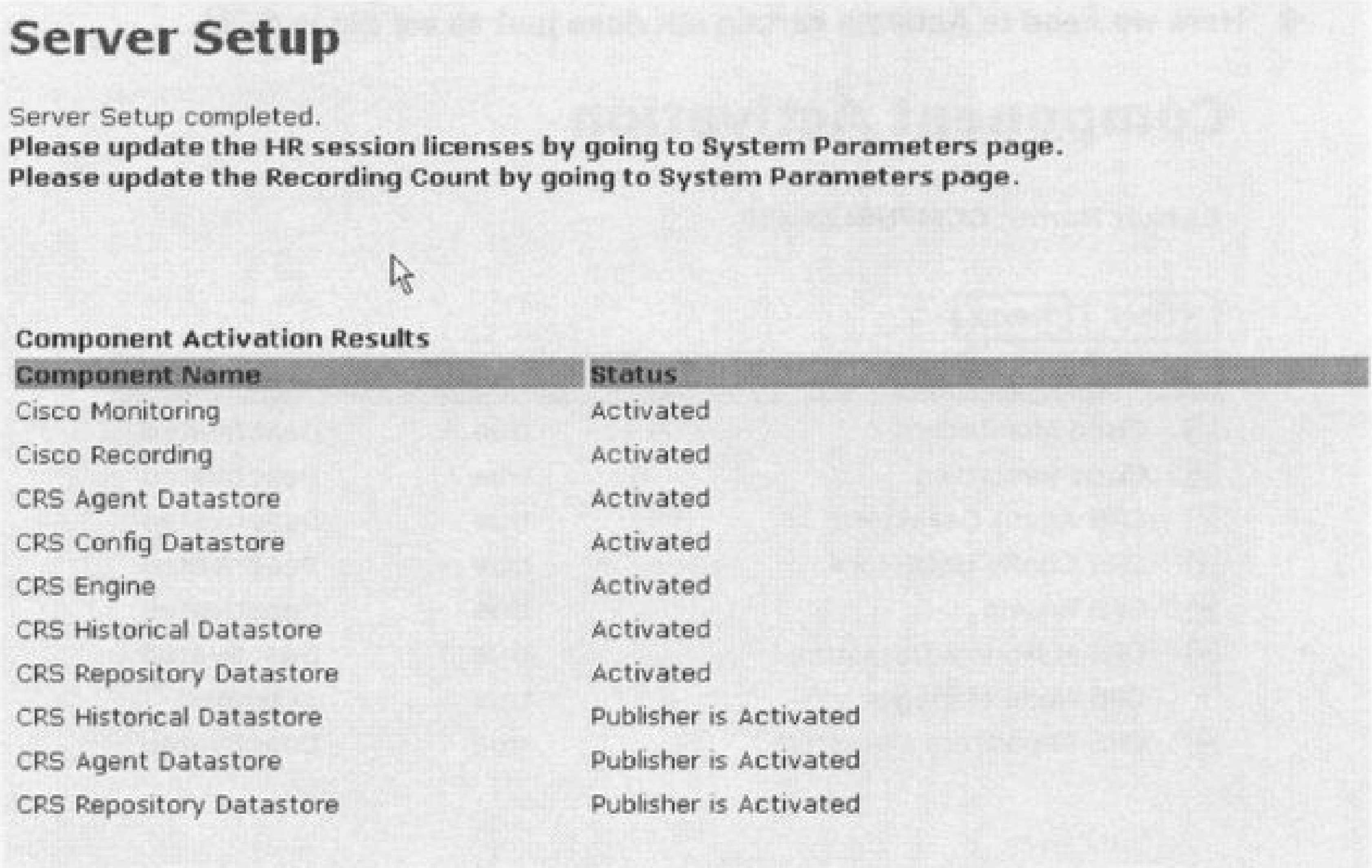
➔ **Here we need to Activate certain services just as we did in CCM.**



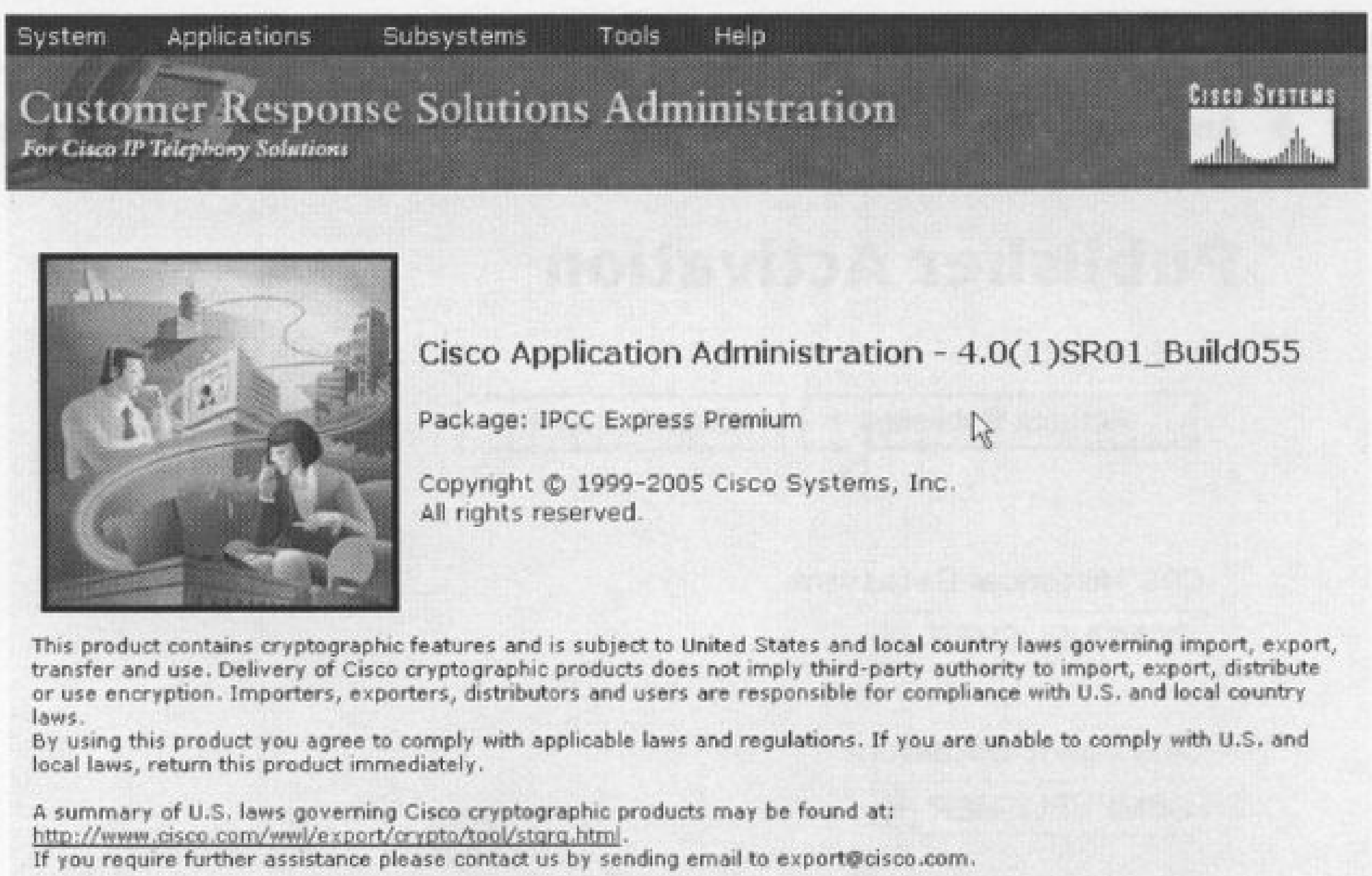


➔ **And we will choose which server will be the Publisher server run for each of these services.**

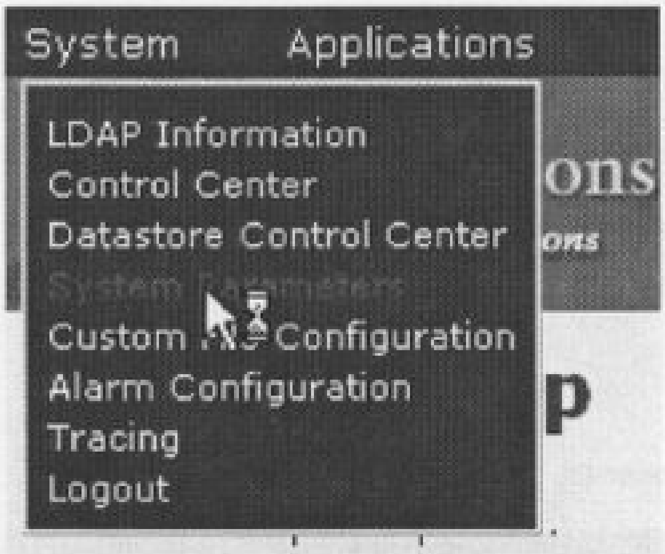


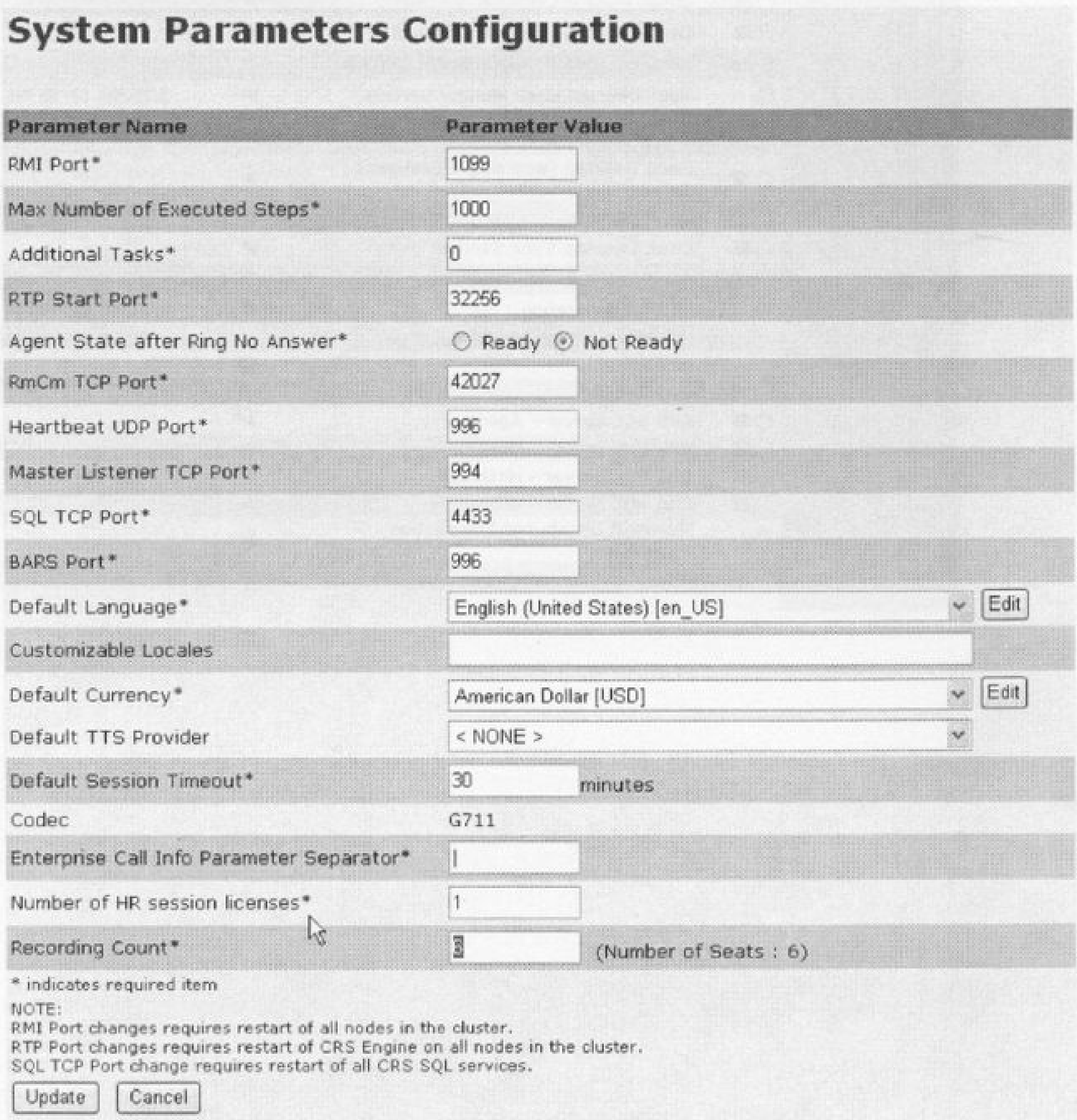


➔ **Finally we are complete and we need to restart our web browser and login with our new 'crsadmin' user.**



➔ **Now we may need to set certain Service Parameters such as the number of Recording Count and Historical Reporting sessions.**





System Parameters Configuration

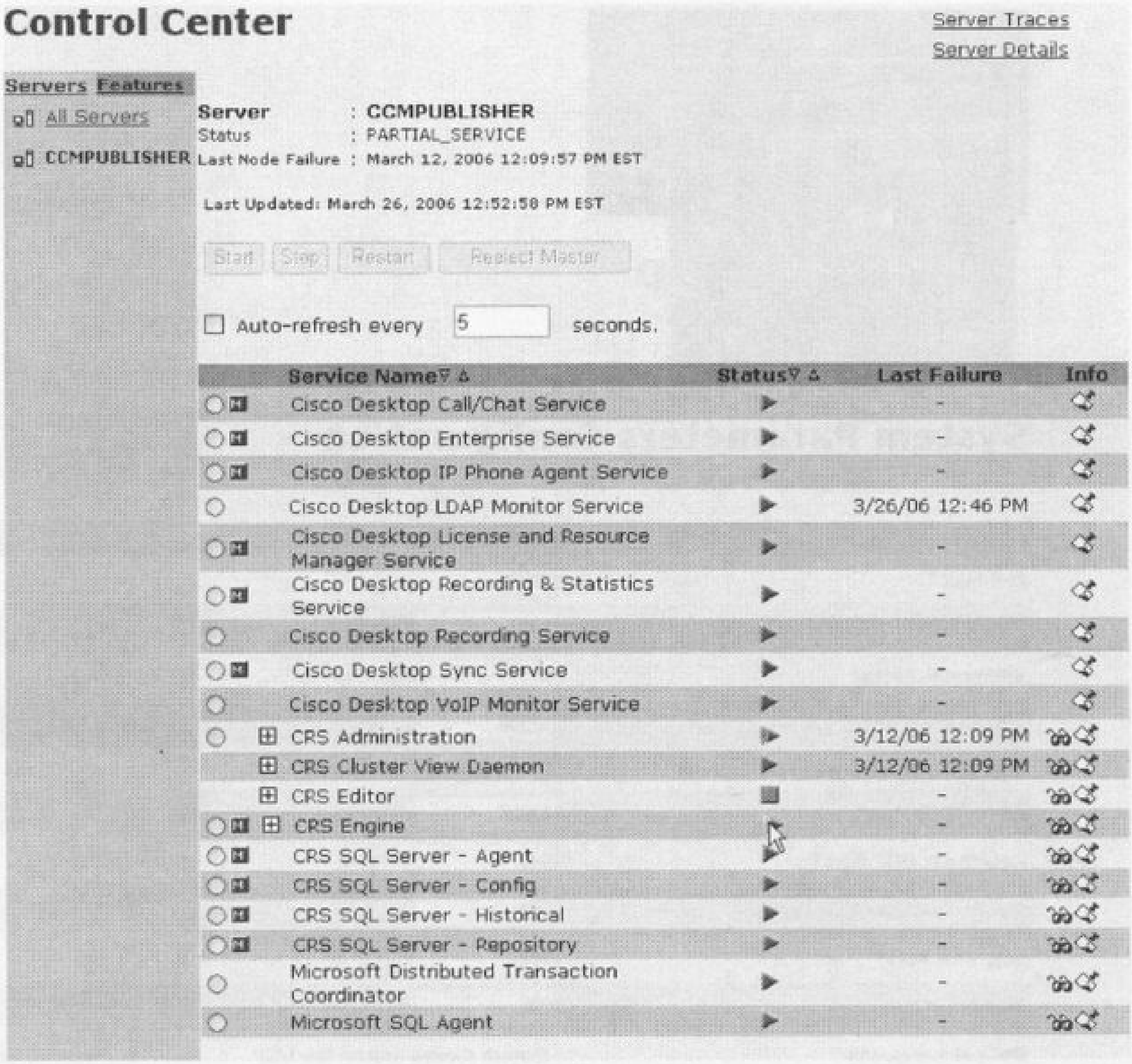
Parameter Name	Parameter Value
RMI Port*	1099
Max Number of Executed Steps*	1000
Additional Tasks*	0
RTP Start Port*	32256
Agent State after Ring No Answer*	○ Ready ⦿ Not Ready
RmCm TCP Port*	42027
Heartbeat UDP Port*	996
Master Listener TCP Port*	994
SQL TCP Port*	4433
BARS Port*	996
Default Language*	English (United States) [en_US] Edit
Customizable Locales	
Default Currency*	American Dollar [USD] Edit
Default TTS Provider	< NONE >
Default Session Timeout*	30 minutes
Codec	G711
Enterprise Call Info Parameter Separator*	|
Number of HR session licenses*	1
Recording Count*	3 (Number of Seats : 6)

* indicates required item

NOTE:
RMI Port changes requires restart of all nodes in the cluster.
RTP Port changes requires restart of CRS Engine on all nodes in the cluster.
SQL TCP Port change requires restart of all CRS SQL services.

Update Cancel

➔ **Now we shall go System ➔ Control Center to see what is running and what still needs setup.**



Control Center

Server Traces
Server Details

Servers Features

All Servers

CCMPUBLISHER

Server : **CCMPUBLISHER**
Status : PARTIAL_SERVICE
Last Node Failure : March 12, 2006 12:09:57 PM EST

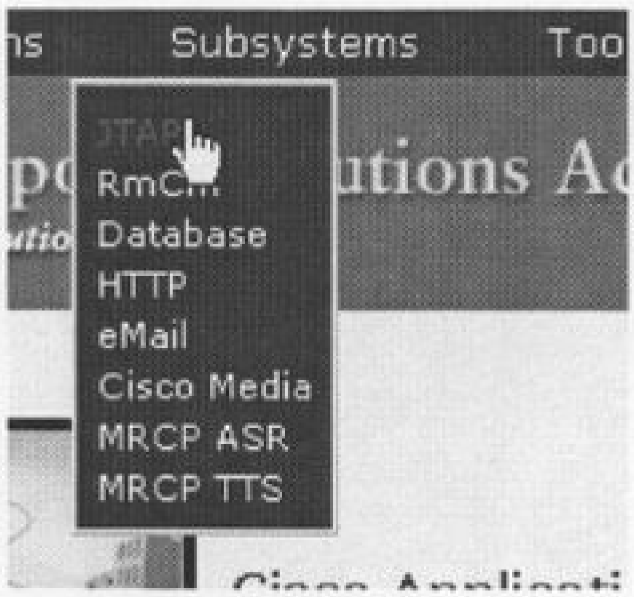
Last Updated: March 26, 2006 12:52:58 PM EST

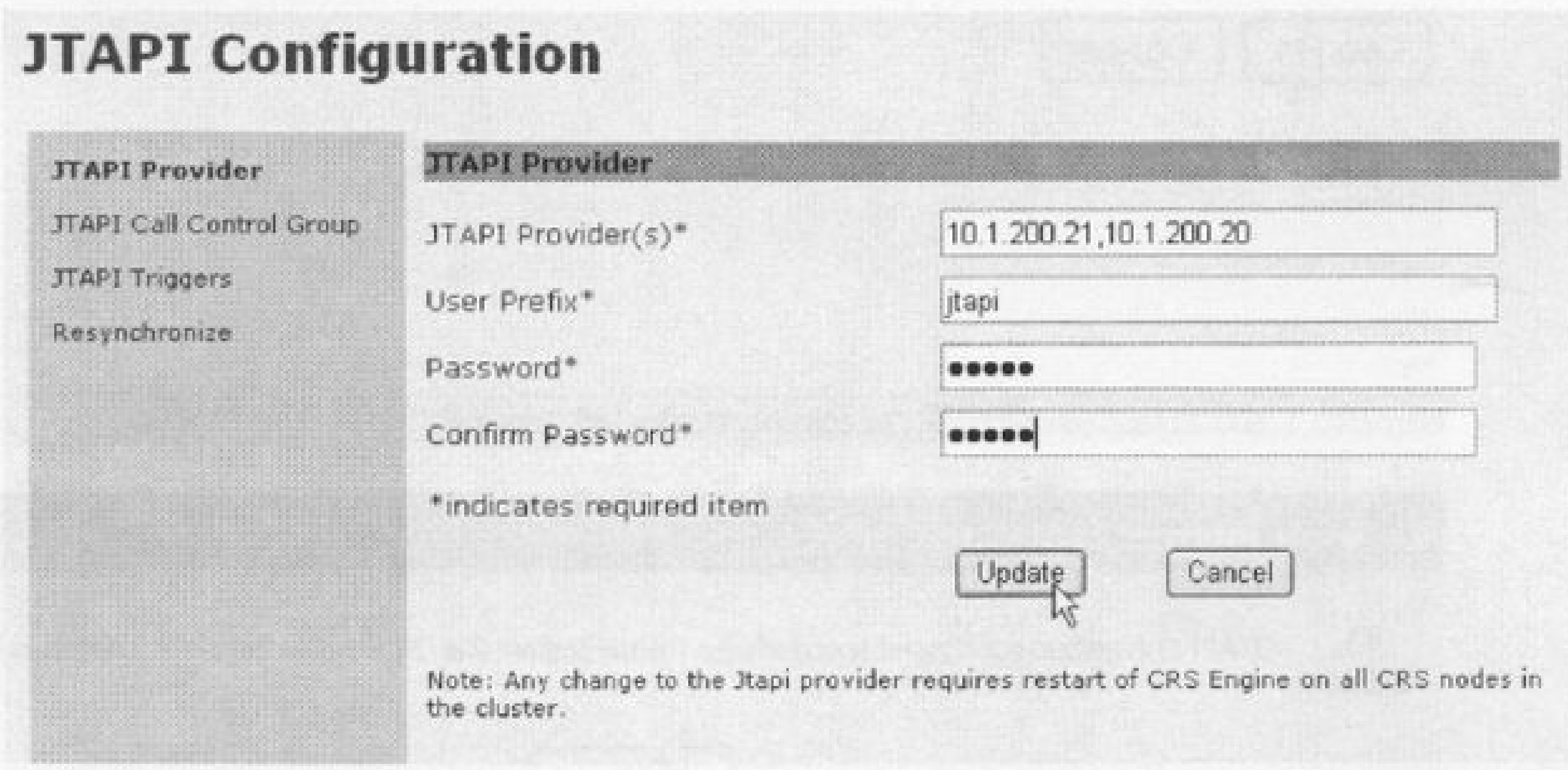
Start Stop Restart Reselect Master

Auto-refresh every 5 seconds.

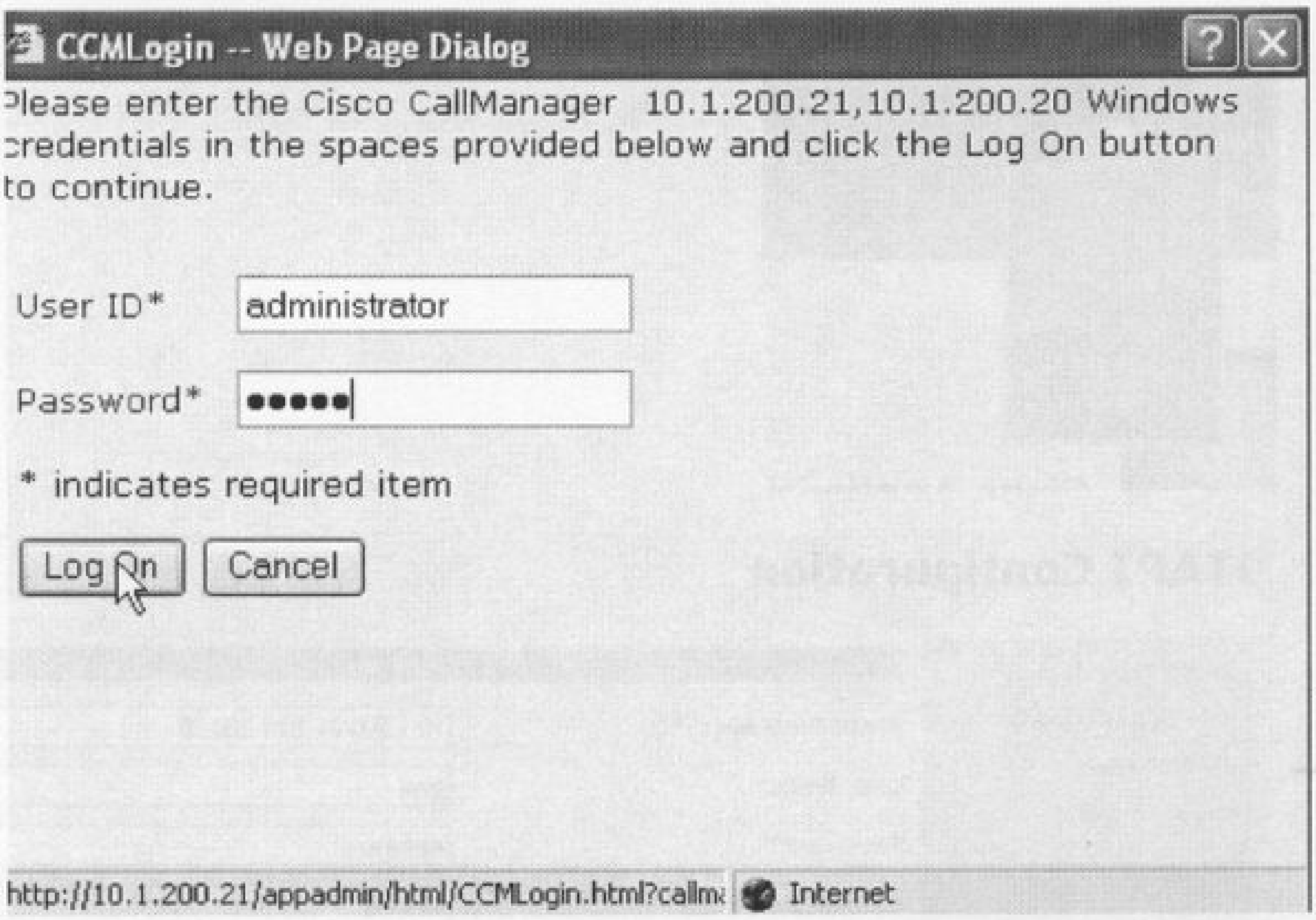
Service Name	Status	Last Failure	Info
Cisco Desktop Call/Chat Service	▶	-	
Cisco Desktop Enterprise Service	▶	-	
Cisco Desktop IP Phone Agent Service	▶	-	
Cisco Desktop LDAP Monitor Service	▶	3/26/06 12:46 PM	
Cisco Desktop License and Resource Manager Service	▶	-	
Cisco Desktop Recording & Statistics Service	▶	-	
Cisco Desktop Recording Service	▶	-	
Cisco Desktop Sync Service	▶	-	
Cisco Desktop VoIP Monitor Service	▶	-	
CRS Administration	▶	3/12/06 12:09 PM	
CRS Cluster View Daemon	▶	3/12/06 12:09 PM	
CRS Editor	■	-	
CRS Engine	▶	-	
CRS SQL Server - Agent	▶	-	
CRS SQL Server - Config	▶	-	
CRS SQL Server - Historical	▶	-	
CRS SQL Server - Repository	▶	-	
Microsoft Distributed Transaction Coordinator	▶	-	
Microsoft SQL Agent	▶	-	

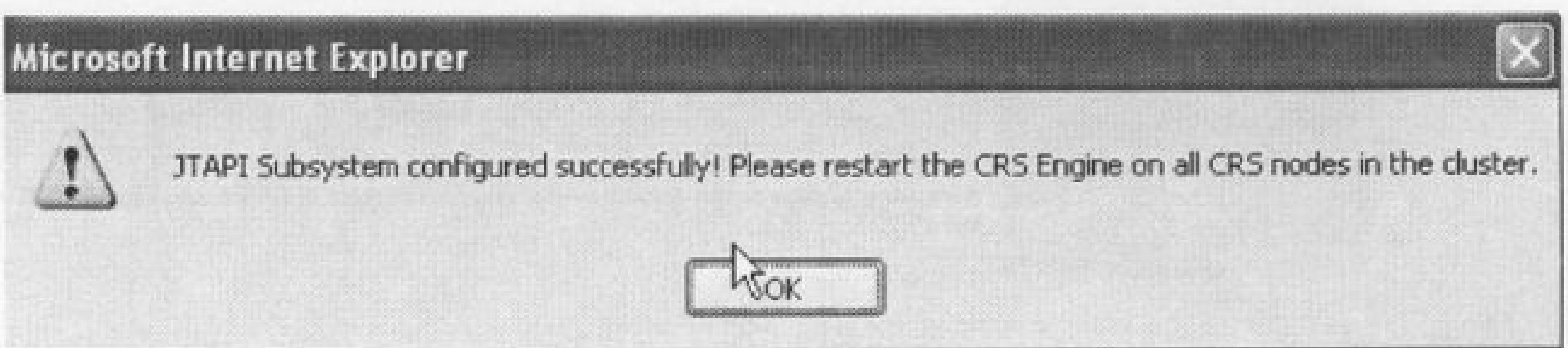
➔ **To configure the JTAPI Provider go to Application Administrator-subsystems➔ JTAPI enter the ip address of the servers running CTI Manager (always Sub then Pub).**



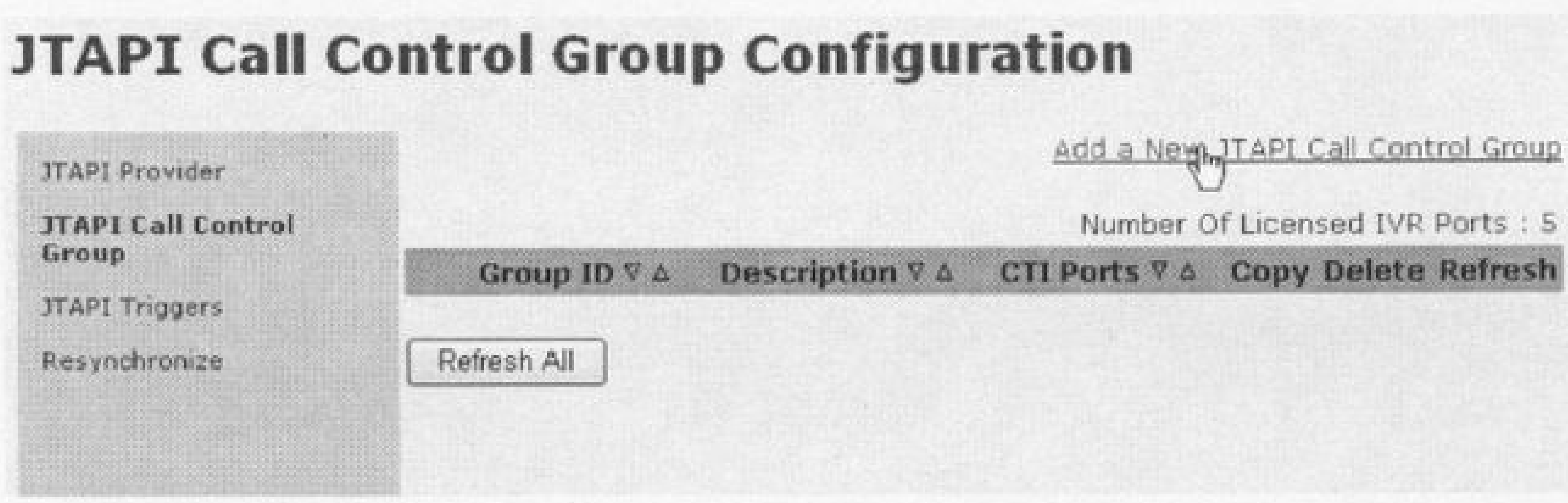


➔ **Now we need to enter the User/Pass of the Admin to authenticate against the CCM so that the IPCC engine can create everything we need in terms of CTI Ports and CTI Route Points for us.**

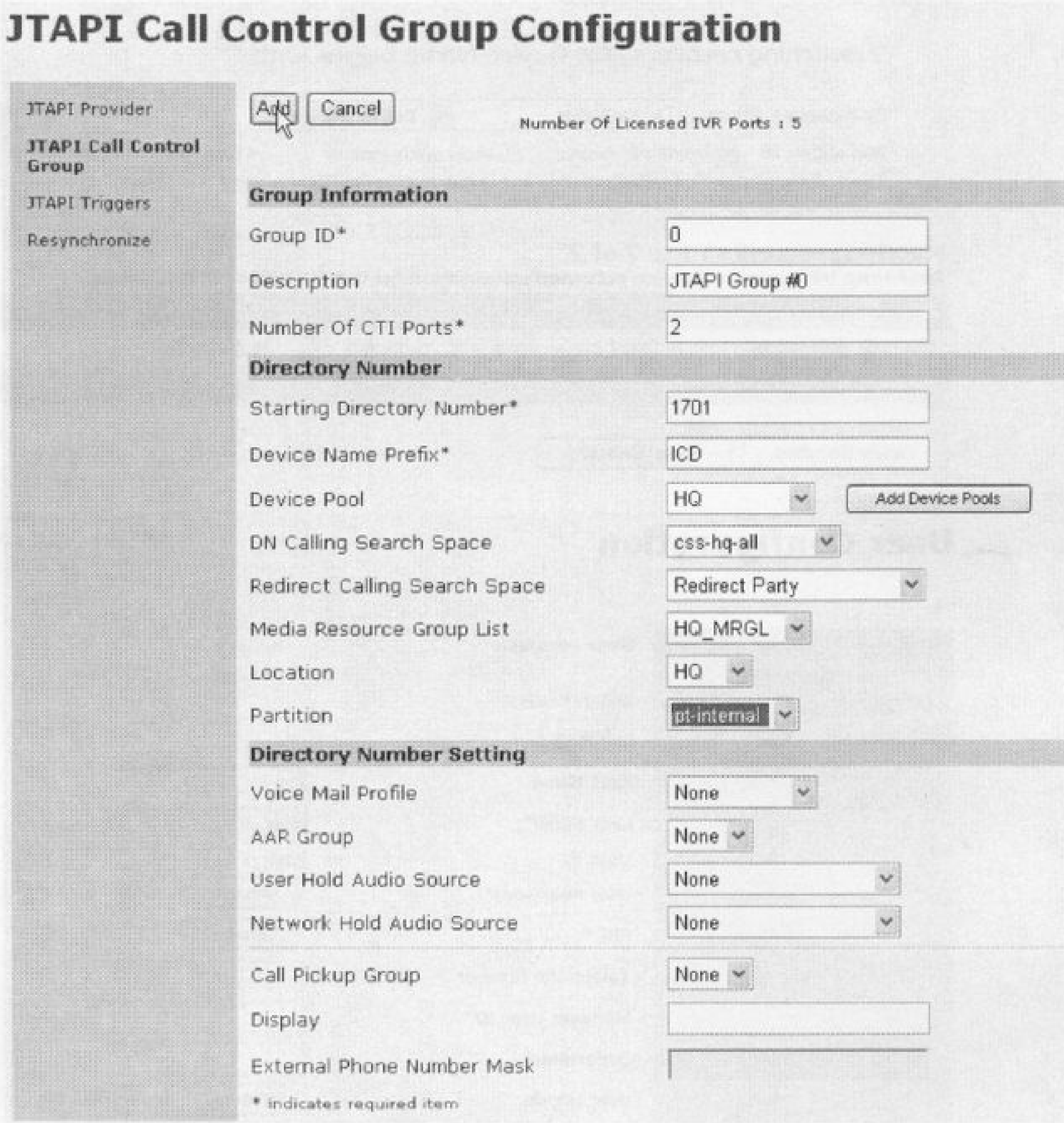




➔ **After we restart the Engine, we will create a Call Control Group on the IPCCX (this will create and be our CTI Ports on CCM) for each application that we have (only one set for one app is pictured here).**

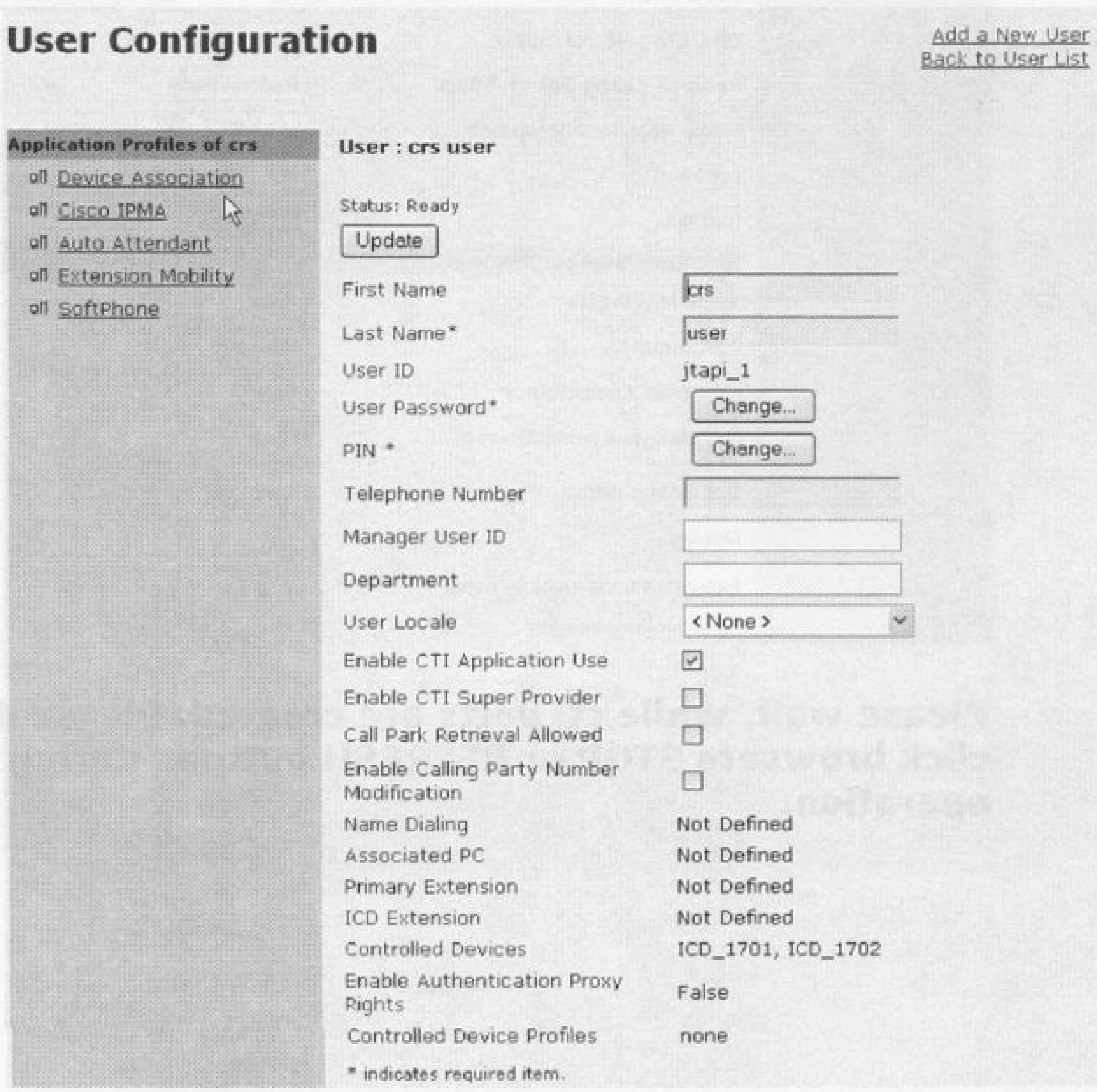


➔ **Remember to include everything you would normally include for a CTI Port on CCM – since you are ONLY creating this here on the IPCCX (it will be done for you on the CCM server) – we need to remember things like CAC, DP, CSS, Partition, etc.**

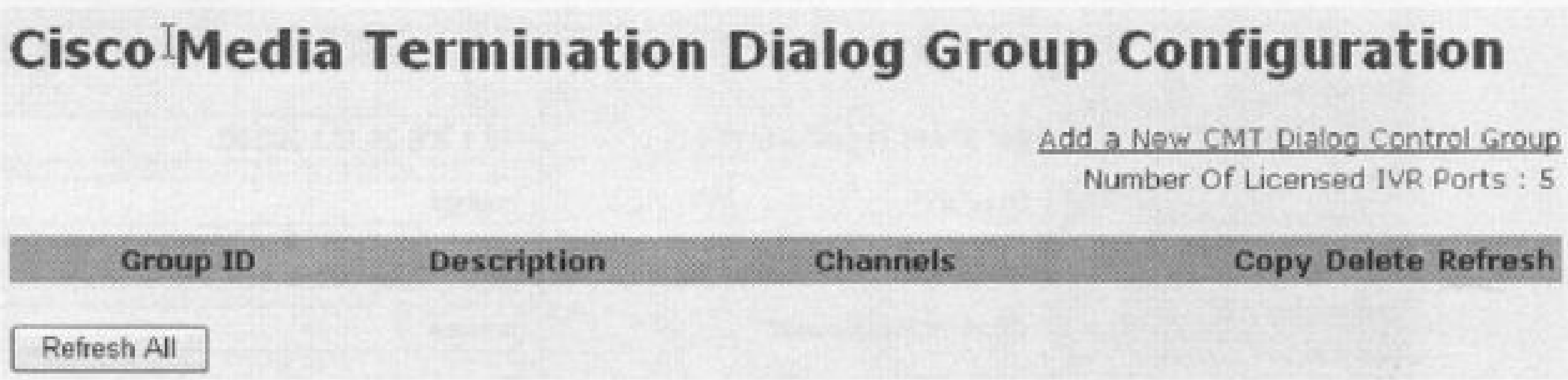


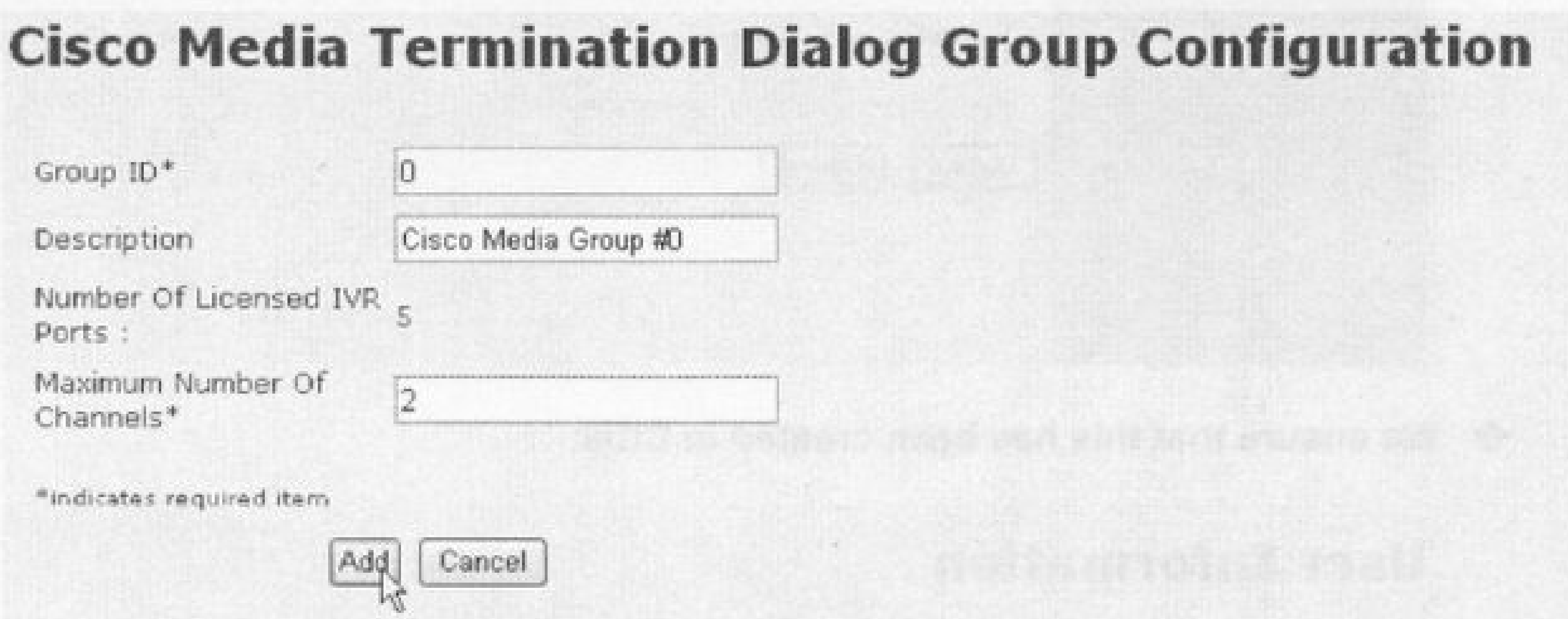
Please wait, while cti ports are created. Please do not click browsers STOP or REFRESH buttons during this operation.

➔ **If we were to go over to the CCM and do a search, we will find the CTI Ports created, and a JTAPI user setup with Device Associations to the CTI Ports and later automatically to the CTI Route Points as well.**

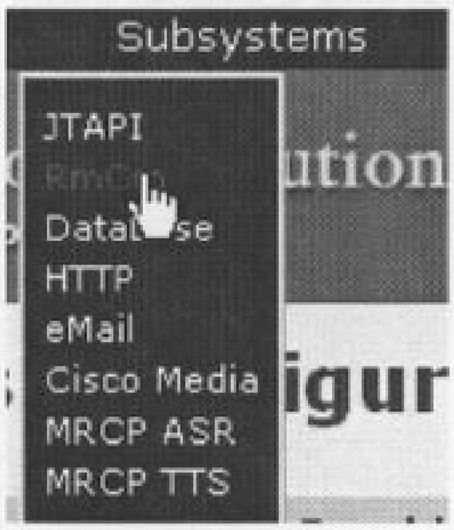


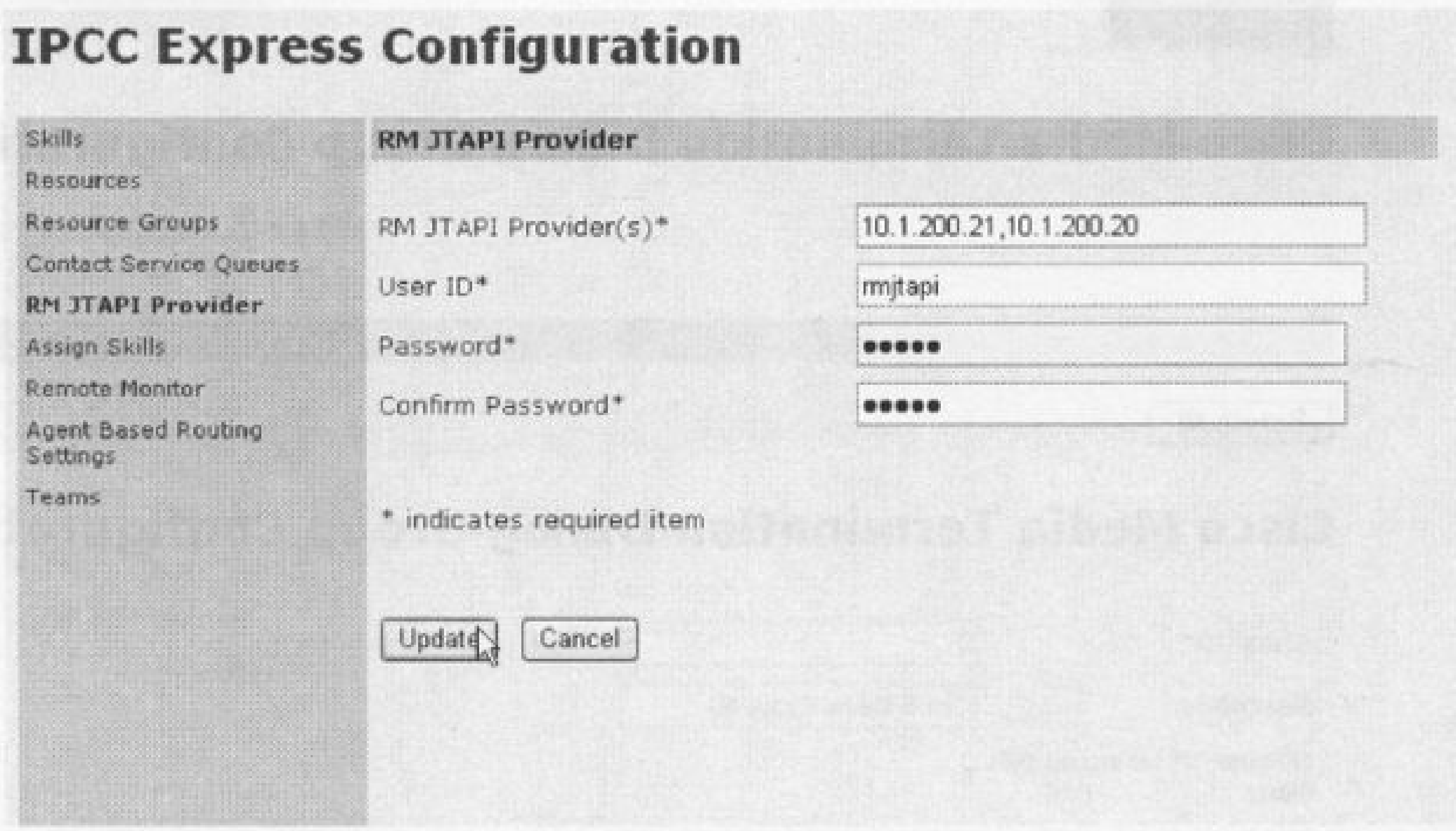
➔ **Now it is time to setup the Media Groups – think of this as a mirror image to the CTI Ports (CallControlGroups) but on the IPCCX side of things – we need to have at least as many of them as we do CTI Ports – so we will create 2 sets of these as well – 1 set for each application.**



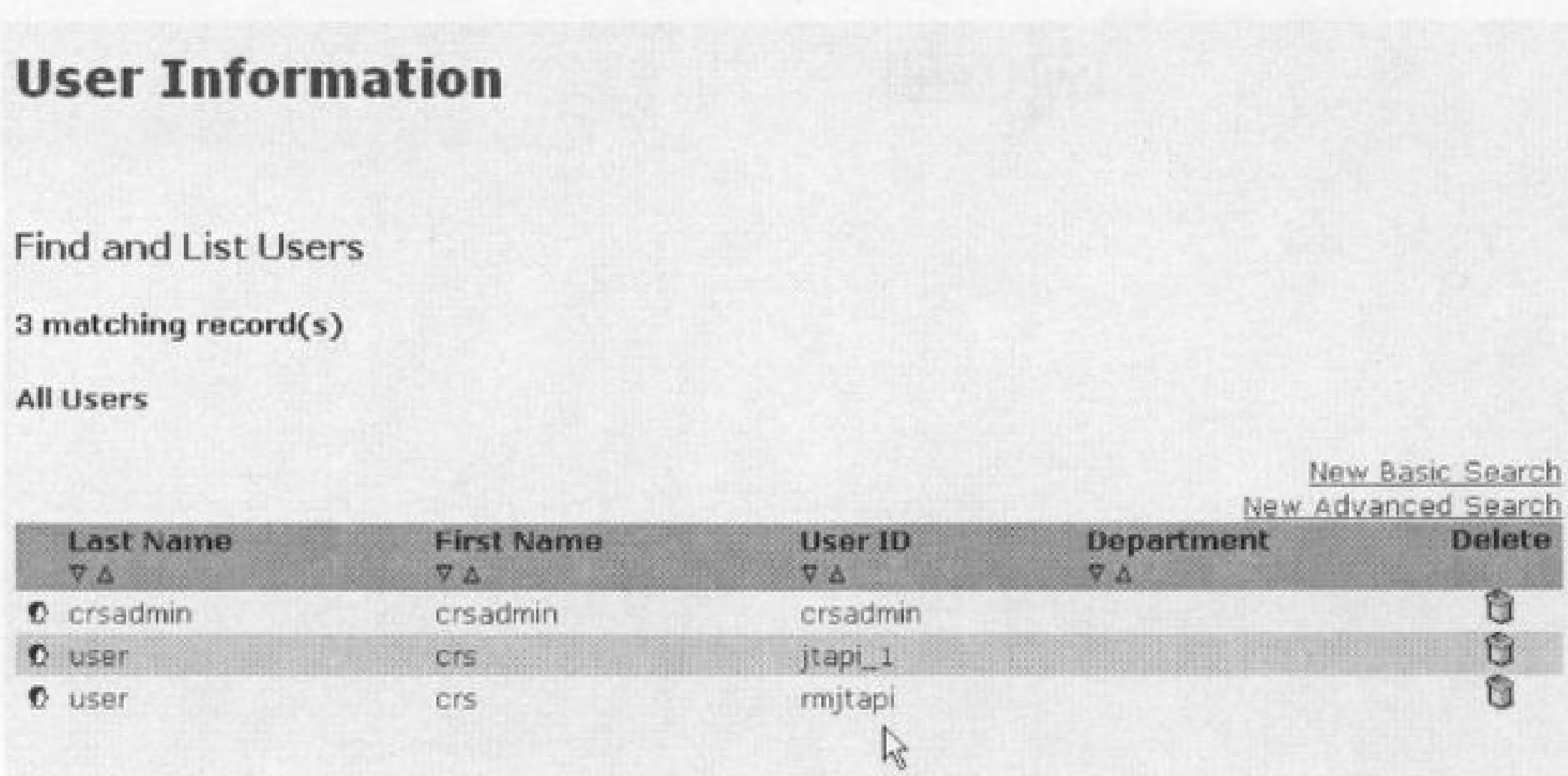


➔ **Now it is time to configure the RmCm Subsystem for the providers, Skills, Queue, and options we wish:**

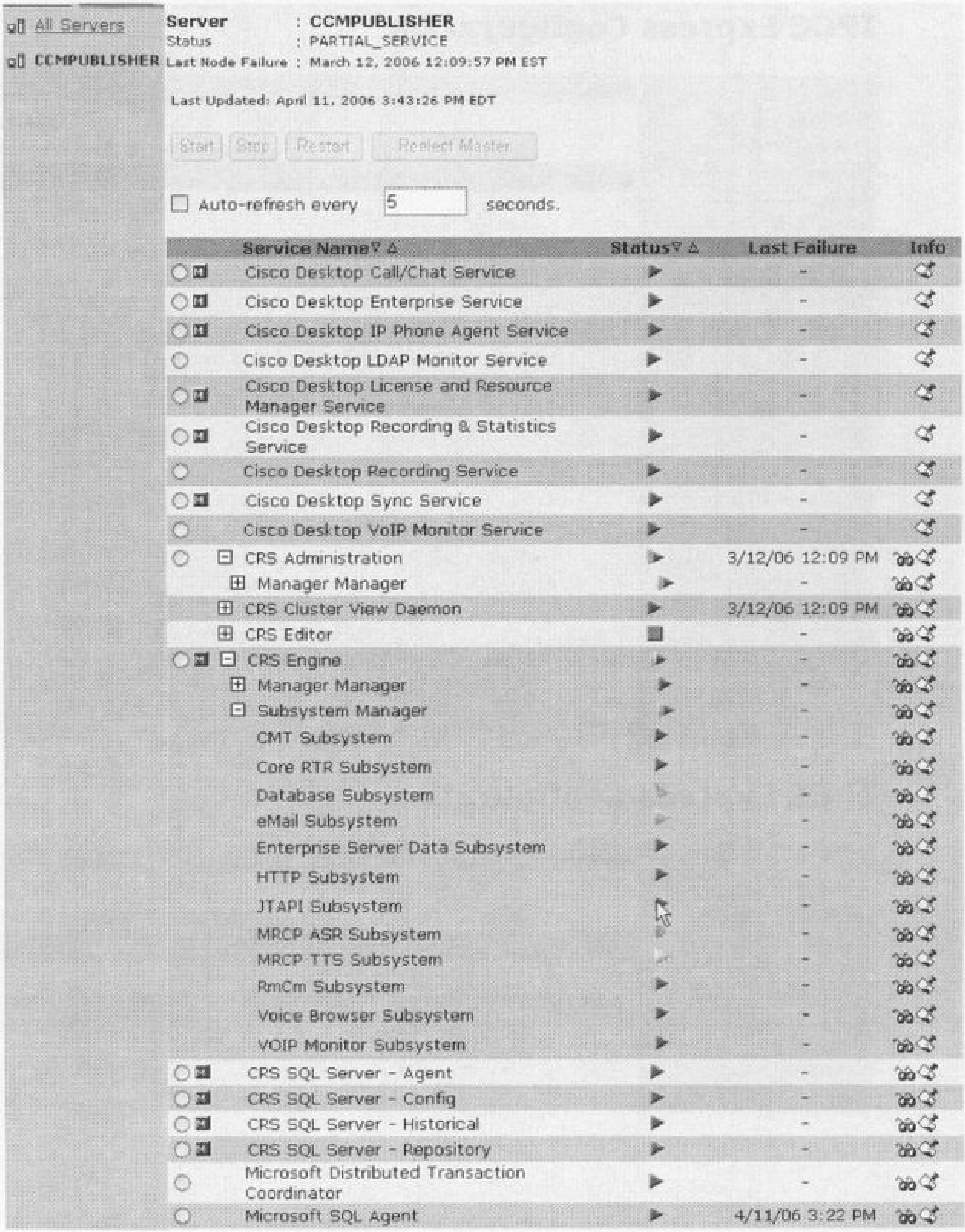




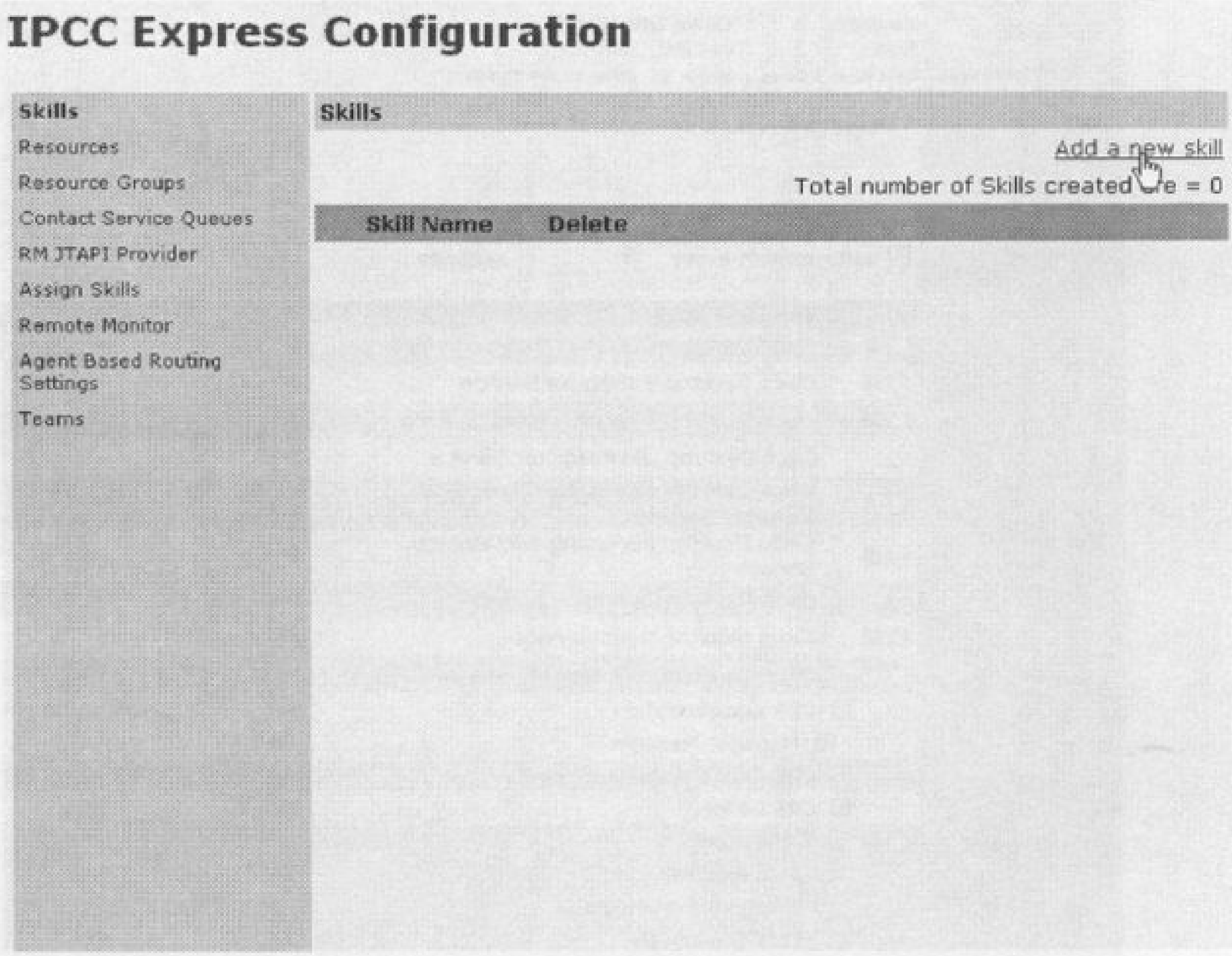
➔ **We ensure that this has been created in CCM:**

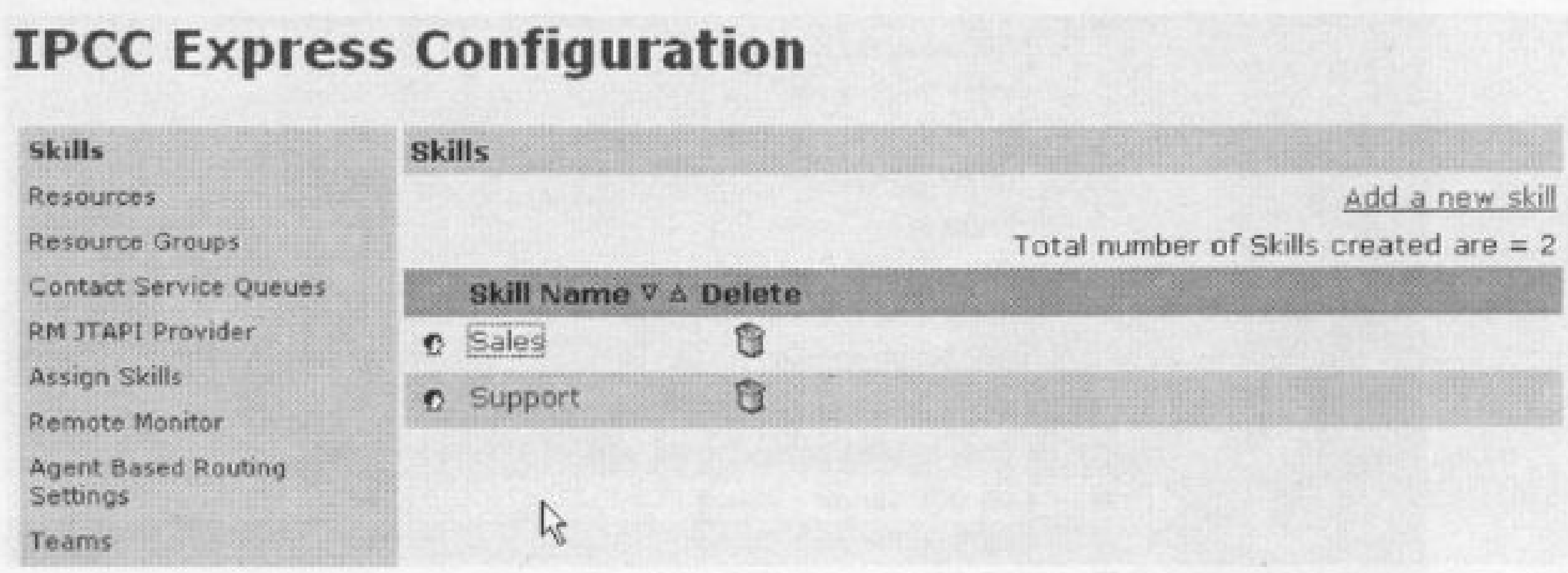


➔ **Before continuing, ensure that the Subsystems are started properly:**

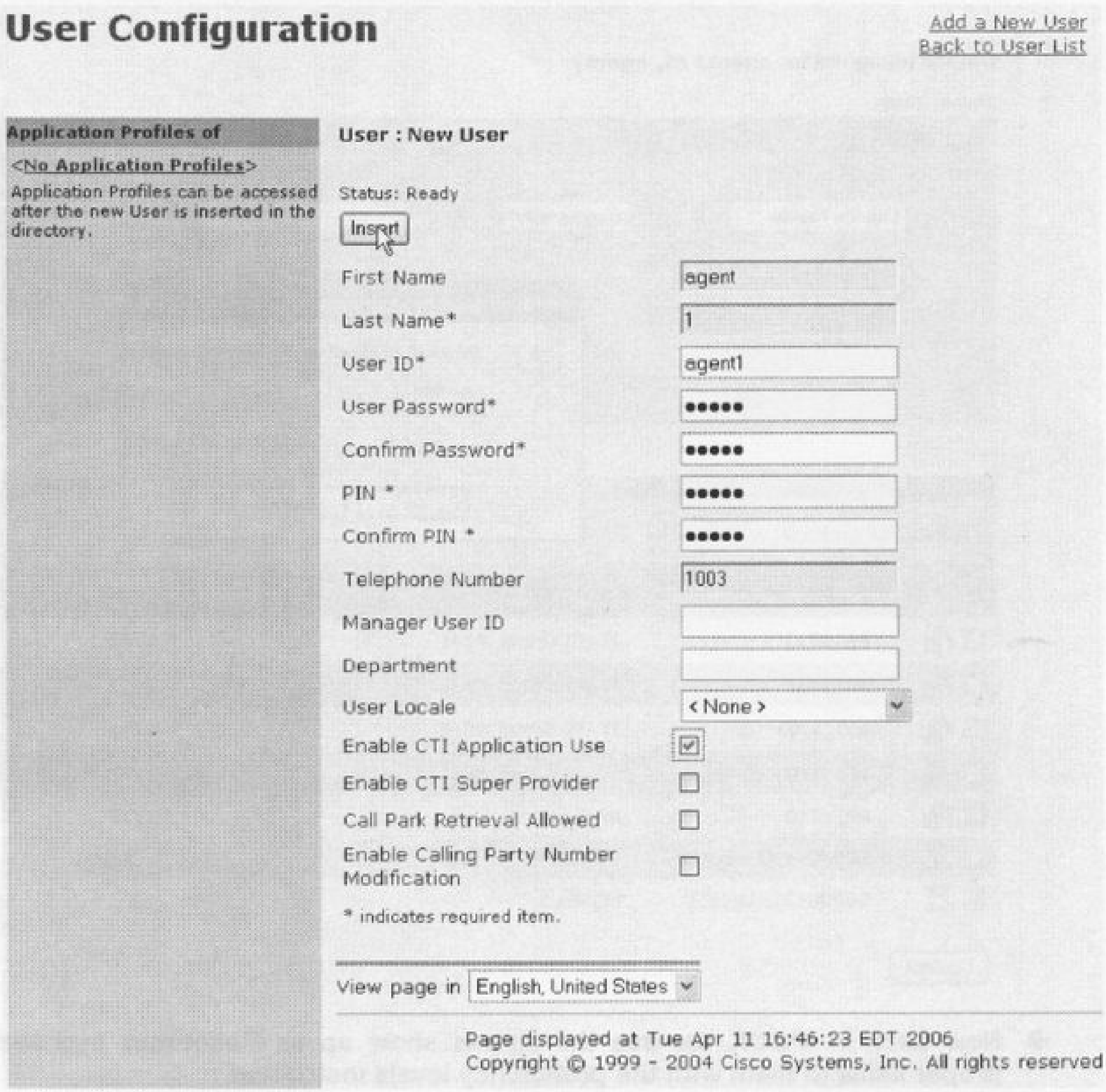


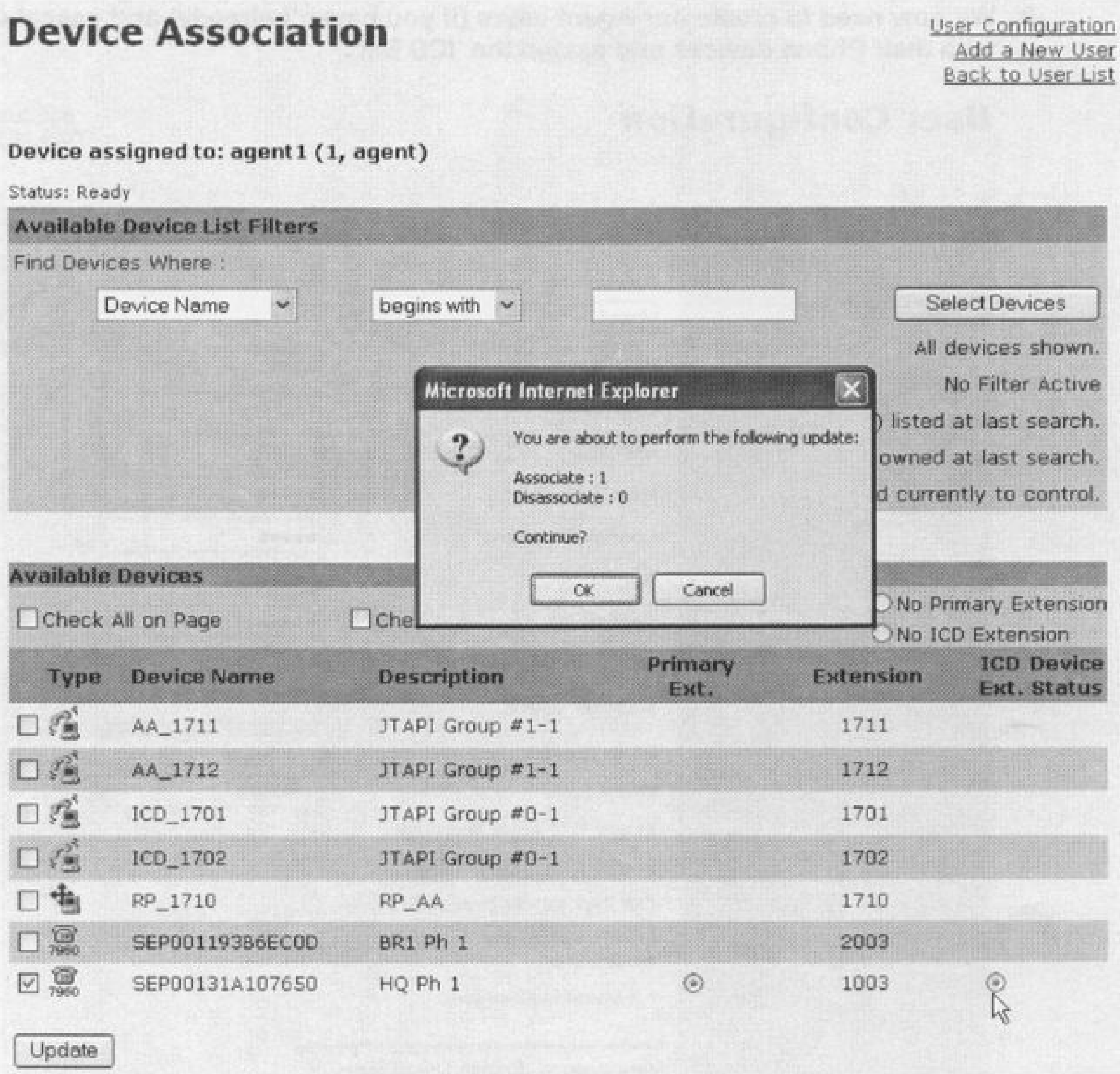
➔ **Now it is time to create our Skills of 'sales' and 'support'.**



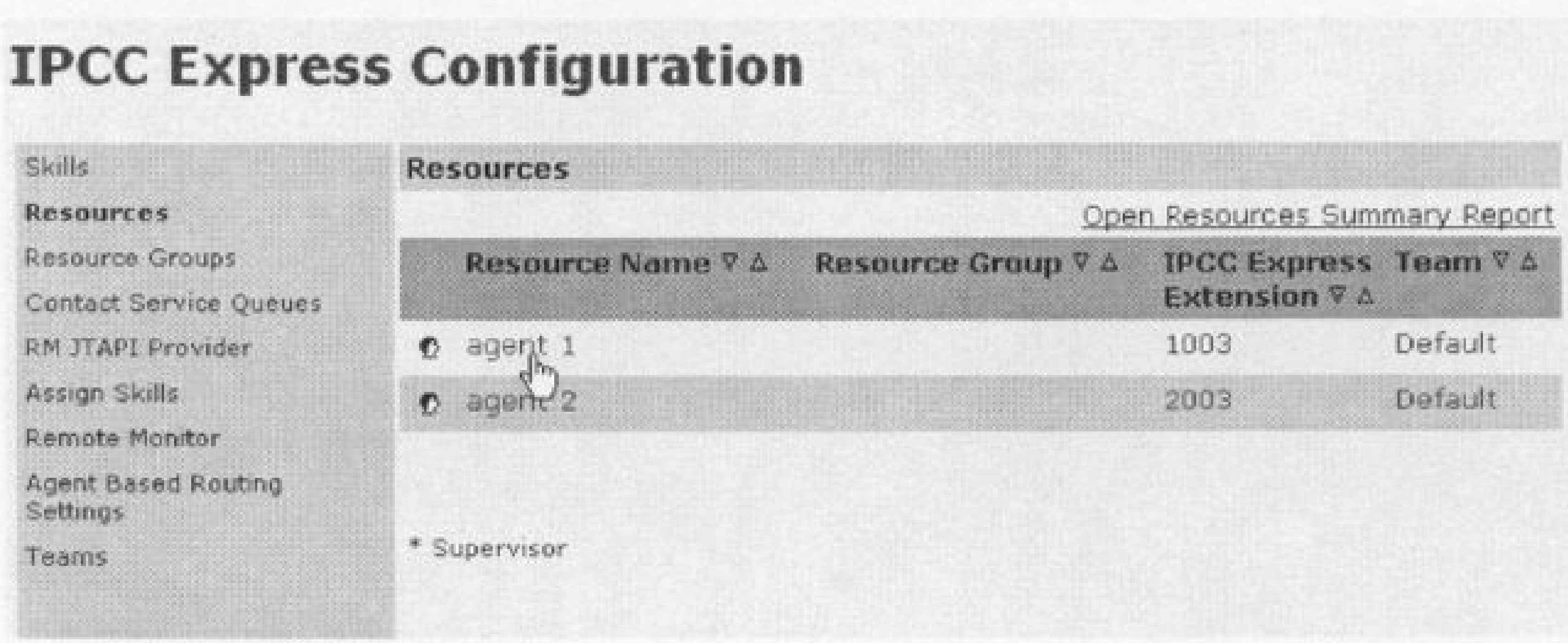


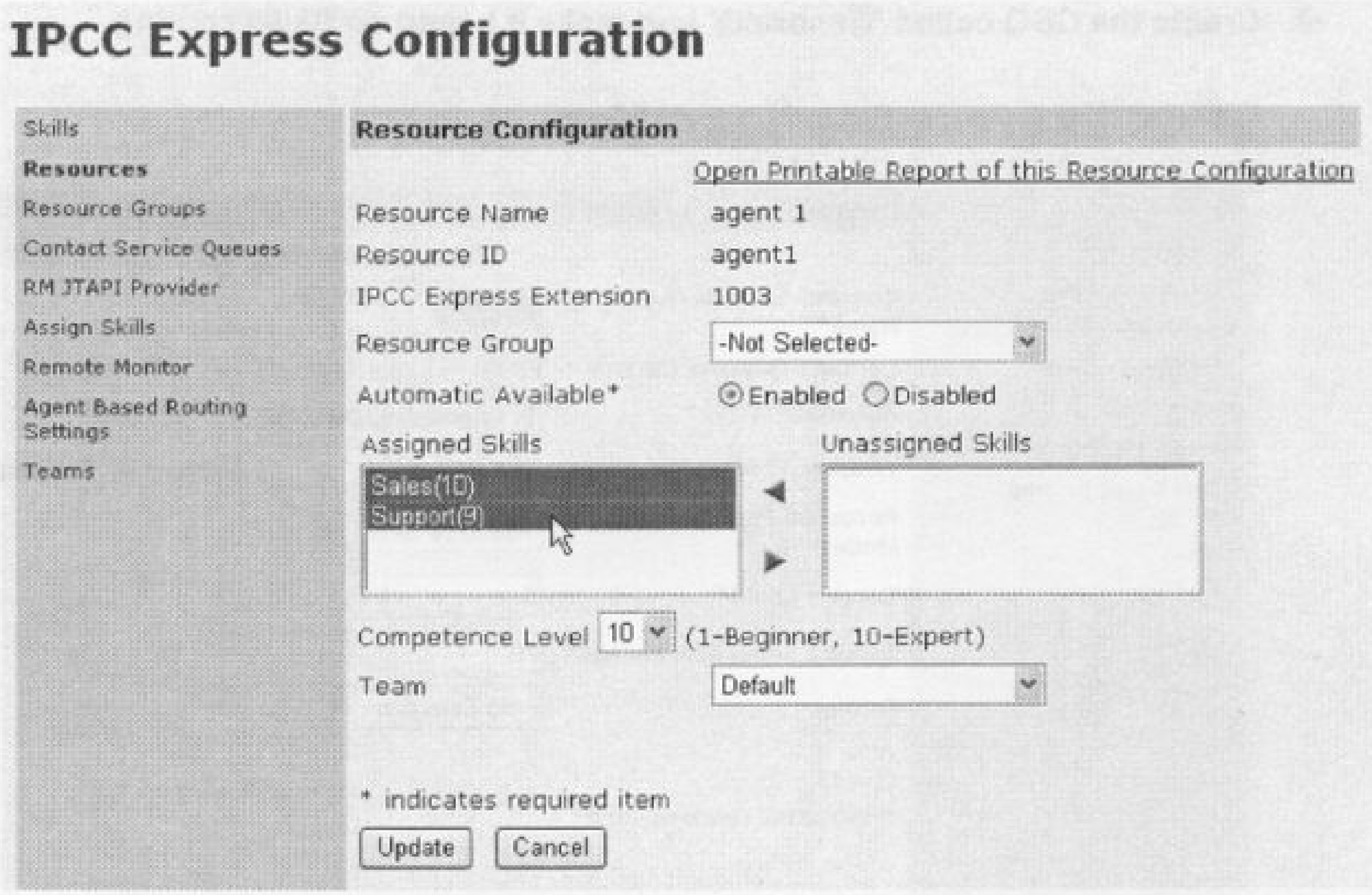
➔ **We now need to create our Agent users (if you haven't already) and associate them with their Phone devices and assign the 'ICD Ext'.**

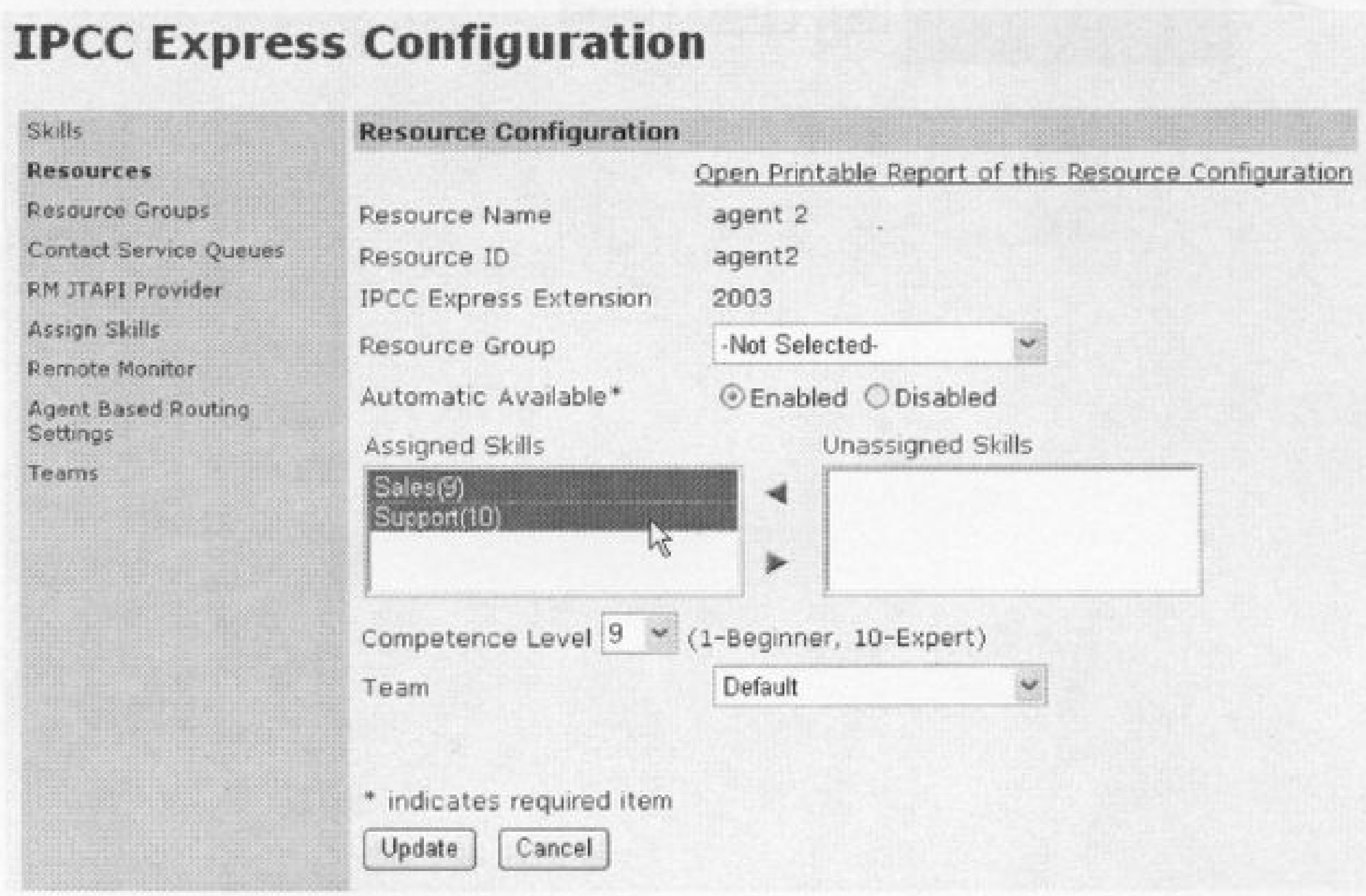




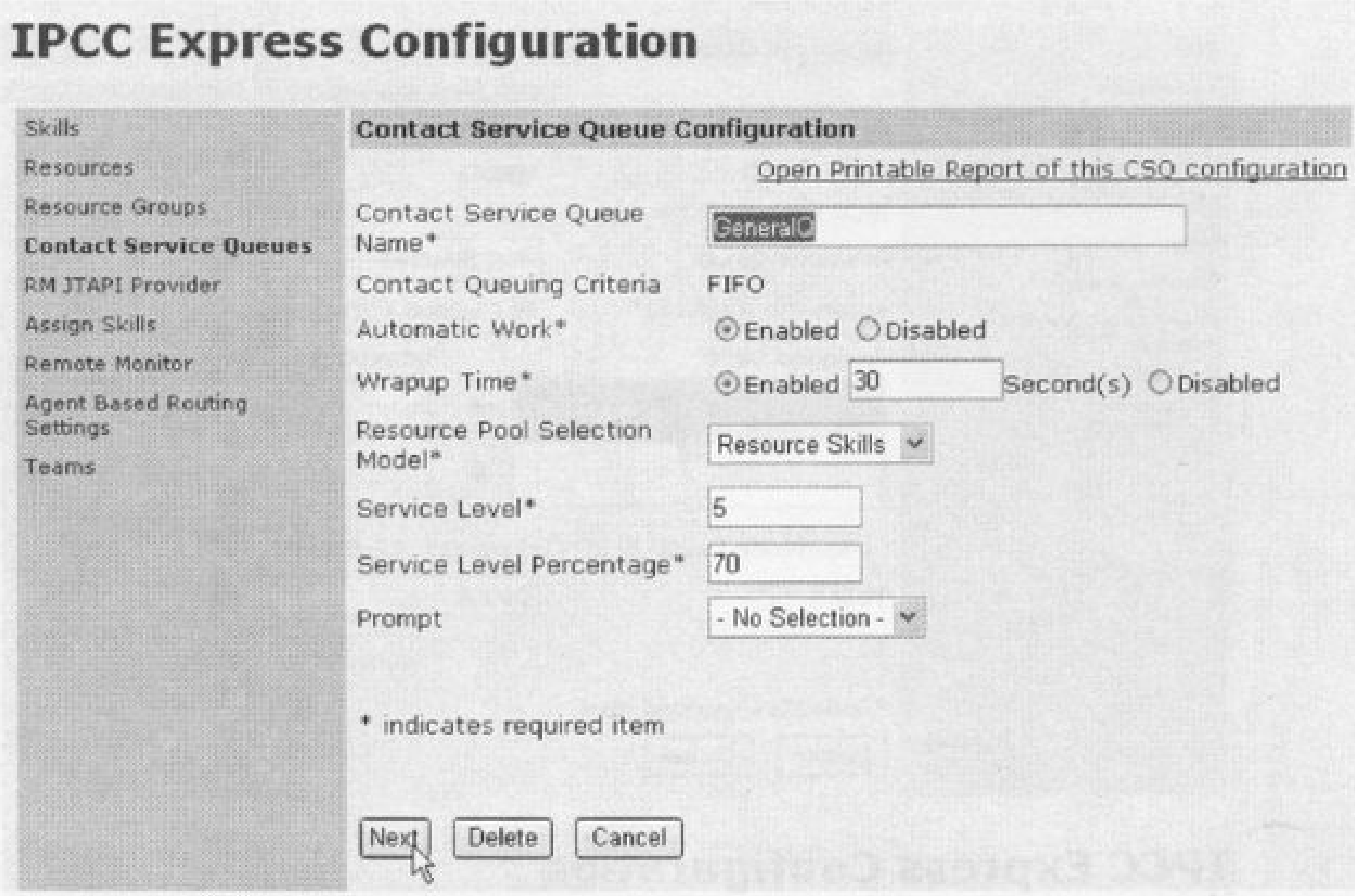
➔ **Now back in IPCCX, we see the agents show up as Resources and assign the proper skills to them with the proficiency levels instructed.**



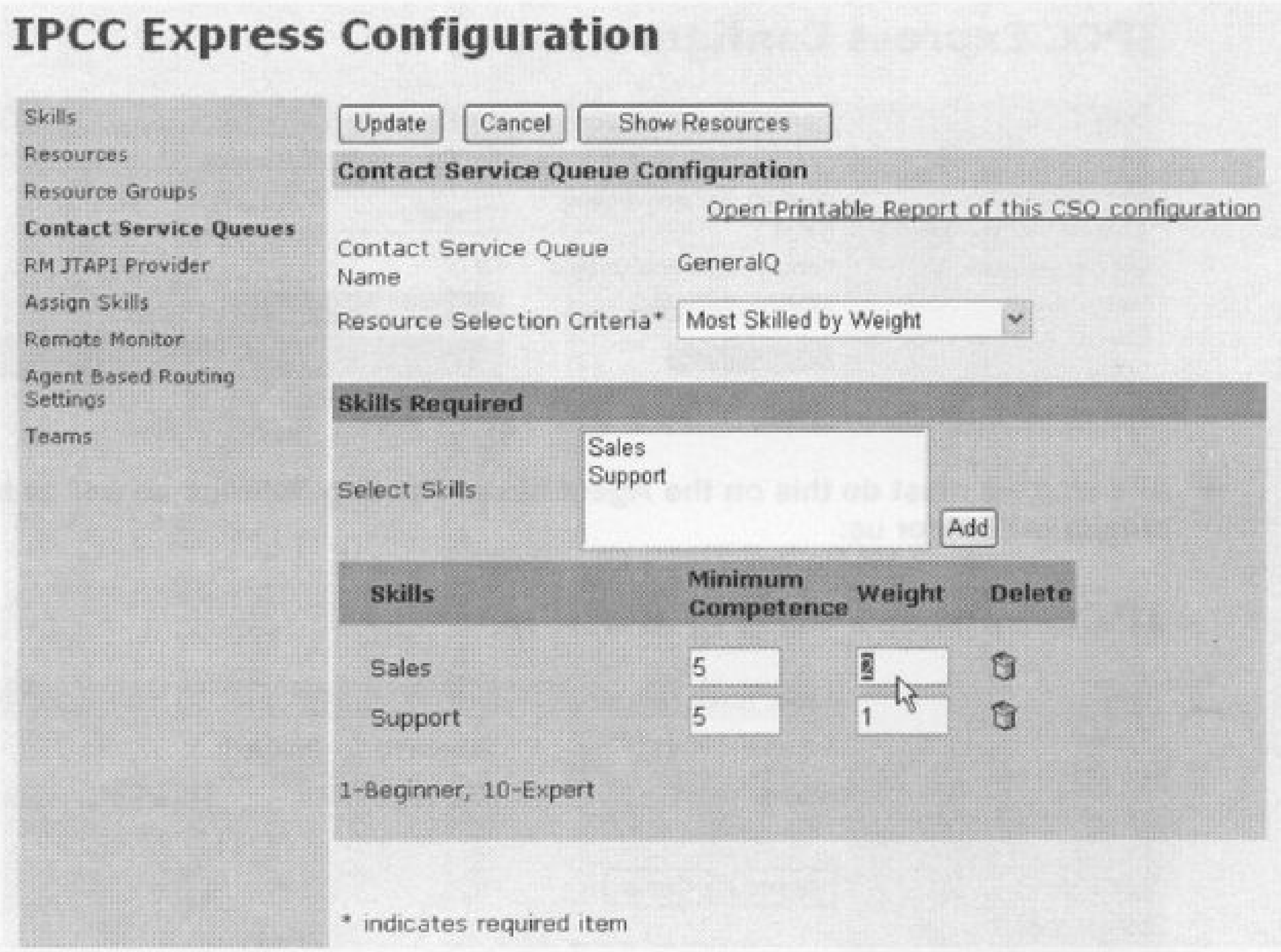

IPCC Express Configuration
Skills
Resources
Resource Groups
Contact Service Queues
RM JTAPI Provider
Assign Skills
Remote Monitor
Agent Based Routing Settings
Teams
Resource Configuration
Open Printable Report of this Resource Configuration
Resource Name agent 1
Resource ID agent1
IPCC Express Extension 1003
Resource Group -Not Selected-
Automatic Available* Enabled Disabled
Assigned Skills
Unassigned Skills
Sales(10)
Support(9)
Competence Level 10 (1-Beginner, 10-Expert)
Team Default
* indicates required item
Update
Cancel


IPCC Express Configuration
Skills
Resources
Resource Groups
Contact Service Queues
RM JTAPI Provider
Assign Skills
Remote Monitor
Agent Based Routing Settings
Teams
Resource Configuration
Open Printable Report of this Resource Configuration
Resource Name agent 2
Resource ID agent2
IPCC Express Extension 2003
Resource Group -Not Selected-
Automatic Available* Enabled Disabled
Assigned Skills
Unassigned Skills
Sales(9)
Support(10)
Competence Level 9 (1-Beginner, 10-Expert)
Team Default
* indicates required item
Update
Cancel

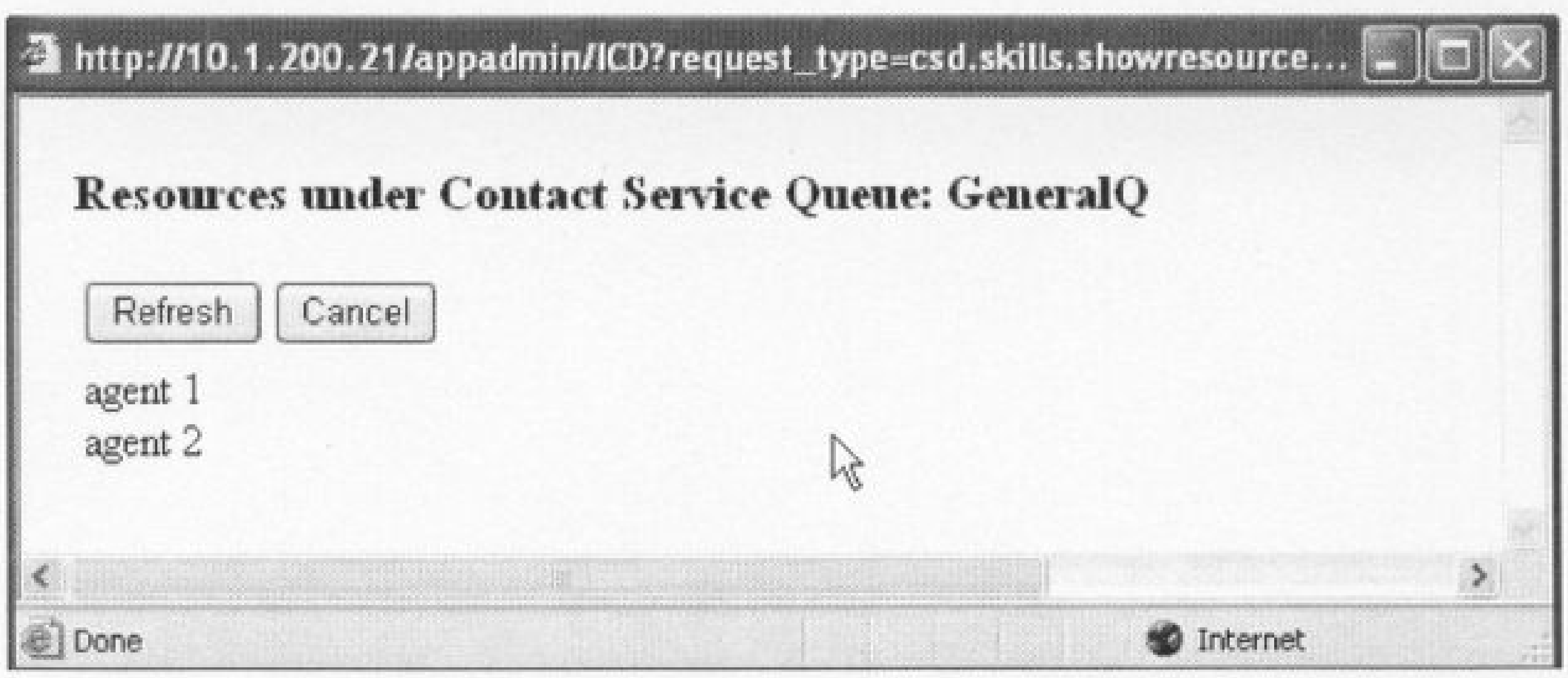
→ **Create the CSQ called 'GeneralQ' and make it based on Skills routing.**



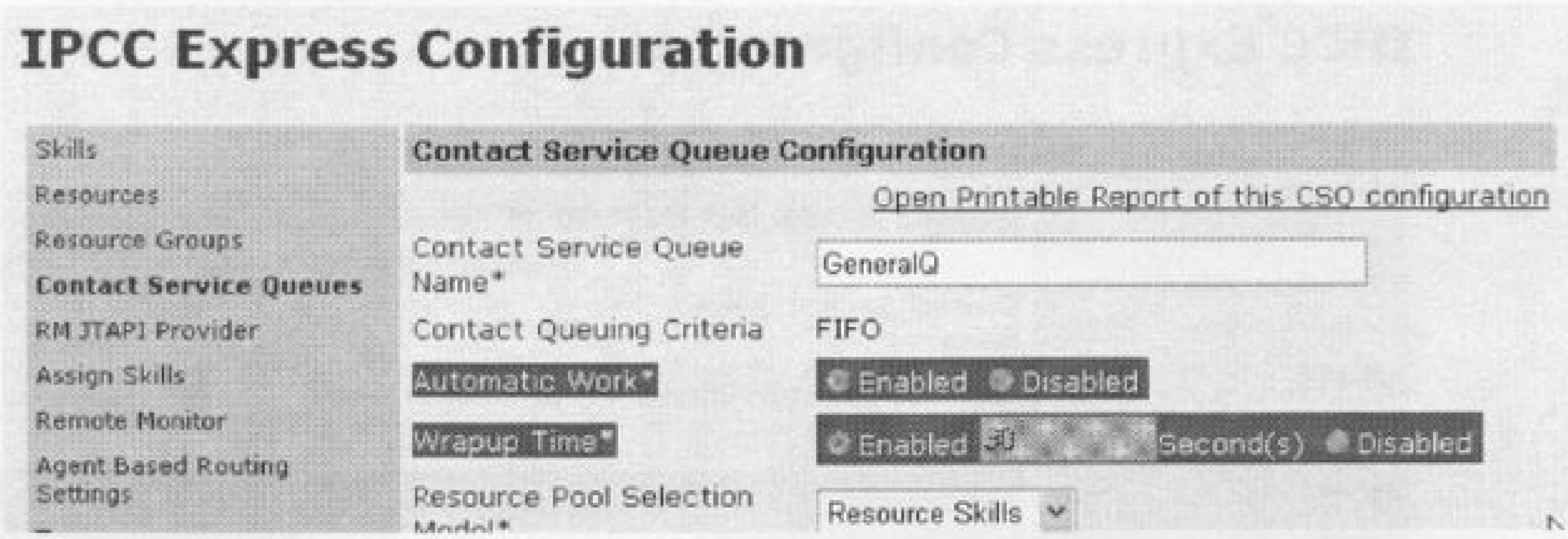
➔ **There are a few ways that we can make Agent 1 win out over Agent 2 but in this case we choose to use the 'Most Skilled by Weight' and weight Sales over Support – 2:1.**



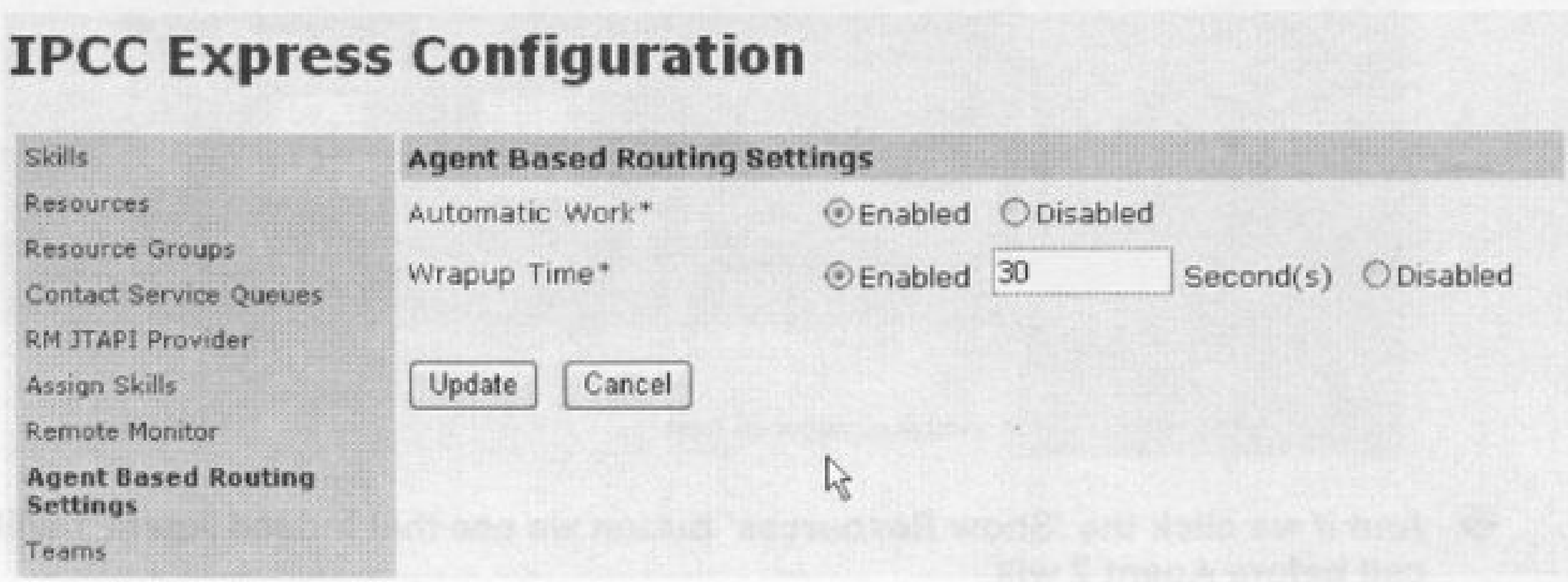
➔ **And if we click the 'Show Resources' button we see that indeed Agent 1 will get the call before Agent 2 will.**



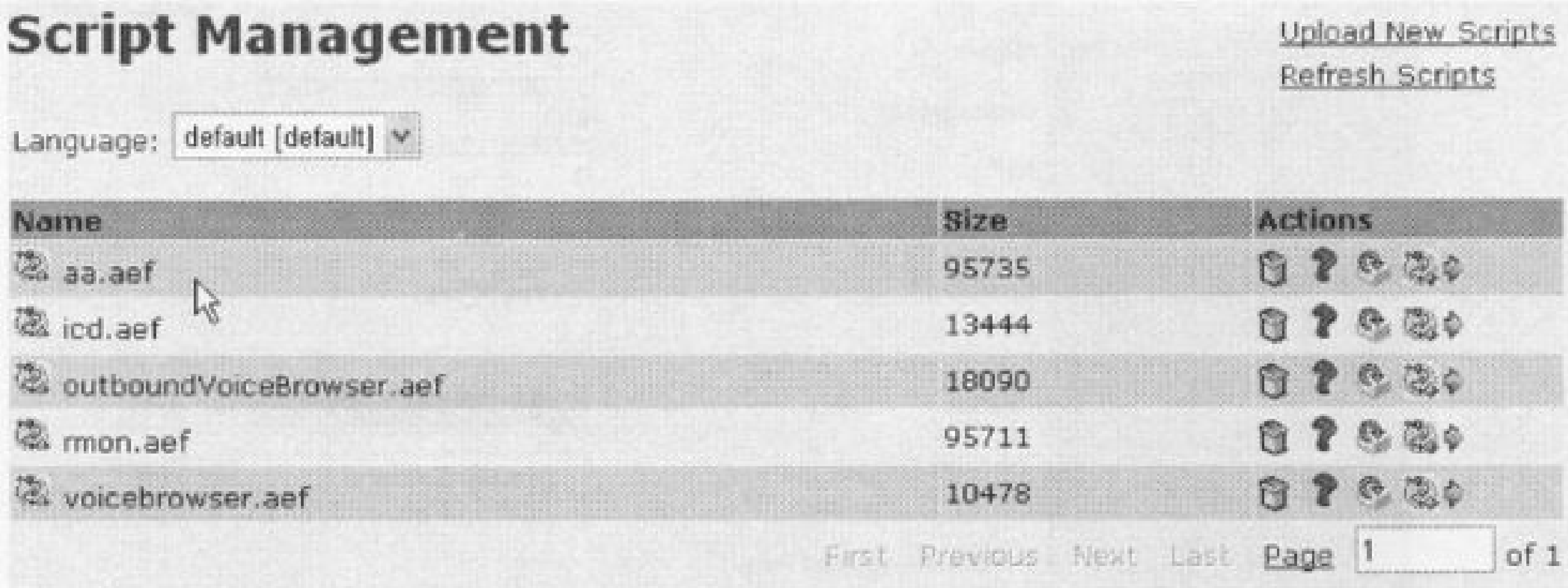
➔ **To ensure that the agent goes into a state of Work but only for 30 seconds before automatically going back to a state of Ready we configure the following under the Contact Service Queues section:**



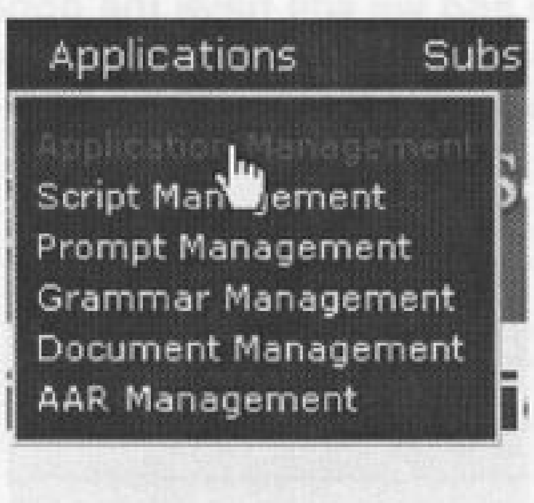
➔ **And also we must do this on the Agent based Routing Settings as well to meet the criteria set out for us:**

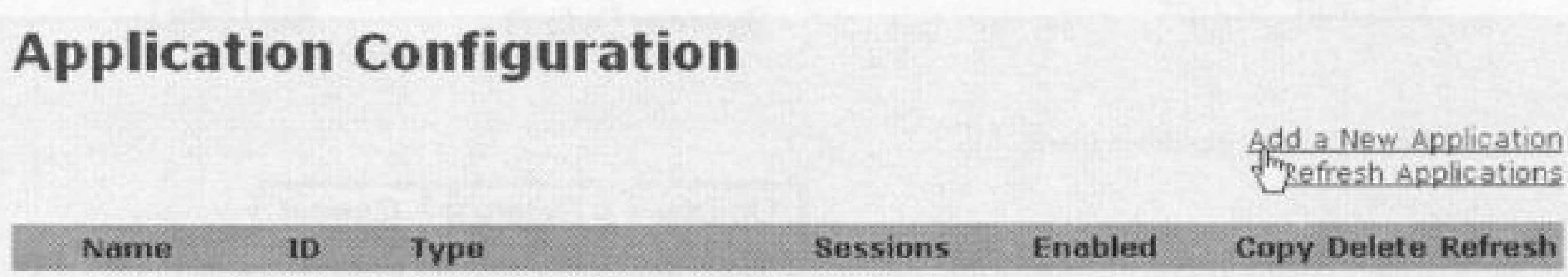


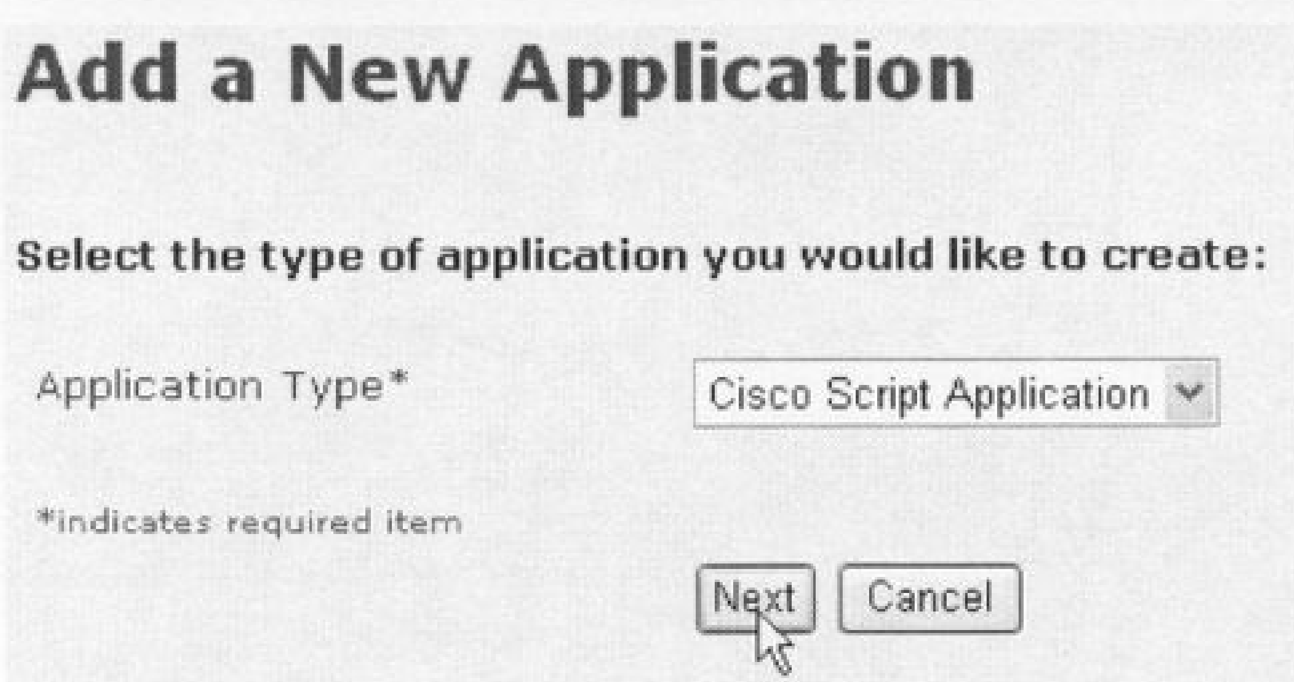
➔ **We are now ready to take a look at the scripts in the Script Management section found under the Applications drop-down.**

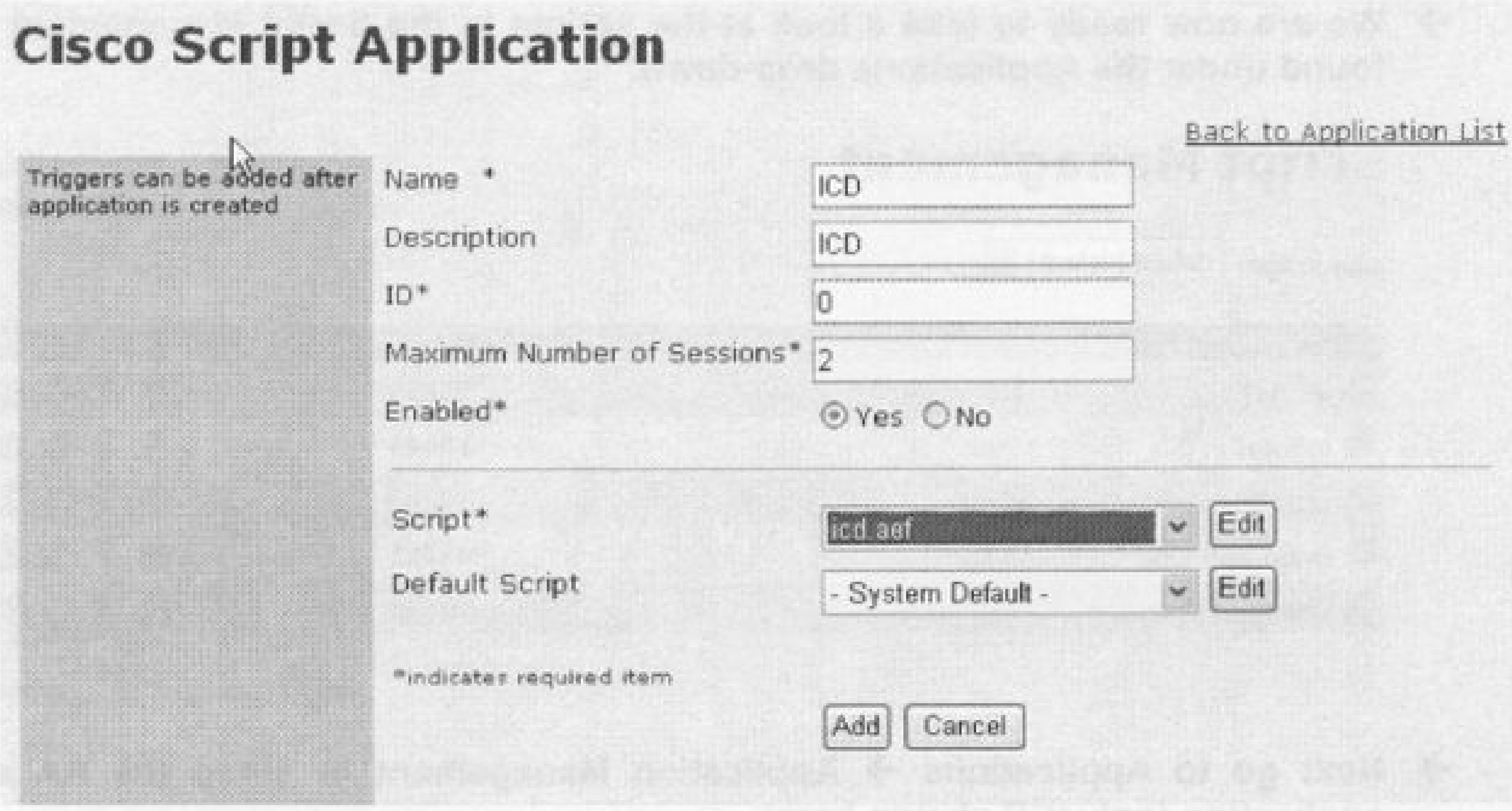


➔ **Next go to Applications ➔ Application Management to setup the AA and ICD application (only ICD shown here).**

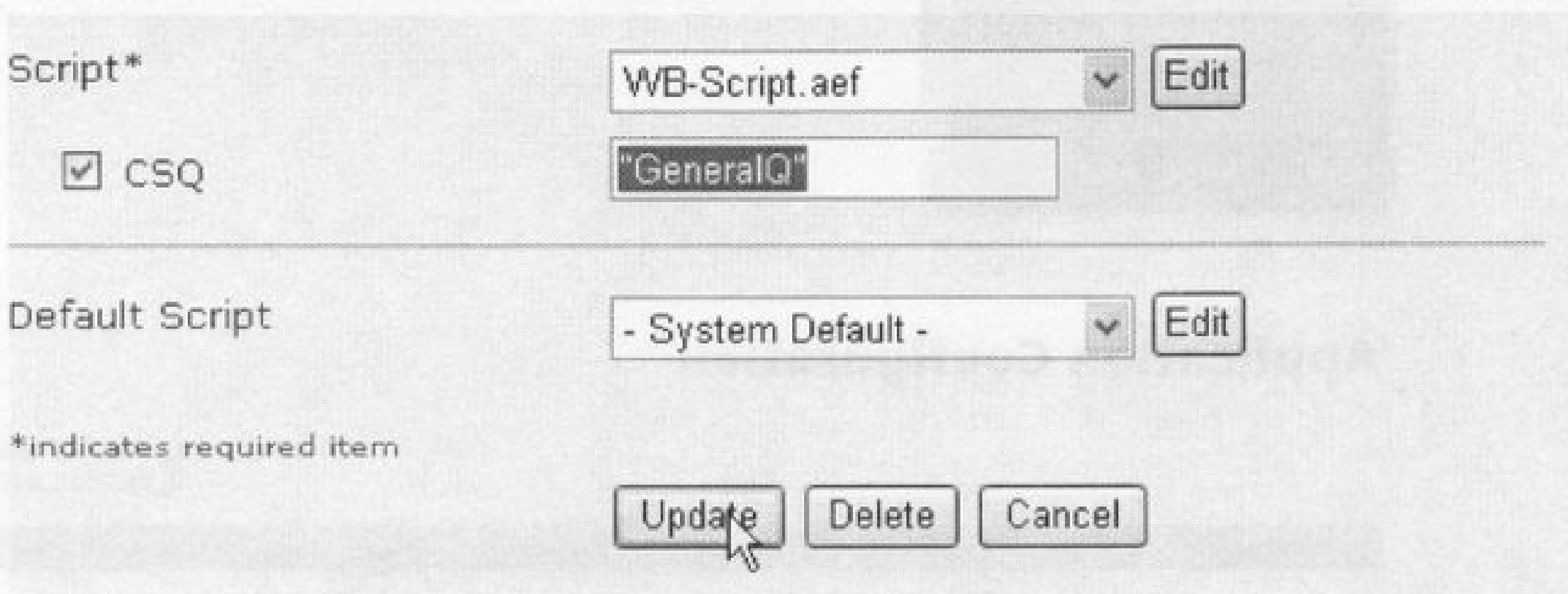




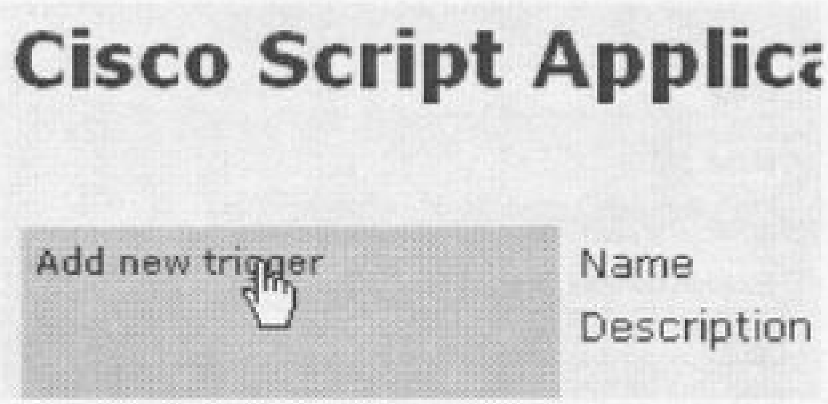


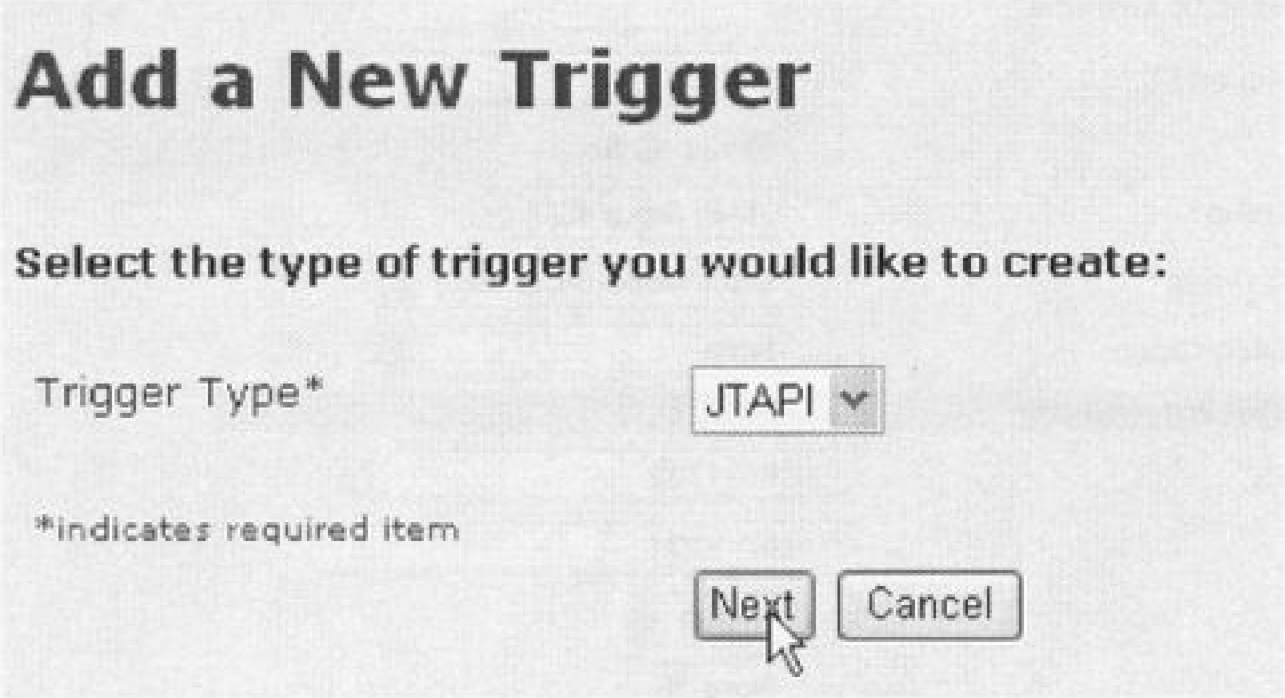


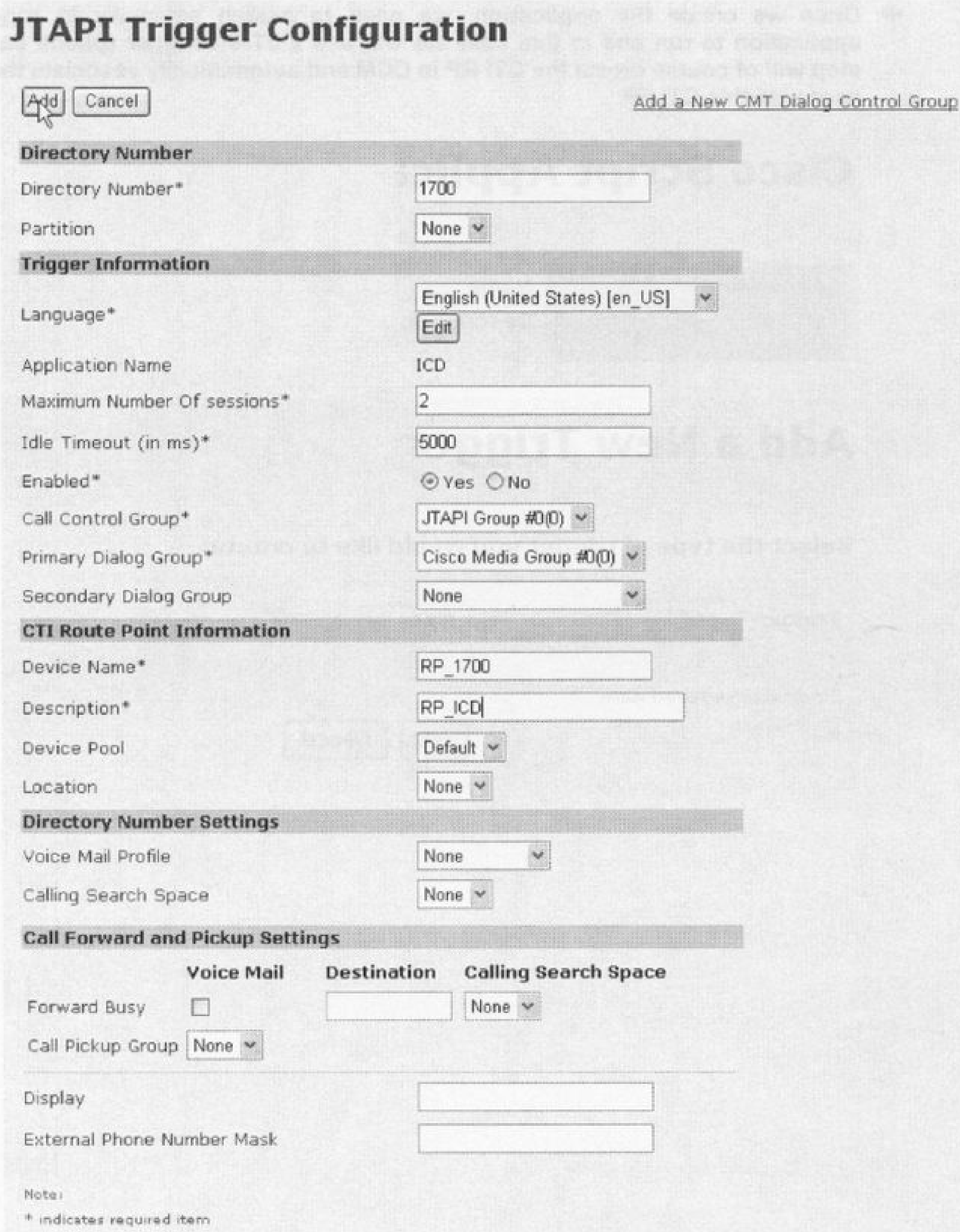
➔ **After we assign the Script – the page will refresh and we will have the opportunity to assign variables that were specified as 'Parameters' in the script – in this case – the name of the CSQ (which must of course match exactly the CSQ name that we previously setup in the RmCm Subsystem).**



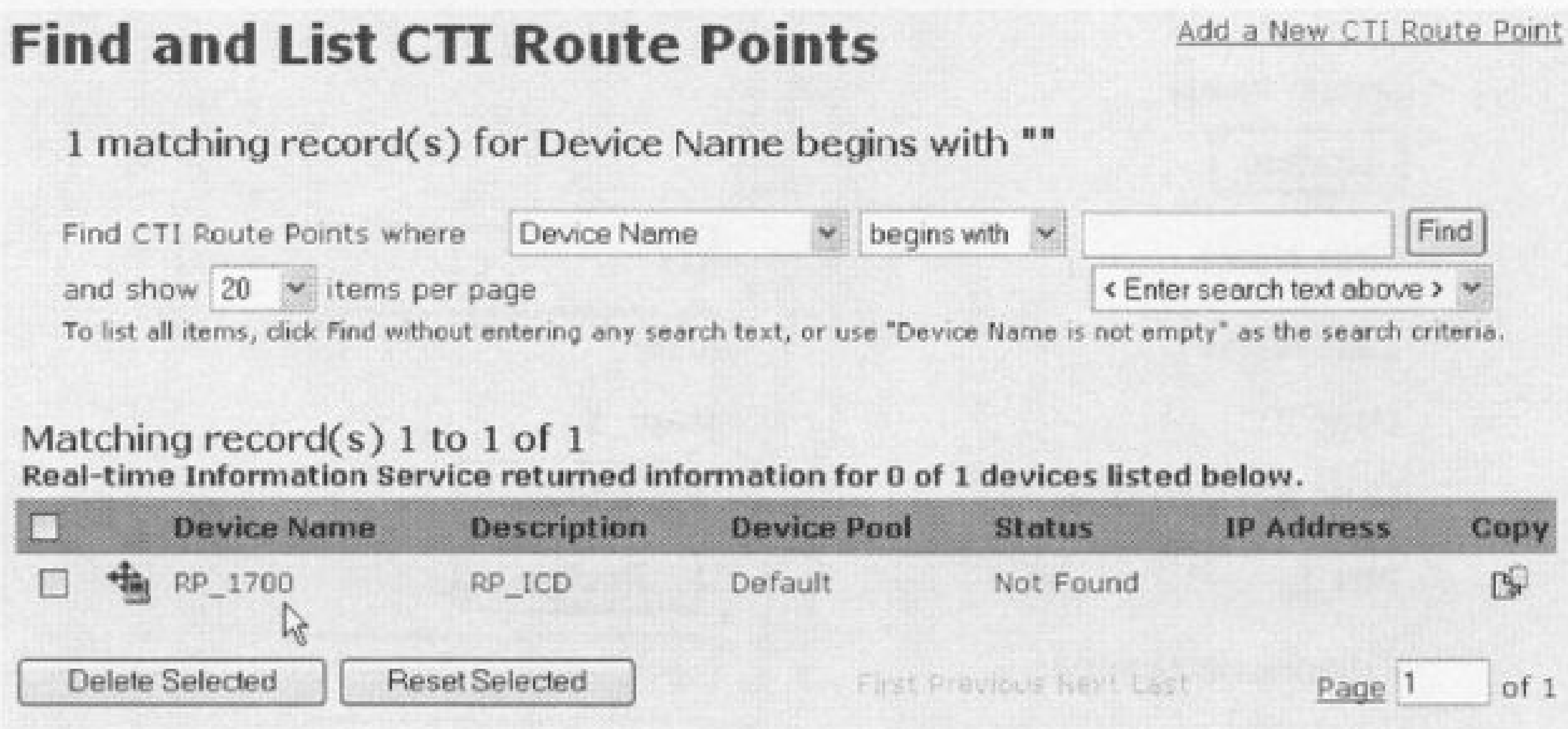
→ **Once we create the application, we need to assign someway to trigger the application to run and in this case we will use a JTAPI trigger (phone call). This step will of course create the CTI RP in CCM and automatically associate the JTAPI user with this CTI RP.**

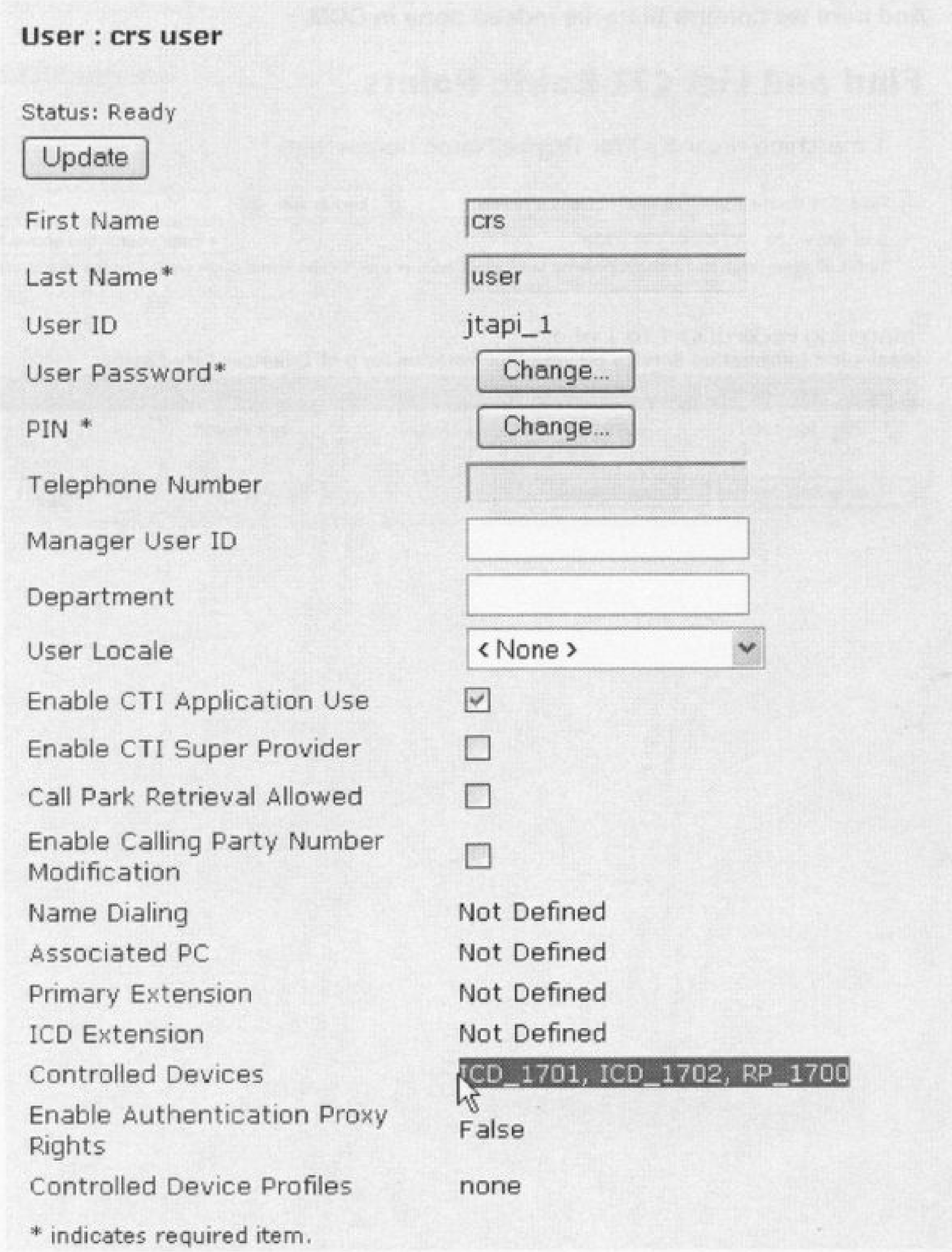





JTAPI Trigger Configuration
Add
Cancel
Add a New CMT Dialog Control Group
Directory Number
Directory Number*
1700
Partition
None
Trigger Information
Language*
English (United States) [en_US]
Edit
Application Name
ICD
Maximum Number Of sessions*
2
Idle Timeout (in ms)*
5000
Enabled*
Yes
No
Call Control Group*
JTAPI Group #0(0)
Primary Dialog Group*
Cisco Media Group #0(0)
Secondary Dialog Group
None
CTI Route Point Information
Device Name*
RP_1700
Description*
RP_ICD
Device Pool
Default
Location
None
Directory Number Settings
Voice Mail Profile
None
Calling Search Space
None
Call Forward and Pickup Settings
Voice Mail
Destination
Calling Search Space
Forward Busy
None
Call Pickup Group
None
Display
External Phone Number Mask
Note:
* indicates required item

➔ **And here we confirm that was indeed done in CCM:**





User : crs user

Status: Ready

Update

First Name	crs
Last Name*	user
User ID	jtapi_1
User Password*	Change...
PIN *	Change...
Telephone Number	
Manager User ID	
Department	
User Locale	< None >
Enable CTI Application Use	☑
Enable CTI Super Provider	☐
Call Park Retrieval Allowed	☐
Enable Calling Party Number Modification	☐
Name Dialing	Not Defined
Associated PC	Not Defined
Primary Extension	Not Defined
ICD Extension	Not Defined
Controlled Devices	ICD_1701, ICD_1702, RP_1700
Enable Authentication Proxy Rights	False
Controlled Device Profiles	none

* indicates required item.

➔ **At this stage it is worth making a test call to both Triggers - in both cases you should be able to hear the appropriate recorded message. Call from HQ and BR1. If the call works for HQ but NOT for BR1 then this is a sure sign that the transcoder in the HQ Device Pool may not be working.**

Task 10.2

Modify the "icd.aef" script with the following information (you may wish to rename it to avoid loosing the original script).

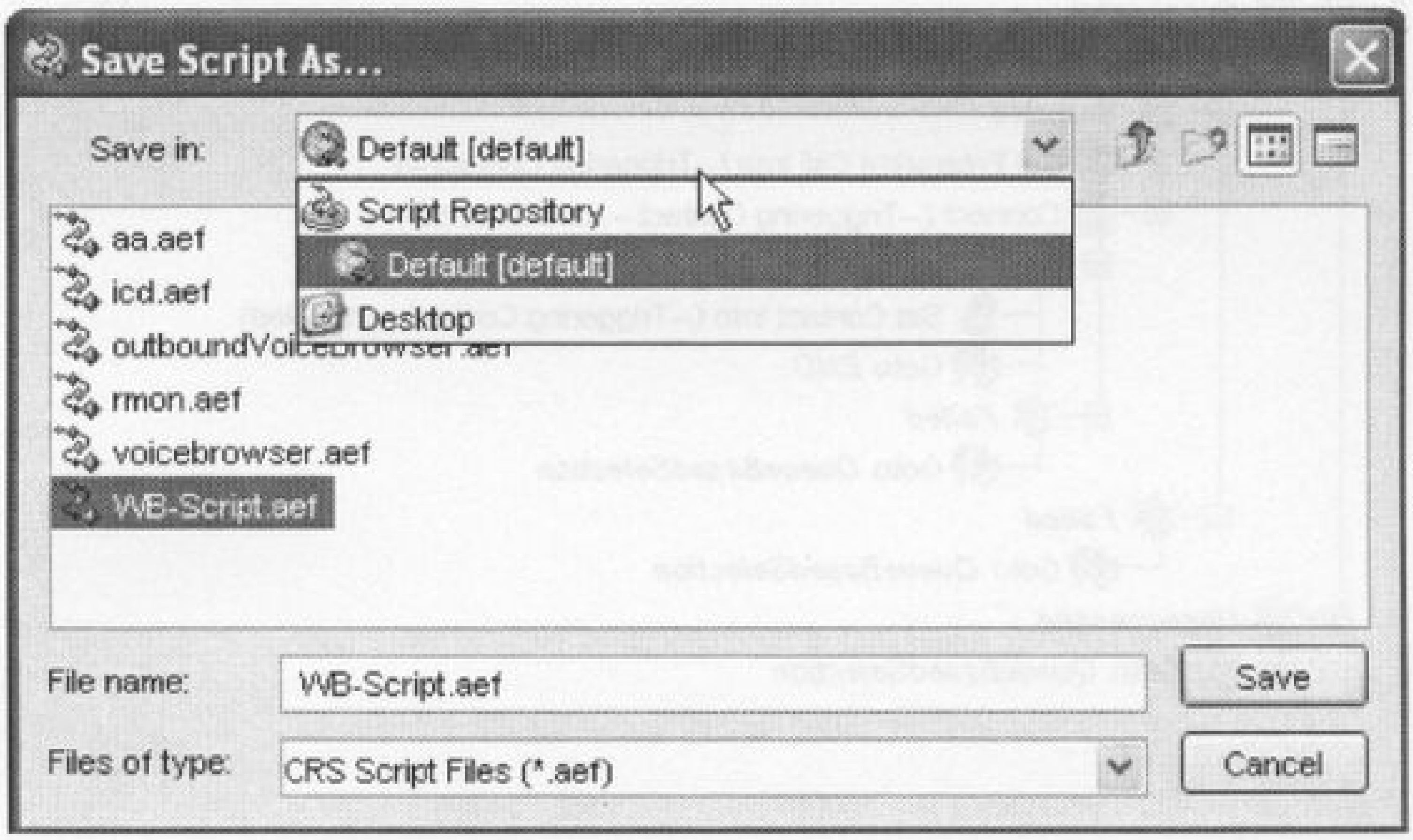
- You must determine if the call is coming from the PSTN from anywhere in the area code of '617' and if the call is coming from the 617 area code then the call must check to see if 'agent1' is available and route the call directly to that agent without queuing the call, however if agent1 is not available, send the call to the 'GeneralQ'

- If the call goes to the GeneralQ, music should be played to the caller while waiting in Q and the caller should also hear the 'QueuePrompt' every 30 seconds

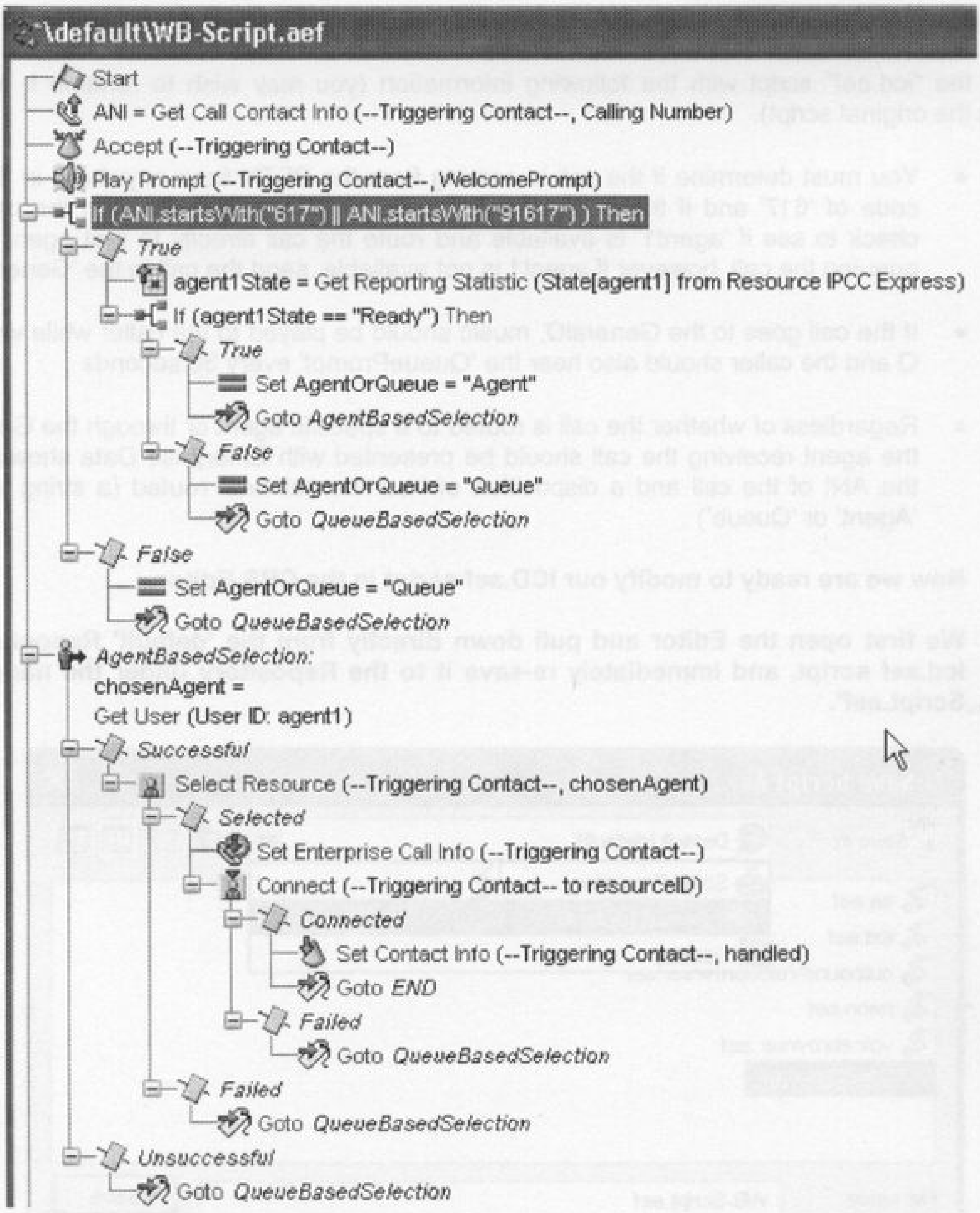
- Regardless of whether the call is routed to a specififc agent or through the GeneralQ, the agent receiving the call should be presented with Enterprise Data showing both the ANI of the call and a disposition of how the call was routed (a string showing 'Agent' or 'Queue')

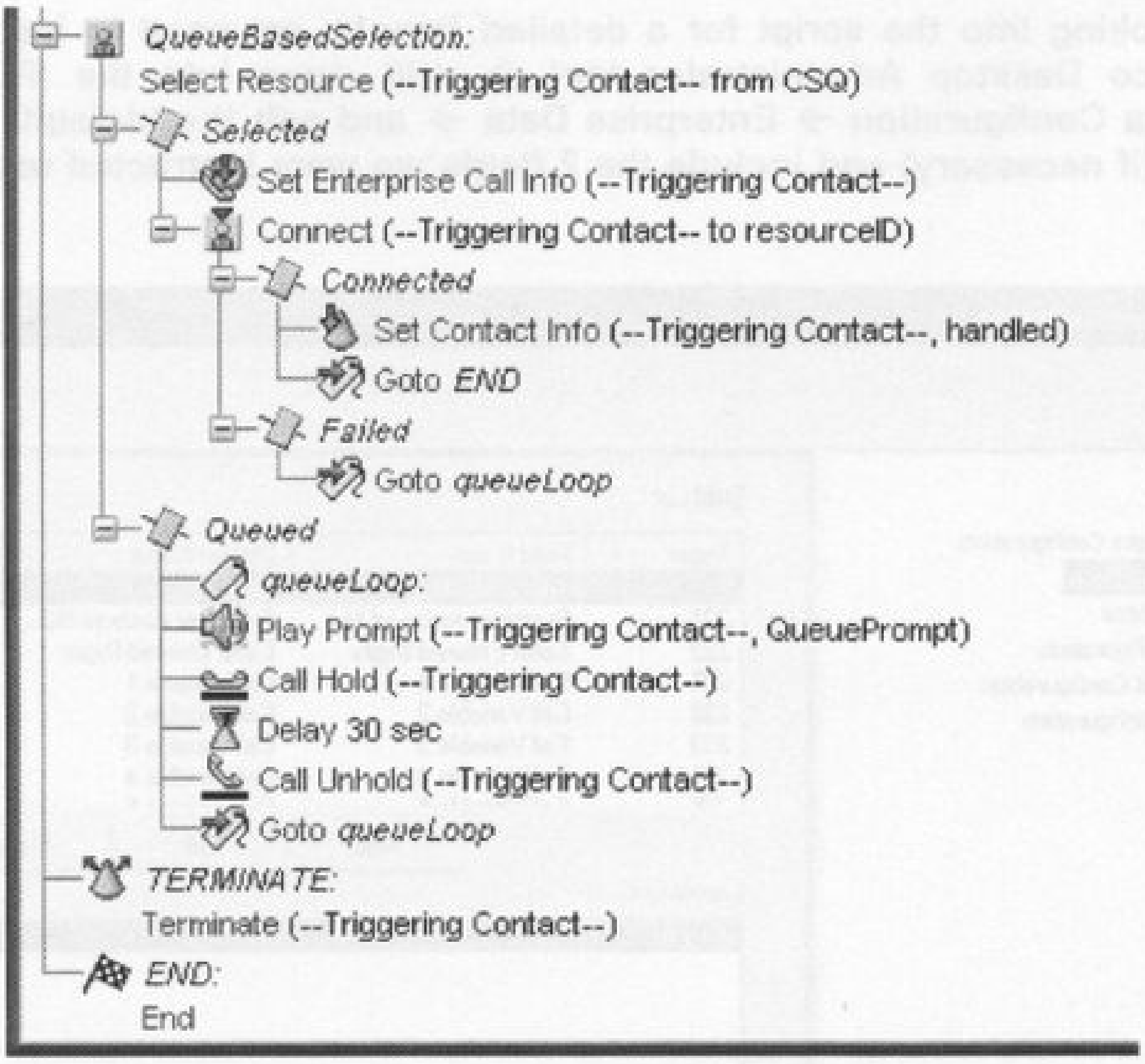
➔ **Now we are ready to modify our ICD.aef script in the CRS Editor.**

➔ **We first open the Editor and pull down directly from the 'default' Repository the icd.aef script, and immediately re-save it to the Repository under the name 'WB-Script.aef'.**



➔ **Here are a few screenshots of the .aef script file and the variables – but you may have a look much more in-depth by downloading from the Solutions PDF (it is embedded in this section of the Solutions Guide).**

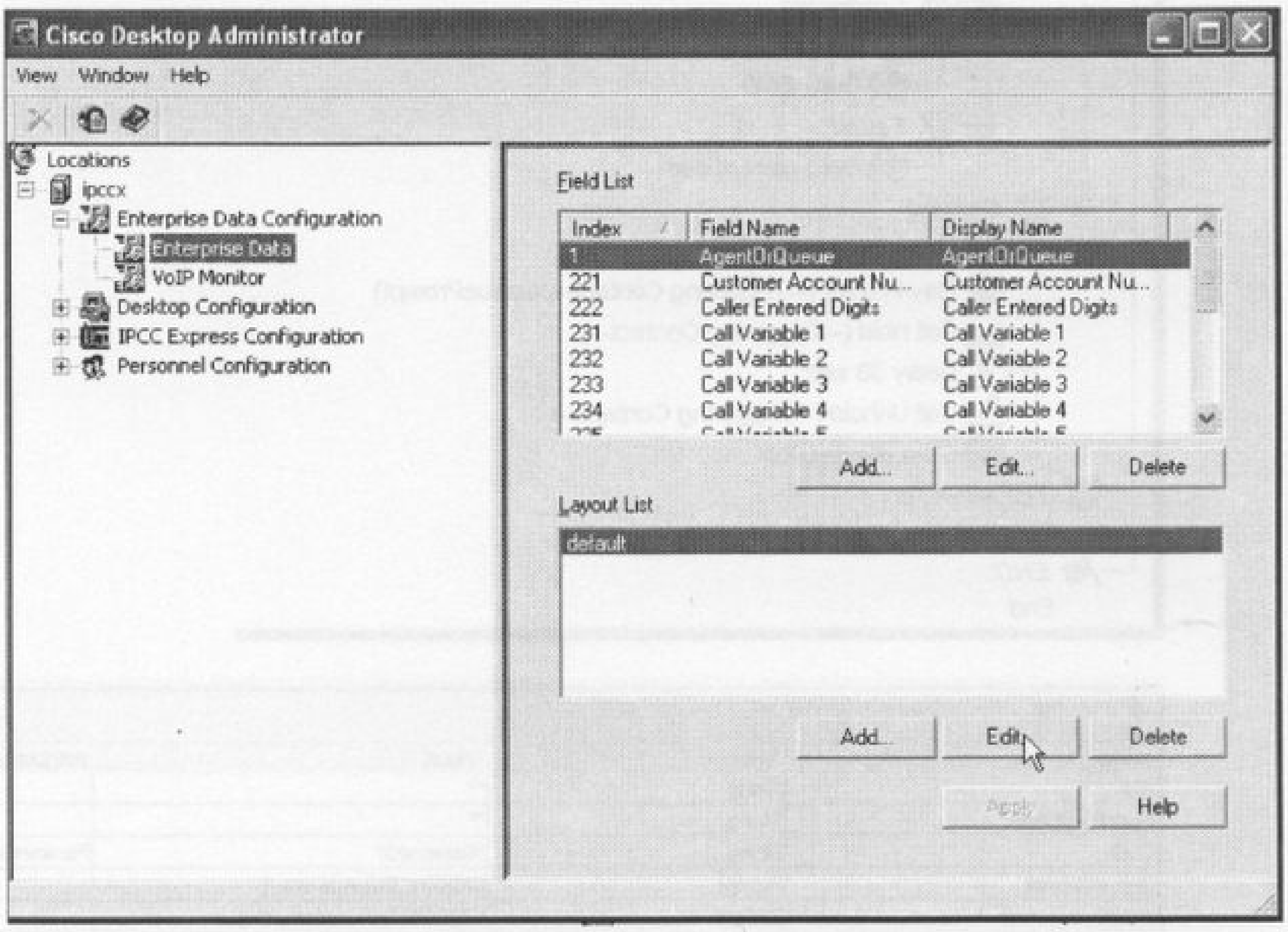

\default\WB-Script.aef
Start
ANI = Get Call Contact Info (--Triggering Contact--, Calling Number)
Accept (--Triggering Contact--)
Play Prompt (--Triggering Contact--, WelcomePrompt)
If (ANI.startsWith("617") || ANI.startsWith("91617")) Then
True
agent1State = Get Reporting Statistic (State[agent1] from Resource IPCC Express)
If (agent1State == "Ready") Then
True
Set AgentOrQueue = "Agent"
Goto AgentBasedSelection
False
Set AgentOrQueue = "Queue"
Goto QueueBasedSelection
False
Set AgentOrQueue = "Queue"
Goto QueueBasedSelection
AgentBasedSelection:
chosenAgent =
Get User (User ID: agent1)
Successful
Select Resource (--Triggering Contact--, chosenAgent)
Selected
Set Enterprise Call Info (--Triggering Contact--)
Connect (--Triggering Contact-- to resourceID)
Connected
Set Contact Info (--Triggering Contact--, handled)
Goto END
Failed
Goto QueueBasedSelection
Failed
Goto QueueBasedSelection
Unsuccessful
Goto QueueBasedSelection

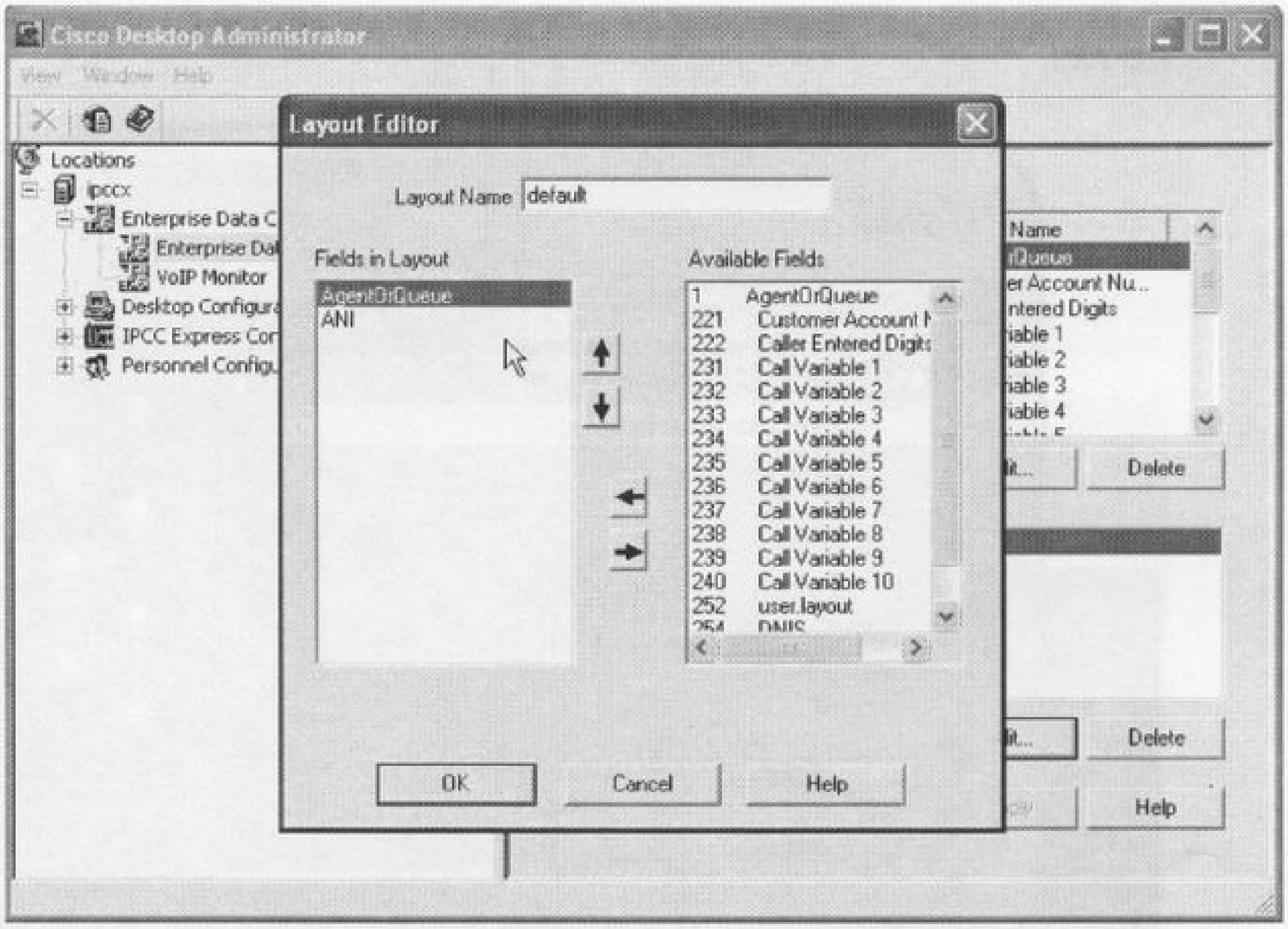


Name	Type	Value	Attributes
ANI	String	""	
AgentOrQueue	String	""	
CSQ	String	"GeneralQ"	Parameter
QueuePrompt	Prompt	SP[ICD\ICDQueue.wav]	
WelcomePrompt	Prompt	SP[ICD\ICDWelcome.wav]	
agent1	String	"agent1"	
agent1State	String	""	
chosenAgent	User	null	
layout	String	"default"	
resourceID	User	null	

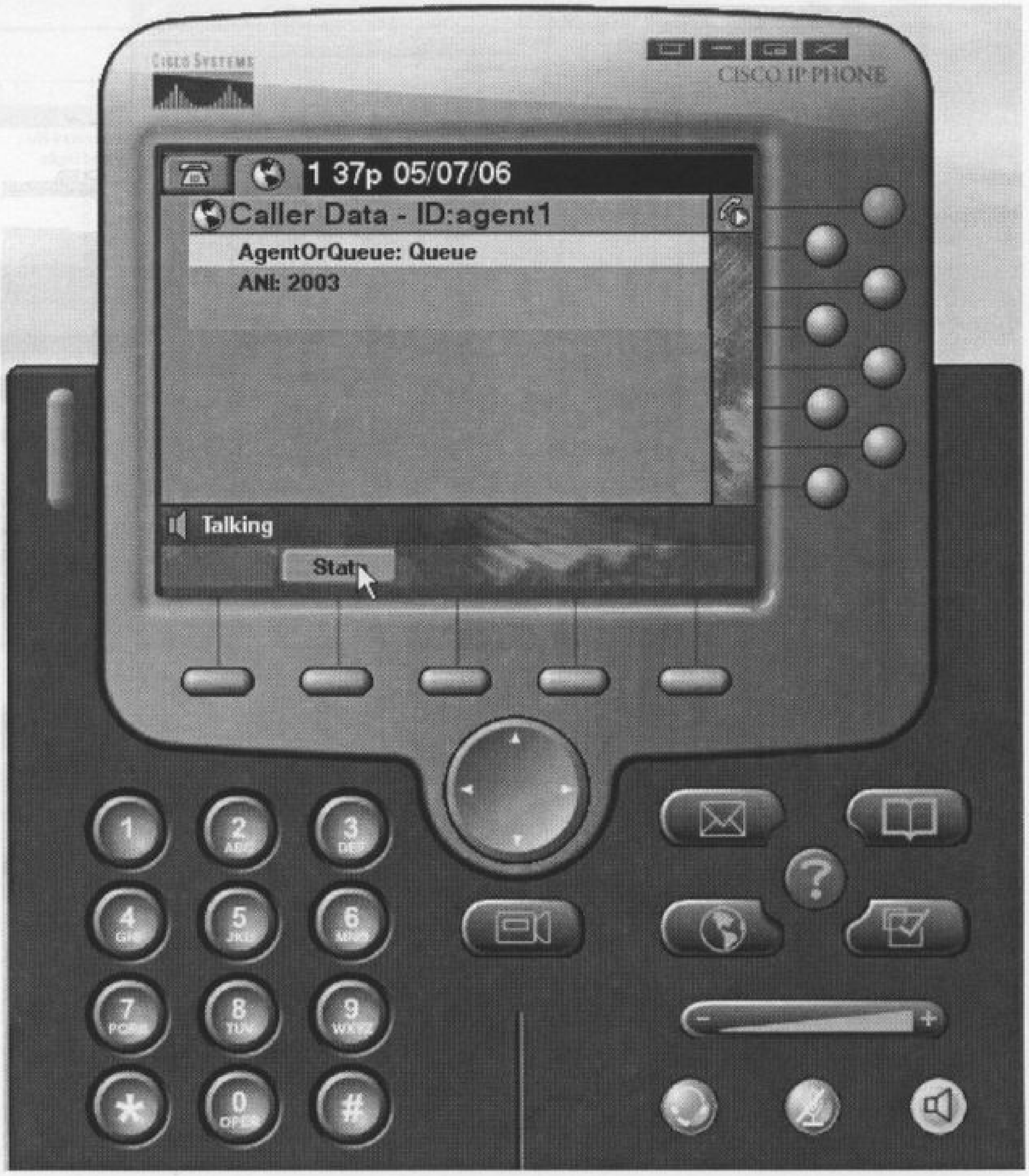
Step 26 / 36 Ln 10 / 50 ipccx crsadmin

➔ **Aside from looking into the script for a detailed how-to, we need to install and open the Cisco Desktop Administrator tool ➔ drill down into the IPCCX ➔ Enterprise Data Configuration ➔ Enterprise Data ➔ and edit the 'default' Layout List to create (if necessary) and include the 2 fields we were instructed to include in the task:**

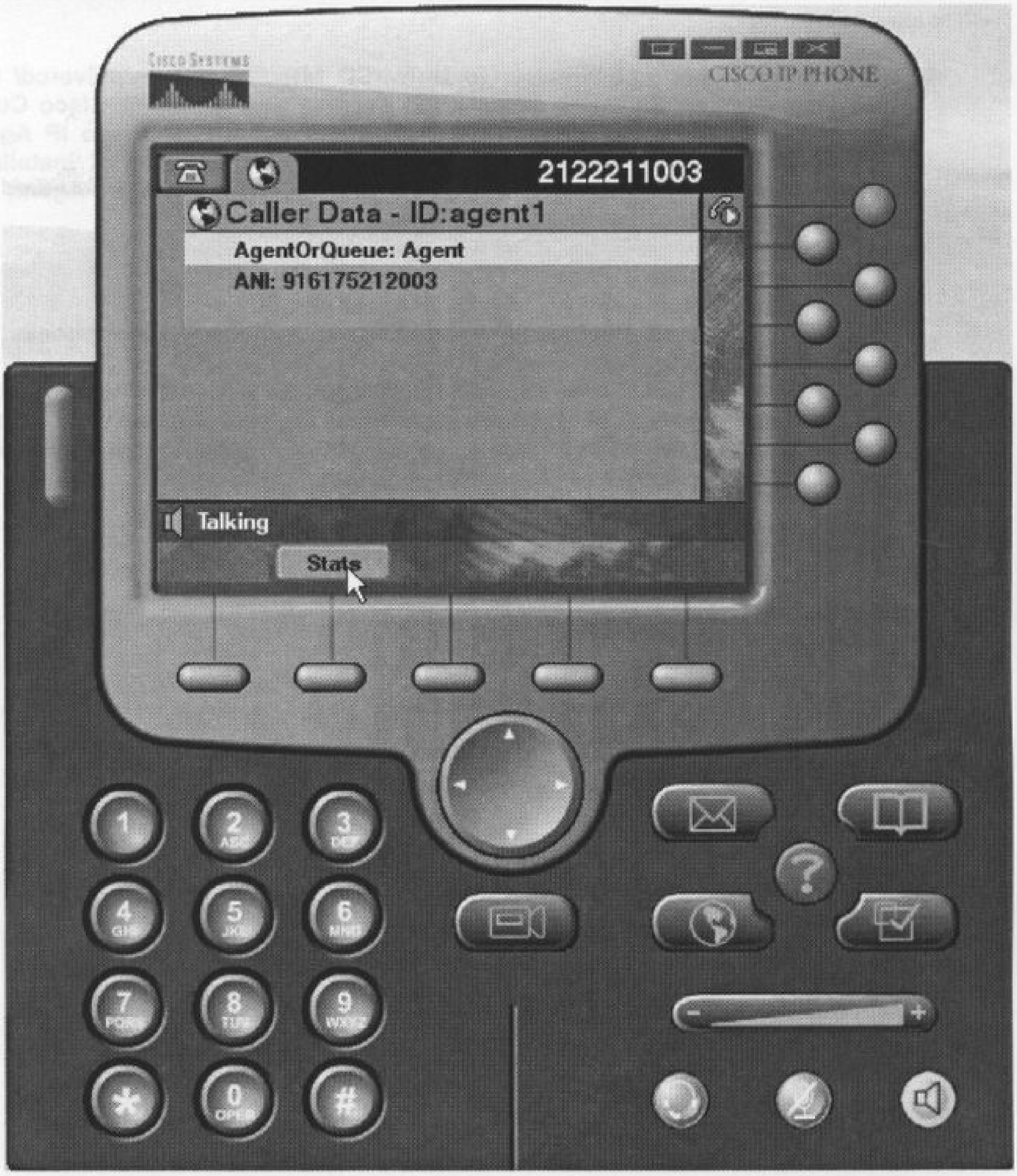



Cisco Desktop Administrator
View Window Help
Locations
ipccx
Enterprise Data C
Enterprise Dat
VoIP Monitor
Desktop Configura
IPCC Express Cor
Personnel Configu
Layout Editor
Layout Name default
Fields in Layout
AgentOrQueue
ANI
Available Fields
1 AgentOrQueue
221 Customer Account N
222 Caller Entered Digits
231 Call Variable 1
232 Call Variable 2
233 Call Variable 3
234 Call Variable 4
235 Call Variable 5
236 Call Variable 6
237 Call Variable 7
238 Call Variable 8
239 Call Variable 9
240 Call Variable 10
252 user.layout
OK
Cancel
Help
Name
Delete
Delete
Help

➔ **And finally we test – first from a BR1 Ph dialing into 1700 and receiving the call on HQ Ph3.**



→ **And then from a BR1 Ph dialing LD 9,12122211700 and receiving the call on HQ Ph3 – and here we see the Enterprise Data indicating that the call was routed using Agent Based Routing instead of through a CSQ.**



Task 10.3

Configure IPCC Phone Agent for both phones and also ensure that they only have to press the services button once (i.e. that they don't have to provide User/Ext/Pin information on the phone when logging in).

→ **If we navigate our web browser to UniverCD http://cisco.com/univercd/ then to Customer Contact Center → Cisco IPCC Express and IP IVR → Cisco Customer Response Solutions 4.0(x) → English → Documentation for Cisco IP Agents → Cisco CAD Installation Guide 6.1 → and then go to the bookmark of 'Installation → Configuring Cisco CallManager IP Phones to Work With IP Phone Agent; we see the 3 main steps that we need to perform including:**

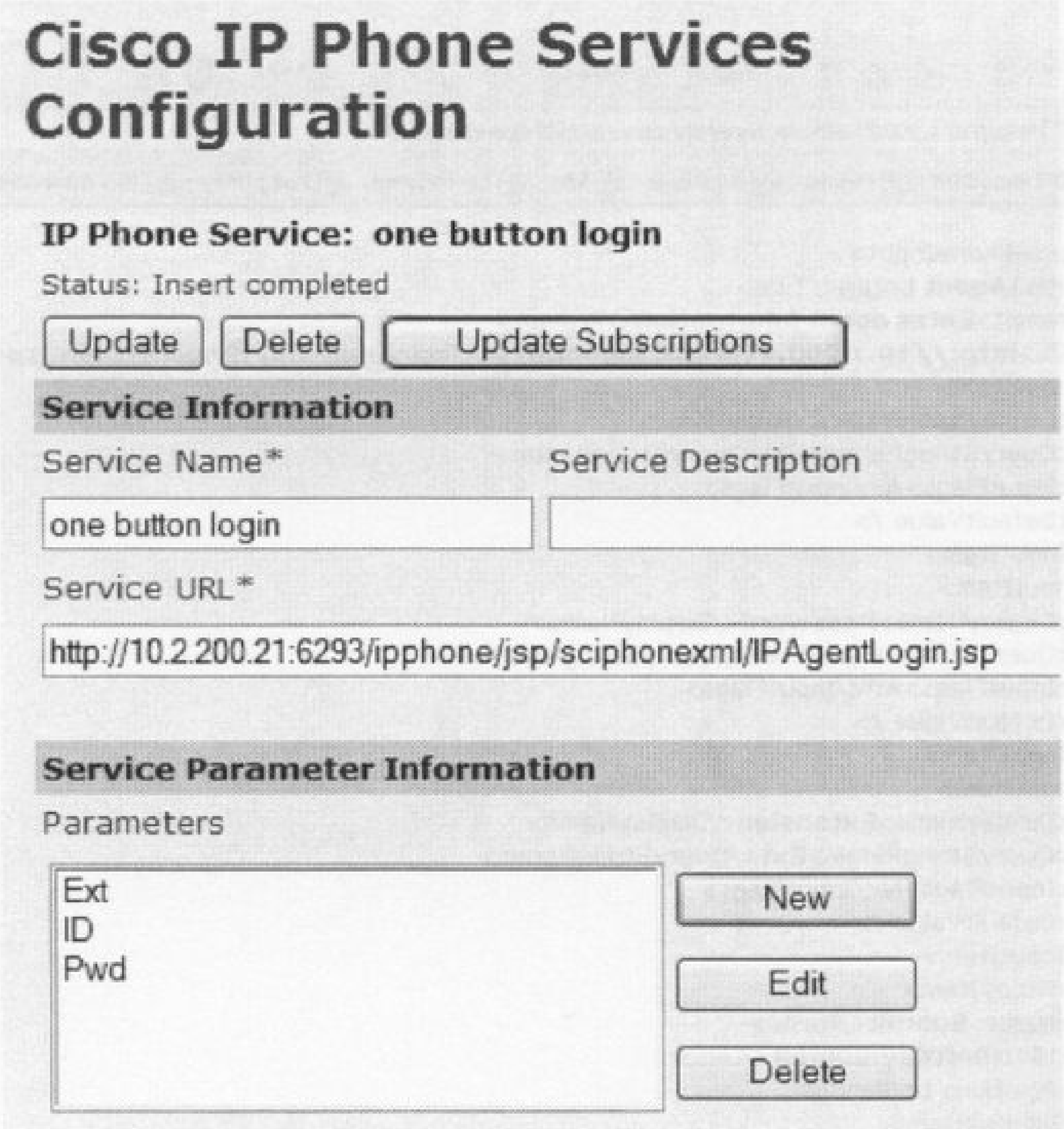
1. Create an IP phone service.
2. Assign the IP phone service to each IP agent phone.
3. Create a user named "telecaster" and assign to it all the IP agent phones.

→ **Here we find the URL that we need to create the service and if we take this URL and paste run it from an IE web browser window then we can find what Parameters and new URL we will need to create the one-button-login required to complete the task:**

➔ **So we can see the new URL here as well as the </QueryStringParam> which will become our new Parameters in the IP Phone Service.**


```
- <CiscoIPPhoneInput>
    <Title>Agent Login</Title>
    <Prompt>Enter agent information</Prompt>
    <URL>http://10.1.200.21:6293/ipphone/jsp/sciphonexml/IPAgentLogin.jsp</URL>
  - <InputItem>
      <DisplayName>ID</DisplayName>
      <QueryStringParam>ID</QueryStringParam>
      <InputFlags>A</InputFlags>
      <DefaultValue />
    </InputItem>
  - <InputItem>
      <DisplayName>Password</DisplayName>
      <QueryStringParam>Pwd</QueryStringParam>
      <InputFlags>AP</InputFlags>
      <DefaultValue />
    </InputItem>
  - <InputItem>
      <DisplayName>Extension</DisplayName>
      <QueryStringParam>Ext</QueryStringParam>
      <InputFlags>N</InputFlags>
      <DefaultValue />
    </InputItem>
  - <SoftKeyItem>
      <Name>Submit</Name>
      <URL>SoftKey:Submit</URL>
      <Position>1</Position>
    </SoftKeyItem>
  - <SoftKeyItem>
      <Name><<</Name>
      <URL>SoftKey:<<</URL>
      <Position>2</Position>
    </SoftKeyItem>
  - <SoftKeyItem>
      <Name>Exit</Name>
      <URL>Key:Services</URL>
      <Position>3</Position>
    </SoftKeyItem>
</CiscoIPPhoneInput>
```


➔ **We will apply this to our new Service.**



➔ **Any device that will be used by an ICD Agent needs to subscribe to the ICD Service. This normally includes 7900 series phones but could also include CIPCs and Device Profiles that are used by the Extension Mobility.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

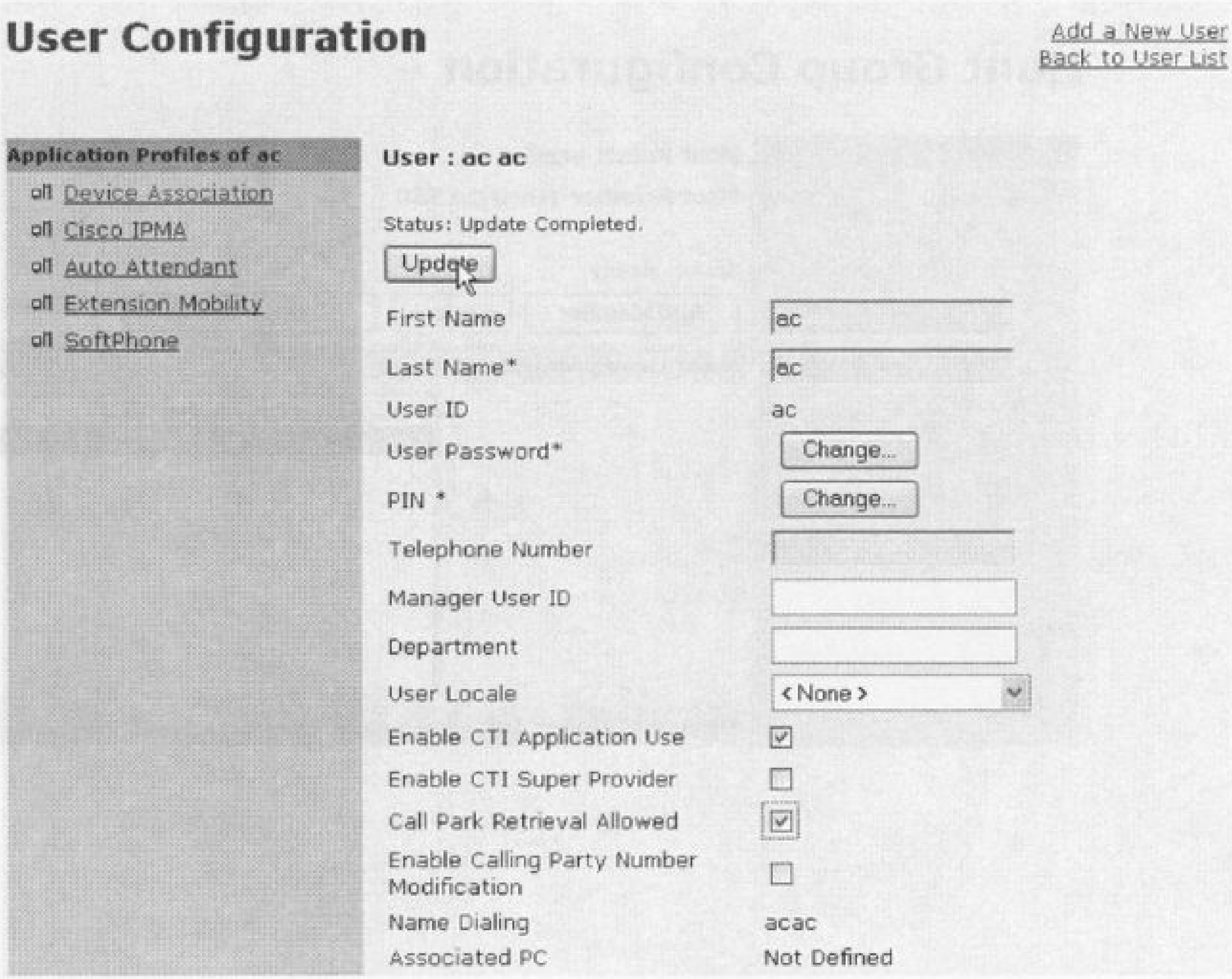
Section 11: Call Manager Features

Estimated Time to Complete: 4 hours

NOTE:

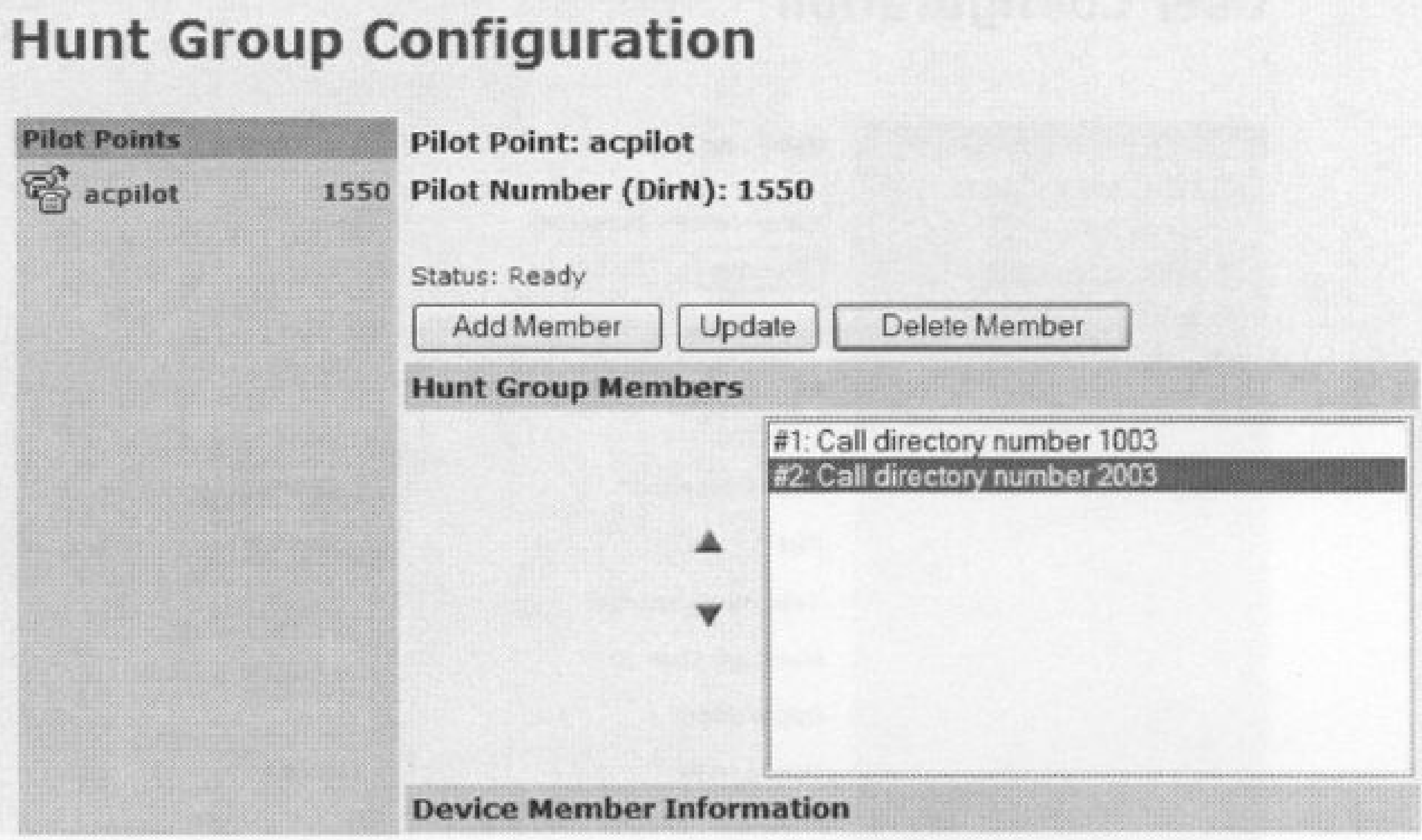
Please reference your Voice Workbook for all diagrams and tables.

➔ **Create the 'ac' user with password '12345'.**

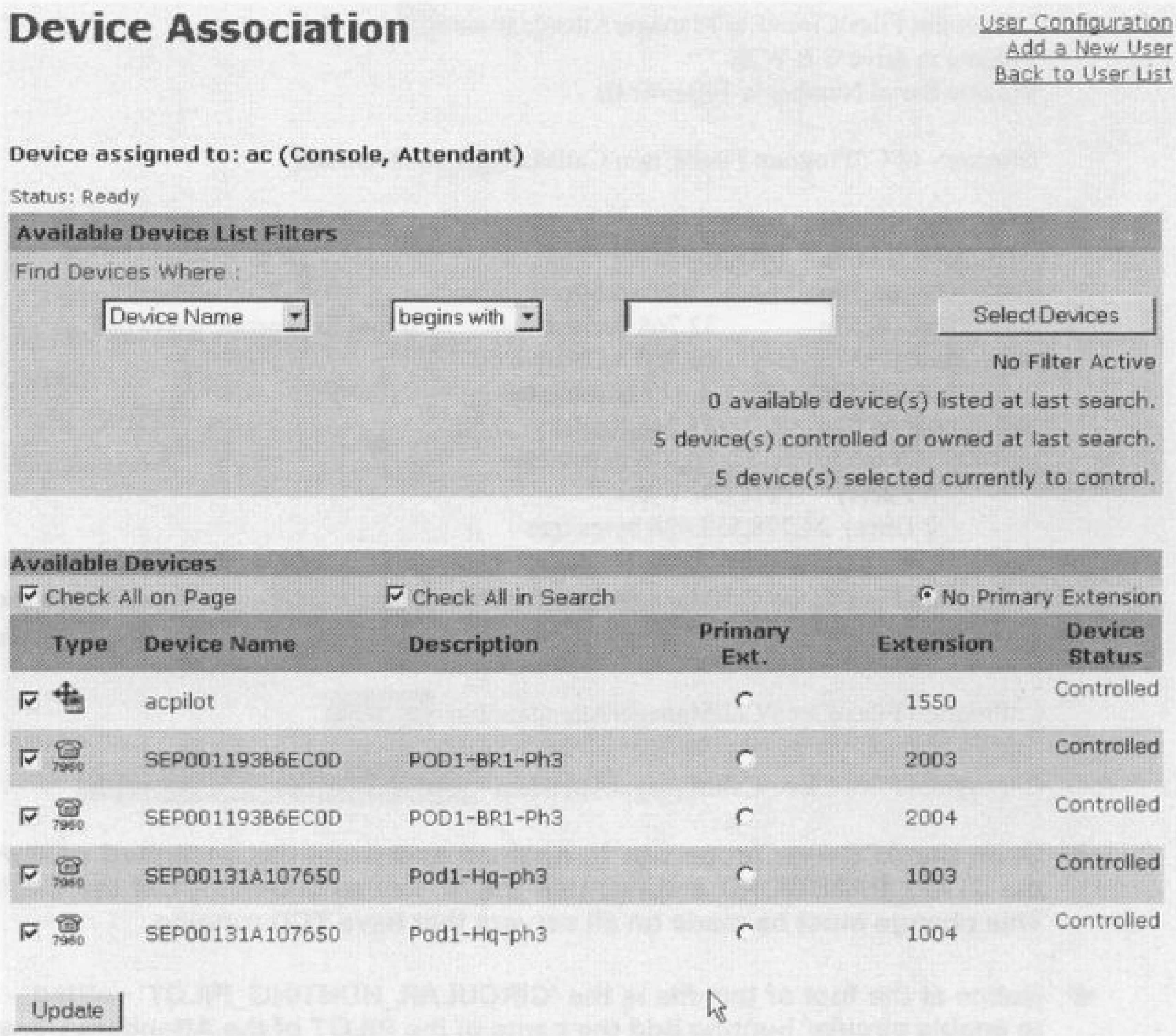


➔ **The Enable CTI Application Use and Call Park Retrieval Allowed check boxes must be checked.**

➔ **To create a huntgroup: From Service > Cisco CM Attendant Console > Hunt Group click 'Add Member'.**



➔ **Finally, the Attendant Console Phones and the Pilot Points must be associated with the ac user.**



Task 11.2

Change the '*ac*' user password to '*cisco*'. Also enable Circular Hunting within the huntgroup.

➔ **As well as making changes for the ac user in the Directory (via the 'User' page), the ACServer.properties files located in Program Files\Cisco\CallManager Attendant Console\etc directory on the Cisco CallManager Attendant Console server must be edited.**

➔ **Before the password can be changed in this text file, the encrypted password must be generated using the acenc.exe tool. Below is the output from the command prompt when changing the ac user password to 'cisco'.**

```
C:\Program Files\Cisco\CallManagerAttendant\bin>dir
 Volume in drive C is W2K
 Volume Serial Number is 70BE-674B

 Directory of C:\Program Files\Cisco\CallManagerAttendant\bin

05/26/2005  12:05a    <DIR>          .
05/26/2005  12:05a    <DIR>          ..
10/07/2004  06:57p               932 accollectlogs.bat
10/07/2004  06:57p            32,768 acenc.exe        // tool to generate password
10/07/2004  06:57p            40,960 ACNative.dll
10/07/2004  06:57p             1,117 builddir.bat
10/07/2004  06:57p            53,248 RegistryCtl.dll
10/07/2004  06:57p            86,016 tcdsrv.exe
               6 File(s)        215,041 bytes
               2 Dir(s)  24,778,538,496 bytes free

C:\Program Files\Cisco\CallManagerAttendant\bin>acenc cisco     // cisco is new passwd
0c0a000a2c                                                      // encrypted passwd

C:\Program Files\Cisco\CallManagerAttendant\bin>cd ../etc

C:\Program Files\Cisco\CallManagerAttendant>notepad AcServer.Properties
```

➔ **Open the ACServer.properties in notepad and paste the encrypted password into the JTAPI_PASSWORD setting. Use the '#' key to comment out the original line. This change must be made on all servers that have TCD running.**

➔ **Notice at the foot of this file is the 'CIRCULAR_HUNTING_PILOT' setting – in order to enable circular hunting add the name of the PILOT of the Attendant Console.**

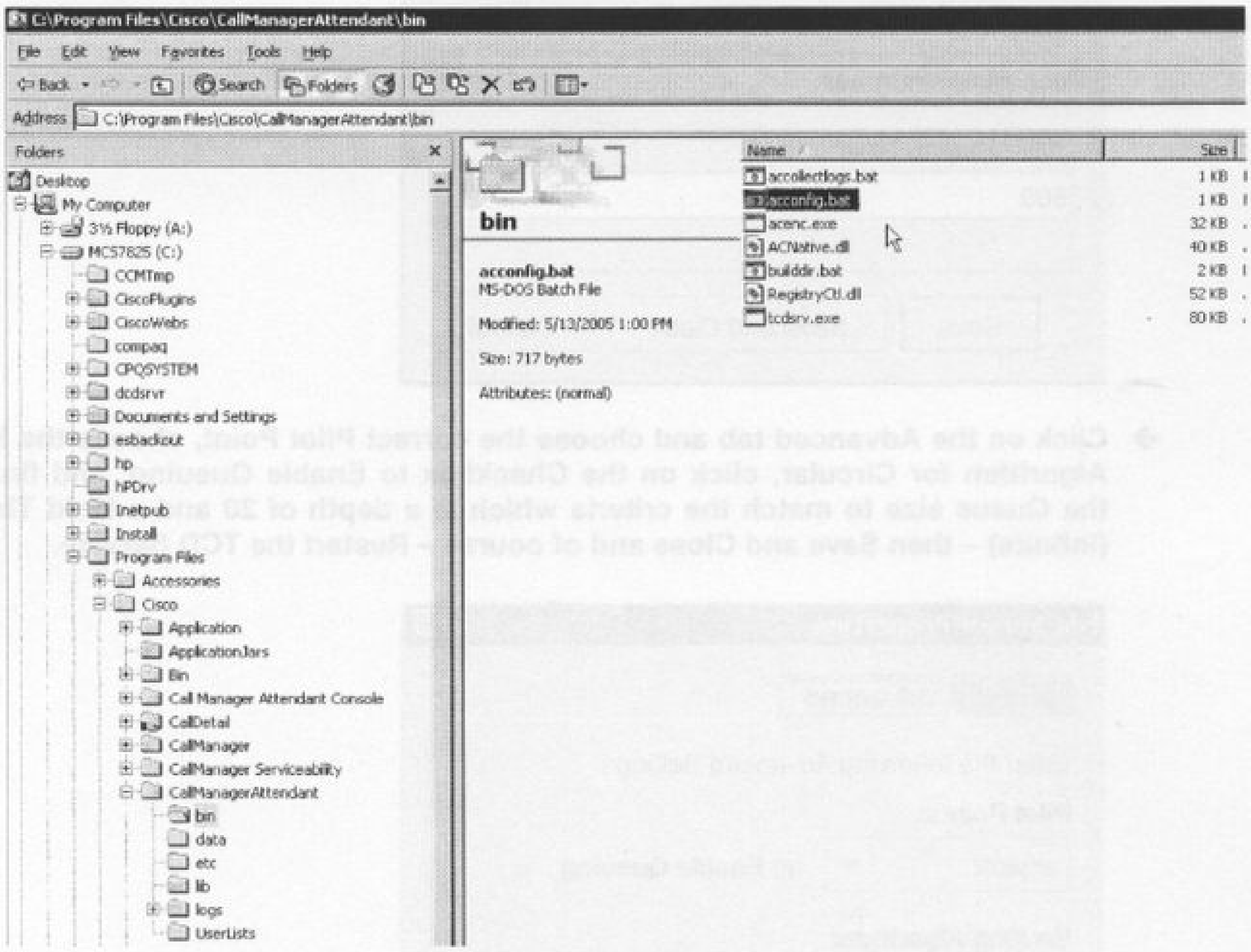
```
#Jtapi Password
#JTAPI_PASSWORD=5e51405d76
JTAPI_PASSWORD=0c0a000a2c

# Specify comma seperated pilot point device names for which
# circular hunting algorithm is used. This will override
# what is configured in the admin pages.
CIRCULAR_HUNTING_PILOT=acpilot
```

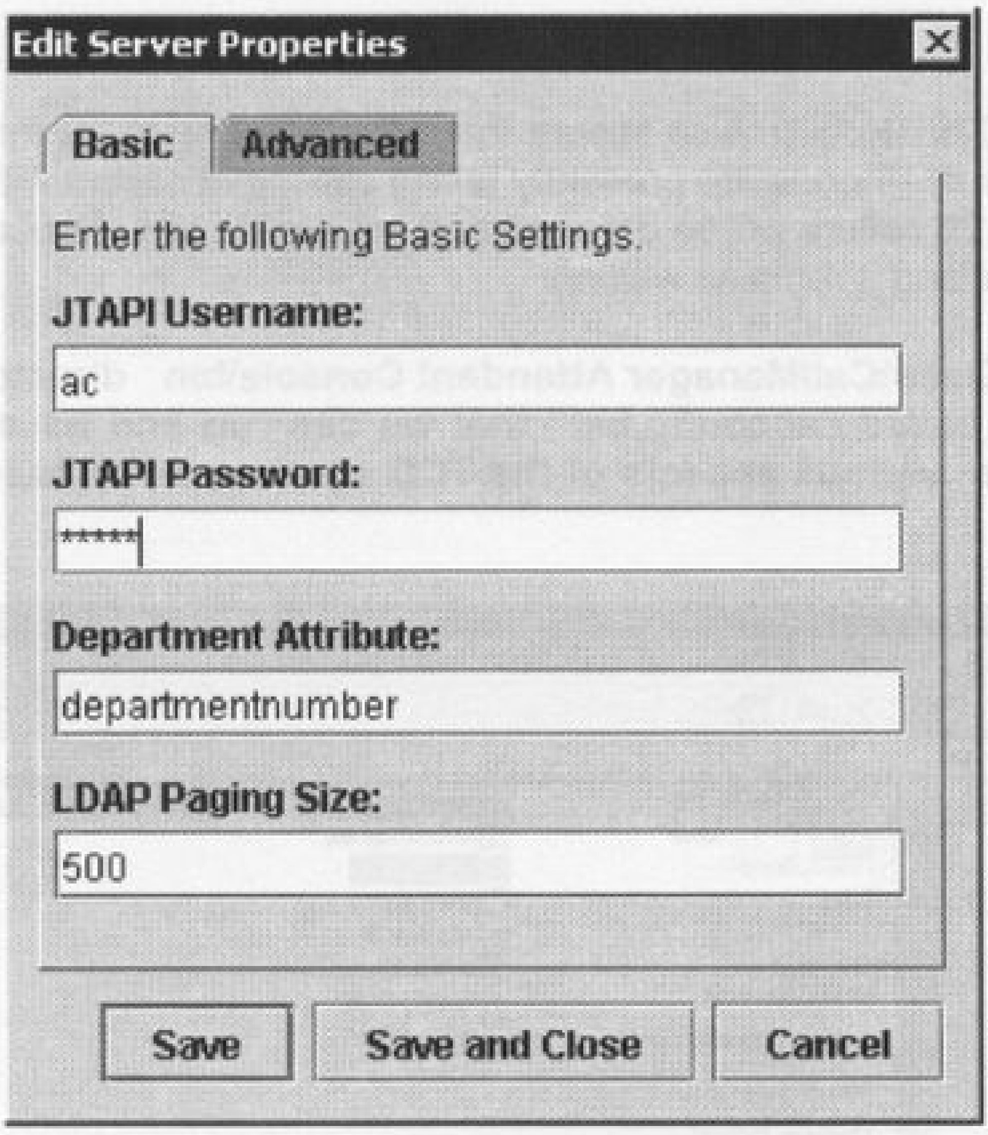
➔ **Once the changes to ACServer.properties are complete the TCD and CTI Manager service on all servers that have TCD running should be restarted.**

Task 11.3

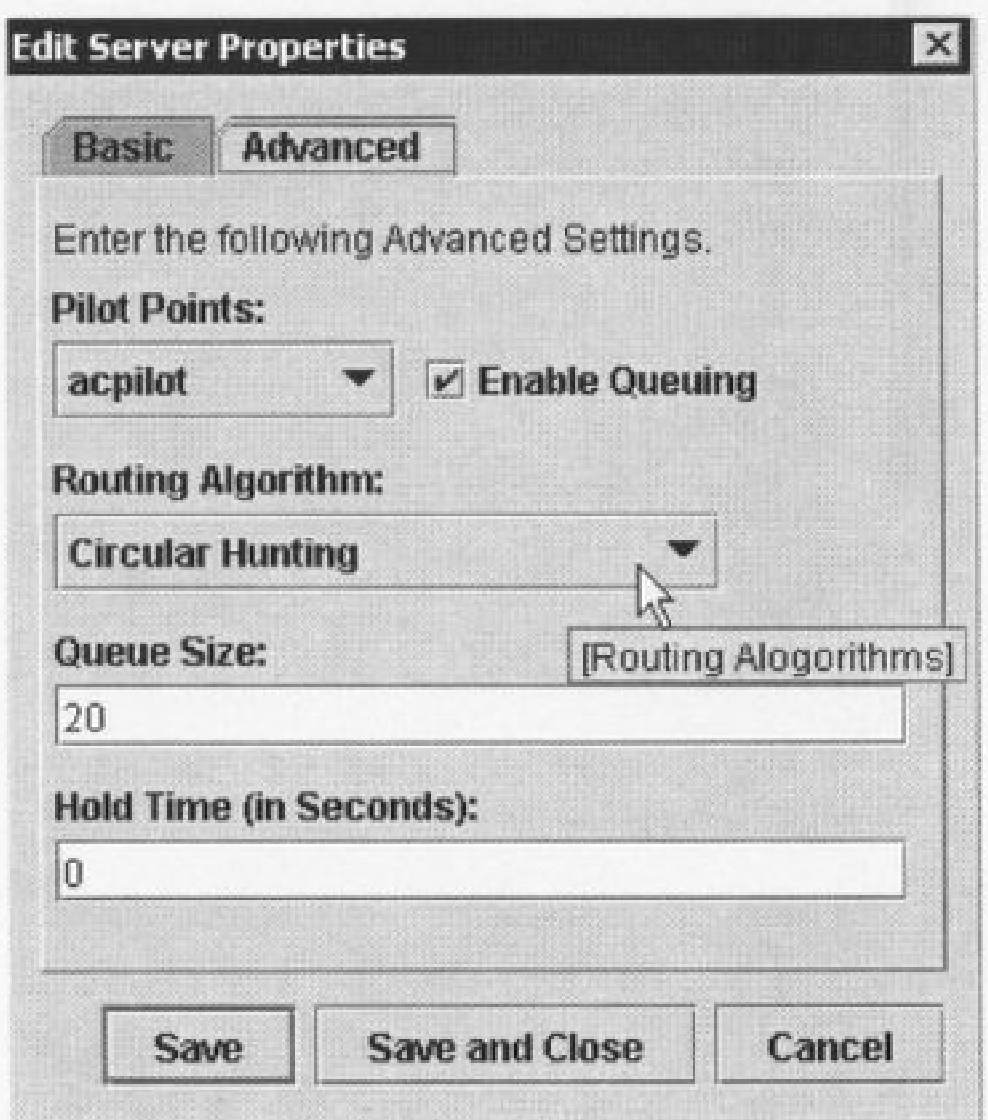
Enable Circular Hunting within the AC huntgroup. Also ensure that if there are up to 20 callers simultaneously calling 1550, and both IP Phones are presently taking calls, that callers will not be dropped but any number greater that 20 callers will be dropped and not sent to VM. Also, a call should not be dropped no matter how long it remains waiting.

➔ **In the C:\Program Files\Cisco\CallManager Attendant Console\bin directory we have a new nifty program called "acconfig.bat" that we can run and have a java window pop open to control various aspects of the TCD service and subsequently the AC application.**





➔ **Click on the Advanced tab and choose the correct Pilot Point, choose the Routing Algorithm for Circular, click on the Checkbox to Enable Queuing, and finally set the Queue size to match the criteria which is a depth of 20 and a Hold Time of 0 (infinite) – then Save and Close and of course – Restart the TCD Service.**



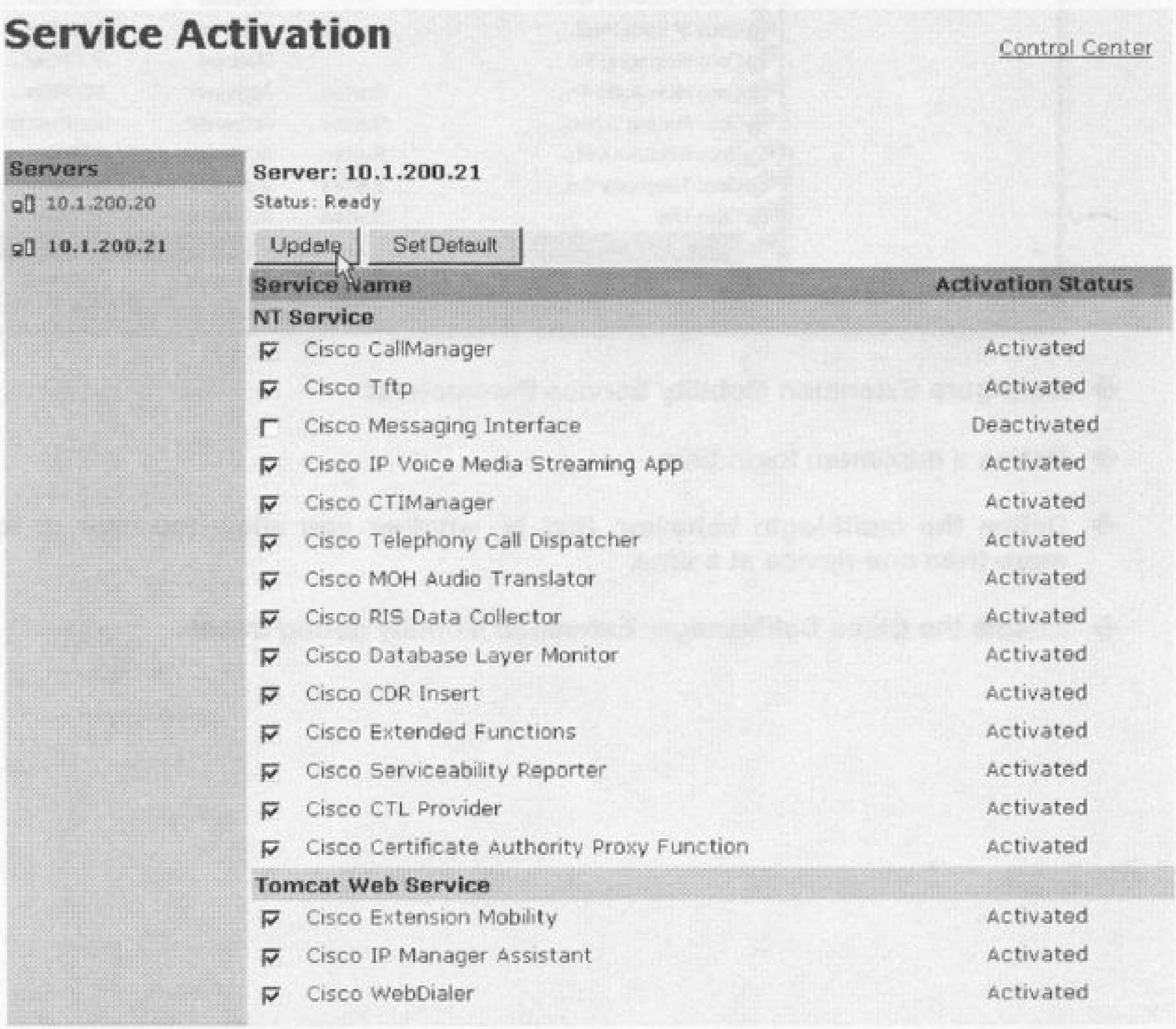
Task 11.4

Configure Extension Mobility such that a Device Profile with DN = '1551' is assigned to the following user.

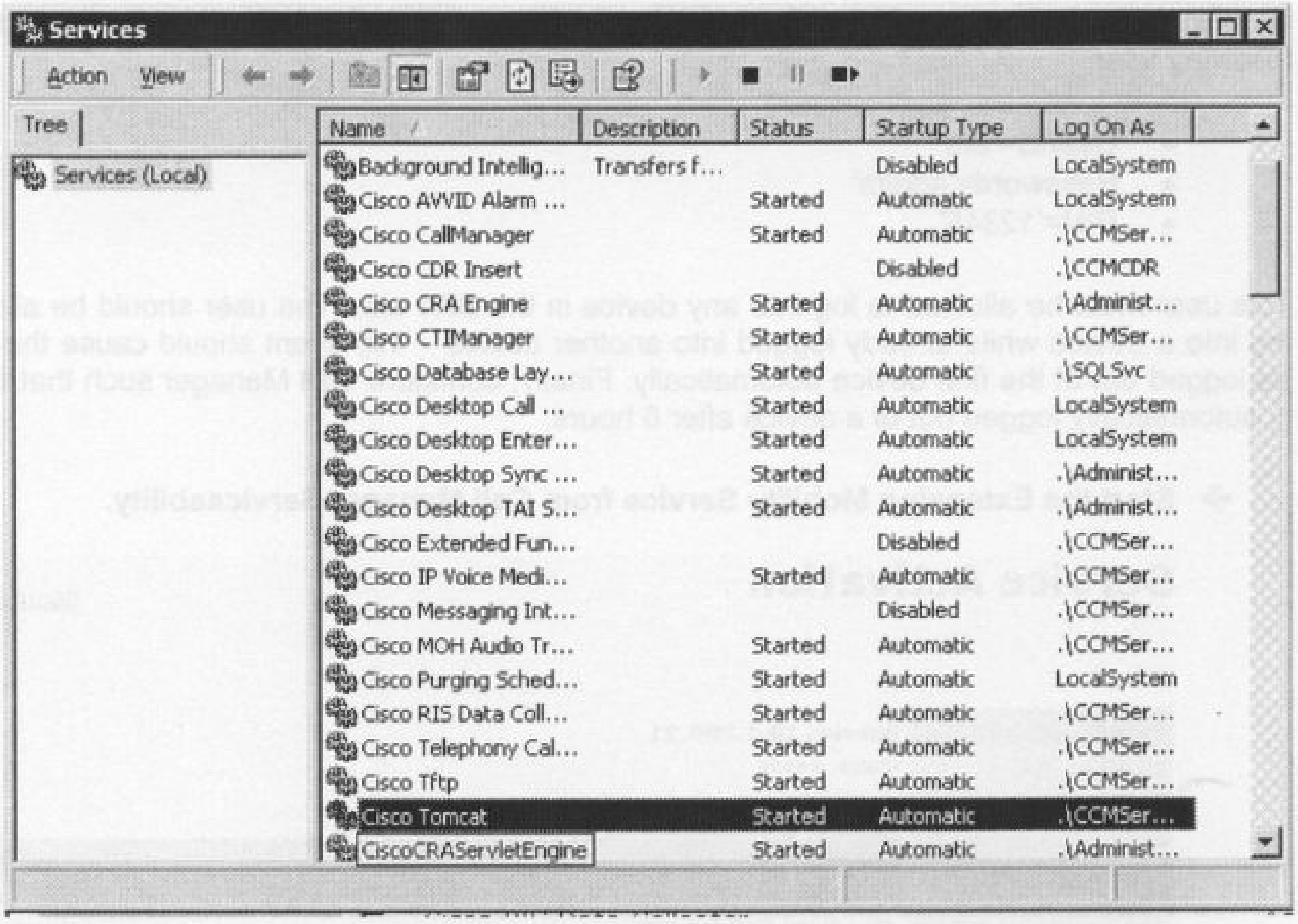
- UserID='em'
- Password='adgjm'
- PIN='12345'

This user must be allowed to log into any device in the BR1 site. The user should be allowed to log into a device while already logged into another device – this event should cause the user to be logged out of the first device automatically. Finally, configure Call Manager such that the user is automatically logged out of a device after 6 hours.

➔ **Start the Extension Mobility Service from Call Manager Serviceability.**



➔ **Ensure that the Cisco Tomcat service is started.**



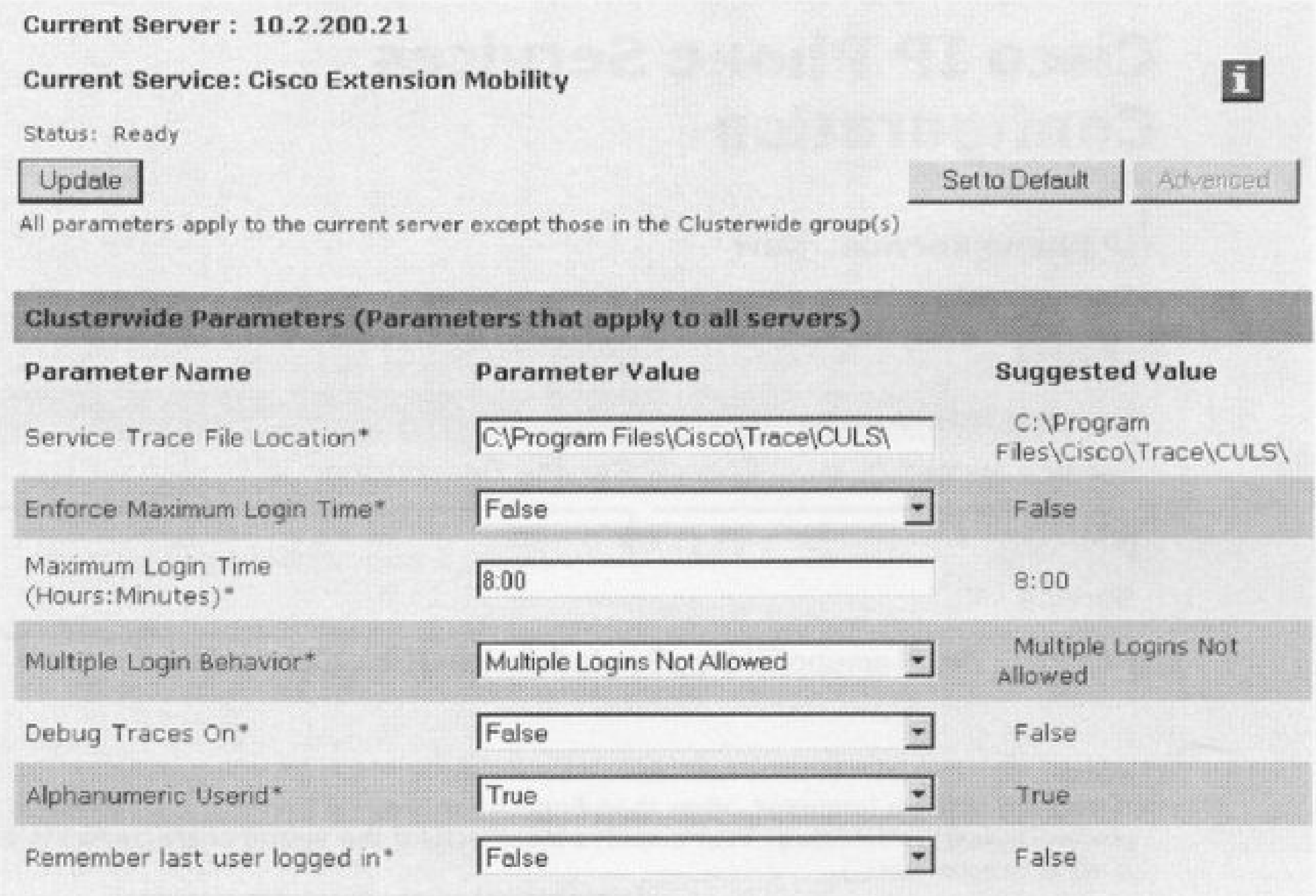
➔ **Configure Extension Mobility Service Parameters:**

➔ **Define a maximum login time.**

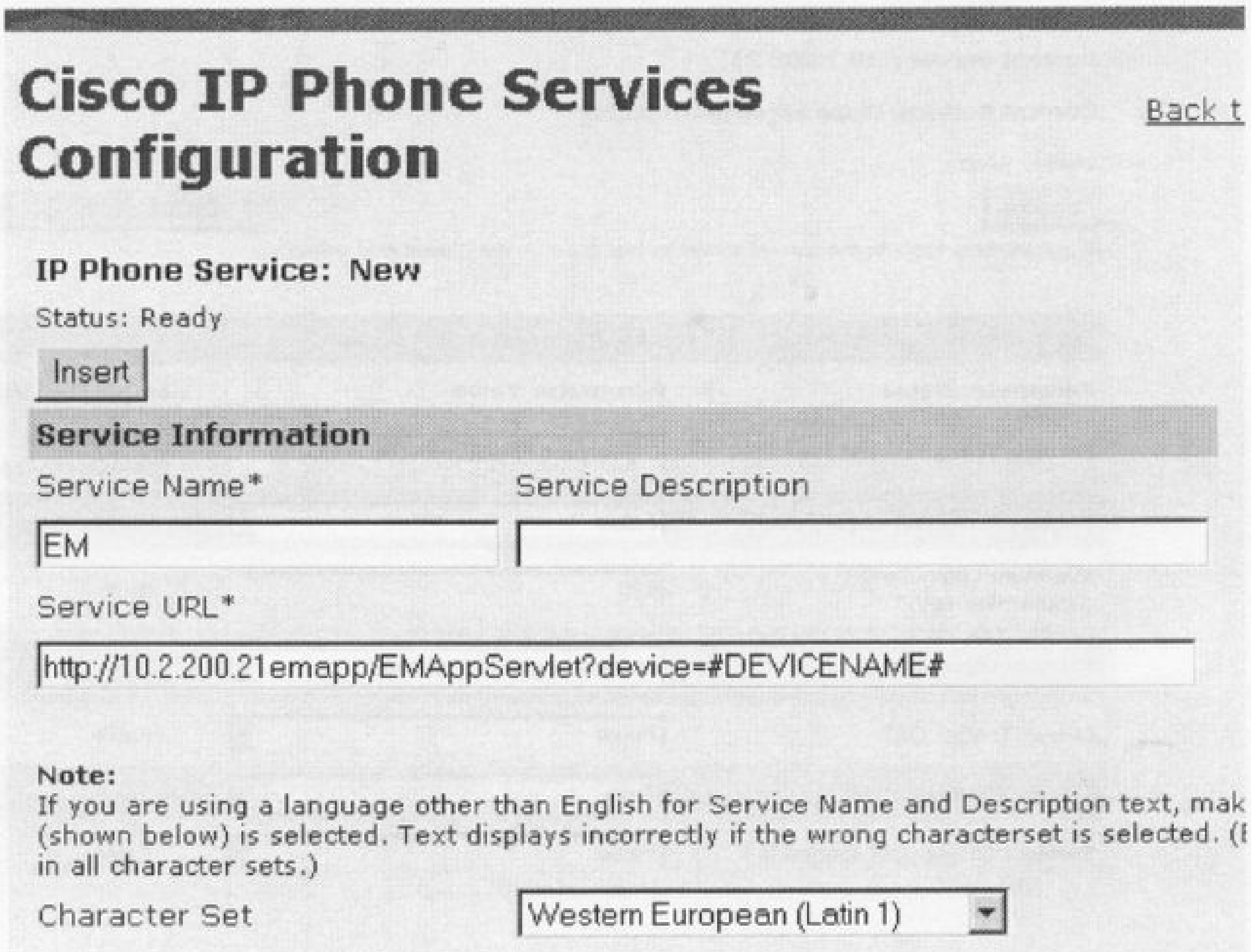
➔ **Define the multi-login behavior, that is, whether you allow the user to log in to more than one device at a time.**

➔ **Enable the Cisco CallManager Extension Mobility debug traces.**

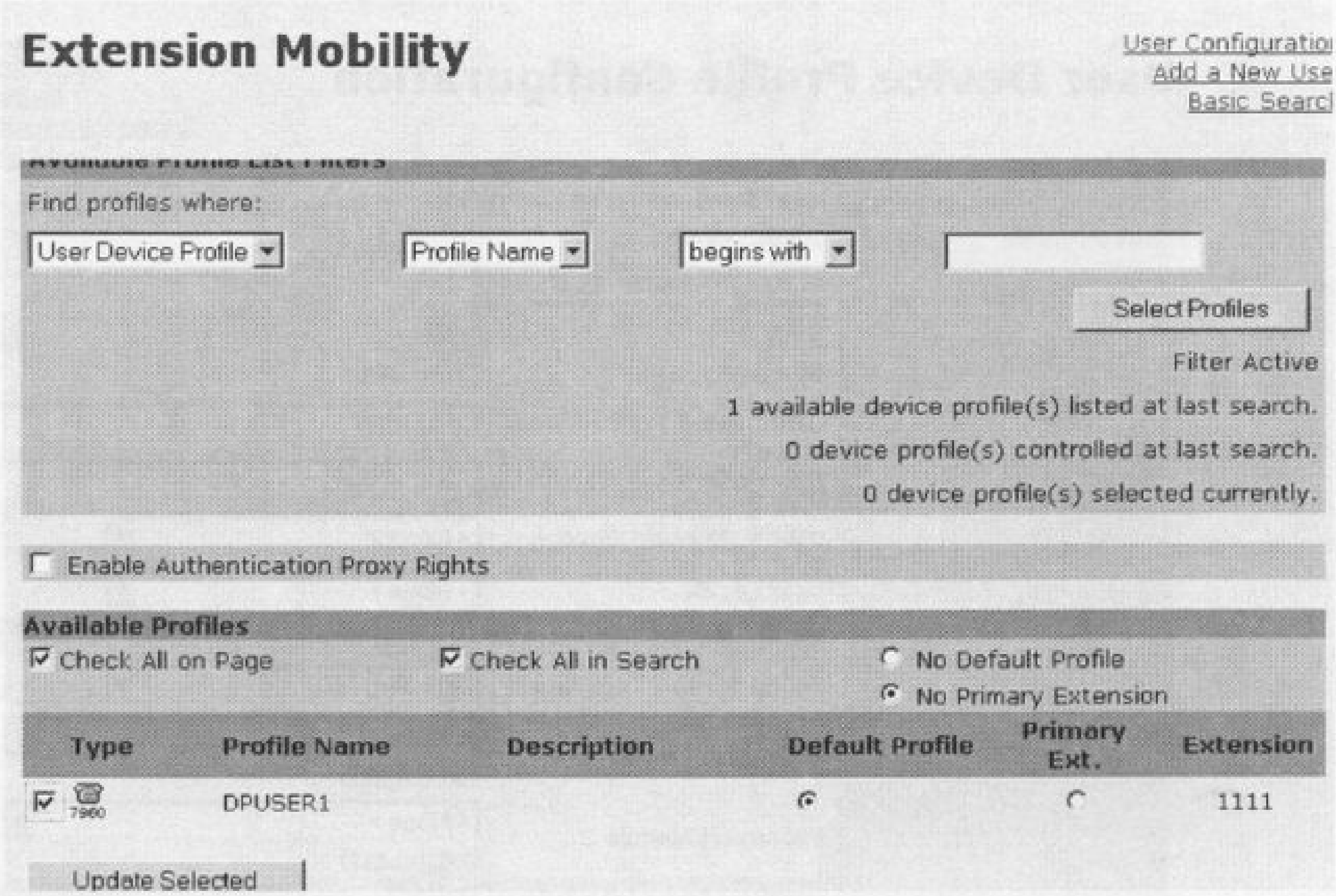
➔ **You must restart the Cisco Tomcat service after changing these Service Parameters.**



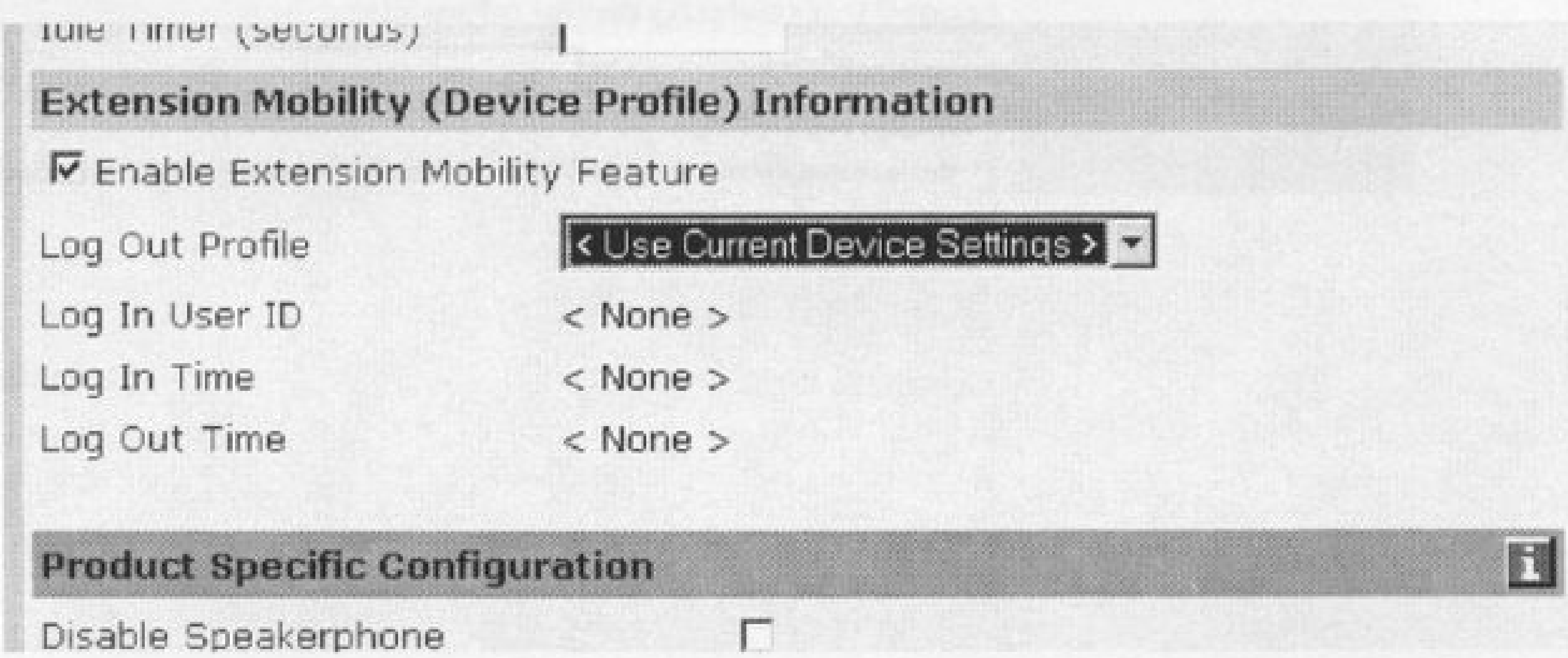
➔ **Create the Cisco CallManager Extension Mobility service.**

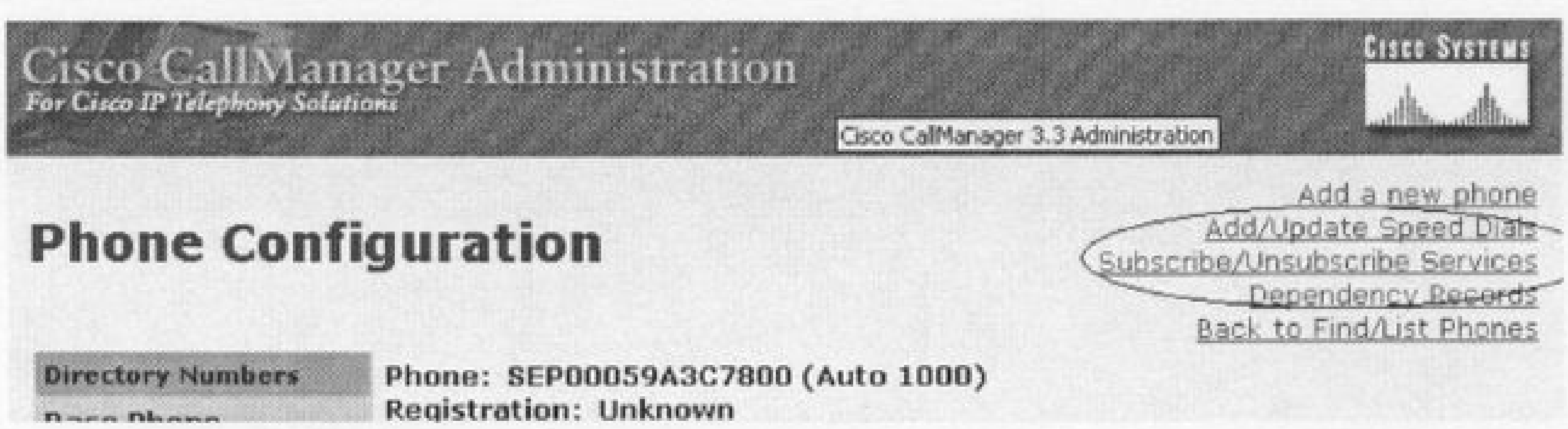


➔ **Associate a User Device Profile to a User.**



➔ **Configure and subscribe Cisco IP Phones to the feature.**





Task 11.5

Create a user with the following information:

- UserID='br1phn3'
- Password='adgjm'
- PIN='12345'
- Associate phone 3 at the BR1 site

Configure Personal Directory and Fast Dials for this user. Create some entries in the Personal Directory and Fast Dials of your choice.

➔ **It is worth pointing out that the Personal Directory/Fast Dials can be located in Documentation CD under CCM3.2 (and not 4.1 – which confuses quite a few people).**

Personal Address Book IP Phone Services

Choose Feature > Cisco IP Phone Services.

In the Service Name field, enter the name "My Address Book"

In the Service Description field, enter the description "Personal Directory - Personal Address Book"

In the Service URL field, enter the URL of the server
http://10.2.200.21/ccmpd/xmlAddressBookInput.asp

Click Insert.

Click the New button to the right of the Parameters list box.
We will create 3 parameters: UserID, UserPIN and PreDial

Parameter Name: UserID
Parameter Display Name: User Identification
Parameter Required: Yes
Parameter Description: Same user identification used with the Cisco IP Phone User Options pane

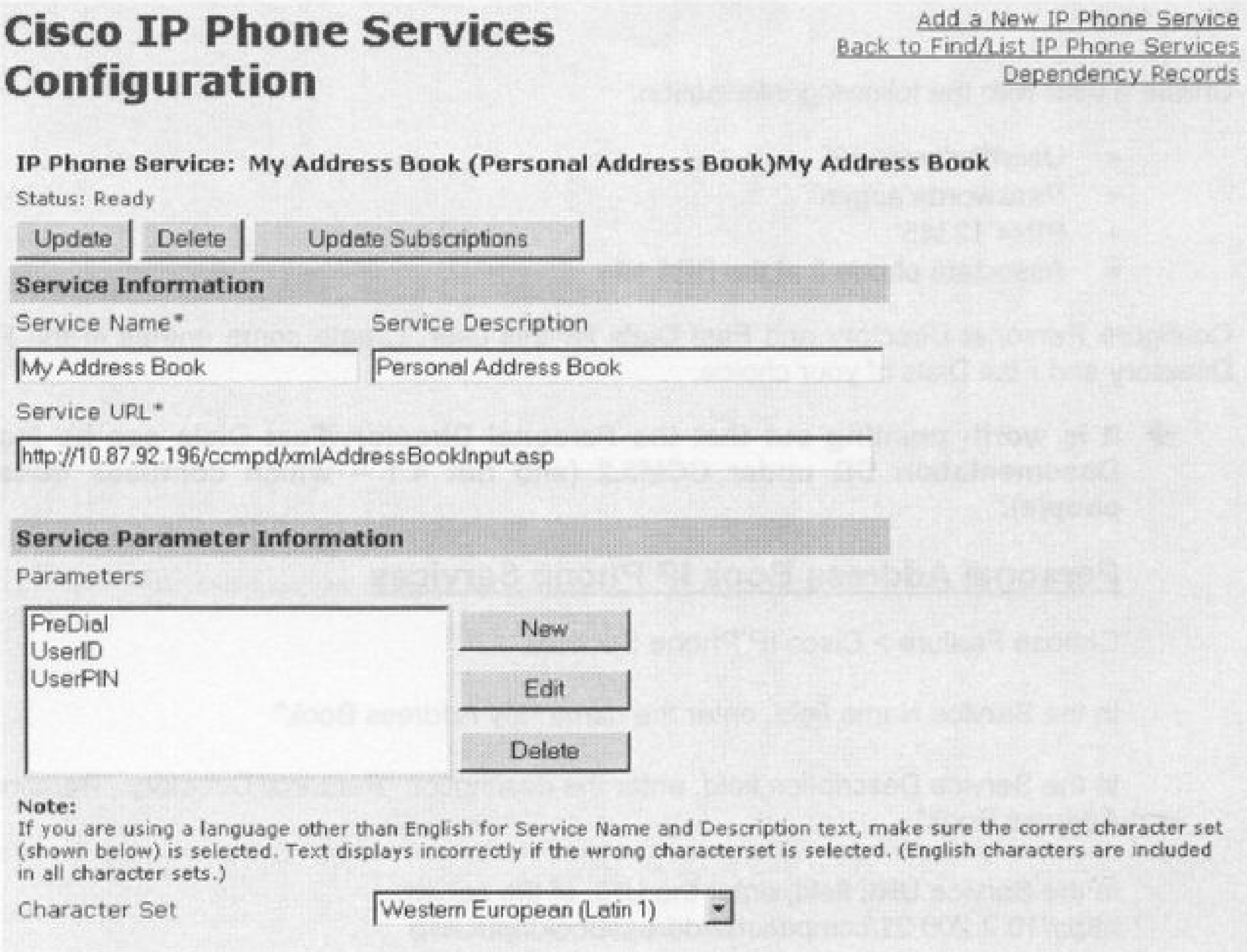
Click Insert to add the parameter.

Parameter Name: UserPIN
Parameter Display Name: PIN
Parameter Required: Yes
Parameter Description: Same user PIN used with the Cisco IP Phone User Options pane

Click Insert to add the parameter.

Parameter Name: PreDial
Parameter Display Name: Outside Access code
Parameter Required: No
Parameter Description: This access code will be added as a prefix to the stored directory number to provide access to an outline line

Click Insert to add the parameter.



Fast Dial IP Phone Services

Choose Feature > Cisco IP Phone Services.

In the Service Name field, enter the name "My Fast Dials"

In the Service Description field, enter the description "Personal Fast Dials"

In the Service URL field, enter the URL of the server
http://10.2.200.21/ccmpd/xmlFastDials.asp

Click Insert.

Click the New button to the right of the Parameters list box.
We will create 3 parameters: UserID, UserPIN and PreDial

Parameter Name: UserID
Parameter Display Name: User Identification
Parameter Required: Yes
Parameter Description: Same user identification used with the Cisco IP Phone User Options pane

Click Insert to add the parameter.

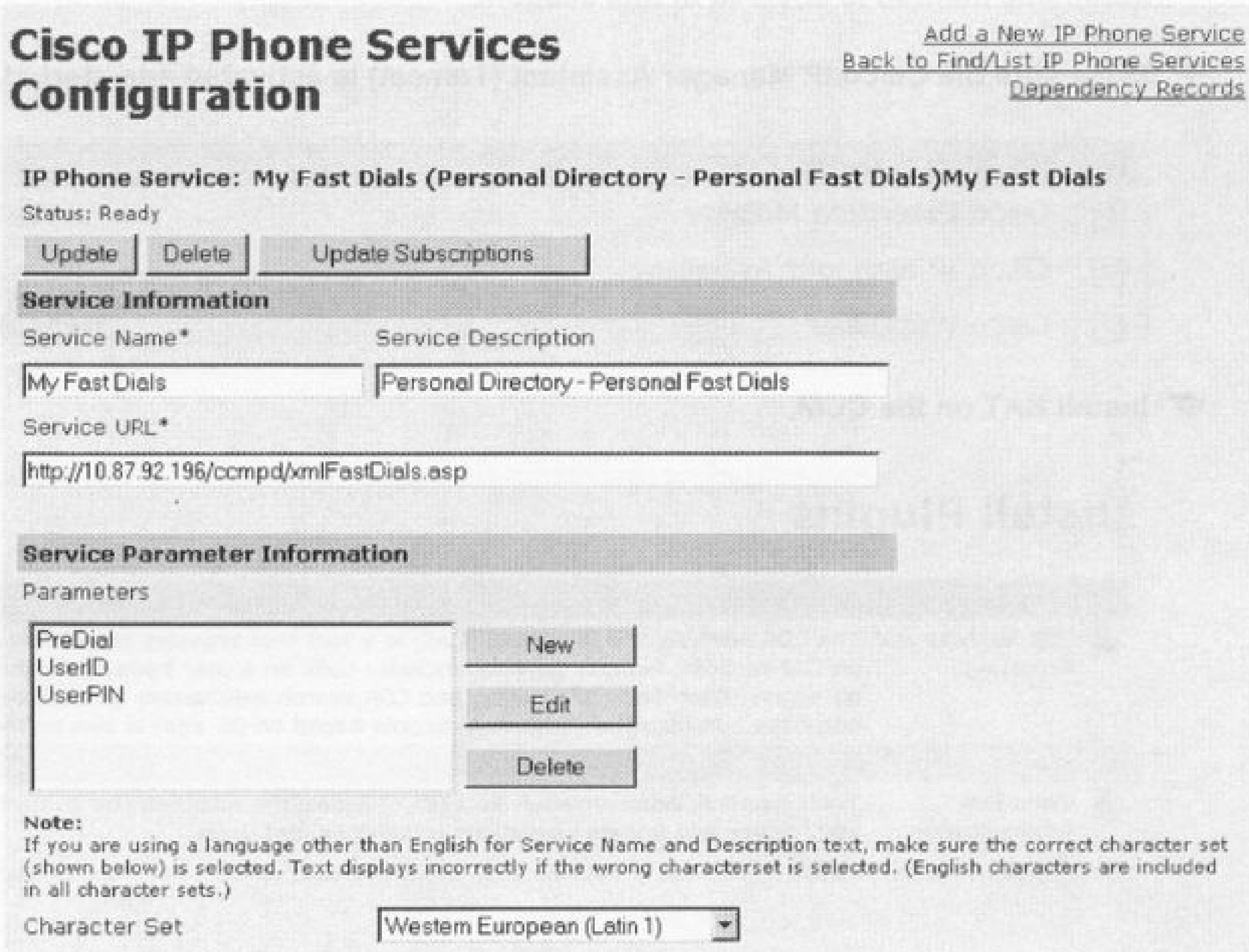
Parameter Name: UserPIN
Parameter Display Name: PIN
Parameter Required: Yes

Parameter Description: Same user PIN used with the Cisco IP Phone User Options pane

Click Insert to add the parameter.

Parameter Name: PreDial
Parameter Display Name: Outside Access code
Parameter Required: No
Parametetr Description: This access code will be added as a prefix to the stored directory number to provide access to an outline line

Click Insert to add the parameter.



➔ **Create the Br1phn3 user and associate the corresponding device. Subscribe the new user to the services.**

Task 11.6

Configure IPMA with the following information: BR1 phone 3 will be used as the manager phone and HQ phone 3 will be used as the assistant phone.

Username: br1phn3	**Username: Assistant**
Primary Line: 2003	Primary Line: 1003
SD to Intercom	Proxy Line: 1560
	Incoming Intercom

➔ **Either use wizard (need to install BAT) or do the whole thing manually! The automatic method is covered in this section.**

➔ **Make sure the Cisco IP Manager Assistant (Tomcat) is activated and started.**

Tomcat Web Service	
☑ Cisco Extension Mobility	Activated
☑ Cisco IP Manager Assistant	Activated
☐ Cisco WebDialer	Deactivated

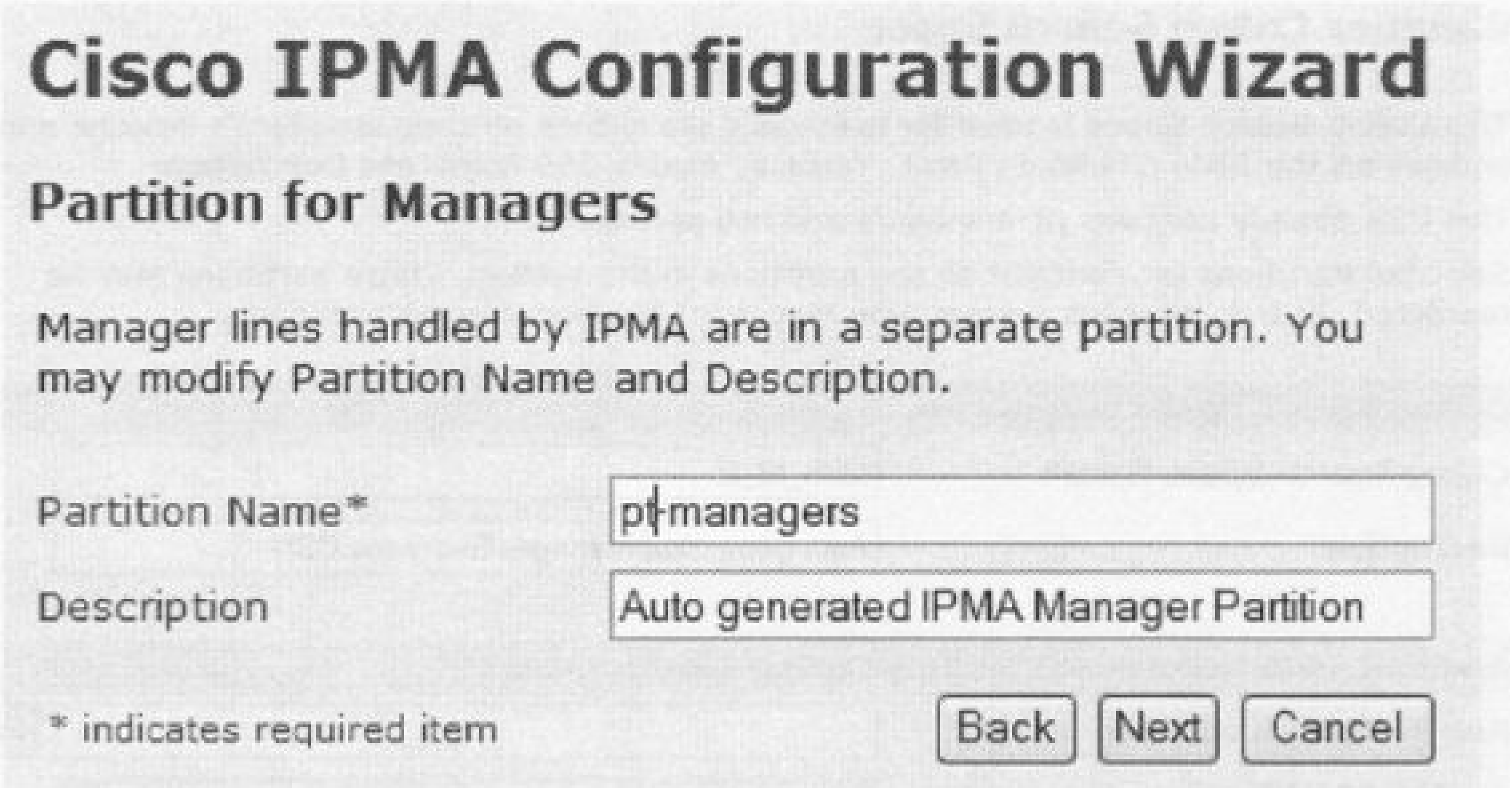
➔ **Install BAT on the CCM.**

Install Plugins

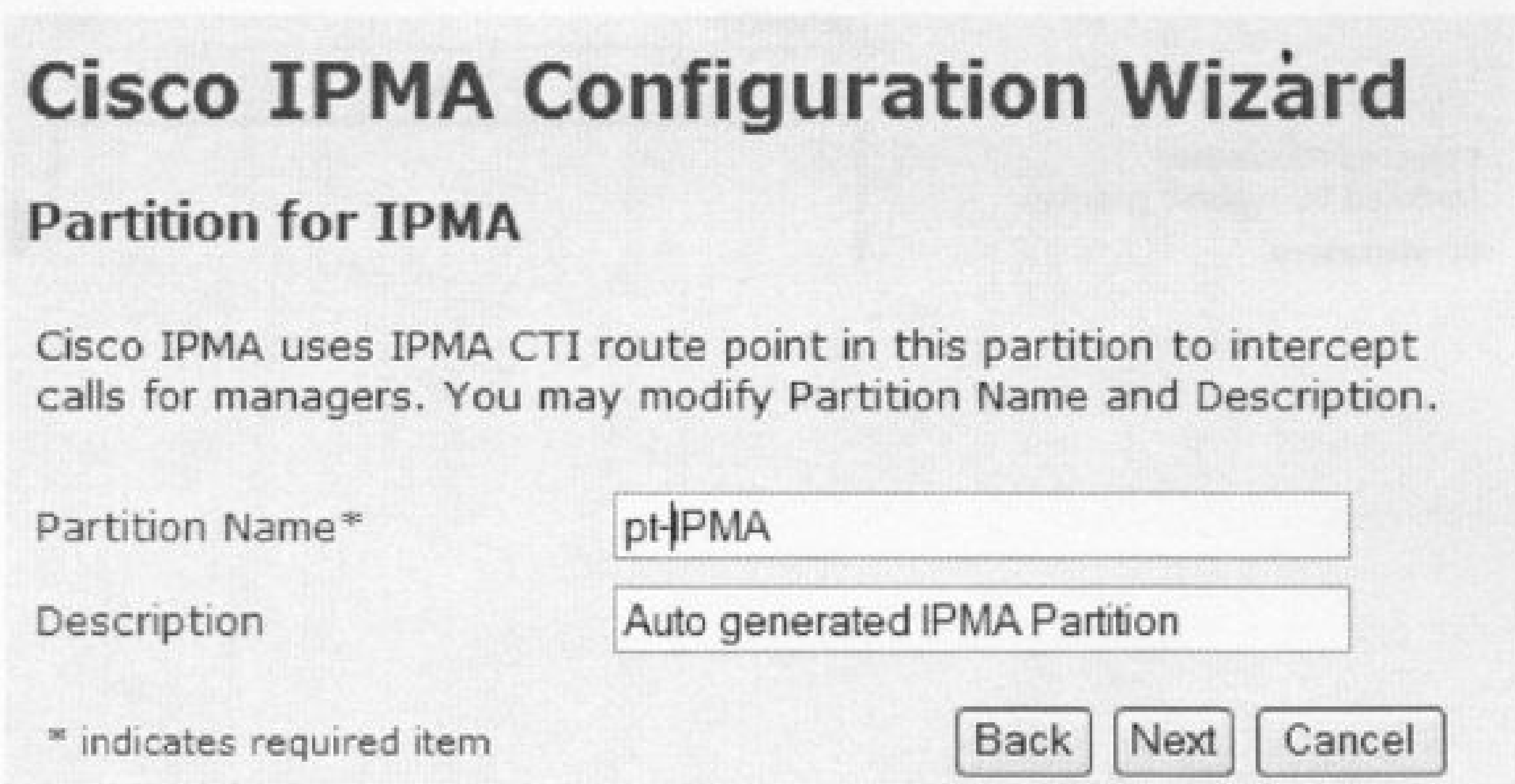
Plugin Name	Description
CDR Analysis and Reporting	The CDR Analysis and Reporting (CAR) is a tool that provides reports on calls base on CDR records. Reports provided include: Calls on a user basis, Calls through gateways, Simplified Call Quality, and CDR search mechanism. In addition, limited database administration (deleting records based on DB size) is also provided.
Cisco Bulk Administration Tool	The Cisco Bulk Administration Tool (BAT) allows the administrator to perform bulk add, delete and update operations on devices and users.

➔ **Run Cisco IPMA Configuration Wizard.**

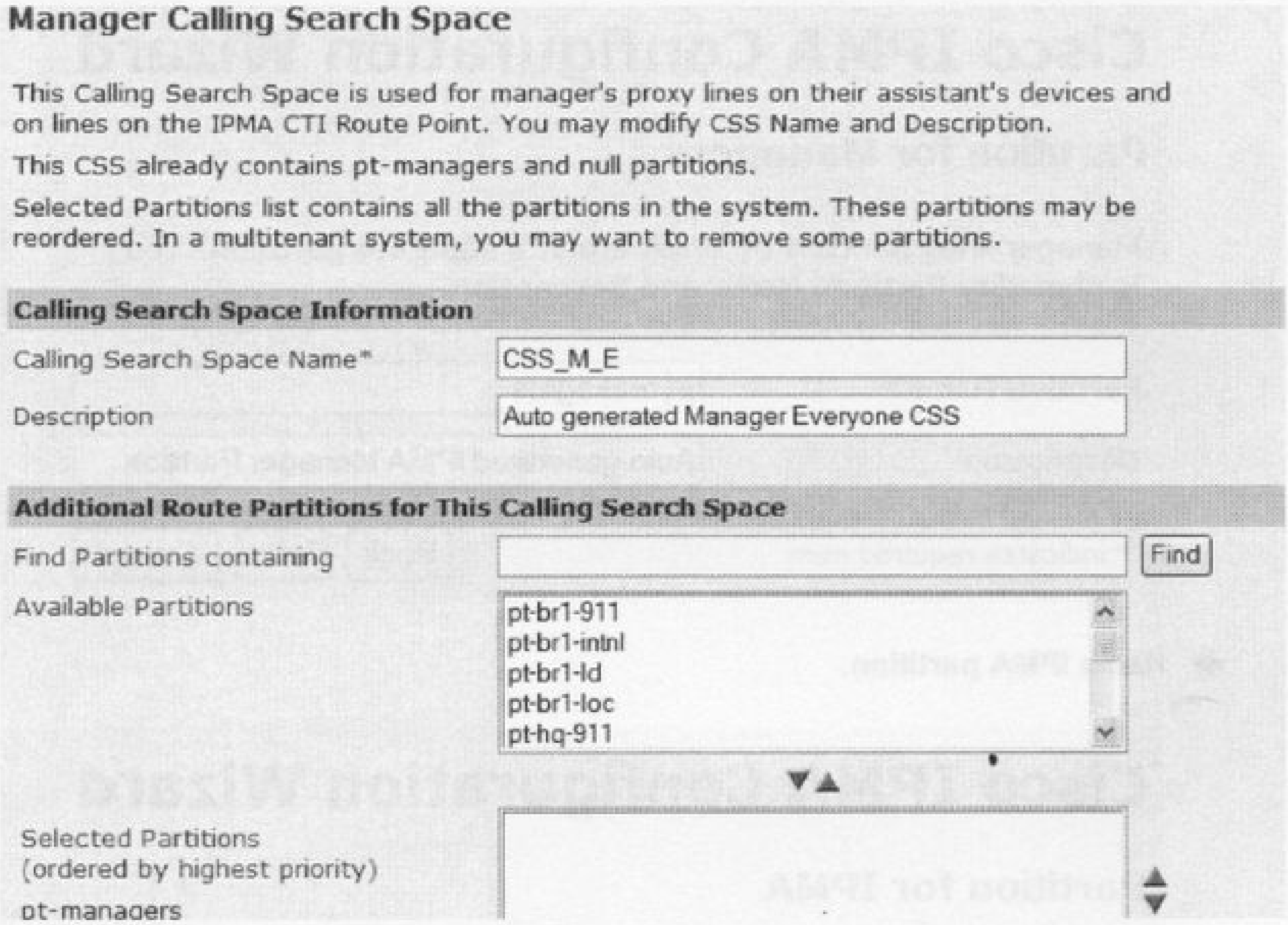
➔ **Name manager partition.**



➔ **Name IPMA partition.**



➔ **We will still be using the <None> partition for the LINES so put garbage in the Generated_Everyone_partition and skip to the CSS for the Assistant proxy line and IPMA Route Point.**



➔ **Create CSS for the Manager line, assistant and user LINES.**

IPMA Calling Search Space

This Calling Search Space is used for manager's and assistant's own lines and all user lines. You may modify CSS Name and Description.

This CSS already contains pt-IPMA and null partitions.

Selected Partitions list contains all the partitions in the system. These partitions may be reordered. In a multitenant system, you may want to remove some partitions.

Calling Search Space Information

Calling Search Space Name* CSS_I_E

Description Auto generated IPMA Everyone CSS

Additional Route Partitions for This Calling Search Space

Find Partitions containing [Find]

Available Partitions
- pt-br1-911
- pt-br1-intnl
- pt-br1-ld
- pt-br1-loc
- pt-hq-911

Selected Partitions (ordered by highest priority)
- pt-IPMA

➔ **Select the CSS to which pt-IPMA will be added.**

Existing Calling Search Spaces

Cisco IPMA requires exisitng calling search spaces to be prepended with pt-IPMA a partitions.

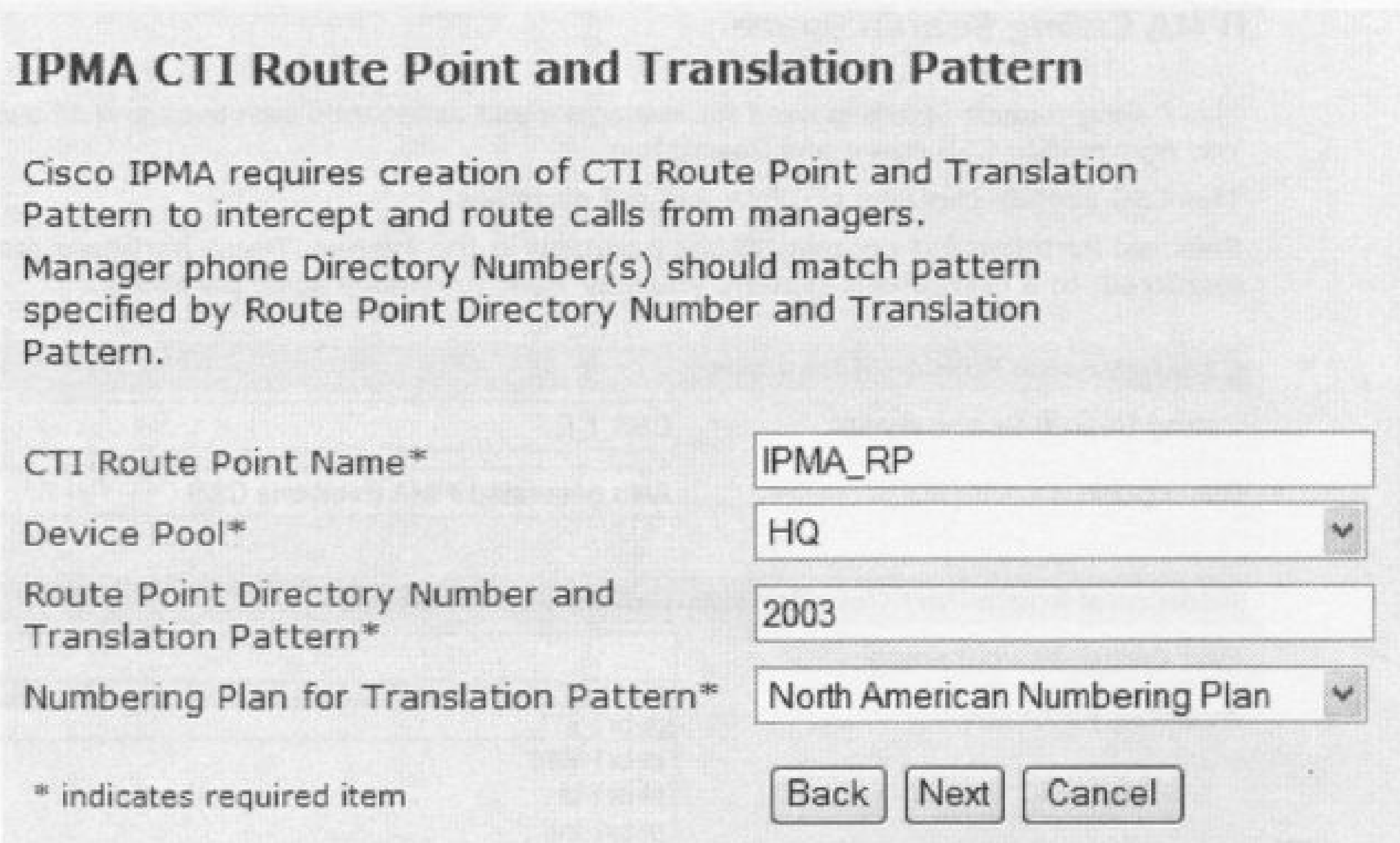
Selected Calling Search Spaces lists all the existing CSSs in the system that will b prepended. In a multitenant system, you may want to remove some CSSs.

Calling Search Spaces

Available Calling Search Spaces
- css-line1
- css-line2
- css-mwi
- css-plar

Selected Calling Search Spaces
- css-br1-911-loc
- css-br1-all
- css-hq-911-loc
- css-hq-all
- css-hq-phn3

➔ **Configure the IPMA Route Point.**



➔ **Configure the IPMA Phone service.**

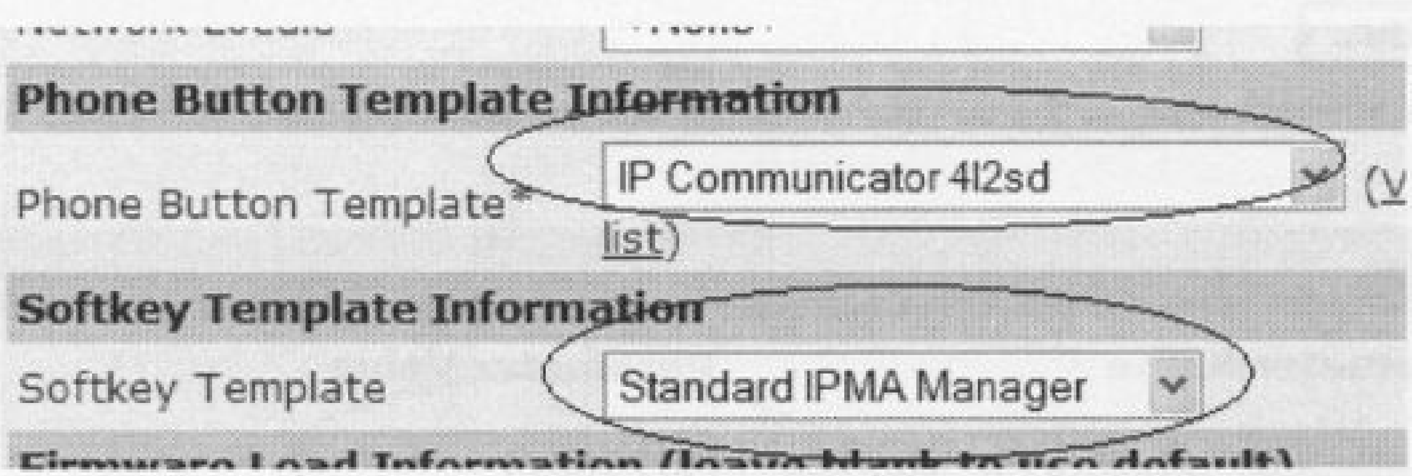
➔ **Check information and Submit.**

➔ **After the wizard is complete, next step is to complete the IPMA service parameters.**

➔ **Create a 4LINE/2SPEED DIAL Phone Button Template for IP Communicator (manager) and 7960 (Assistant).**

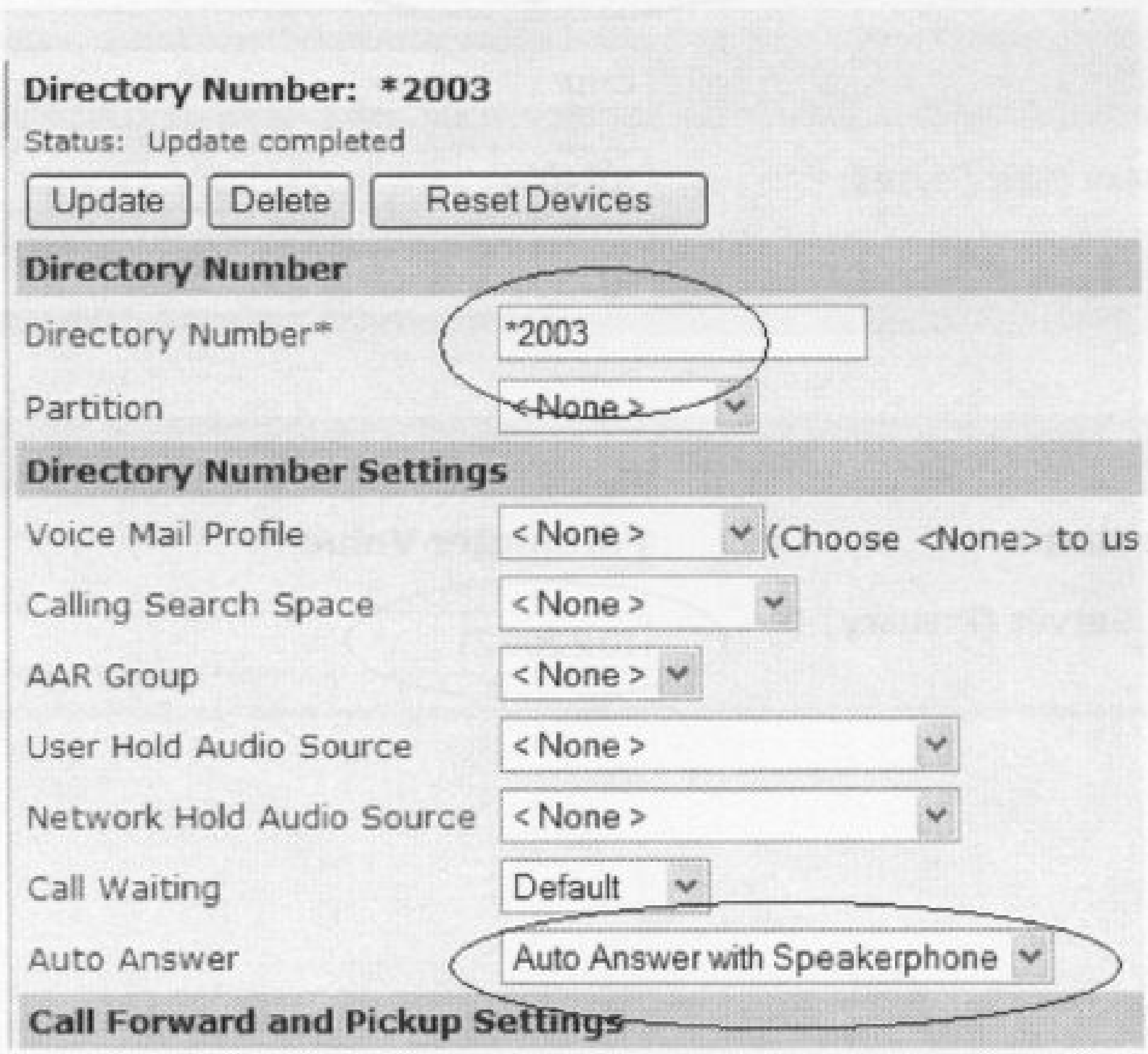
➔ **On the Manager phone:**

➔ **Assign the 4L-2SD Template to the IP Communicator and also the Softkey Template.**



➔ **Subscribe the Manager phone to the IPMA Service.**

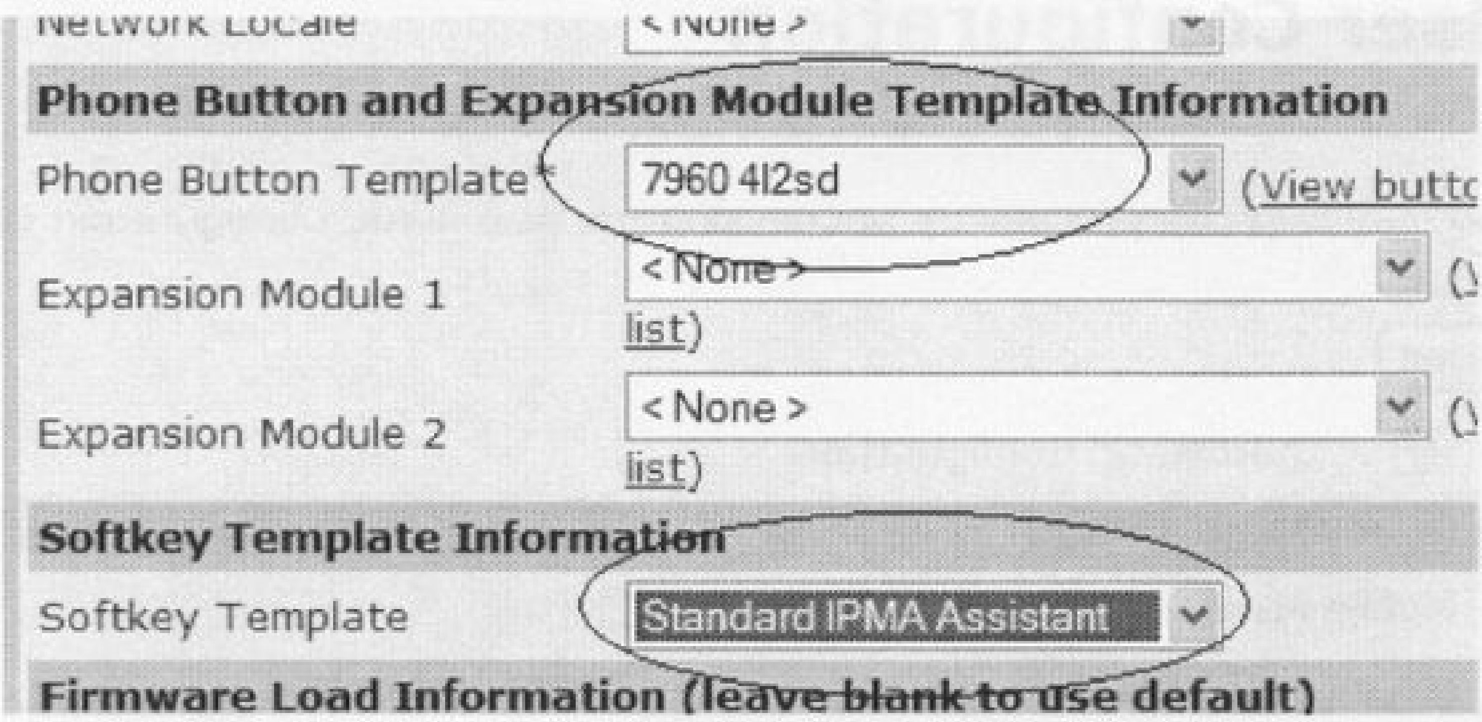
➔ **Create the incoming intercom line on the Manager phone (give it DN=*2003).**



➔ **Also create a Speed Dial for the outgoing intercom (Speed Dial to *1003).**

➔ **On the Assistant phone:**

➔ **Assign phone Template and Softkey Template.**



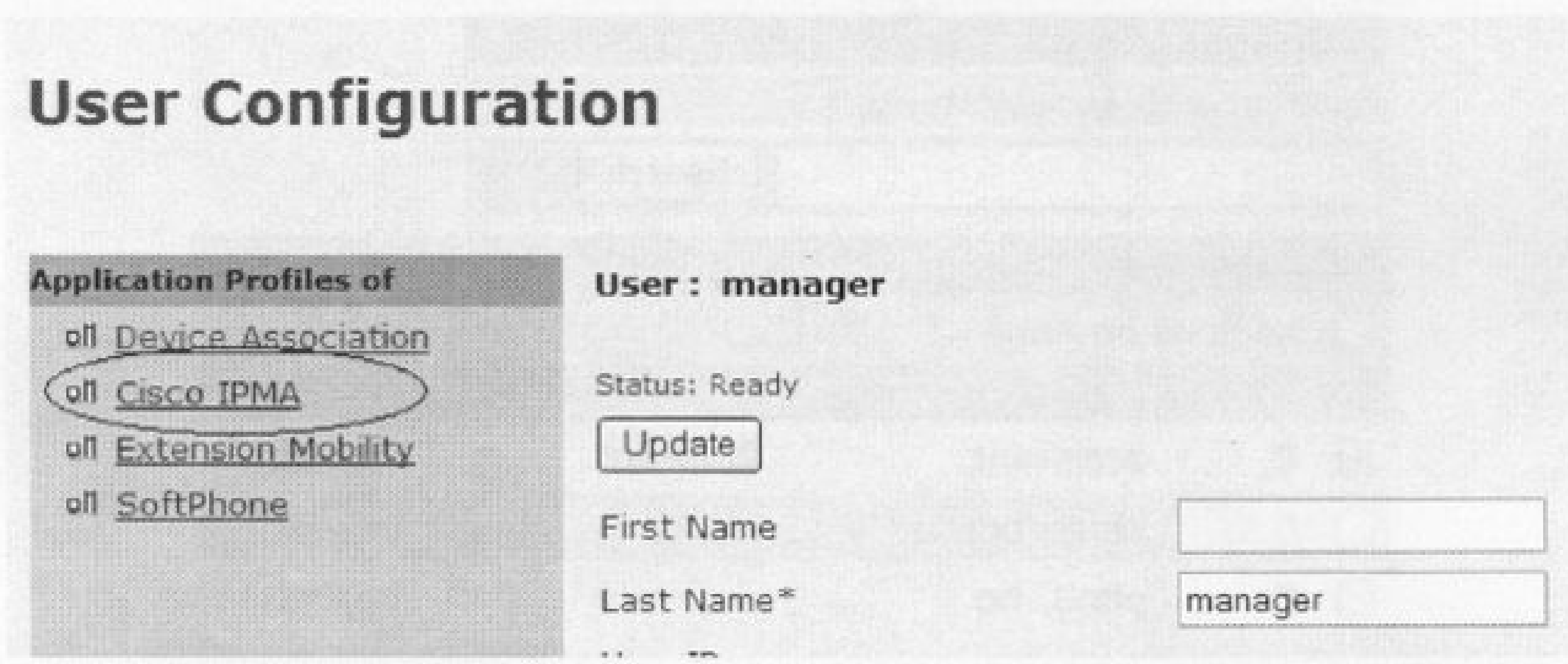
➔ **Create the proxy line with DN=1560 and assign the LINE CSS-M-E.**

➔ **Create the incoming intercom line on the Assistant phone (give it DN=*1003) with auto-answer set to speakerphone.**

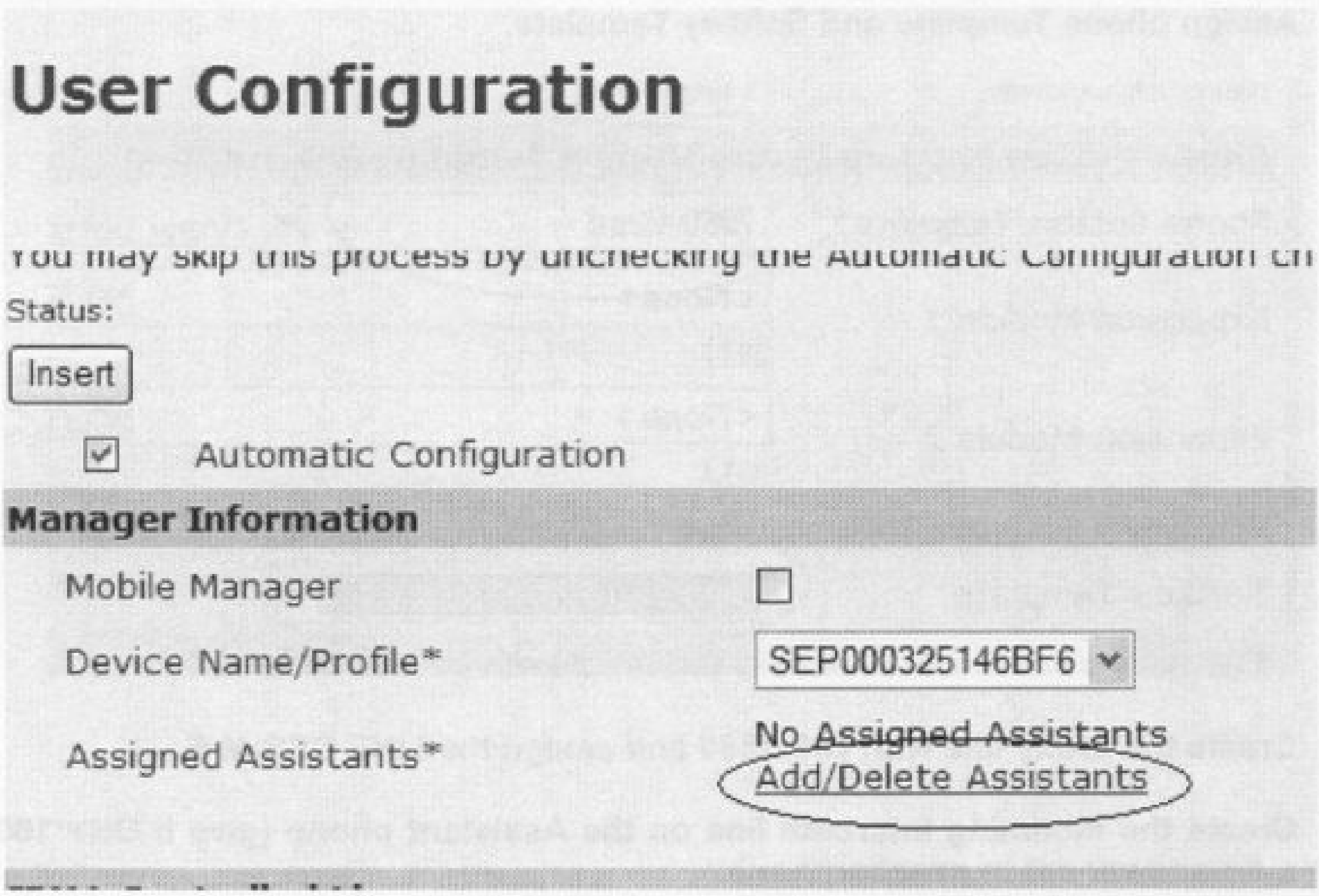
➔ **Create the outgoing Speed Dial to the Manager Intercom.**

➔ **Create two users (manager and assistant) for testing. Check "Enable CTI Application Use" and associate the user with the IP phone.**

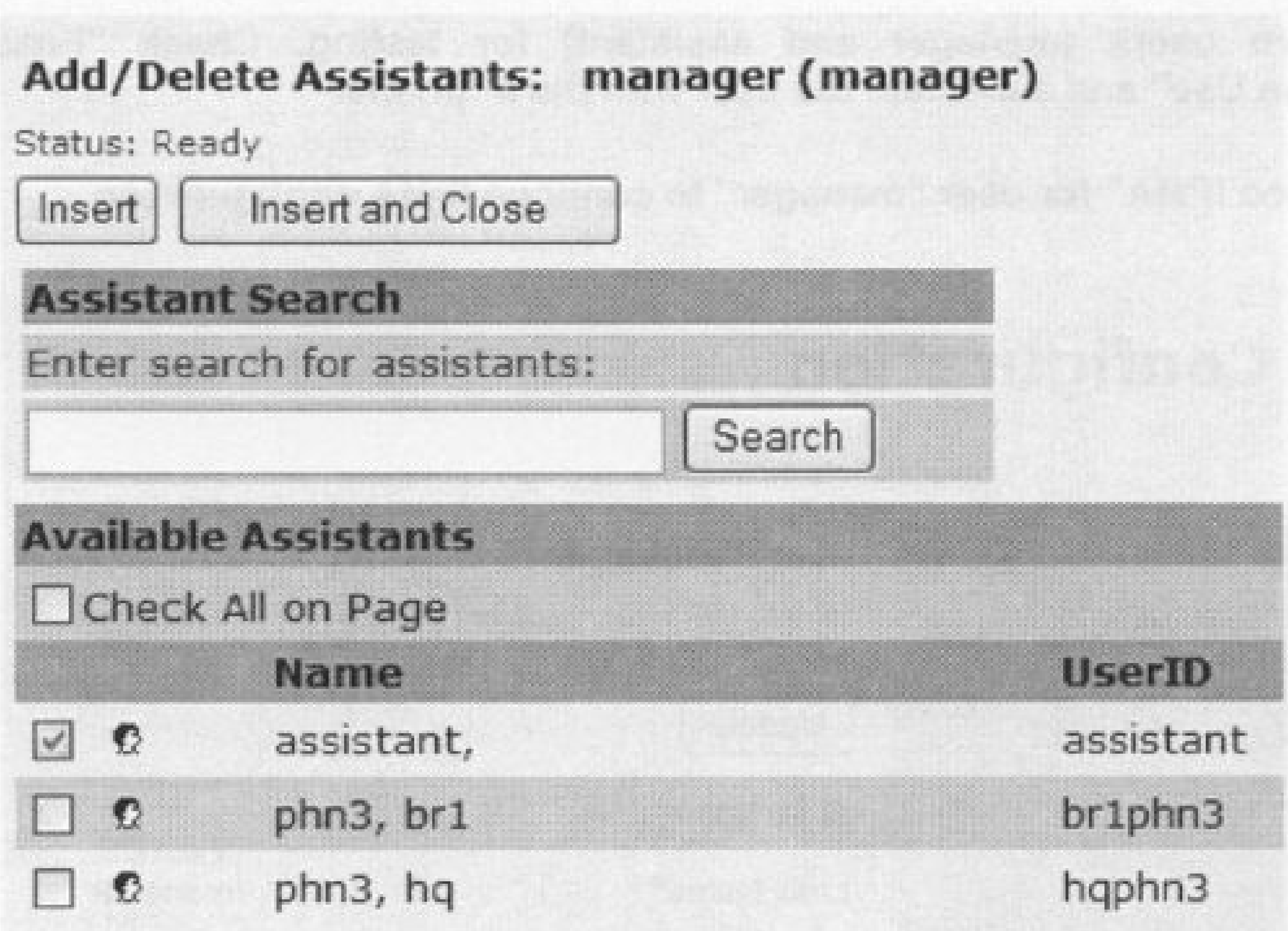
➔ **Click "Cisco IPMA" for user "manager" to continue IPMA configuration.**



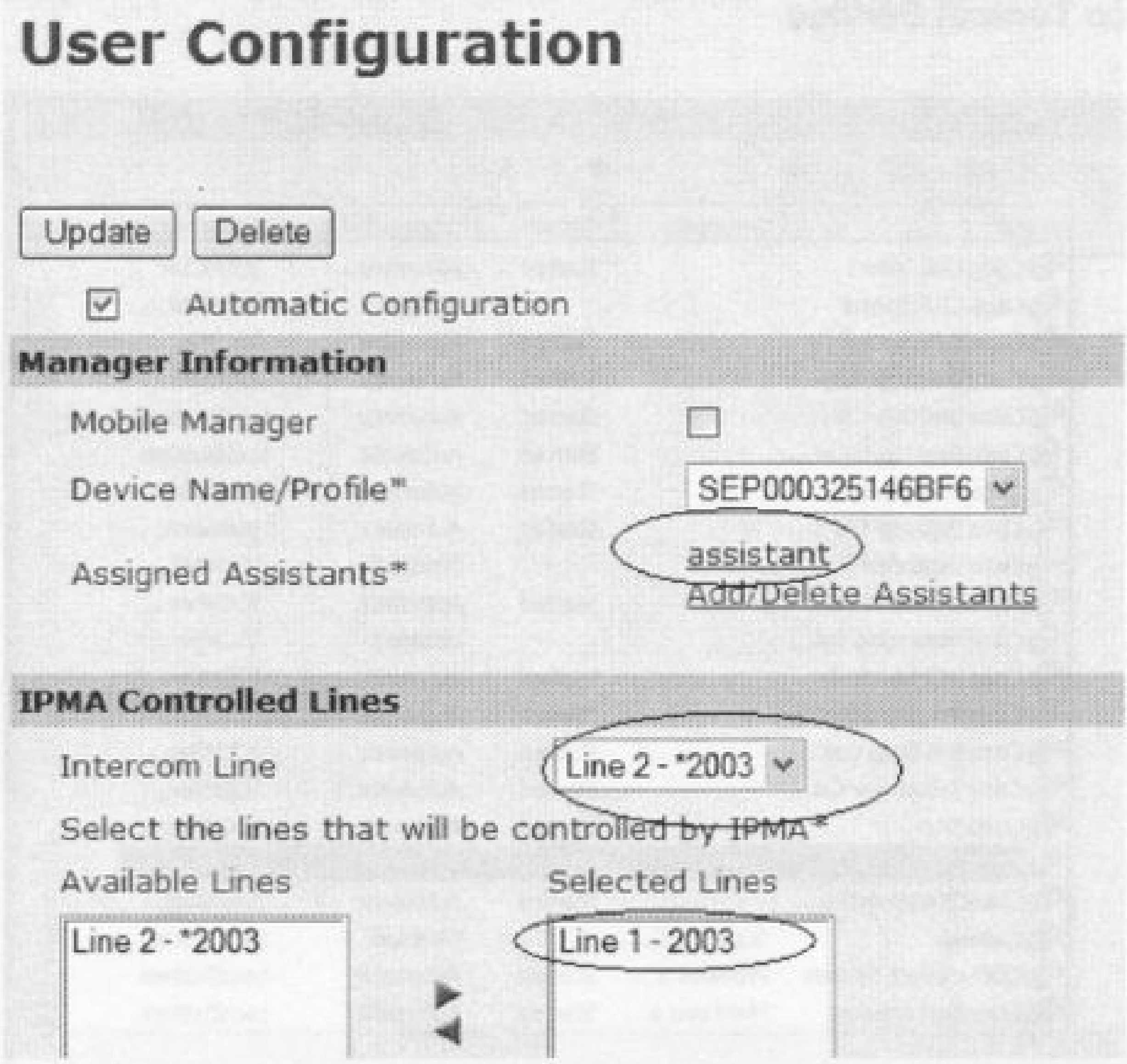
➔ **Add an Assistant:**



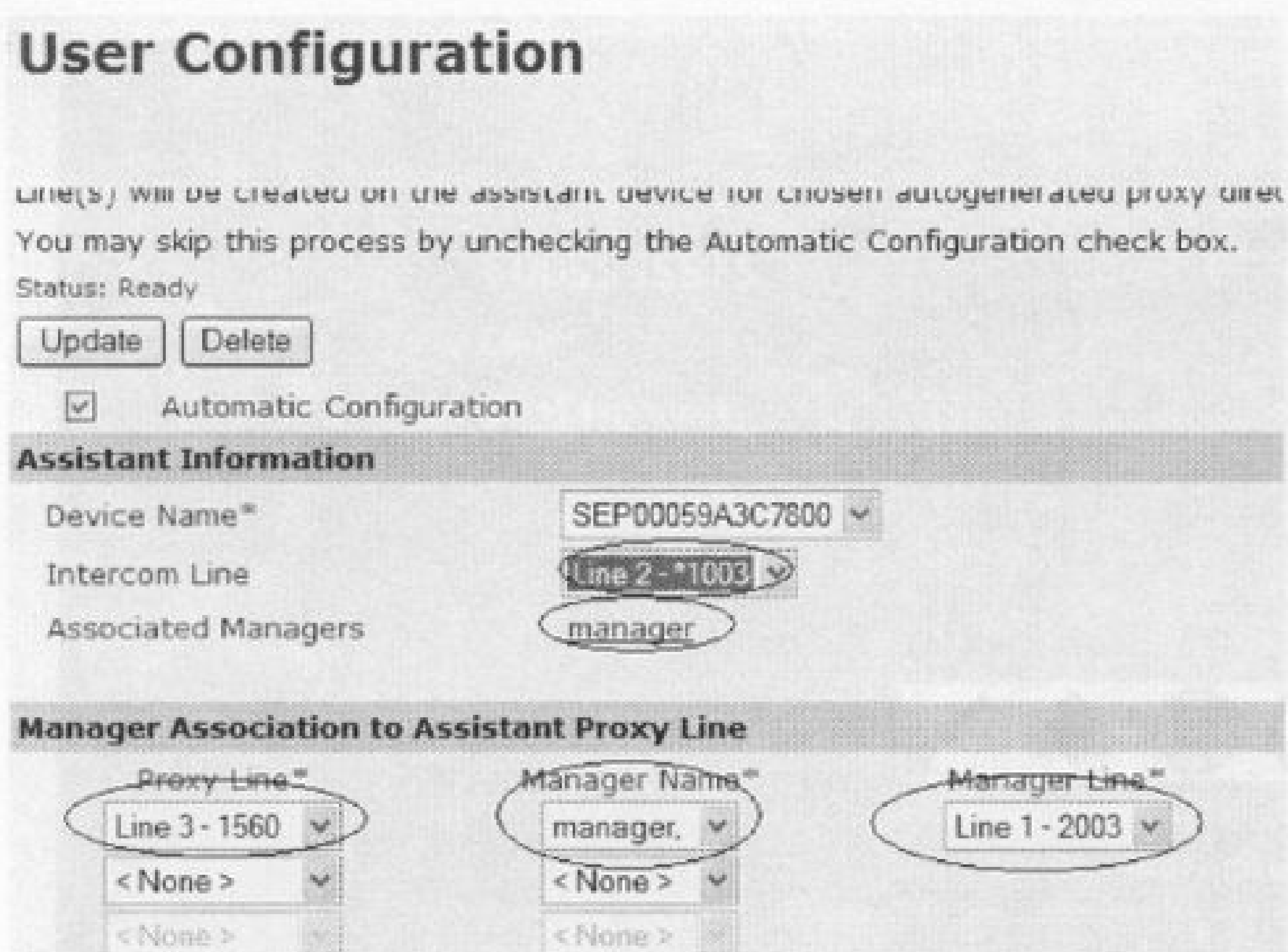
➔ **Select correct Assistant:**



➔ **Select Manager Intercom line and Manager main line.**



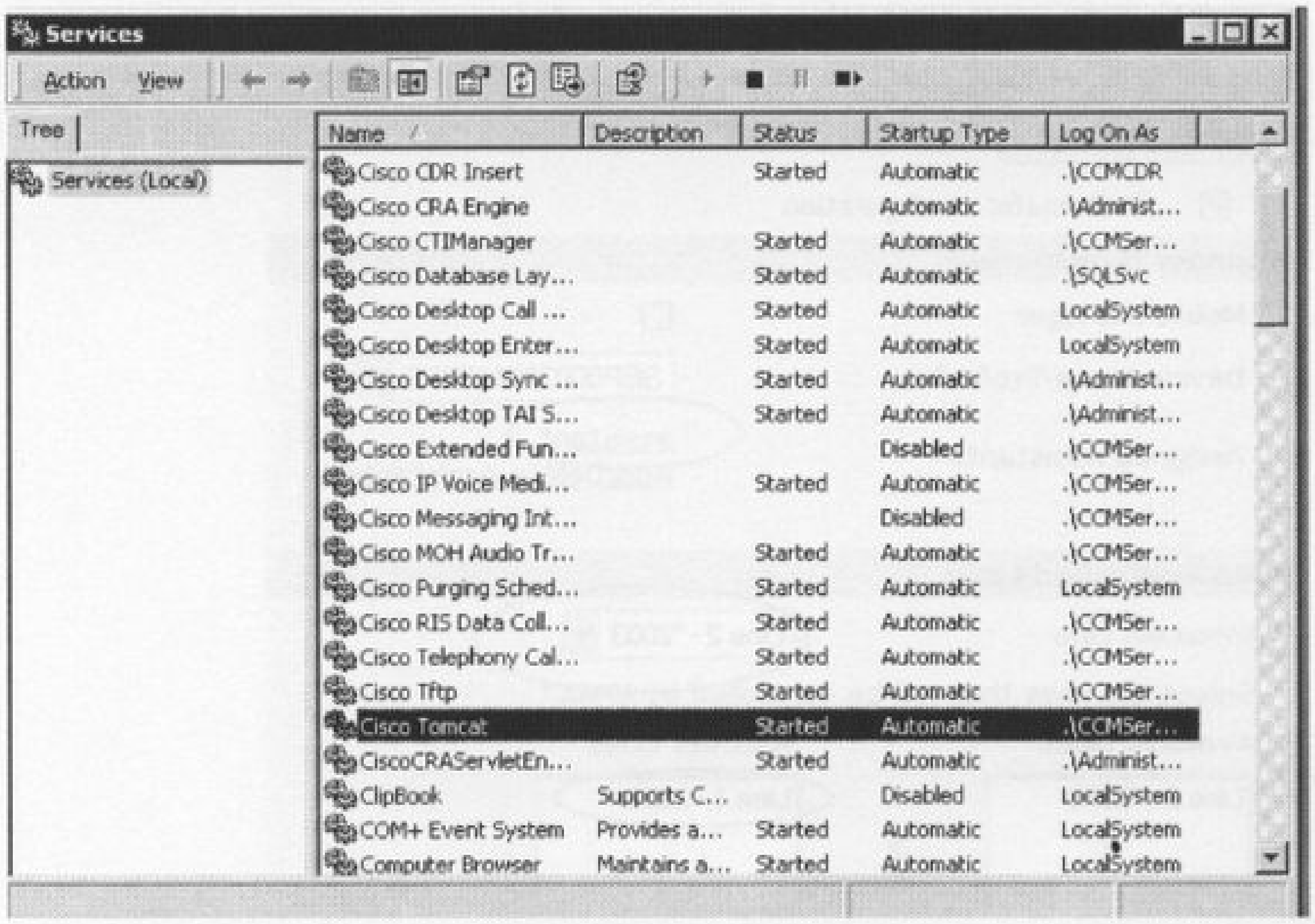
➔ **In the Assistant IPMA section, select the correct Intercom, Proxy and Manager lines.**



➔ **Put the Translation Pattern back to the <None> partition. Do the same for any LINES the wizard placed into the Garbage partition (Null or PT_Generated_Everyone).**

➔ **Assign Gateways and Trunks the CSS-I-E partition.**

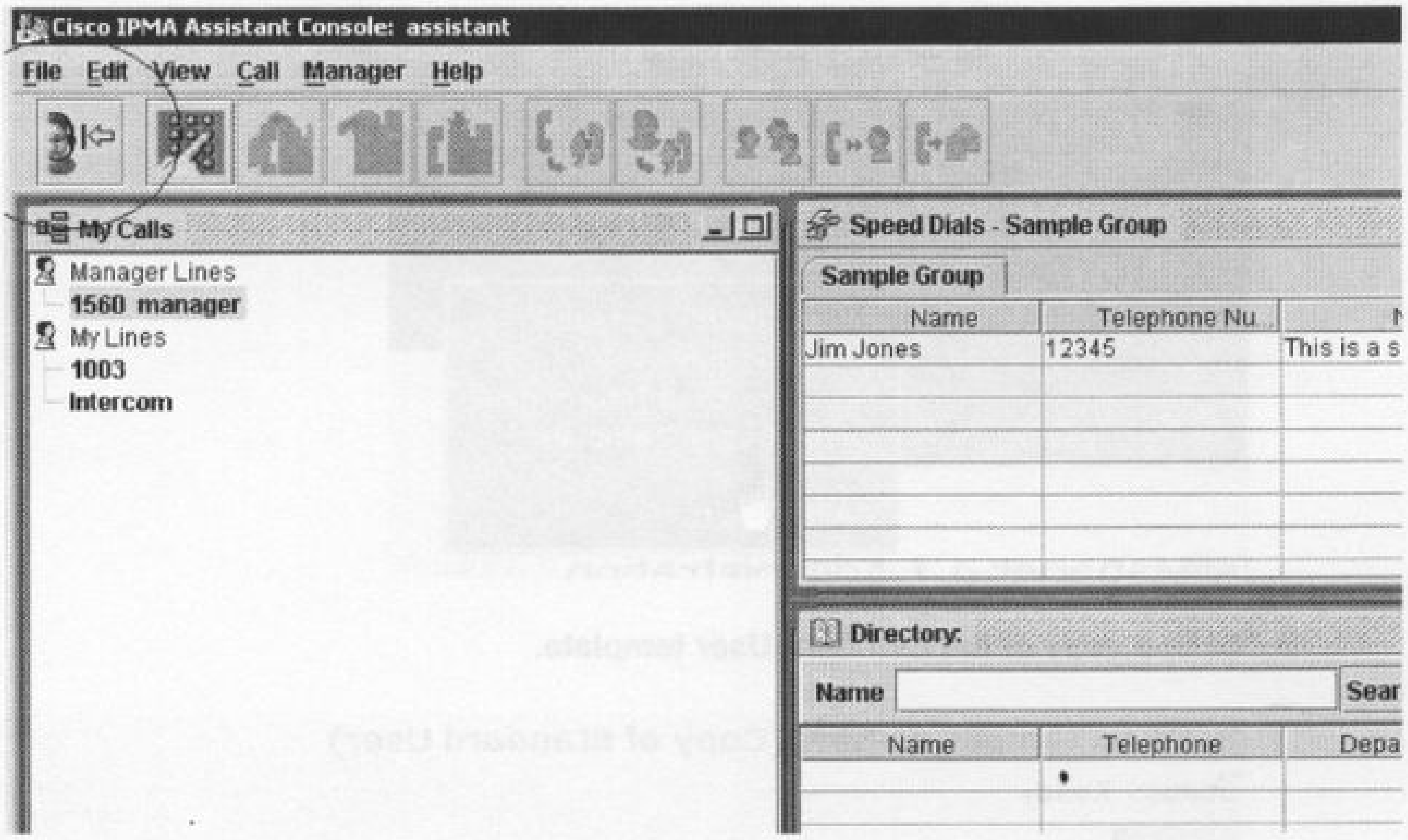
➔ **Restart the Cisco Tomcat Service**



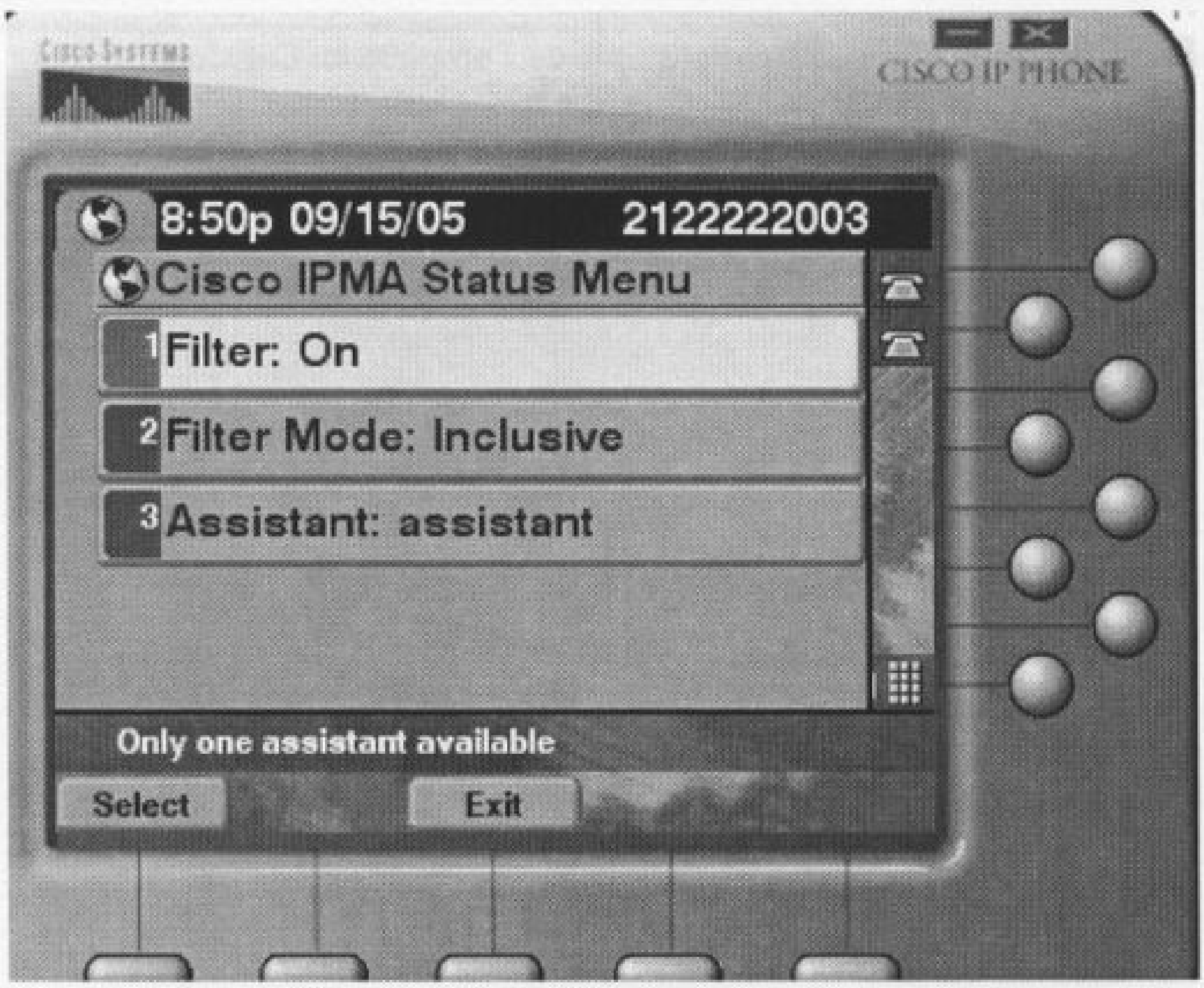
➔ **You should see the IP Communicator have a few strange icons on the LCD – that means IPMA is running.**

➔ **To install IPMA Assistant Console application, use the following URL: http://<IPMA server>/ma/Install/IPMAConsoleInstall.jsp.**

➔ **Log on as the Assistant.**



➔ **From the Manager Phone log onto the IPMA Service and select your assistant.**

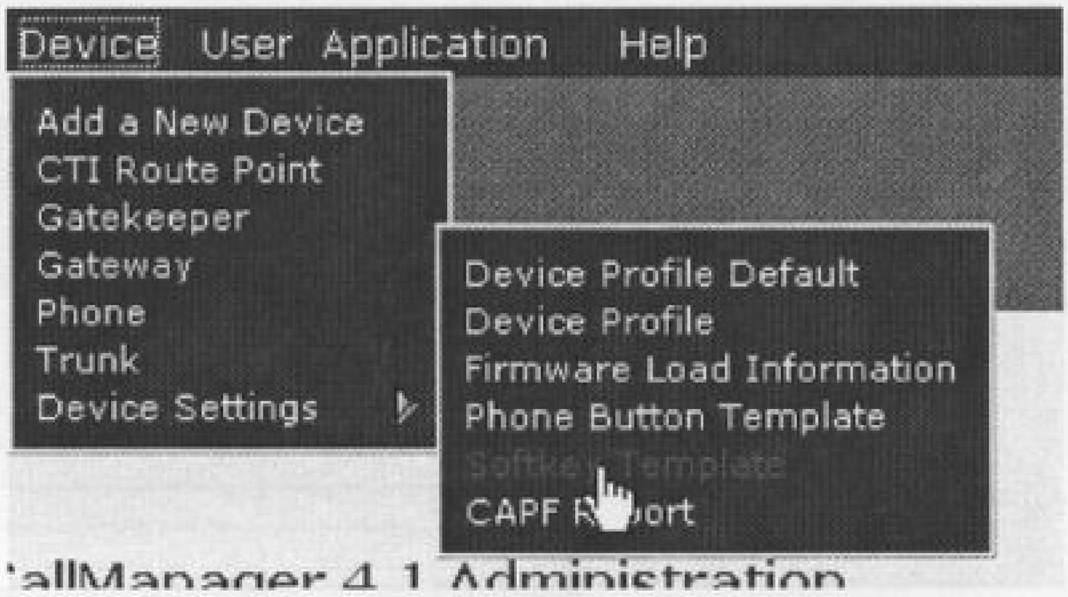


➔ **Make the call from a third phone and check that IPMA is working.**

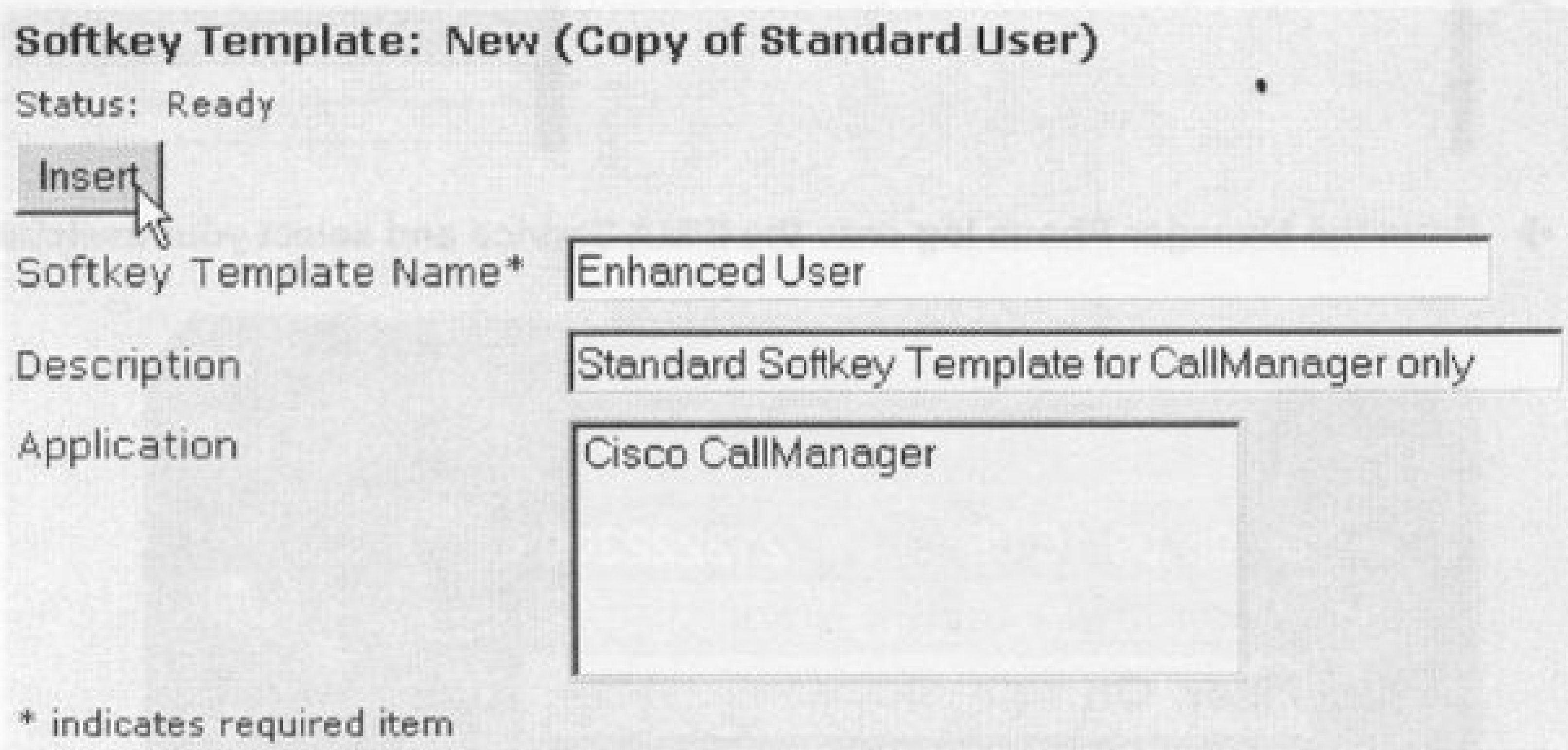
Task 11.7

If a call rings into HQ Phone 3, that user must have the option of sending that call to VM without exhausting the CallFwdNoAn timer.

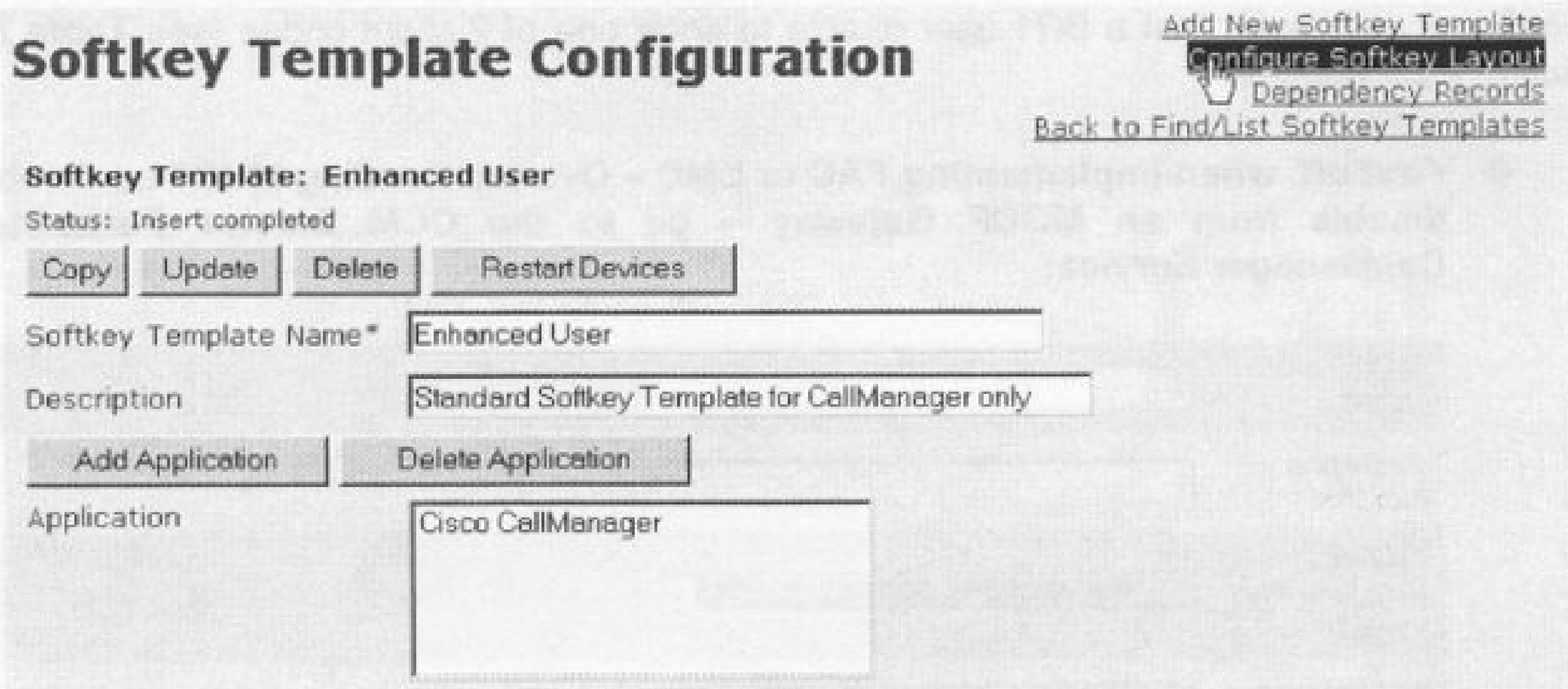
➔ **Go to Device ➔ Device Settings ➔ Softkey Template.**



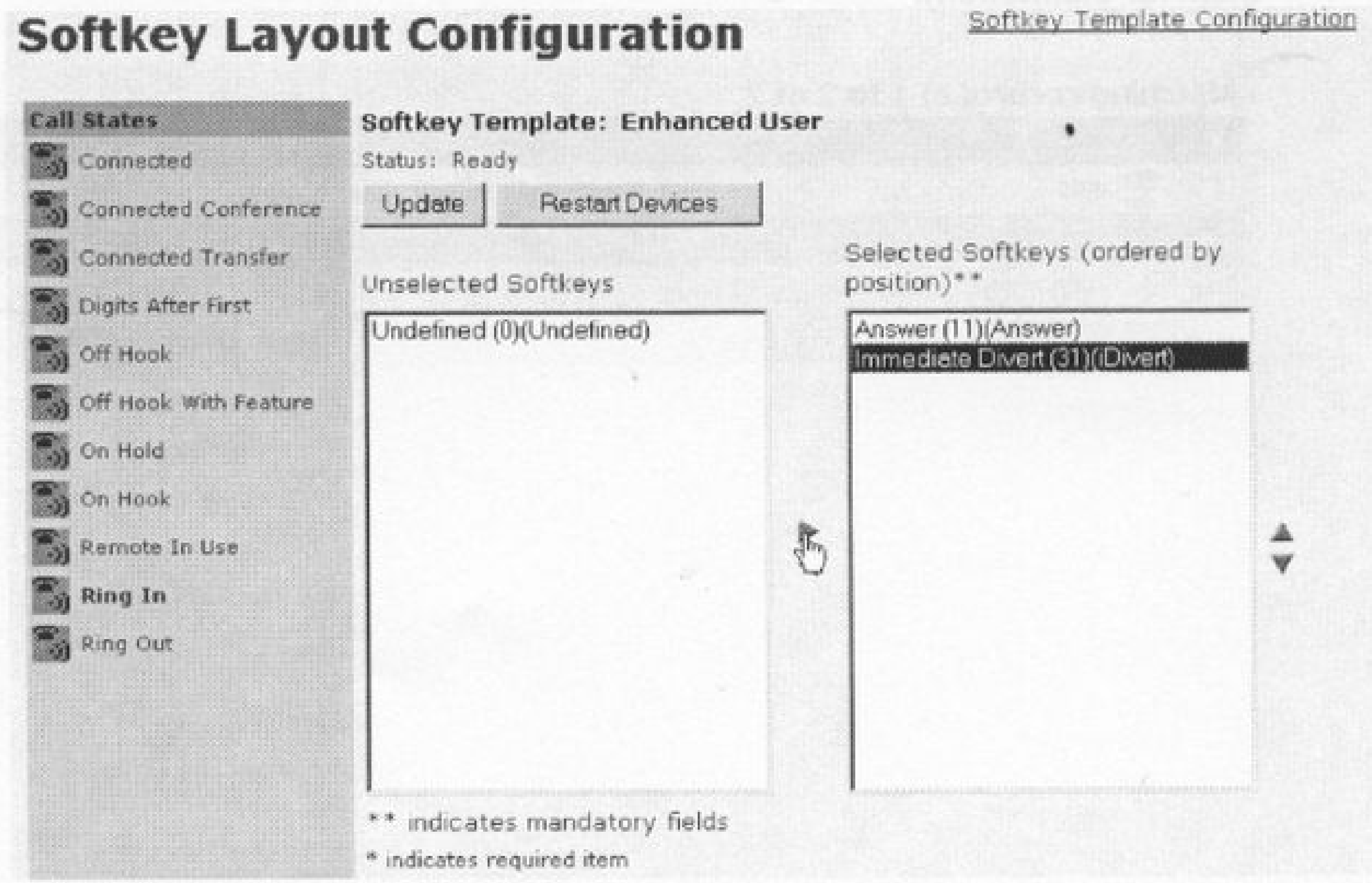
➔ **Make a copy of the Standard User template.**



➔ **Click on Configure Softkey Layout.**



➔ **Now click on the Call State of "Ring In" and move "Immediate Divert" over to the Selected Softkeys field.**



➔ **Finally you must apply this new softkey to the HQ Phone 3 Device.**

Task 11.8

Configure calls such that a BR1 user is able to enter one of 2 client codes (see **Table 3**) when dialing a LD number.

➔ **First off, when implementing FAC or CMC – Overlap Sending MUST be disabled. To disable from an MGCP Gateway – go to the CCM Service Parameters for CallManager Service:**

MGCP Timer (sec)*	3	3
Numbering Plan Info*	1	1
Overlap Receiving Flag for PRI*	False	True
Port Release Timer (sec)*	0	0

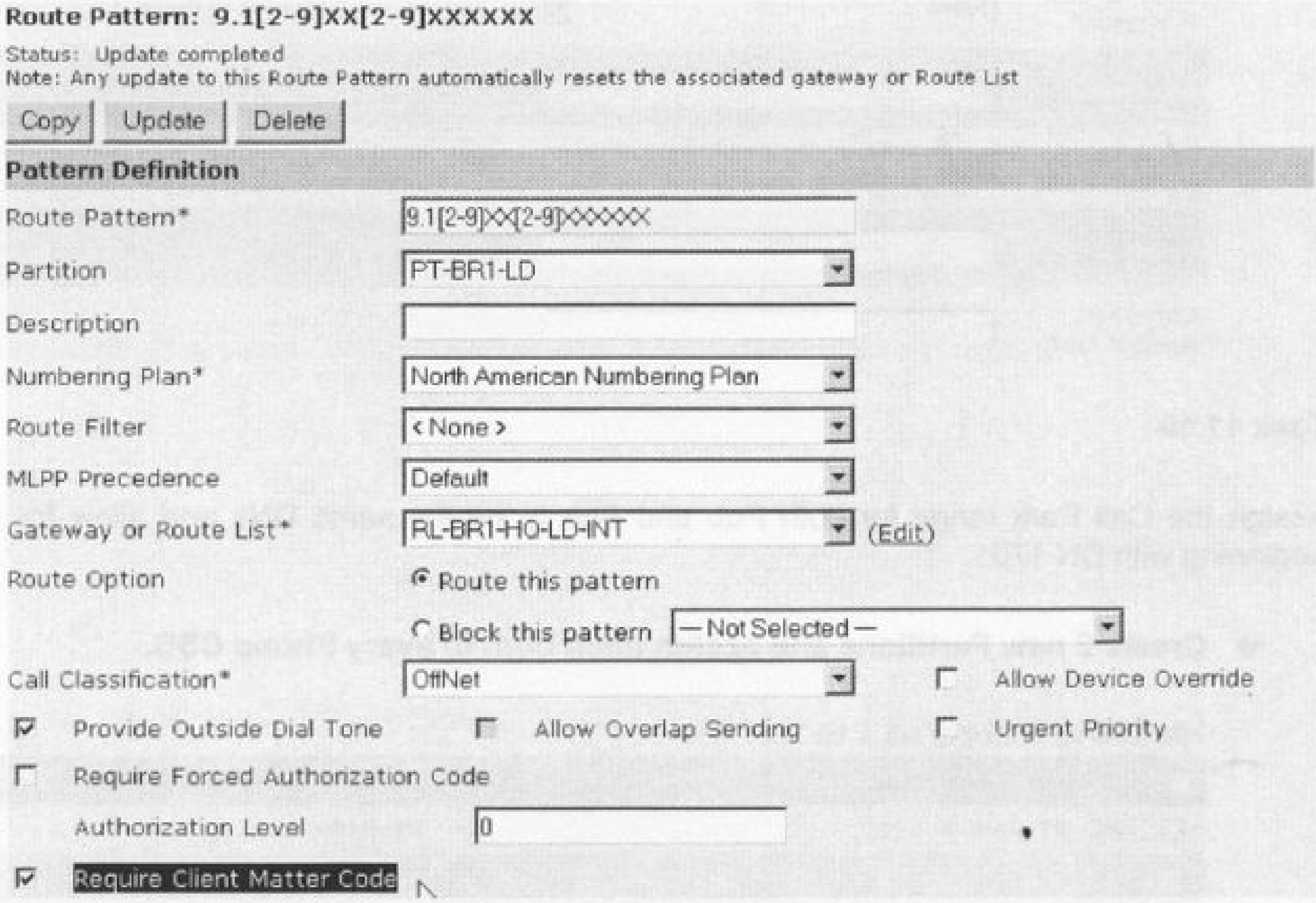
➔ **Next from Feature → Client Matter Code – create 2 CMCs for 555 and 701 (label them for distinction):**

Matching record(s) 1 to 2 of 2

	Client Matter Code	Description
☐	555	LD Calls to any other number
☐	701	LD calls to PSTN Phone

Delete Selected First Previous Next Last Page 1 of 1

➔ **Now go back to your Route Patterns for LD and configure them to require a CMC (do this for both sites):**



➔ **Finally test by making a LD call – you should dial the number as usual – then after dialing the necessary digits, the phone will change the number to all ***** and play another tone – indicating that you must input the CMC. Dial the CMC (701 or 555) and then press # and your call should complete.**

Task 11.9

Ensure that missed calls coming in to an IP Phone do not need any user intervention in order for them to be redialed as an outgoing call (you may not use a translation pattern to accomplish this task).

➔ **This task actually is actually predicated on the assumption that you are in fact using some sort of PRI and probably a Numbering Plan of sorts. We of course in fact know that while the IE Voice lab may certainly test PRIs, it does not allow for any numbering plan. While this may be true – it is still very good to know about this service parameter and how to manipulate incoming digits in this manner.**

➔ **This may also possibly cause problems in other places in your IE lab configurations later on – and should be remembered – such as possibly if you are trying to match a certain DNIS say maybe in your IPCCX configuration.**

➔ **From CCM Service Parameters for CallManager Service (Advanced).**

User-to-User IE Status*	False	False
National Number Prefix	91	
International Number Prefix	3011	
Subscriber Number Prefix		
Unknown Number Prefix		

Task 11.10

Assign the Call Park range for both Pub and Sub to be the same DNs and allow for 10 slots beginning with DN 1701.

➔ **Create 2 new Partitions and assign them both to every Phone CSS.**

Matching record(s) 1 to 2 of 2

	Partition Name	Description
	PT-Park-1	PT-Park-1
	PT-Park-2	PT-Park-2

Delete Selected First Previous Next Last Page 1 of 1

➔ **Now create 2 ranges of the same DNs for Call Park for each CCM (Pub and Sub) (Note that they must be in separate PTs to allow this to occur).**

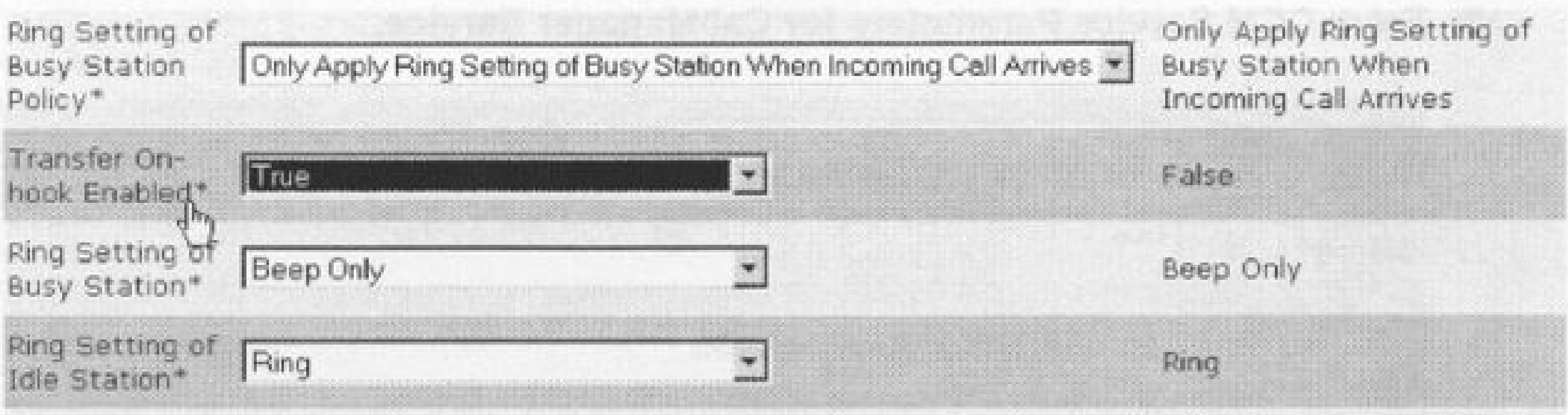
Matching record(s) 1 to 4 of 4

	Call Park Number	Partition	Description	CallManager	Copy
	170[1-9]	PT-Park-1		CCMPub	
	170[1-9]	PT-Park-2		CCMSub	
	1710	PT-Park-1		CCMPub	
	1710	PT-Park-2		CCMSub	

Task 11.11

Make sure that if during a call, the user presses the Transfer softkey, dials the extension, and immediately hangs up, that the transfer succeeds (without having to press the transfer key a second time).

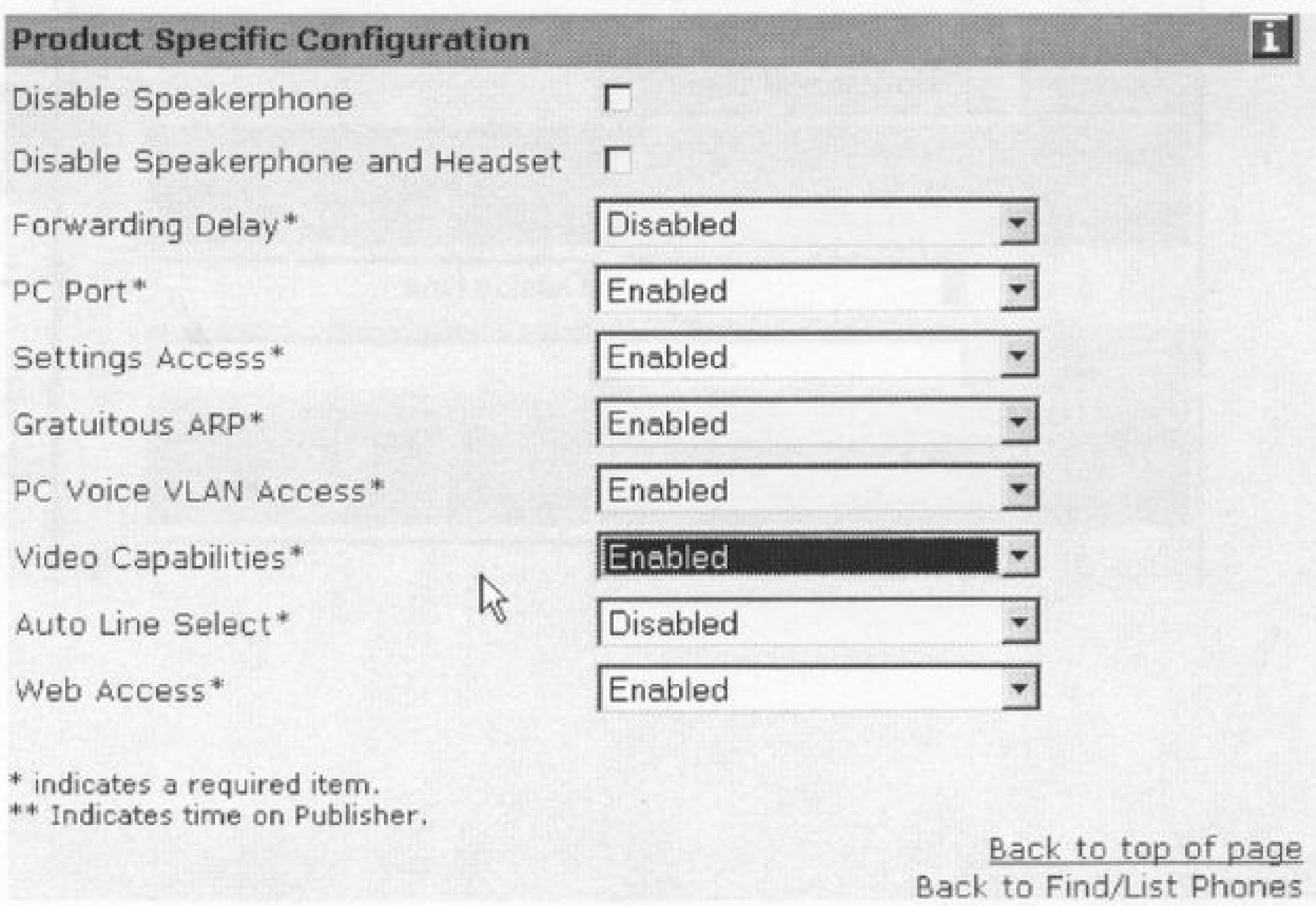
→ **From CCM Service Parameters for CallManager Service.**



Task 11.12

Enable support for a VTA camera on HQ Phone 3.

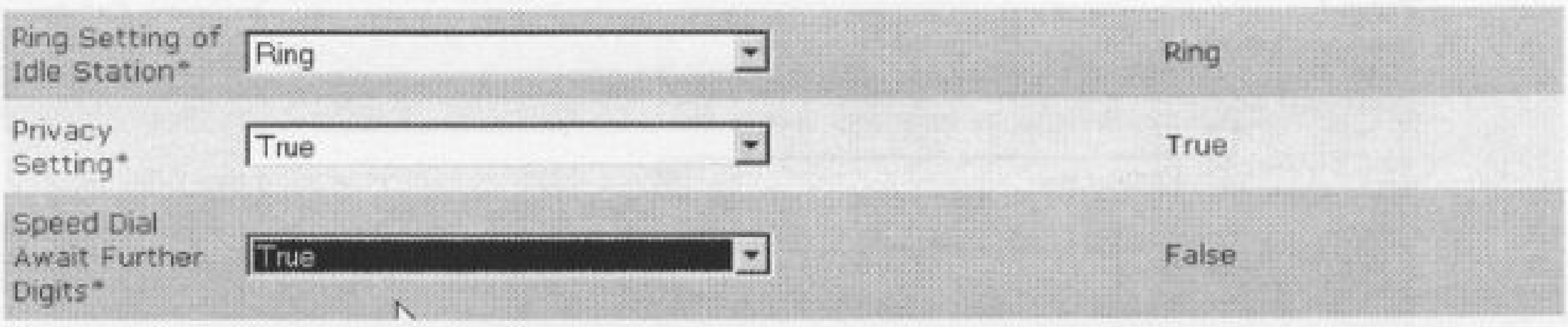
→ **On Device → HQ Phone 3.**



Task 11.13

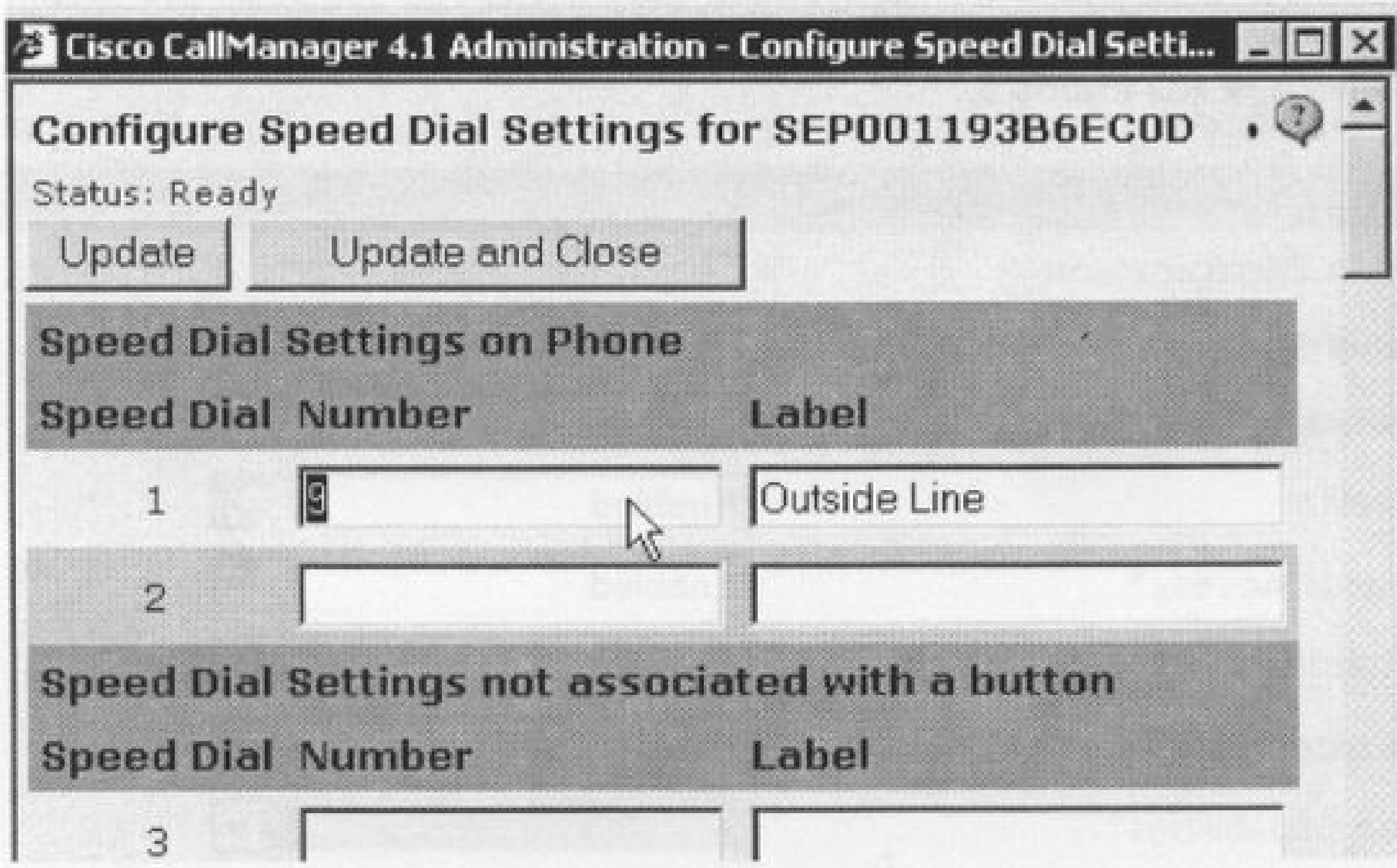
Configure CCM to 'appear' as an older KSU would have appeared at a remote site – so that if a BR1 Phone3 was to pick up their handset and select what they believed to be a "line" to dial out of, that they would not need to first dial a 9 in order to access a trunk. Make this "Line" access separate from their main extension DN. Also ensure that the Caller does **not** see the 9 before their dialed number when they place the call.

➔ **From CCM Service Parameters for CallManager Service.**

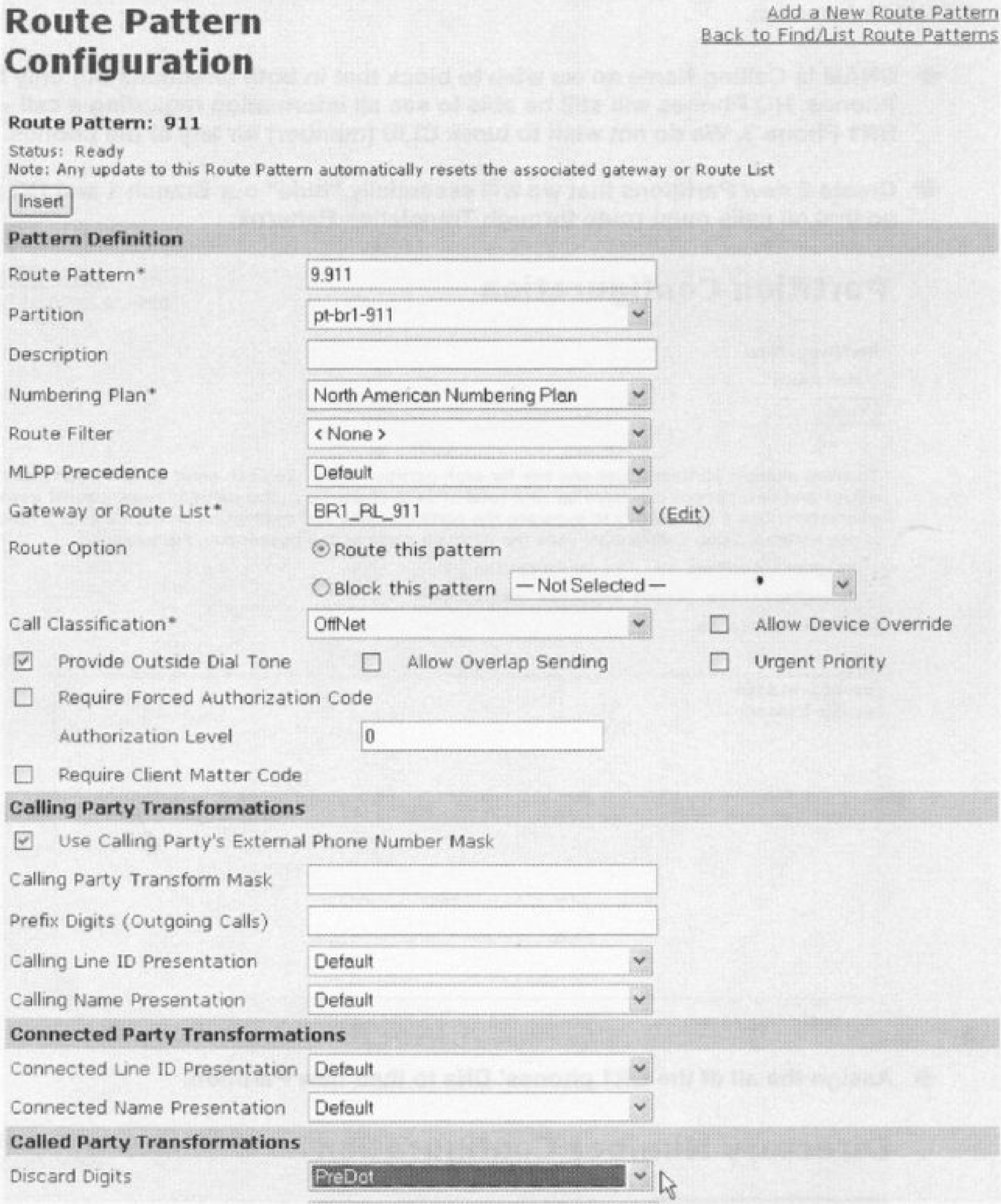


➔ **Next create a Speed Dial button on BR1 Phone 3 to simply dial a 9.**

Phone: SEP001193B6EC0D (POD1-BR1-Ph3)



➔ **Finally ensure that all Route Patterns have the Discard Digit set to "PreDot" on the actual Route Pattern page as well as set on the RG within the RL. This will ensure that the 9 does not show up on the caller's display.**

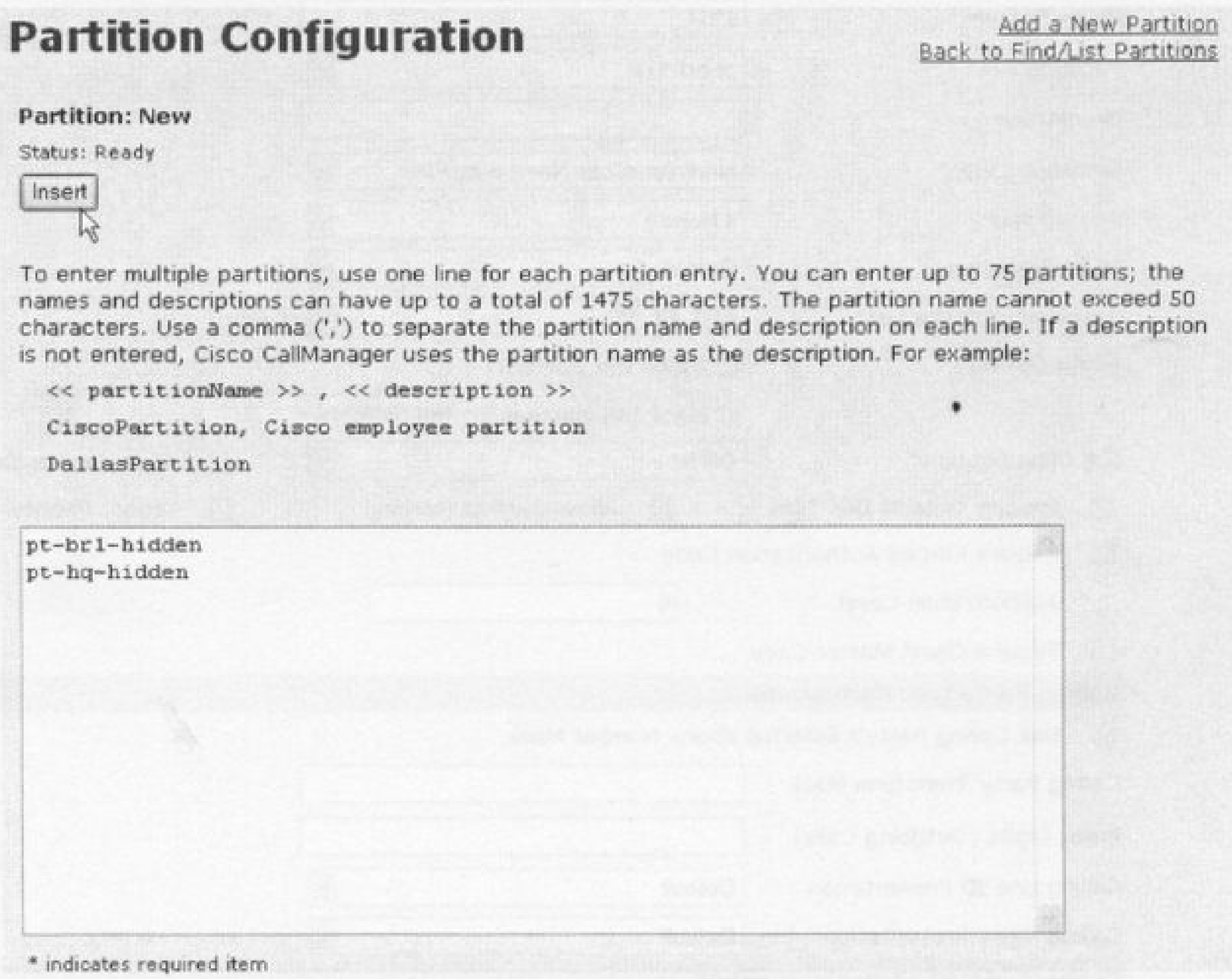


Task 11.14

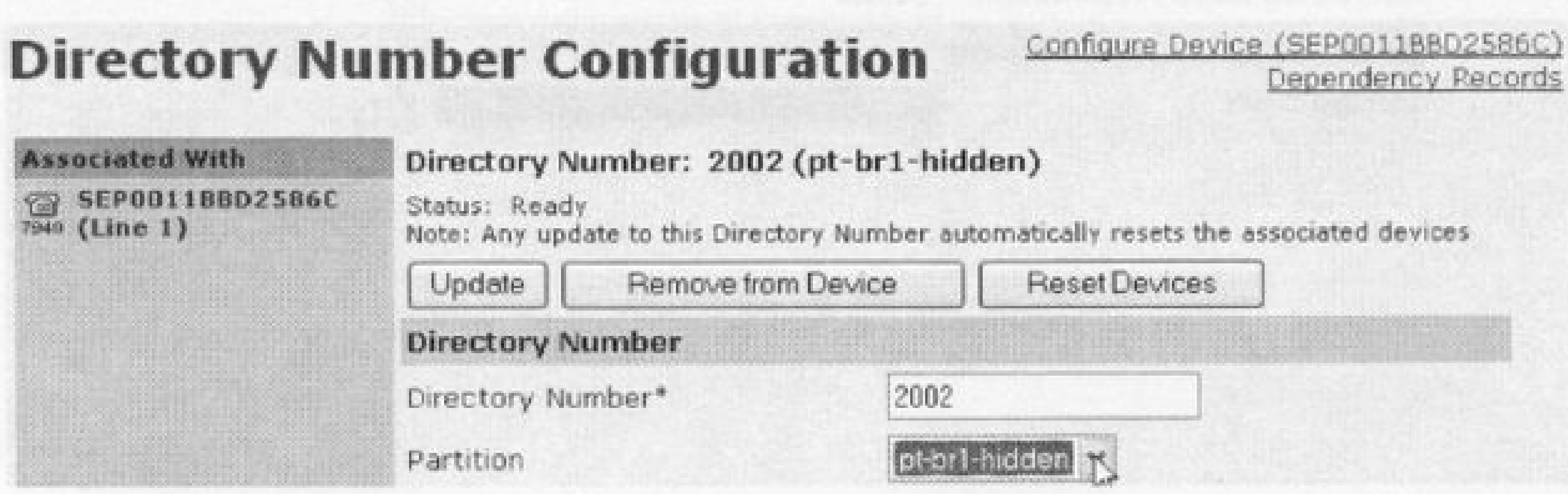
Restrict internal callers from BR1 only, so that they may not see CNAM information only regarding who they are calling or who is calling them, however ensure that BR1 Phone 3 **can** see all CNAM information.

➔ **CNAM is Calling Name so we wish to block that in both directions but only for BR1 Phones. HQ Phones will still be able to see all information regarding a call – as will BR1 Phone 3. We do not wish to block CLID (number) for any of the phones.**

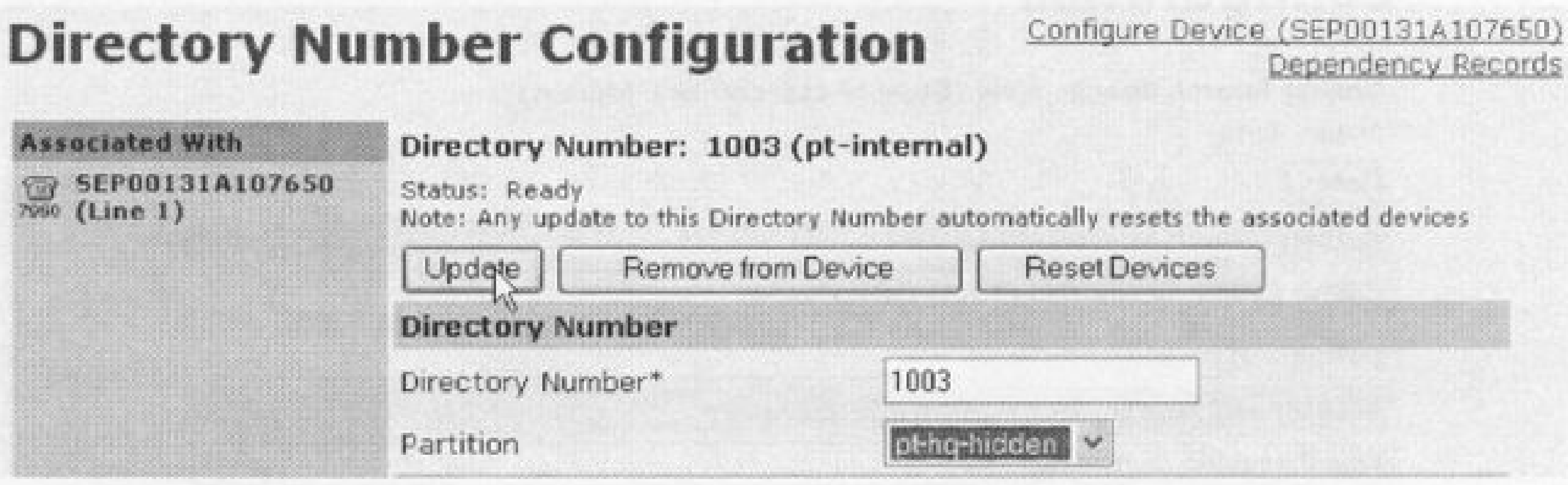
➔ **Create 2 new Partitions that we will essentially "hide" our Branch 1 and HQ phones so that all calls must route through Translation Patterns.**



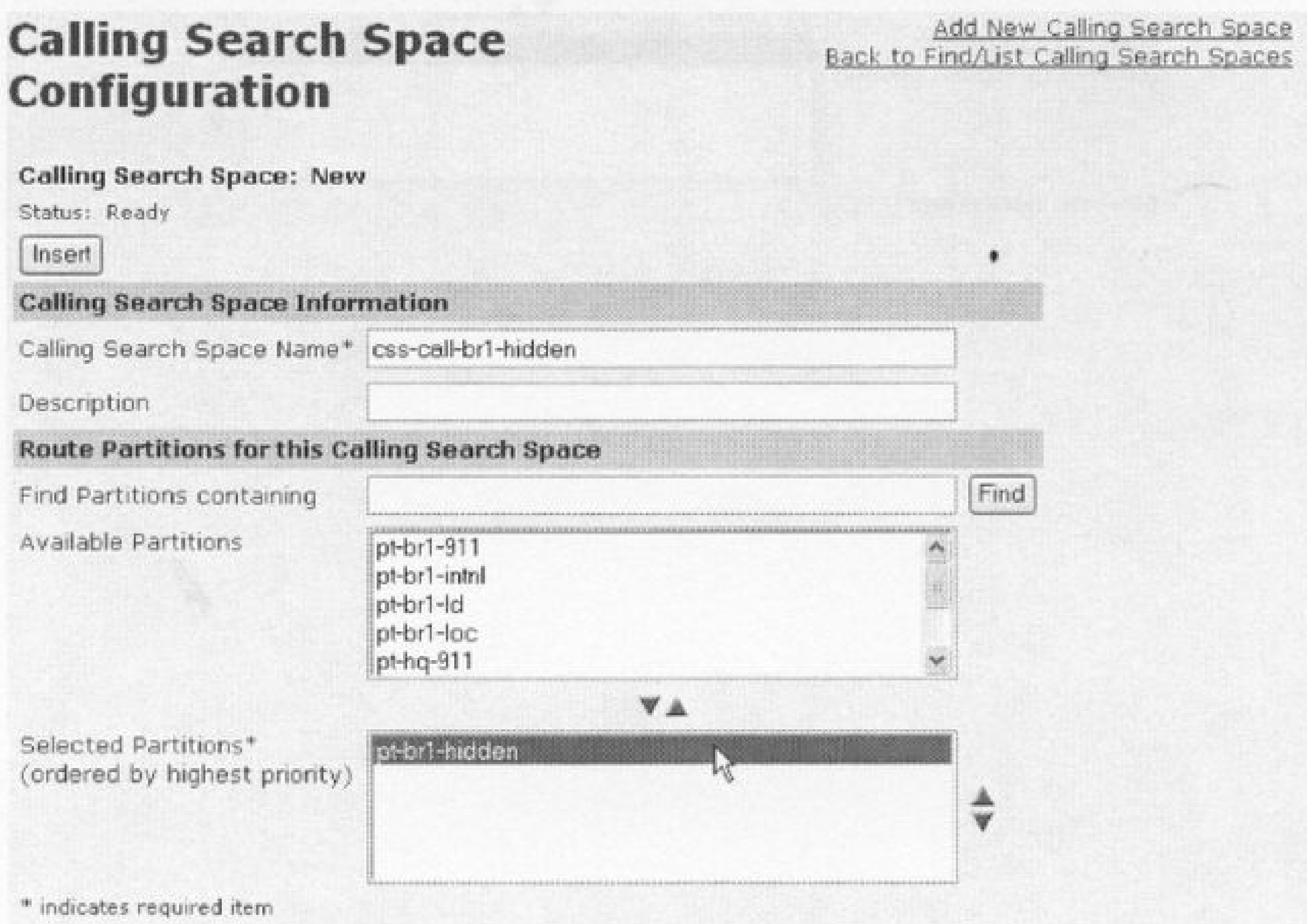
➔ **Assign the all of the BR1 phones' DNs to their new Partition:**

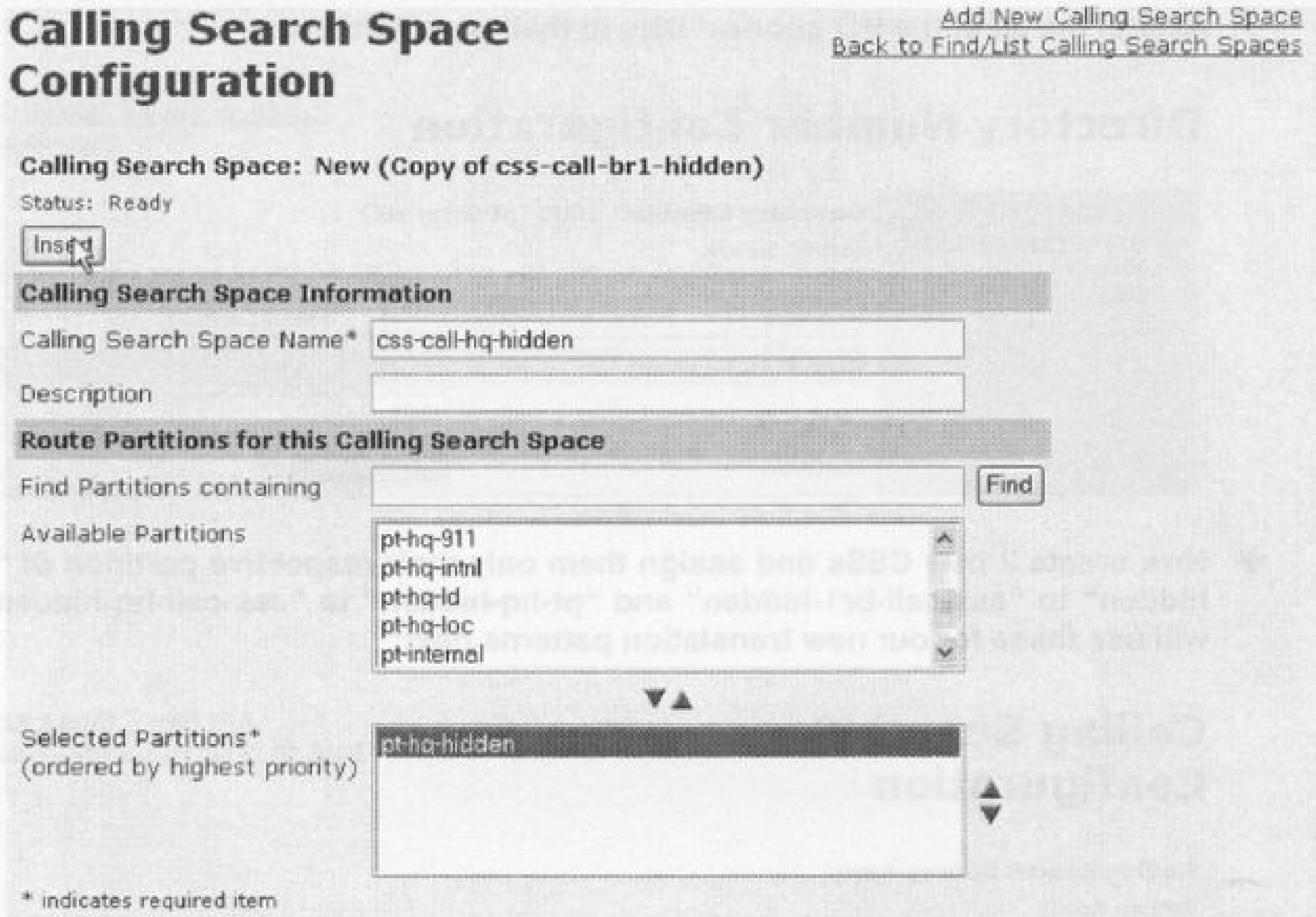


➔ **Assign the all of the HQ phones' DNs to their new Partition:**

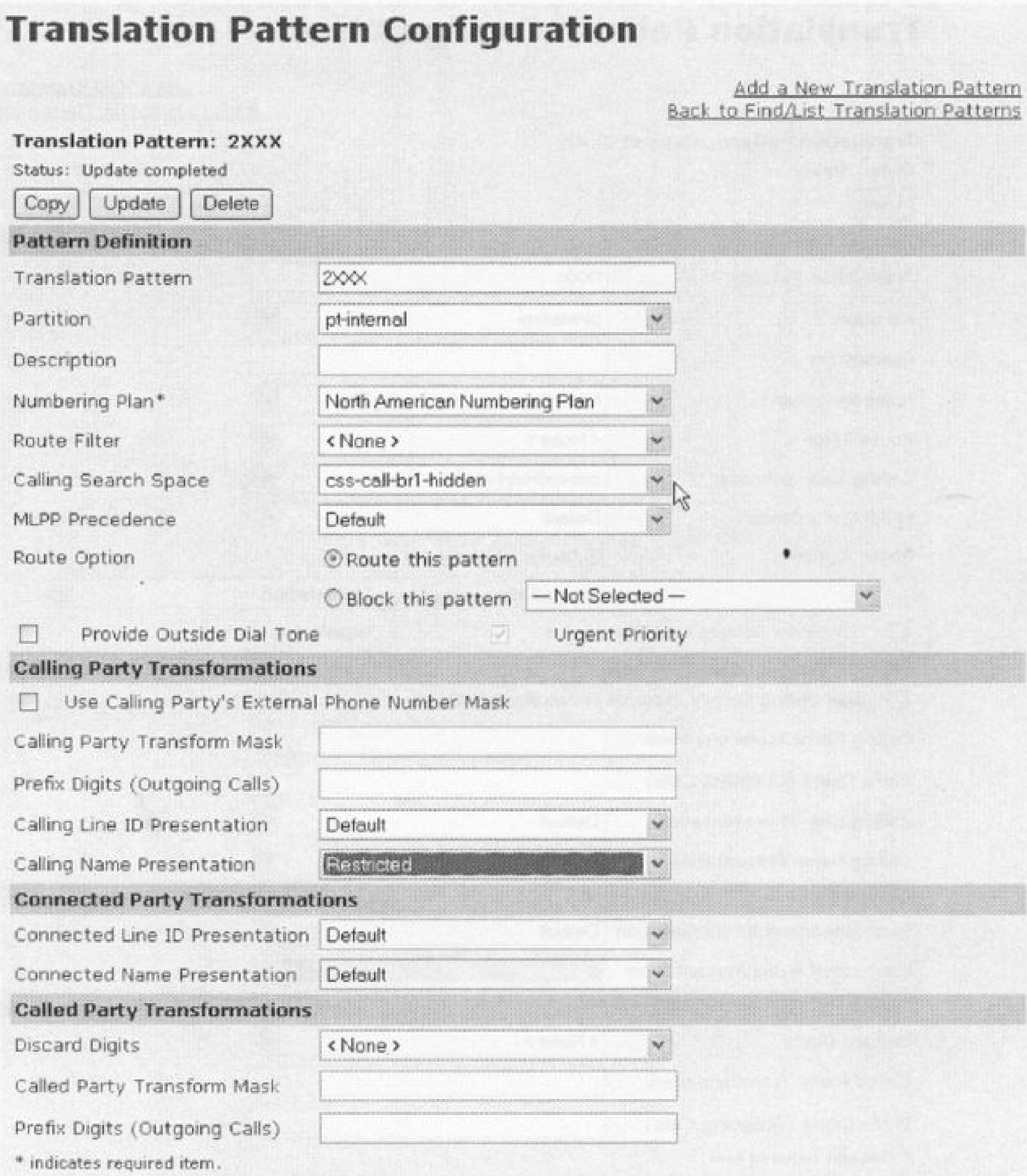


➔ **Now create 2 new CSSs and assign them only their respective partition of "pt-br1-hidden" to "css-call-br1-hidden" and "pt-hq-hidden" to "css-call-hq-hidden" – we will use these for our new translation patterns next:**

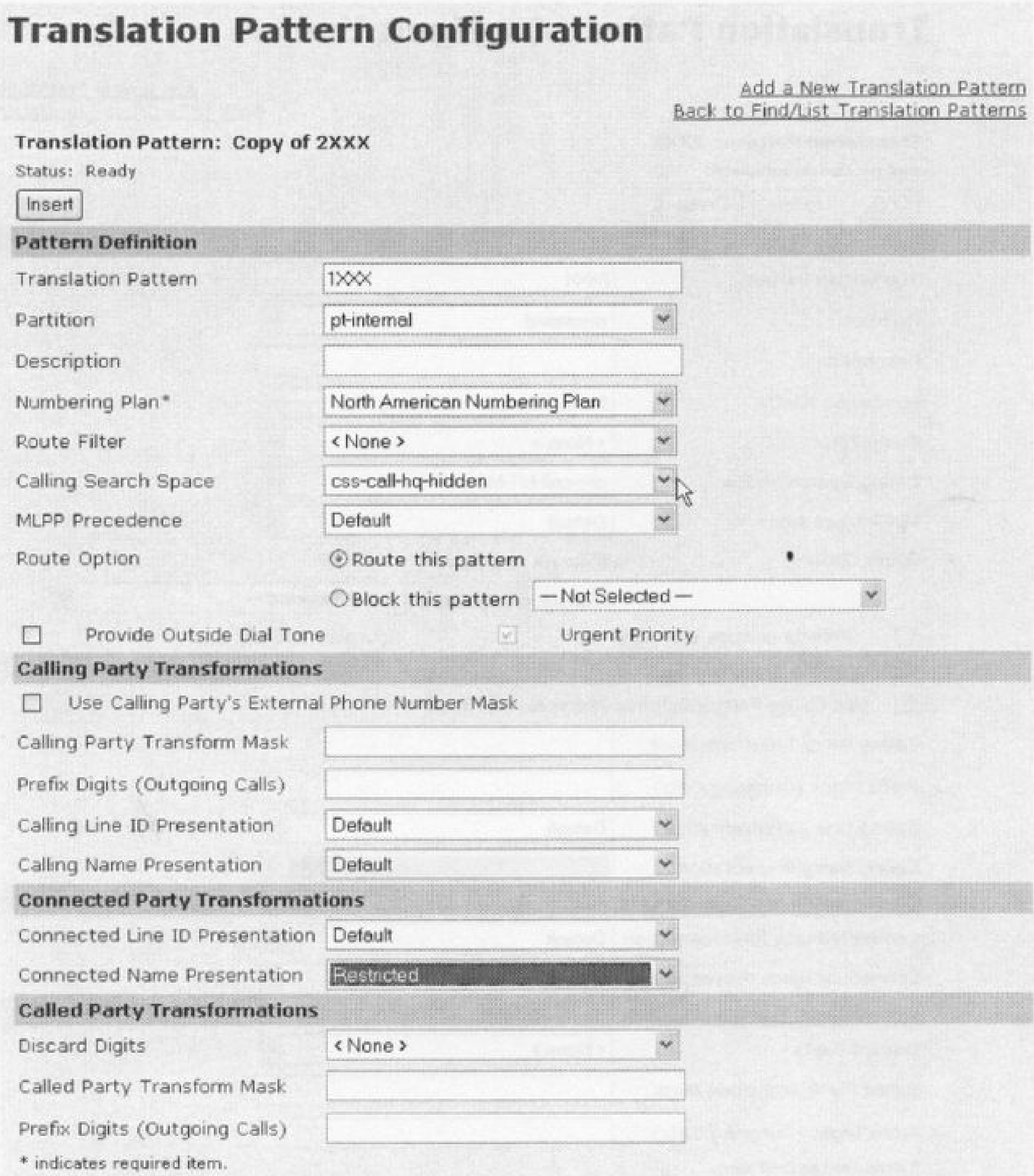



Calling Search Space Configuration
Add New Calling Search Space
Back to Find/List Calling Search Spaces
Calling Search Space: New (Copy of css-call-br1-hidden)
Status: Ready
Insert
Calling Search Space Information
Calling Search Space Name* css-call-hq-hidden
Description
Route Partitions for this Calling Search Space
Find Partitions containing
Find
Available Partitions
pt-hq-911
pt-hq-intnl
pt-hq-ld
pt-hq-loc
pt-internal
Selected Partitions* (ordered by highest priority)
pt-hq-hidden
* indicates required item

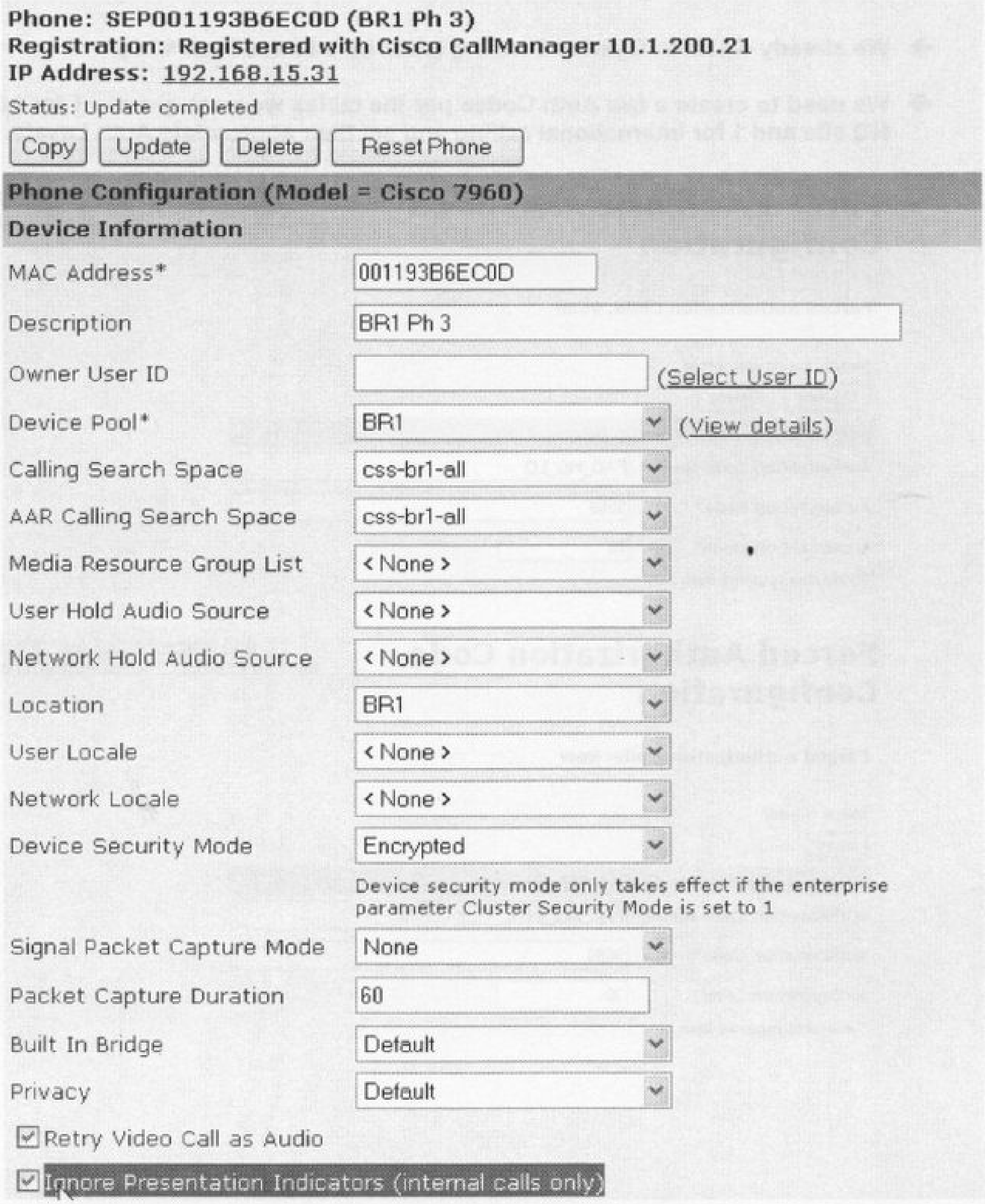
➔ **Create a new Translation Pattern with the DN pattern of 2xxx and restrict the necessary information. Assign it in the Partition of Internal, and give it rights to call the Branch 1 Phones by means of the newly created CSS. Ensure that the "Calling Name Presentation" field is set to Restricted, but leave the "Connected Name Presentation" field at Default.**



➔ **Now create another new Translation Pattern with the DN pattern of 1xxx and restrict the necessary information. Assign it in the Partition of Internal, and give it rights to call the HQ Phones by means of the newly created CSS. Ensure that the "Connected Name Presentation" field is set to Restricted, but leave the "Calling Name Presentation" field at Default.**



➔ **Finally Ensure that the BR1 Phone 3 and all of the HQ Phones have the "Ignore Presentation Indicators (internal calls only)" checkbox – checked to ensure that they will NOT follow the restrictions of the newly created Translation patterns. (Only BR1 Ph 3 is pictured, but this must be done on all HQ phones as well.)**

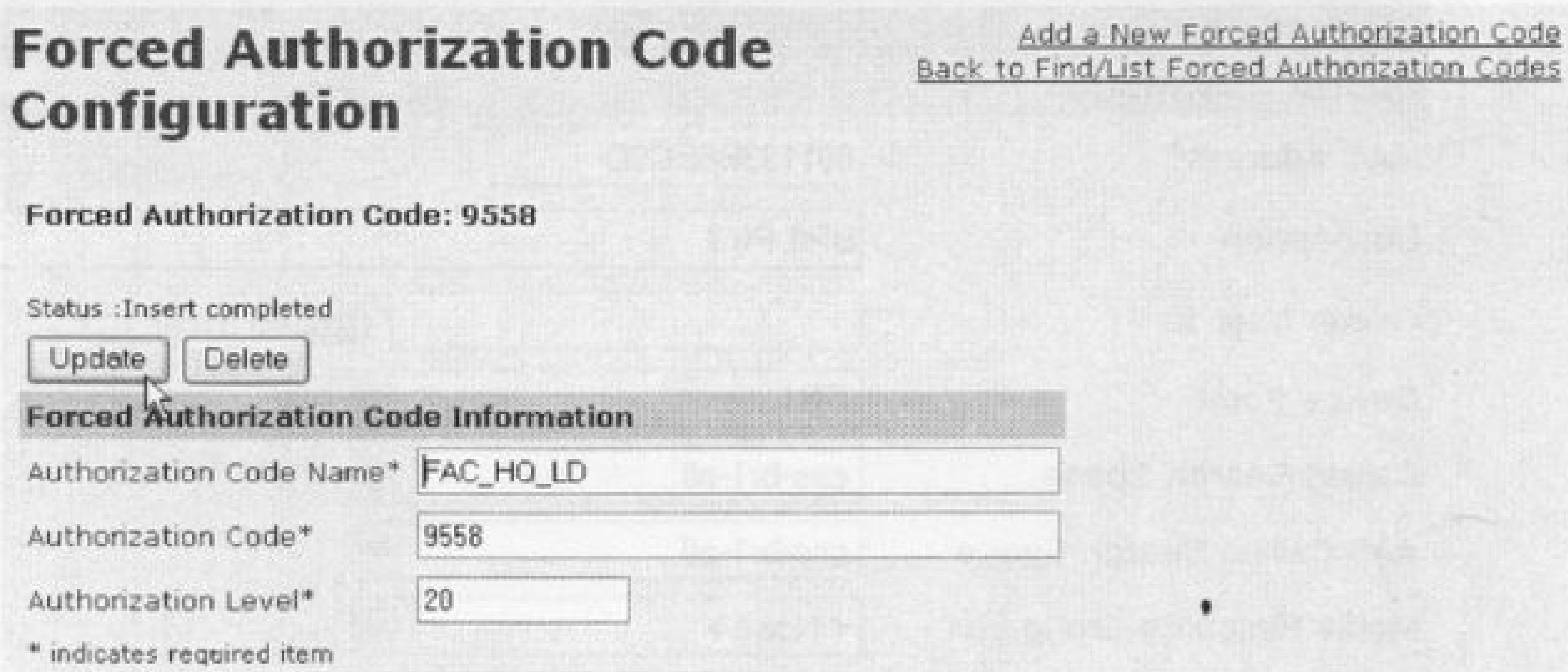


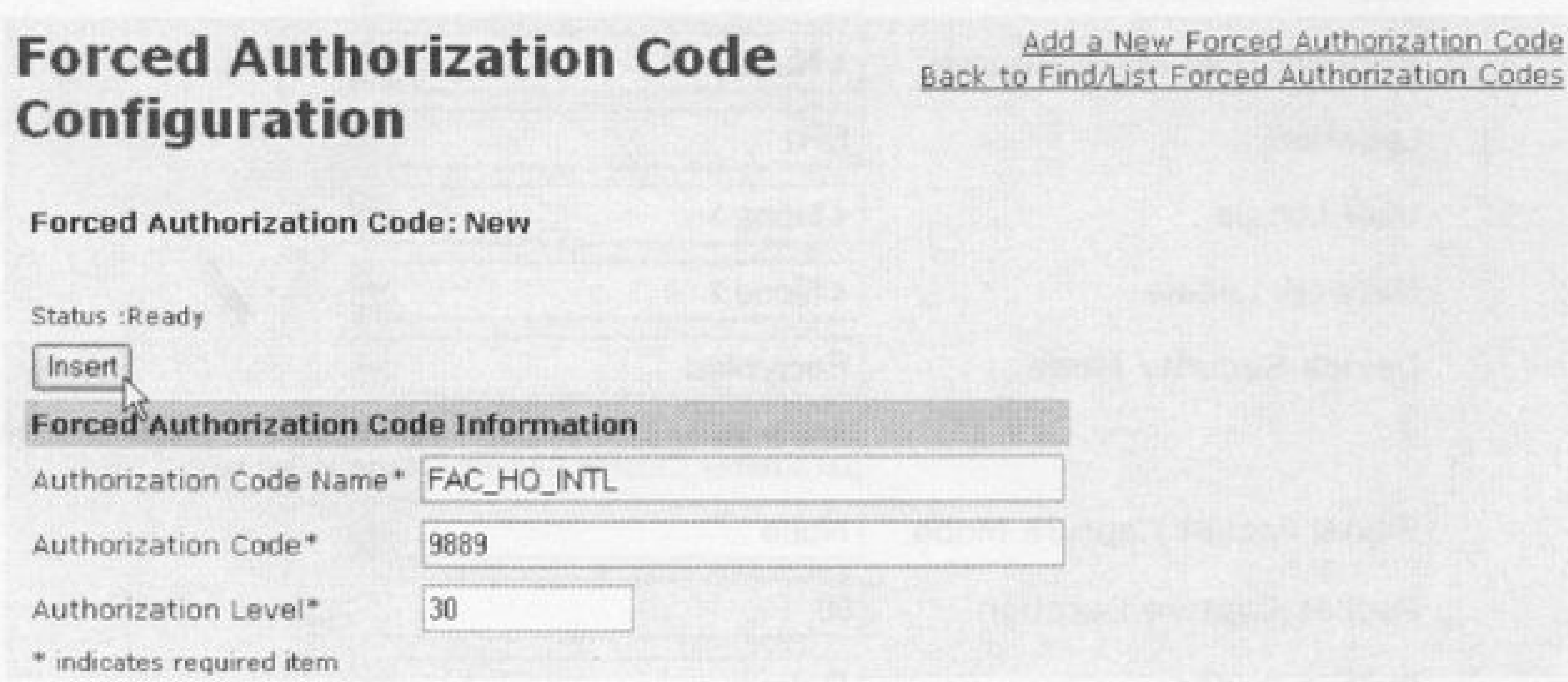
Task 11.15

Configure calls such that a HQ user must enter a forced auth code with a level of at least 20 or better in order to be allowed to dial an LD number and one of 30 or better in order to be allowed to dial an International number. See **Table 4** for Auth Codes.

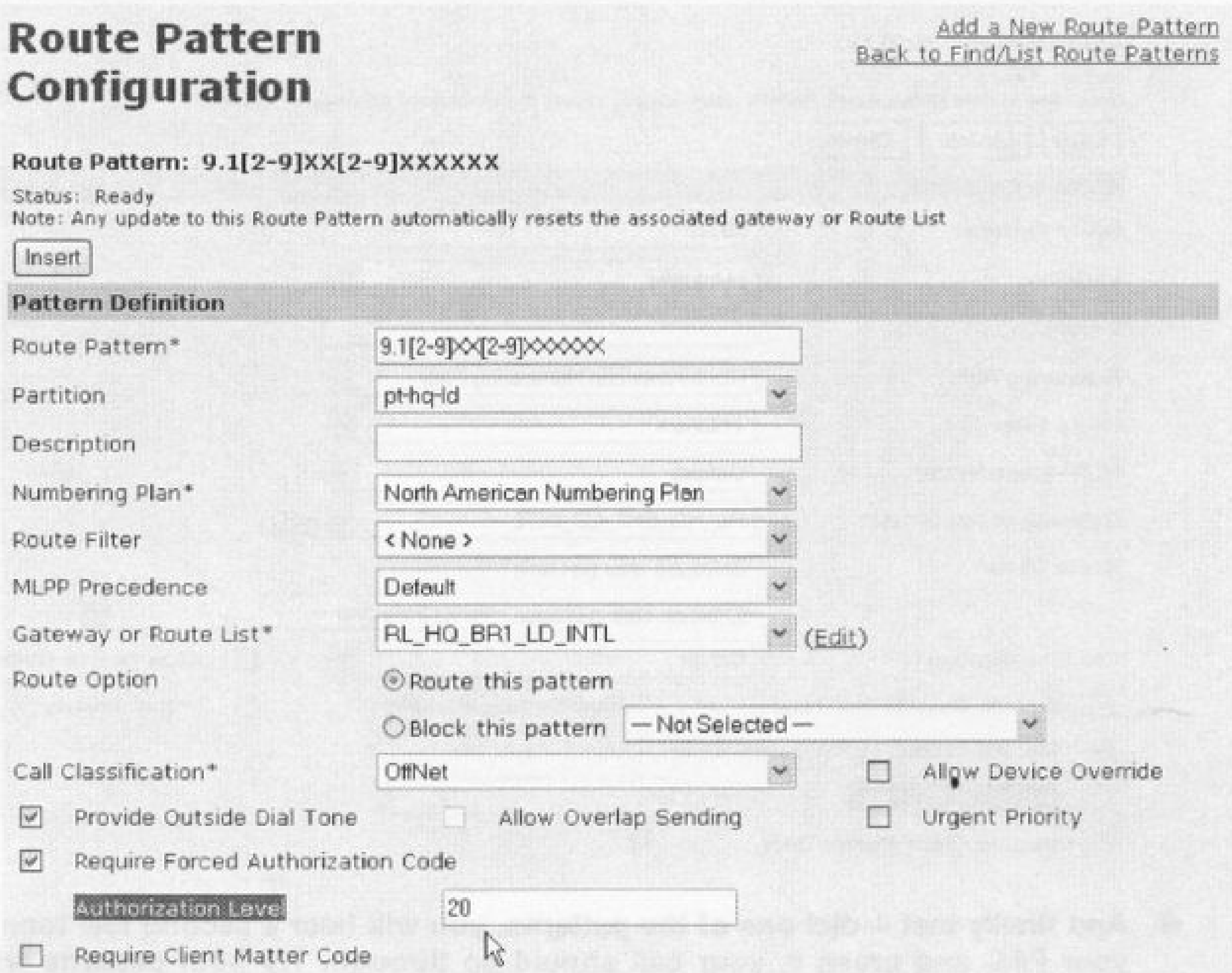
- ➔ **We already disabled Overlap Sending (click here to see Task 11.8).**

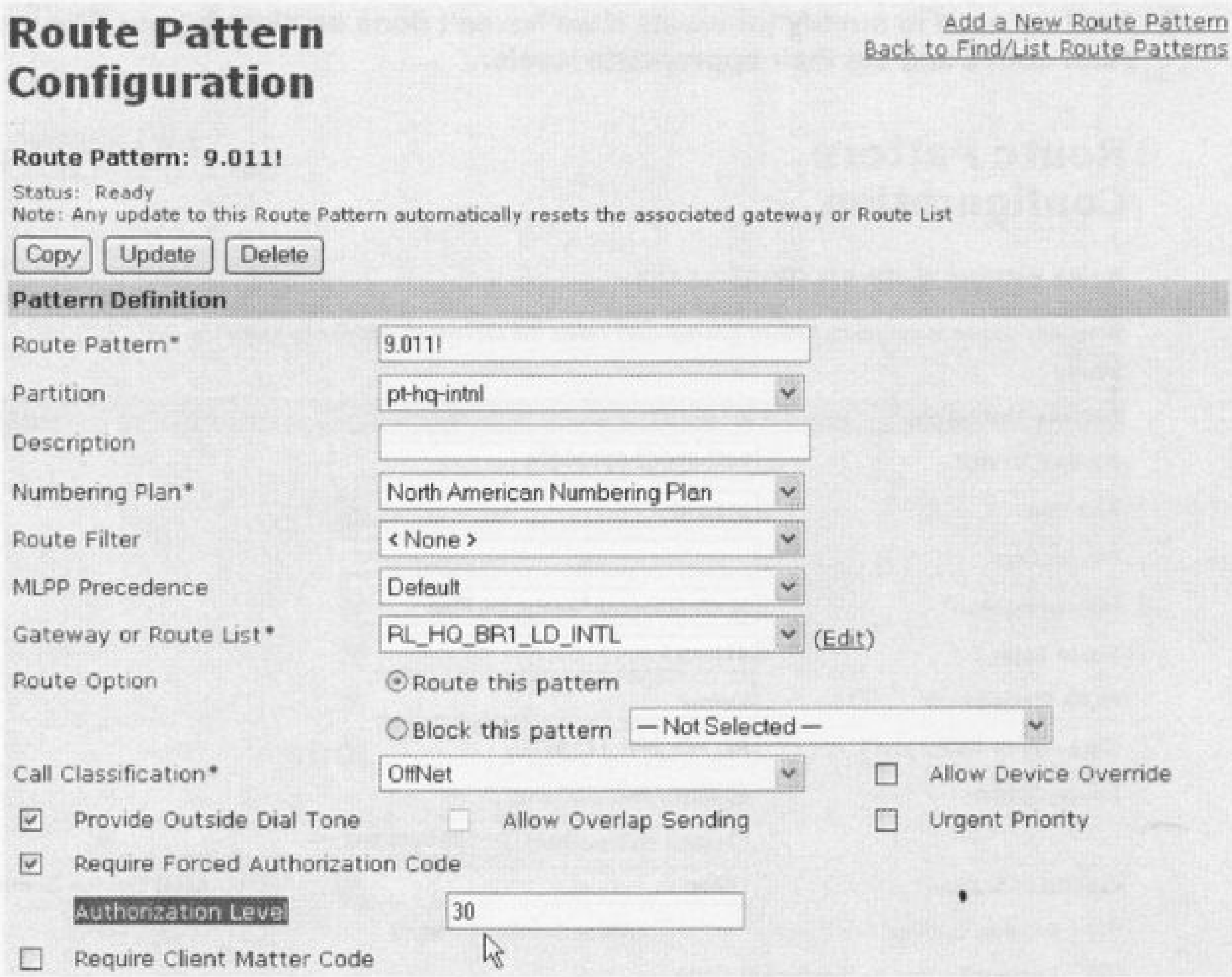
- ➔ **We need to create a few Auth Codes per the tables we were given – 1 for LD at the HQ site and 1 for International calling and set their appropriate Auth Levels.**





➔ **Now we need to modify (or create if we haven't done so already) our RPs to include Auth codes and set their appropriate levels.**





➔ **And finally test – dial one of the patterns, you will hear a second low tone – input your FAC and press #, your call should go through. Try both patterns with both codes – only one code (the 30 level code) should work on both patterns.**

Task 11.16

Assume that an H323 Video endpoint is at our HQ site but may be taken over to the BR1 site at any time without notice. This Video endpoint has a DN of 1815 and should be allowed to call Local and LD. Ensure that when this Video endpoint moves, that no admin intervention is required on CCM.

➔ **What we need to add is known as a Dynamic H323 Addressing Video Client with a GK-Controlled RAS Aggregator Trunk.**

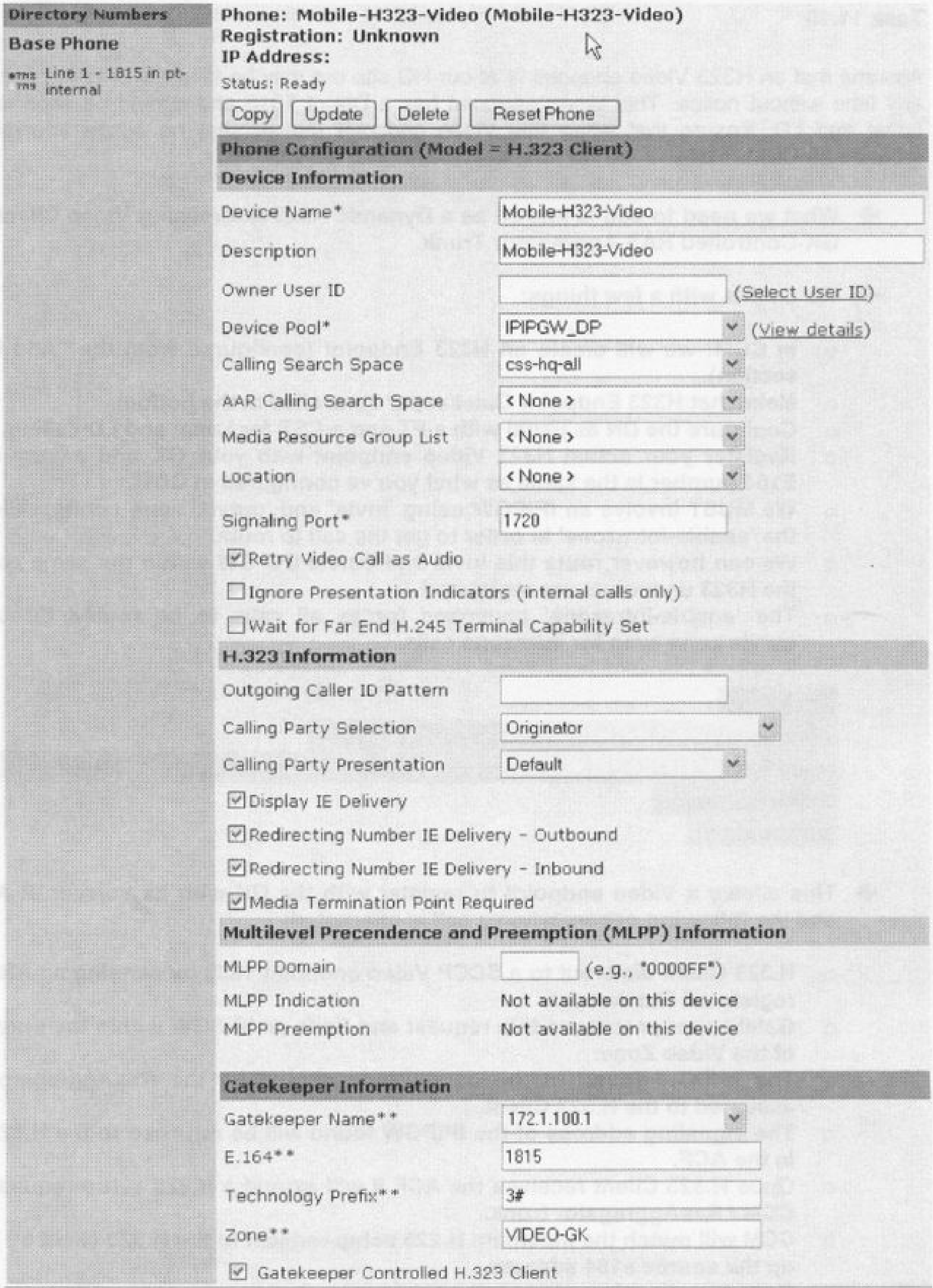
➔ **We do this with a few things:**

- **In CCM: we will create an H323 Endpoint (configured from the "Add Phone" section).**
- **Make that H323 Endpoint Gatekeeper controlled at the bottom.**
- **Configure the DN as usual with a PT and a CSS for Local and LD calling.**
- **Register your actual H323 Video endpoint with your GK and ensure that its E164 number is the same as what you've configured in CCM.**
- **We MUST involve an IPIPGW using 'invia' and 'outvia' zone configuration with the 'enable-intrazone' in order to get the call to route.**
- **We can however route this invia and outvia IPIPGW within the same zone that the H323 endpoints are registered.**
- **The 'enable-intrazone' command forces all calls to be routed through the outvia zone even for intrazone calls.**

```
gatekeeper
 zone local CCM-GK ipexpert.com 172.1.100.1
 zone local VIDEO-GK ipexpert.com invia VIDEO-GK outvia VIDEO-GK
enable-intrazone
 no shutdown
```

➔ **This allows a Video endpoint to register with the GK with its *current* IP Address and the following occurs when a call is attempted:**

- **H.323 Client dials out to a SCCP Video endpoint 1835 by sending an ARQ to its registered Gatekeeper.**
- **Gatekeeper processes this request and finds an IPIPGW within the outvia zone of the Video Zone.**
- **The IPIPGW found in the outvia zone should be the RasAggregator trunk assigned to the H.323 Client.**
- **The signaling address of the IPIPGW found will be returned to the H.323 client in the ACF.**
- **Once H.323 Client receives the ACF it will extend a H.225 setup request to the CCM / RasAggregator trunk.**
- **CCM will match the incoming H.225 setup request to the H.323 client by looking up the source e164 address.**
- **Once the client is matched, the call is routed as usual pending Digit analysis.**


Directory Numbers
Base Phone
Line 1 - 1815 in pt-internal
Phone: Mobile-H323-Video (Mobile-H323-Video)
Registration: Unknown
IP Address:
Status: Ready
Copy
Update
Delete
Reset Phone
Phone Configuration (Model = H.323 Client)
Device Information
Device Name* Mobile-H323-Video
Description Mobile-H323-Video
Owner User ID (Select User ID)
Device Pool* IPIPGW_DP (View details)
Calling Search Space css-hq-all
AAR Calling Search Space < None >
Media Resource Group List < None >
Location < None >
Signaling Port* 1720
Retry Video Call as Audio
Ignore Presentation Indicators (internal calls only)
Wait for Far End H.245 Terminal Capability Set
H.323 Information
Outgoing Caller ID Pattern
Calling Party Selection Originator
Calling Party Presentation Default
Display IE Delivery
Redirecting Number IE Delivery - Outbound
Redirecting Number IE Delivery - Inbound
Media Termination Point Required
Multilevel Precendence and Preemption (MLPP) Information
MLPP Domain (e.g., "0000FF")
MLPP Indication Not available on this device
MLPP Preemption Not available on this device
Gatekeeper Information
Gatekeeper Name** 172.1.100.1
E.164** 1815
Technology Prefix** 3#
Zone** VIDEO-GK
Gatekeeper Controlled H.323 Client

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 12: Quality of Service

Estimated Time to Complete: 4 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 12 Quality of Service

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab Section 1 and the basics within the CCM/gateways/gatekeeper/dial plan section must be completed (in order to test affectively).

Section 12 Configuration Tasks

Task 12.1

Assume the single cable solution is used, configure the switches to trust the Layer 2 QoS classification of the IP phones but not the attached PC.

➔ **On the Cat 6000 enable QoS globally and create an ACL to trust cos – this ACL is a workaround the hardware restriction of the 6348 linecard which does not support trust-cos on the port. [Well, to be factually correct, when applying trust-cos directly on the ports the linecard does NOT overwrite the COS but when forwarding the frame to the switching engine it does not preserve the Layer 2 COS.**

```
set qos enable

set port qos 2/7-8 vlan-based
set port qos 2/7-8 trust-ext untrusted
set qos acl ip POD12_IP-PHONES trust-cos ip any any
commit qos acl POD12_IP-PHONES
set qos acl map POD12_IP-PHONES 220
```

➔ **On the 3550 enable QoS globally and enter the interface commands.**

```
3550G-Access(config)#mls qos
3550G-Access(config)#interface range FastEthernet0/23 - 24
Switch(config-if-range)# mls qos trust cos
Switch(config-if-range)# switchport priority extend cos 0
```

➔ **On the 3825 Etherswitch same as 3550 except no need to enable qos globally.**

Task 12.2

Configure the Catalyst 6500 to mark all VOIP control traffic from the Call Manager to the appropriate L3 setting.

➔ **Set the CCM port to port-based qos (the default) and create an ACL on the Cat 6000 to mark SCCP, H323 and MGCP control traffic to DSCP AF31.**

```
set port qos 2/42 port-based
set qos acl ip POD12_SERVER dscp 26 tcp any range 2000 2002 any
set qos acl ip POD12_SERVER dscp 26 tcp any any range 11000 11999
set qos acl ip POD12_SERVER dscp 26 tcp any any range 1024 4999
set qos acl ip POD12_SERVER dscp 26 tcp any any  range 1719 1720
set qos acl ip POD12_SERVER dscp 26 udp any eq 2427 any
set qos acl ip POD12_SERVER dscp 26 tcp any eq 2428 any
commit qos acl POD12_SERVER
set qos acl map POD12_SERVER 2/42
```

Task 12.3

Configure the Catalyst 6500 to move VOIP control traffic to the 2nd queue and 1st threshold.

➔ **On the trunk port connected to HQ-RTR create an ACL to trust-dscp and apply to the port. DSCP AF31 will be mapped to COS 3.**

```
set port qos 2/21 port-based
set qos acl ip POD12_TRUNK trust-dscp ip any any
commit qos acl POD12_TRUNK
set qos acl map POD12_IP-PHONES 2/21
```

➔ **Configure traffic with COS = 3 to the 2nd queue 1 Threshold.**

```
PL-VoicePod-6500> (enable) set qos map 2q2t tx 2 1 cos 3
QoS tx priority queue and threshold mapped to cos successfully.
PL-VoicePod-6500> (enable) set qos map 1p2q2t tx 2 1 cos 3
QoS tx priority queue and threshold mapped to cos successfully.
```

Task 12.4

Configure the Catalyst 6500 and 3550 to map the CoS to DSCP value.

➔ **On the 6500 in global configuration enter the following command.**

```
PL-VoicePod-6500> (enable) set qos cos-dscp-map 0 8 16 26 34 46 48 56
QoS cos-dscp-map set successfully.
```

➔ **On the 3550 in global configuration enter the following command.**

```
3550G-Access(config)#mls qos map cos-dscp 0 8 16 26 34 46 48 56
```


Task 12.5

The speed of the FR PVC between the HQ and Branch 2 is 768 kbps. Configure FRTS and apply to this PVC.

➔ **We will need to define the Frame Relay parameters for CIR, MINCIR, BC and BE and Frame-Relay Fragment. Using page 130 of the QoS SRND (Aug 2002) the commands for the link with PVC speed of 768kbps is as follows:**

```
P2-HQ-RTR(config)# map-class frame-relay FRTS
P2-HQ-RTR(config-map-class)# frame-relay cir 764940
P2-HQ-RTR(config-map-class)#frame-relay mincir 764940
P2-HQ-RTR(config-map-class)#frame-relay bc 7560
P2-HQ-RTR(config-map-class)# frame-relay be 0
```

Task 12.6

Add the LFI mechanism of FRF.12 between the HQ and Branch 2 to the previous question and apply this to the PVC. Configure such that the serialization delay is 10 ms.

➔ **On the HQ-RTR:**

```
P2-HQ-RTR(config)#map-class frame-relay FRTS
P2-HQ-RTR(config-map-class)# frame-relay fragment 960

P2-HQ-RTR(config-map-class)# interface Serial0/1/0:0
P2-HQ-RTR(config-map-class)# bandwidth 768
P2-HQ-RTR(config-if)#frame-relay traffic-shaping
P2-HQ-RTR(config-if)#interface Serial0/1/0:0.2
P2-HQ-RTR(config-subif)# frame-relay interface-dlci 202
P2-HQ-RTR(config-fr-dlci)# class FRTS
```

➔ **On the BR2 Router.**

➔ **We will need to define the Frame Relay parameters again on BR2 using the same parameters for CIR, MINCIR, BC and BE and Frame-Relay Fragment.**

```
P2-BR2-RTR(config)#map-class frame-relay FRTS
P2-BR2-RTR(config-map-class)#frame-relay cir 764940
P2-BR2-RTR(config-map-class)#frame-relay mincir 764940
P2-BR2-RTR(config-map-class)#frame-relay bc 7560
P2-BR2-RTR(config-map-class)#frame-relay be 0
P2-BR2-RTR(config-map-class)#frame-relay fragment 960
```

➔ **Enable frame-relay traffic shaping on the physical and assign map-class to the DLCI.**

```
P2-BR2-RTR(config-subif)#interface Serial0/1/0
P2-BR2-RTR(config-subif)#bandwidth 768
P2-BR2-RTR(config-if)#frame-relay traffic-shaping
P2-BR2-RTR(config-if)#interface Serial0/1/0.1 point-to-point
P2-BR2-RTR(config-subif)# frame-relay interface-dlci 102
P2-BR2-RTR(config-fr-dlci)#class FRTS
```

Task 12.7

Configure Low Latency Queuing (LLQ) for the HQ and Branch 2. Allocate 33% of the total bandwidth to Media and 2% as one of the CBWFQ for the control traffic.

➔ **On both the HQ-RTR and BR2 router configure class-maps and policy maps shown below.**

```
class-map match-any RTP
 match ip dscp ef
class-map match-any SIG
 match ip dscp af31
!
!
policy-map LLQ
 class RTP
  priority percent 33
 class SIG
  bandwidth percent 2
 class class-default
  fair-queue
```

➔ **Apply the service policy to the frame-relay map-class on both routers.**

➔ **On BR2:**

```
P2-BR2-RTR(config)#map-class frame-relay FRTS
P2-BR2-RTR(config-map-class)#service-policy output LLQ
```

➔ **On HQ-RTR:**

```
P2-HQ-RTR(config)#map-class frame-relay FRTS
P2-HQ-RTR(config-map-class)#service-policy output LLQ
```

```
P2-HQ-RTR#sh policy-map interface Serial0/1/0:0.2
 Serial0/1/0:0.2: DLCI 202 -

  Service-policy output: LLQ

    Class-map: RTP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp ef
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 72
        Bandwidth 33 (%)
        Bandwidth 252 (kbps) Burst 6300 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: SIG (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Output Queue: Conversation 73
        Bandwidth 2 (%)
        Bandwidth 15 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      1 packets, 84 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 64
        (total queued/total drops/no-buffer drops) 0/0/0
```


Task 12.8

Configure LLQ between the HQ and Branch 1 sites. Allocate 256Kbps for media and 8Kbps for signaling. Assume the speed of the PVC between HQ and Branch 1 is 1544 Kbps.

➔ **As before, create class-maps and policy-maps to fit the requirement.**

➔ **Apply the Service Policy enabling LLQ in the PVC.**

➔ **On HQ-RTR:**

```
policy-map LLQ-BR1
 class RTP
  priority 256
 class SIG
  bandwidth 8
 class class-default
  fair-queue

map-class frame-relay FRTS
 frame-relay cir 1466800
 frame-relay bc 14668
 frame-relay be 0
 frame-relay mincir 1466800
 service-policy output LLQ-BR1

interface Serial0/1/0:0
 no ip address
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0/1/0.1 point-to-point
 ip address 162.2.101.1 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf mtu-ignore
 frame-relay interface-dlci 201
  class FRTS
```

➔ **On BR1:**

➔ **As before, create class-maps and policy-maps to fit the requirement.**

➔ **Apply the Service Policy enabling LLQ in the map-class.**

```
interface Serial0/1/0
 no ip address
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0/1/0.1 point-to-point
 ip address 162.2.101.2 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf mtu-ignore
 frame-relay interface-dlci 101
  class FRTS

map-class frame-relay FRTS
 frame-relay cir 1466800
 frame-relay bc 14668
 frame-relay be 0
 frame-relay mincir 1466800
 service-policy output LLQ-BR1
```

NOTE:

- In policy-map statements the PQ and CBWFQ should both be specified as a percentage or both be explicitly stated – you can't mix 'n match.
- If the table in the QoS SRND does not have an entry for the PVC speed, CIR should be set to 95% of the PVC speed to take into account FR headers.
- To verify issue the command *sh policy-map interface*

Task 12.9

Use the Catalyst 6500 policer to police all control traffic originating from Call Manager to 32 Kbps – the exceed action should be to remark control traffic to DSCP 10.

➔ **In the Cat 6000:**

➔ **Define the policer – either microflow or aggregate. The name of the policer given in this example is "remark-sig". The policed rate is 64Kbps with a burst size of 13Kbits. The exceed action (all packets on the VLAN/Interface which are in excess of 32Kbps traffic) is to remark the DSCP value.**

➔ **The DSCP will be marked down to DSCP=10 – this step is performed in global configuration.**

➔ **Apply the policer to the ACL we created earlier. Commit and apply to the CCM port.**

```
PL-VoicePod-6500> (enable) set qos policer aggregate REMARK-SIG rate 32 burst 13
policed-dscp
QoS policer for aggregate REMARK-SIG updated successfully.
PL-VoicePod-6500> (enable) set qos policed-dscp-map 26:10
QoS policed-dscp-map set successfully.
PL-VoicePod-6500> (enable) set qos acl ip POD12_SERVER dscp 26 aggregate
REMARK-SIG any
POD12_SERVER editbuffer modified. Use 'commit' command to apply changes.
PL-VoicePod-6500> (enable) commit qos acl POD12_SERVER

QoS ACL 'POD12_SERVER' successfully committed.
PL-VoicePod-6500> (enable) set qos acl map POD12_SERVER 2/42
ACL POD12_SERVER is successfully mapped to port 2/42.
```

NOTE:

- To determine the burst parameter, use this equation:

  Burst = (Rate [bps]) * 0.00025 [sec/interval]) *or* (maximum packet size [bits]), whichever is greater.

- For example, if you want to calculate the minimum burst value needed to sustain a rate of 1 Mbps on an Ethernet network, the rate is defined as 1 Mbps and the maximum Ethernet packet size is 1518 bytes. The equation is:

  Burst = (1,000,000 bps * 0.00025) *or* (1518 bytes * 8 bits/byte) = 250 *or* 12144.

- The larger result is 12144, which you round to 13 kbps.

Task 12.10

Re-configure FRTS between HQ and BR2 such that the traffic shaper only engages when Voice traffic is present on the link. For this task you may assume that the FR port speed is 768kbps and that the CIR provided by the carrier is 384. A proper LFI mechanism should be engaged at all times and should be relevant to the CIR not the Port speed.

➔ **VATS (Voice Adaptive Traffic Shaping) is a mechanism by which, if we use Frame Relay (and most don't any longer ☺), we can use the full Port speed for our data traffic, and when voice presents itself on the line, we dynamically adapt back to the CIR speed.**

➔ **On HQ-RTR:**

```
policy-map FR-VATS
 class class-default
  shape average 729600 3648 0
  shape adaptive 364800
  shape fr-voice-adapt deactivation 30
!
interface Serial0/1/0:0
 frame-relay fragmentation voice-adaptive deactivation 30
!
interface Serial0/1/0:0.2
 bandwidth 768
 frame-relay interface-dlci 202
  class FRTS-FRF12
!
map-class frame-relay FRTS-FRF12
 service-policy output FR-VATS
 frame-relay fragment 480
```

➔ **On BR2:**

```
policy-map FR-VATS
 class class-default
  shape average 729600 3648 0
  shape adaptive 364800
  shape fr-voice-adapt deactivation 30
!
interface Serial0/1/0
 frame-relay fragmentation voice-adaptive deactivation 30
!
interface Serial0/1/0.1
 bandwidth 768
 frame-relay interface-dlci 102
  class FRTS-FRF12
!
map-class frame-relay FRTS-FRF12
 service-policy output FR-VATS
 frame-relay fragment 480
```


Task 12.11

Now re-configure LFI for the link between HQ and Branch 2. This time you may **not** use FRF.12. Configure such that the serialization delay is 10 ms.

➔ **On HQ-RTR:**

```
interface Serial0/1/0:0.2 point-to-point
 no ip address
 no frame-relay interface-dlci 202
 frame-relay interface-dlci 202 ppp virtual-template 1
!
interface virtual-template 1
 bandwidth 768
 ip address 162.1.102.1 255.255.255.0
 ip pim dense-mode
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink interleave
 service-policy output FR-VATS
```

➔ **On BR2:**

```
interface Serial0/1/0.1 point-to-point
 no ip address
 no frame-relay interface-dlci 102
 frame-relay interface-dlci 102 ppp virtual-template 1
!
interface virtual-template 1
 bandwidth 768
 ip address 162.1.102.2 255.255.255.0
 ip pim dense-mode
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink interleave
 service-policy output FR-VATS
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 13: Fax

Estimated Time to Complete: 1 hour

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 13 Fax

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab is primarily theoretical since there are currently no fax machines attached to the Proctor Labs setup. However valuable time can be well spent becoming familiar with the configuration steps.

Section 13 Configuration Tasks

Task 13.1

Configure VG248 for Fax Passthru.

➔ **Main Menu> Configure >Telephony >Port Specific Parameters Use the arrow keys to select the port to configure and press ENTER.**

```
 -------------------
| Configure         |
|-------------------|
| Network interface |
| Passwords         |
| Telephony         |
| Voice mail   -------------------------------------------
| SNMP         | Telephony                                 |
| Suspend      |-------------------------------------------|
| Resume       | CallManager TFTP server (10.5.200.21)     |
| Restart      | CallManager device name (VGC0653d6b48a)   |
 --------------| Feature codes                             |
               | Country                                   |
               | Port enable polic 1 Enabled 1006          |
               | Port specific par 2 Disabled              |
               | Advanced settings 3 Disabled              |
                -----------------  4 Disabled
                                   5 Disabled
                                   6 Enabled 1007
```

➔ **Configure these Options:**

Fax relay: (disabled)

Passthrough mode: (passthrough only: ECAN disabled)

```
 ---------- ---------------------------------------------------------- -
| Port sele| Port 1 parameters                                       | |
|----------|---------------------------------------------------------|-|
|   1 Enab | Status                     (enabled)                    | |
|   2 Enab | Call control mode          (feature)                    | |
|   3 Enab | Caller ID                  (enabled)                    | |
|   4 Disa | MWI method                 (lamp)                       | |
|   5 Disa | VMWI variant               (<country default>)          | |
|   6 Disa | Call supervision method    (none)                       | |
|   7 Disa | Input gain                 (0)                          | |
|   8 Disa | Output gain                (0)                          | |
|   9 Disa | Dialing digit detection    (default: use DSP)           | |
|  10 Disa | Fax relay                  (disabled)                   | |
|  11 Disa | Fax relay ECM              (disabled)                   | |
|  12 Disa | Fax relay NSF              (override with 000000)       | |
|  13 Disa | Passthrough mode           (passthrough only: ECAN disabled) | |
|  14 Disa -----------------------------------------------------------  |
|  15 Disabled           31 Disabled            47 Disabled             |
|  16 Disabled           32 Disabled            48 Disabled             |
|        '*' - port in use          press 'R' to enter range            |
 ----------------------------------------------------------------------
```

NOTE:

- If Fax Relay is Required then these options should be configured as:
    - Fax relay enable
    - Fax relay ECM disable
    - Fax relay NSF override with 000000 (use this value if the far end gateway is IOS (e.g.2600/3600/etc)). If the far end gateway is a WS-X6608-T1 or E1, then the default value of Preserved should be kept.

➔ **Main Menu >Configure >Telephony >Advanced Setting.**

➔ **Configure these Options:**

Passthrough signaling: (IOS mode)

Passthrough codec: (G.711 u-law)

```
| Telephony                                    |
|-----------------------------------------------|
                        ---------------------------------------------------
| CallManager | Advanced settings
| CallManager |--------------------------------------------------------
| Feature cod | Allow last good configuration (enabled)
| Country     | SRST policy                   (disabled)
| Port enable | SRST provider                 ()
| Port specif | Call preservation             (enabled: no timeou
| Advanced se | Media receive timeout         (disabled)
 -------------| Busy out off hook ports       (disabled)
              | DTMF tone duration            (default: 100ms)
              | Echo cancelling policy        (default: use SLIC)
              | Hook flash timer              (<country default>)
              | Hook flash reject period      (none)
              | Distinctive ringing           (internal calls are
              | Passthrough signaling         (IOS mode)
              | Passthrough codec             (G.711 u-law)
              | Fax relay payload size        (default: 20)
              |vFax relay maximum speed       (7200 bps)
```

➔ **To configure Fax Relay:**

NOTE:

- If Fax Relay is Required then these options should be configured as:

  Fax relay maximum speed = 7200bps

Task 13.2

Configure ATA for Fax Passthru.

➔ **ATA only supports Fax Passthru and not Fax Relay.**

➔ **To enable Fax Passthru configure the following parameters:**

➔ **AudioMode: Audio mode bit '1' should be set to 1 to force G711. The Audiomode parameter should be '0x00140014'.**

➔ **ConnectMode should be set to '0x00000400'.**

Task 13.3

Configure H323 Gateway for Fax Passthru.

➔ **Fax relay is on by default, to enable Fax Passthru change the settings in the dial-peer.**

```
dial-peer voice 100 voip
 incoming called-number <DN of local fax machine>
 destination-pattern <DN of remote faxmachine>
 modem passthrough nse codec g711ulaw
 session target ipv4:<IP Address of remote fax gateway>
 fax rate disable
 no vad
```

➔ **See below example for Fax Relay settings.**

```
dial-peer voice 100 voip
incoming called-number <DN of local fax machine>
fax-relay ecm disable
fax rate 7200
fax protocol cisco
destination-pattern <DN of remote faxmachine>
session target ipv4:<IP Address of remote fax gateway>
```

Task 13.4

Configure MGCP Gateway for Fax Passthru.

➔ **Fax relay is on by default.**

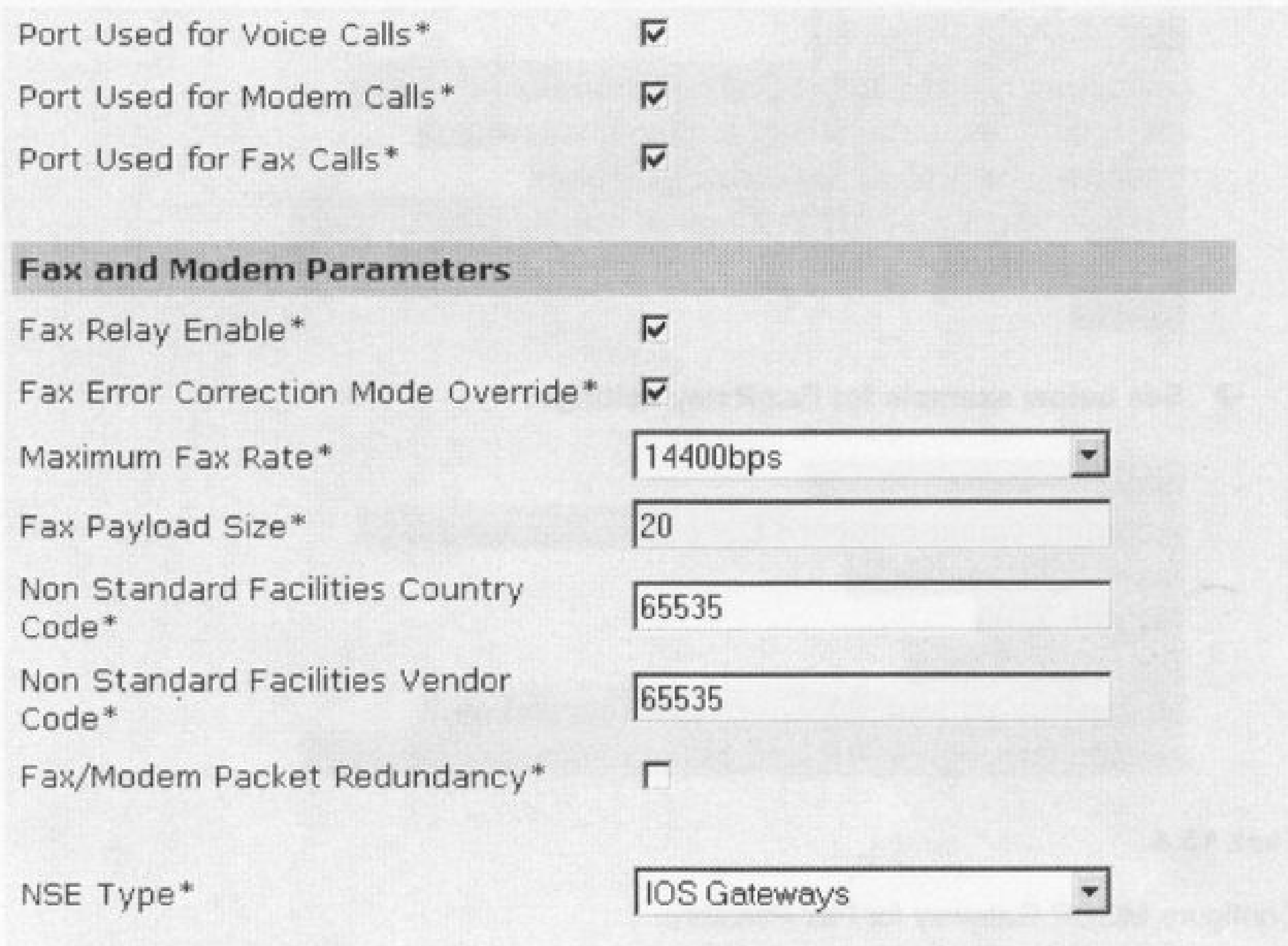
➔ **To configure Fax Passthru configure as follows:**

```
no ccm-manager fax protocol
mgcp modem passthrough voip mode nse
```

Task 13.5

Configure Catalyst 6608 for Fax Passthru.

➔ **The 6608 gateway supports both fax passthru and fax relay. To configure for Fax Relay:**



➔ **To configure for Fax Passthru:**

- **Port Used for Fax Calls => Checked**
- **Fax Relay Enable => Unchecked**
- **Fax/Modem Packet Redundancy => Unchecked**
- **NSE Type => IOS Gateway**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 14: CME Features

Estimated Time to Complete: <u>2 hours</u>

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 14 CME Features

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure Section 1 must be completed along with the CCME Gateway section. The Basics in Section 3 and 4 must also be completed.

Section 14 Configuration Tasks

Task 14.1

Change Phone 3 at BR2 so that the user cannot permanently invoke the Do-Not-Disturb function.

➔ **On BR2 – the only way to disable the DND feature is if you first have a Feature Ring on a line, which is done by separating the button and the ephone-dn with a "f".**

```
ephone 3
 no dnd feature-ring
 button  1f3
```

Task 14.2

Change Phone 2 at BR2 so that the user may not utilize the Callback feature.

➔ **On BR2 – the only way to disable the CallBack feature is basically not to give the user the option of a softkey button to push.**

```
ephone-template  1
 softkeys alerting  Endcall
!
ephone  2
 ephone-template 1
```

Task 14.3

Configure phones 1 and 2 at BR2 so that they can intercom each other and have an immediate 2-way conversation – security should be in place so that no one else can dial their respective intercom numbers. Use whatever DNs you wish for this. Also, if another intercom call happened to be present on phone 1 when phone 2 places the intercom call – the first call should be automatically put on hold.

➔ **On BR2:**

➔ **The A3001, A3002 make the intercom # so it is not dialable from a phone.**

➔ **The barge-in feature puts any existing intercom calls on hold.**

```
ephone-dn 1
 number 3001
!
ephone-dn 2
 number 3002
!
ephone-dn 21
 number A3001
 name "Intercom Ph2"
 intercom A3002 barge-in
!
ephone-dn 22
 number A3002
name "Intercom Ph1"
 intercom A3001 barge-in
!
ephone 1
 button 1:1 2:21
!
ephone 2
 button 1:2 2:22
```


Task 14.4

Allow that if a user dials *67 and then a pattern (PSTN or Internal), that the caller's ANI will not show up on the other side.

➔ **On BR2:**

```
telephony-service
 caller-id block code *67
```

Task 14.5

Continuing from Task 3.7 – allow phone 3 at BR2 to be able to enter a code in order to make International calls after hours, and make phone 2 to never be restricted for after hours international calls.

➔ **On BR2:**

```
ephone 3
 pin 12345
!
ephone 2
 after-hour exempt
```

Task 14.6

Ensure that any conference call at BR2 in which the conference initiator hangs up – that the conference terminates upon that person's leaving. However Phone 3 should be allowed to hang up or press the 'end-call' softkey and leave a conference but allow it to continue running.

➔ **On BR2 – under the desired ephone, the "keep-conference endcall" config will accomplish this desired functionality.**

```
telephony-service
 transfer-system full-consult

ephone 3
 keep-conference endcall
```

Task 14.7

Create a circular hunt group for Support with a DN of 3210 at BR2 between phones 1 and 3, and ensure that those phones can login-to and out-of the hunt group in order to receive calls. Allow the call to ring at around 3 times before searching for the next member.

➔ **On BR2:**

```
ephone-hunt 1 peer
 pilot 3210
 list 3001, 3003
 timeout 12
```

➔ **Here is what the Hunt Group would look like from the show command before one member is "logged out":**

```
P1-BR2-RTR#sh ephone-hunt
Group 1
  type: peer
  pilot number: 3210, peer-tag 20016; expanded-number 3313213210, peer-tag 20017
  list of numbers:
    3001, aux-number A3210A000, # peers 1, logout 0, down 0
      peer-tag:dn-tag [ 20015:1]
    3003, aux-number A3210A001, # peers 1, logout 0, down 0
      peer-tag:dn-tag [ 20018:3]
  preference: 0
  preference (sec): 7
  timeout: 12
  hops: 2
  E.164 register: yes
  auto logout: no
  stat collect: no
```


➔ **Typically along with the .tcl scripts in flash, you will find a .ReadMe file that you can use the GNU *nix command of 'more' to read right on the router – then copy and paste the contents of that file into MS Notepad, edit the sample config, and then copy and paste that config right back into Global config mode in the router.**

```
P1-BR2-RTR#sh flash
-#- --length-- -----date/time------ path
1      1222 Feb 05 2005 22:49:20 -05:00 startup-config
2      1538 Dec 02 2004 09:24:48 -05:00 sdmconfig-2811.cfg
.........................................
60     18346 Apr 18 2006 19:34:06 -05:00 app-b-acd-2.1.0.0.ReadMe
61     24679 Apr 18 2006 19:34:08 -05:00 app-b-acd-2.1.0.0.tcl
62     33870 Apr 18 2006 19:34:10 -05:00 app-b-acd-aa-2.1.0.0.tcl
17014784 bytes available (46870528 bytes used)

P1-BR2-RTR#more app-b-acd-2.1.0.0.ReadMe
```

➔ **On BR2:**

```
ephone-hunt 1 peer
 pilot 3210
 list 3001, 3003
 timeout 12
 statistics collect
!
!
!
application
 service queue flash:app-b-acd-2.1.0.0.tcl
  param queue-len 20
  param aa-hunt2 3210
  param number-of-hunt-grps 1
  !
 service aa flash:app-b-acd-aa-2.1.0.0.tcl
  paramspace english index 1
  param number-of-hunt-grps 1
  param handoff-string aa
  param dial-by-extension-option 3
  paramspace english language en
  param aa-pilot 3313213000
  param max-extension-length 4
  paramspace english location flash:
  param second-greeting-time 30
  param welcome-prompt en_bacd_welcome.au
  param call-retry-timer 15
  param max-time-call-retry 600
  param service-name queue
  !
!
```



```
dial-peer voice 5 pots
 service aa
 incoming called-number 3313213000
```

➔ **Now verify your statistics:**

```
P1-BR2-RTR#sh ephone-hunt 1 statistics last 1 hour
Tue 20:00 - 21:00
  Max Agents: 2
  Min Agents: 0
  Per agent statistics:
   Agent: 3001
    From queue:
     Total calls answered : 2
     Average Time in Call (secs) : 2
     Longest Time in Call (secs) : 3
   Agent: 3003
    From queue:
     Total calls answered : 2
     Average Time in Call (secs) : 47
     Longest Time in Call (secs) : 95
  Queue related statistics:
   Total calls presented to the queue:  6
   Calls answered by agents:  4
   Number of calls in the queue:  0
   Average time to answer (secs):  38
   Longest time to answer (secs):  68
   Number of abandoned calls:  2
   Average time before abandon (secs):  31
   Calls forwarded to voice mail:  1
   Calls answered by voice mail:  0
```

Task 14.10

Ensure that all calls that are placed internally (from IP Phone to IP Phone) receive not only CLID but also CNAM display with their respective names (you may name them whatever you wish).

➔ **On BR2 – One way to accomplish this is using the 'name' command on an ephone-dn – but that will carry out onto the PSTN if we use a PRI-NI2 among other protocols. The other way is use the 'directory entry' command under Telephone-Service as seen below:**

```
telephony-service
 directory entry 1 3001 name BR1 Phone 1
 directory entry 2 3002 name BR1 Phone 2
 directory entry 3 3003 name BR1 Phone 3
```


Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 15: CUE Fundamentals

Estimated Time to Complete: **1 hours**

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 15 CUE Fundamentals

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure Section 1 must be completed along with the CCME Gateway section. The Basics in Section 3 must also be completed.

Section 15 Configuration Tasks

Task 15.1

Configure the BR2 router to support the CUE module using information from Table 2. Setup the basic information needed to work the CUE module including what is needed to access the web-based GUI to manipulate user's extensions and mailboxes.

Un-integrate CME from Unity (performed in Task 9.2) and integrate into Unity Express using the same information as follows:

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

Finally setup mailboxes for all 3 phones at BR2.

➔ **On BR2:**

➔ **Since we need to give an IP address directly to the Service Module itself, and IOS also makes us specify one for the actual interface, but does not allow us to use the same IP (overlapping issues with routing) – then we use the special 'ip unnumbered' command on the interface, and the 'service-module ip address' command on the interface to specify the ip of the actual CUE engine.**

➔ **Since technically this is not a directly connected interface – but an Engine that hangs off of an interface, we also need a Static route to tell the router how to route packets destined for the IP of the Service Module/Engine.**

➔ **The 'web admin' command under the Telephony-Service gives us the ability to login to the CUE engine (though we still must initialize it first).**

➔ **Creating Usernames and passwords on the Ephones along with having DNs registered to them - allows them to be dynamically imported into the CUE engine upon setup.**

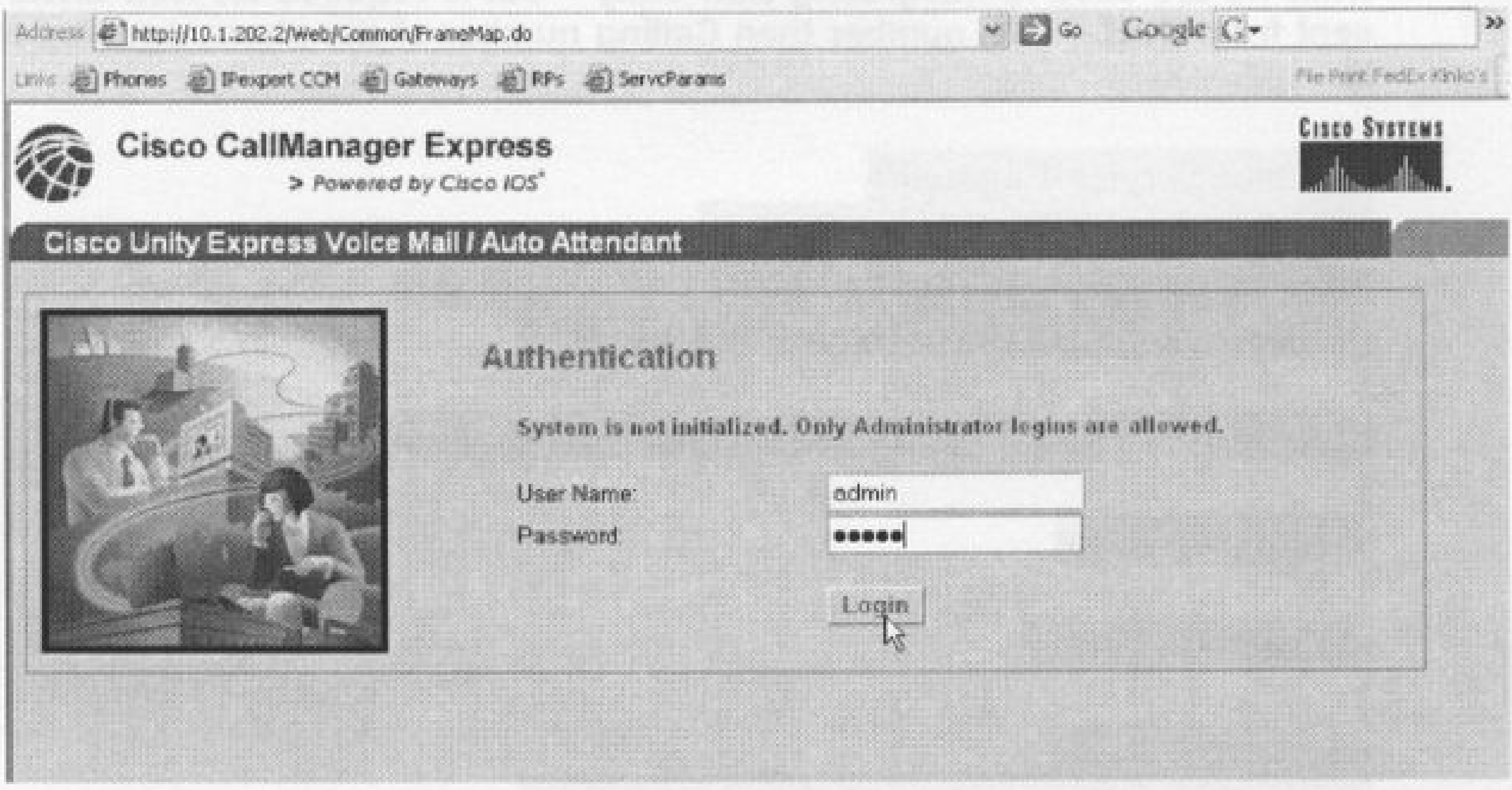
➔ **NTP is a MUST – whether Peer, Server, or Master mode – doesn't matter.**

➔ **CUE only uses SIP signaling protocol – so a Dial Peer configured for such is needed to route voice packets into CUE.**

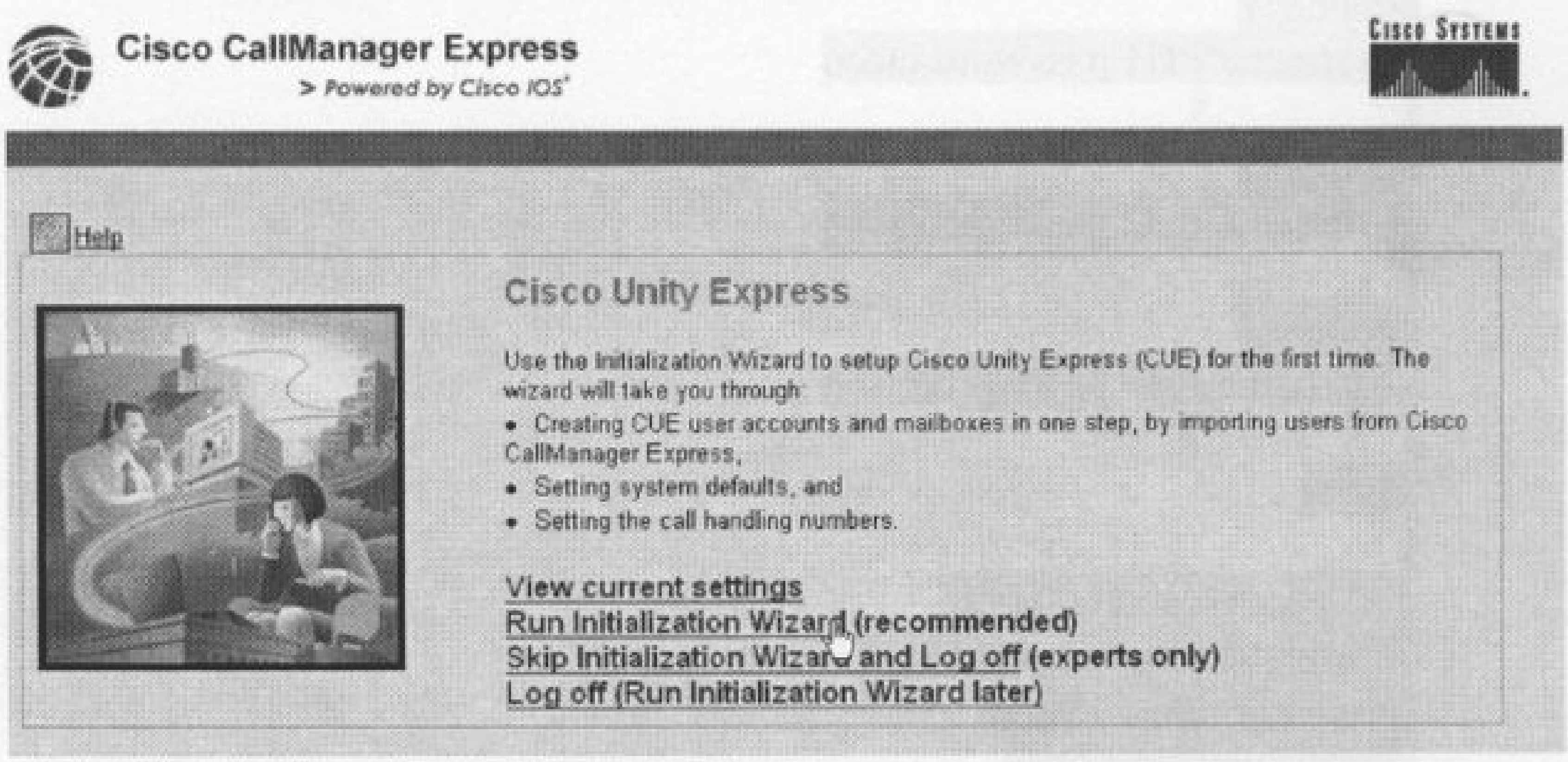
➔ **And ephone DNs for MWI with the format of 3999 are certainly a departure from what we are used to integrating with Unity – but is required for how MWIs will be sent from CUE – MWI number then Calling number of the phone needing the light lit.**

```
interface Service-Engine0/1
 ip unnumbered FastEthernet0/0.210
 service-module ip address 10.1.202.2 255.255.255.0
 service-module ip default-gateway 10.1.202.1
!
ip route 10.1.202.2 255.255.255.255 Service-Engine0/1
!
ip http path flash:
!
ntp peer 10.1.200.3
!
telephony-service
 web admin system name admin secret 0 cisco
!
ephone  1
 username PH1 password cisco
!
ephone  2
 username PH2 password cisco
!
ephone  3
 username PH3 password cisco
!
sip-ua
!
dial-peer voice 3600 voip
 destination-pattern 3[126]00
 session protocol sipv2
 dtmf-relay sip-notify
 session target ipv4:10.1.202.2
 codec g711ulaw
 no vad
!
ephone-dn 36
 number 3999….
 mwi on
!
ephone-dn 37
 number 3998….
 mwi off
!
```

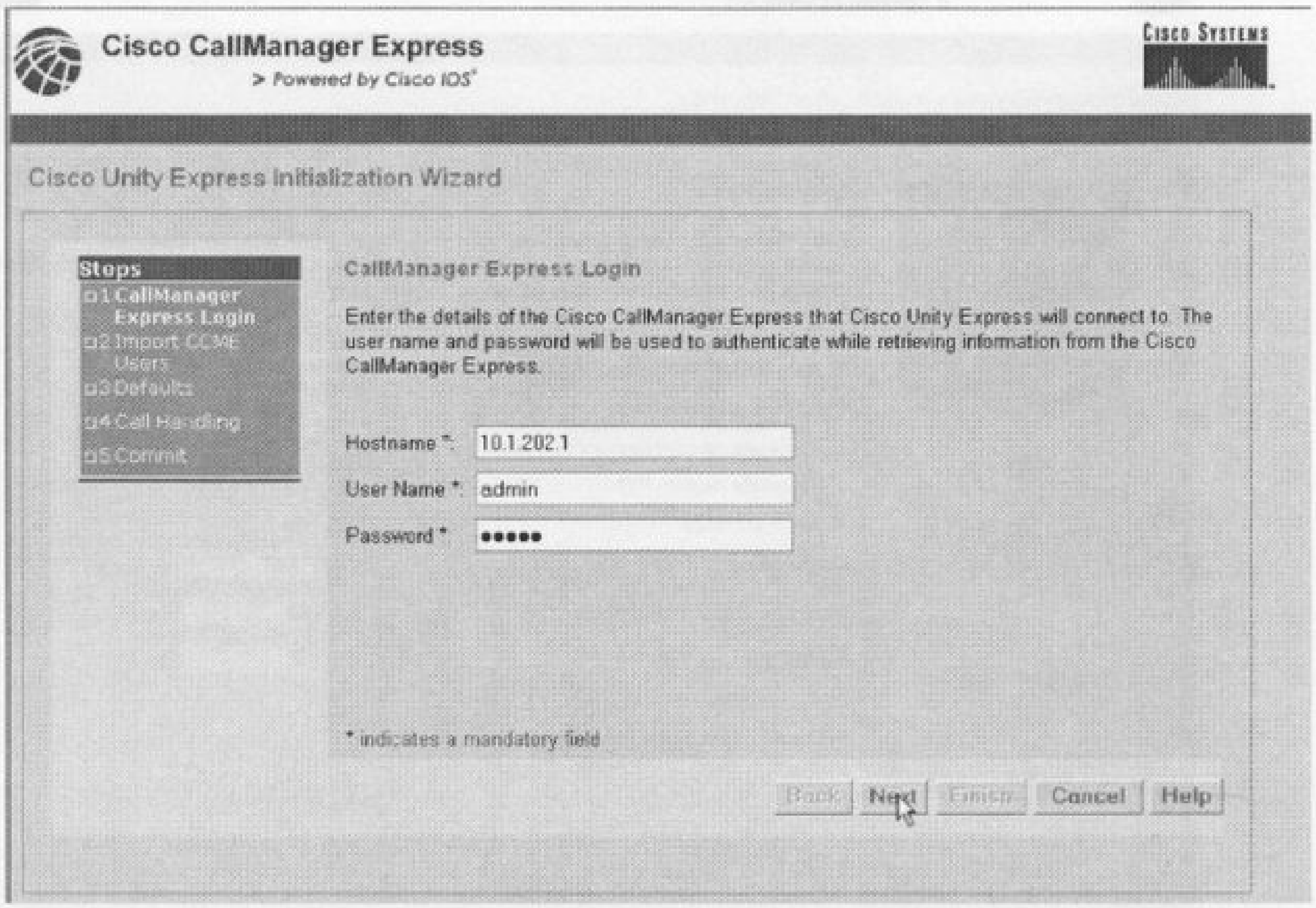
➔ **From Internet Explorer browse to http://10.1.202.2/Web.**

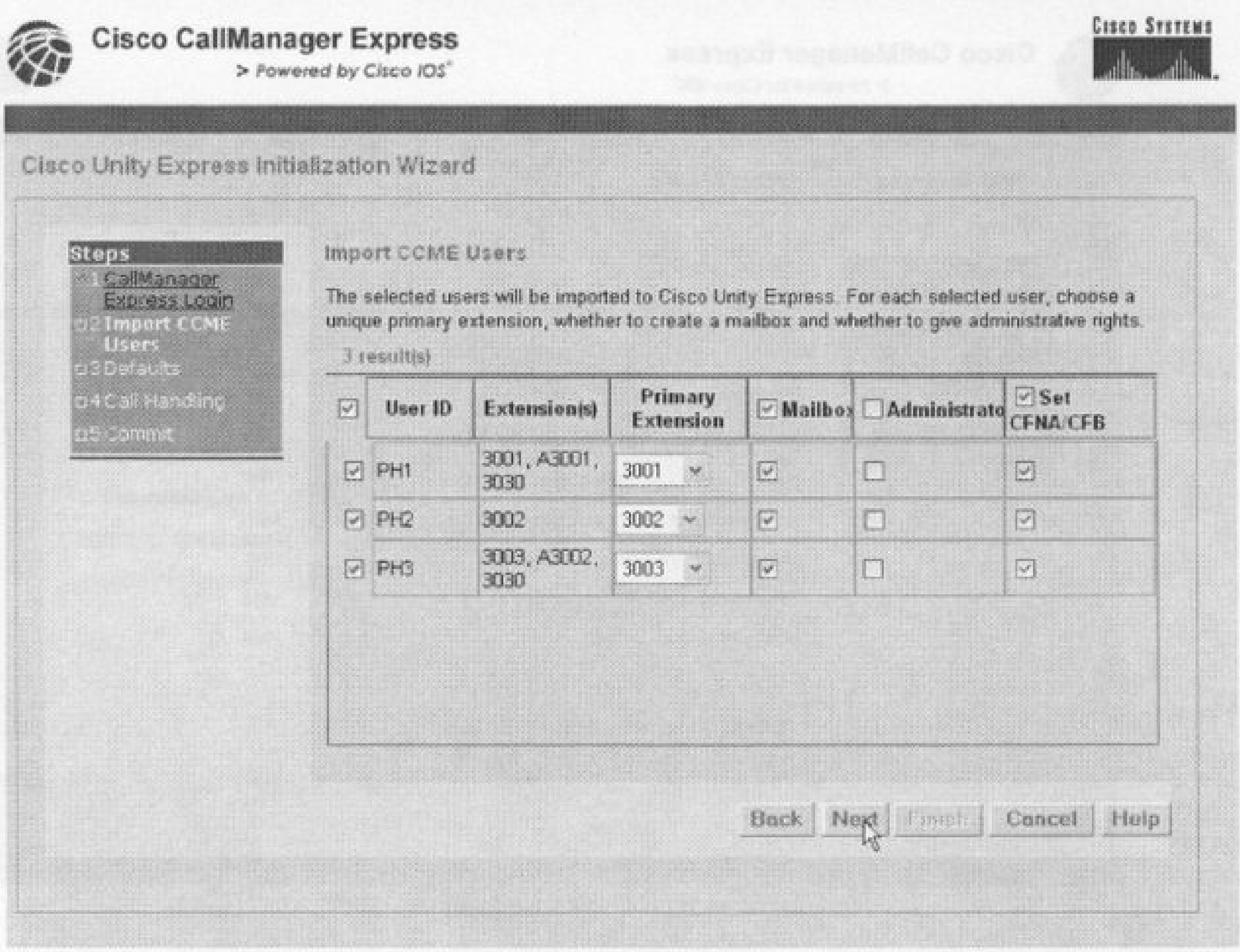


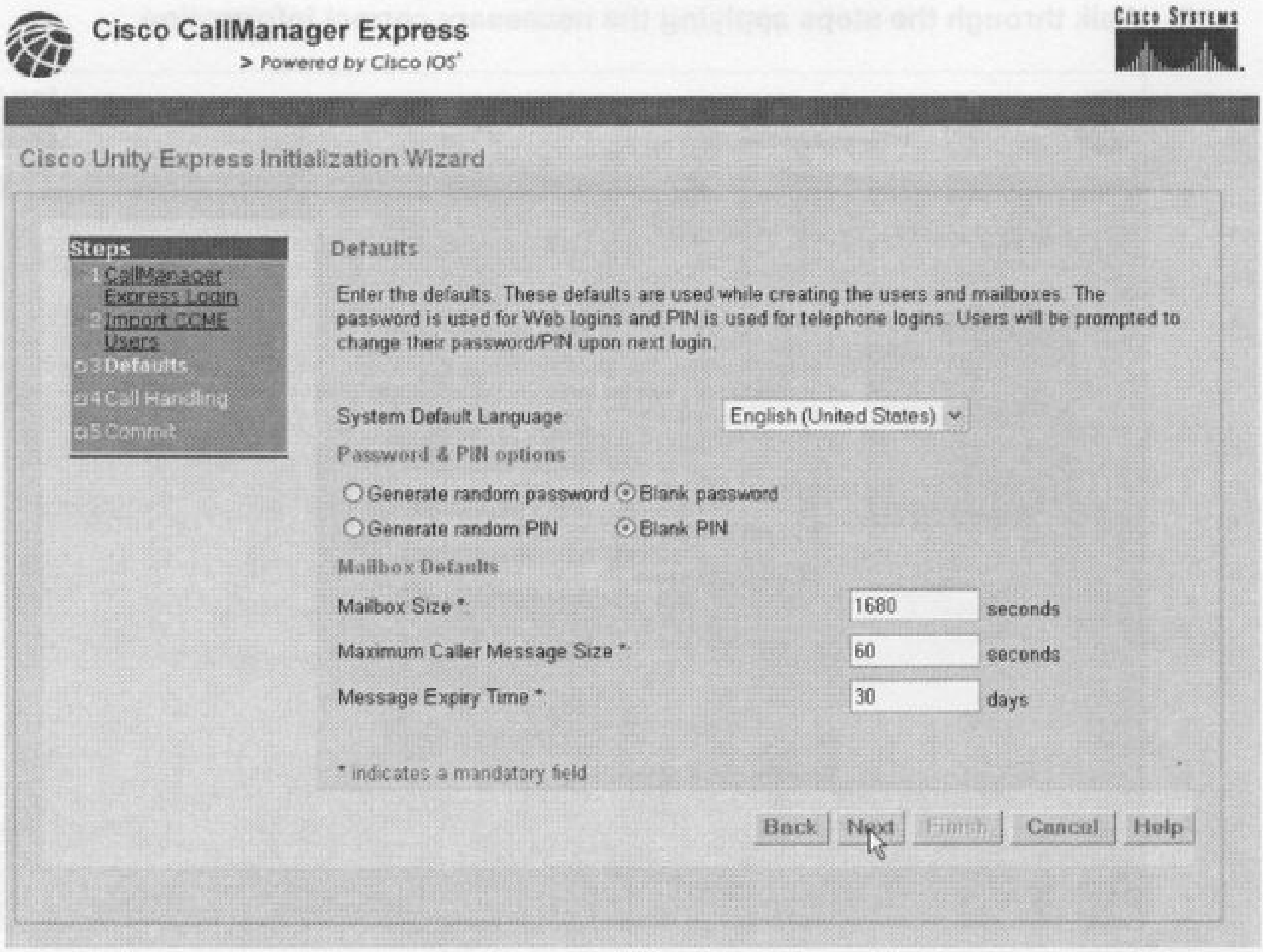
➔ **Run the Initialization Wizard.**

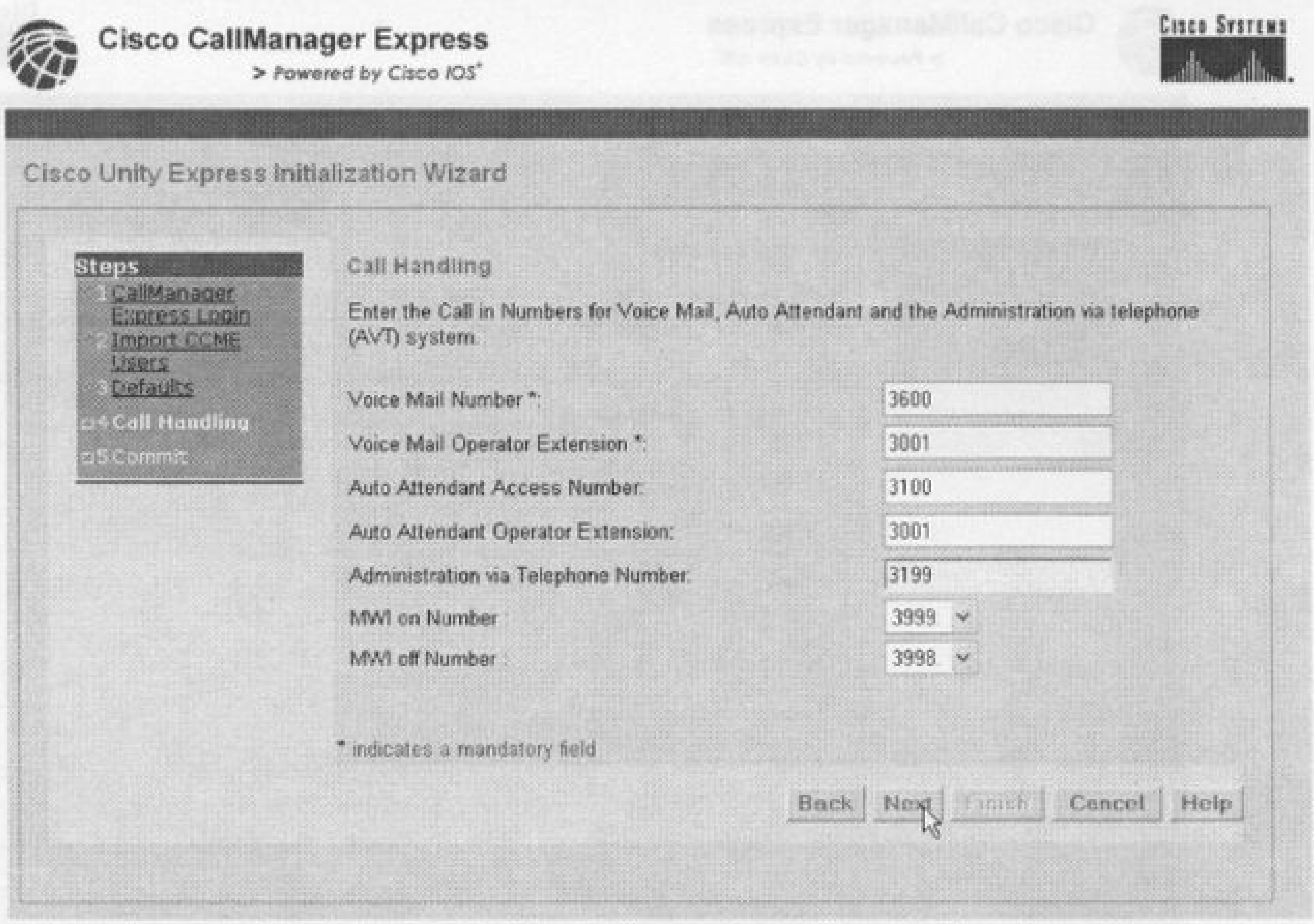


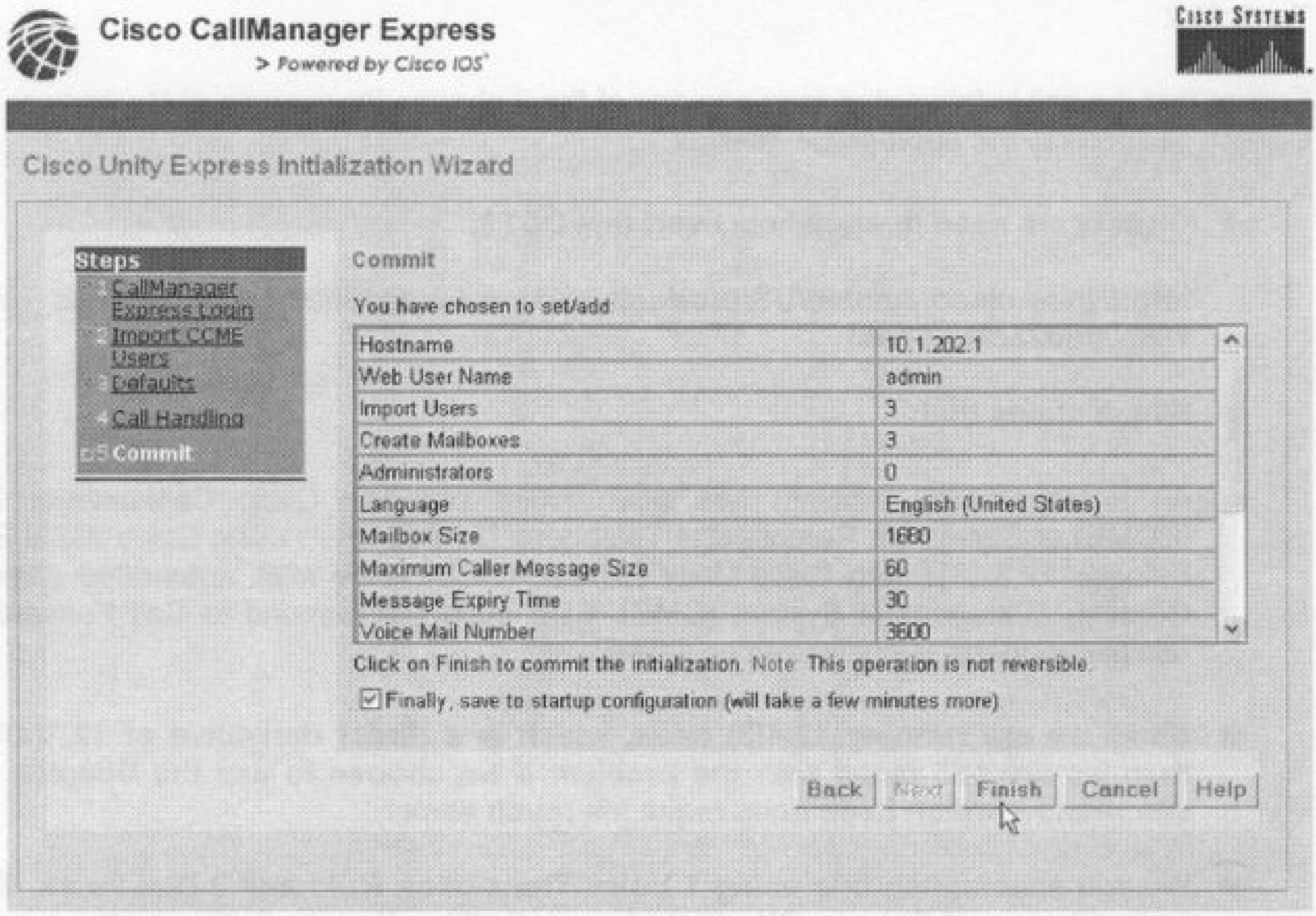
→ **Walk through the steps applying the necessary correct information.**

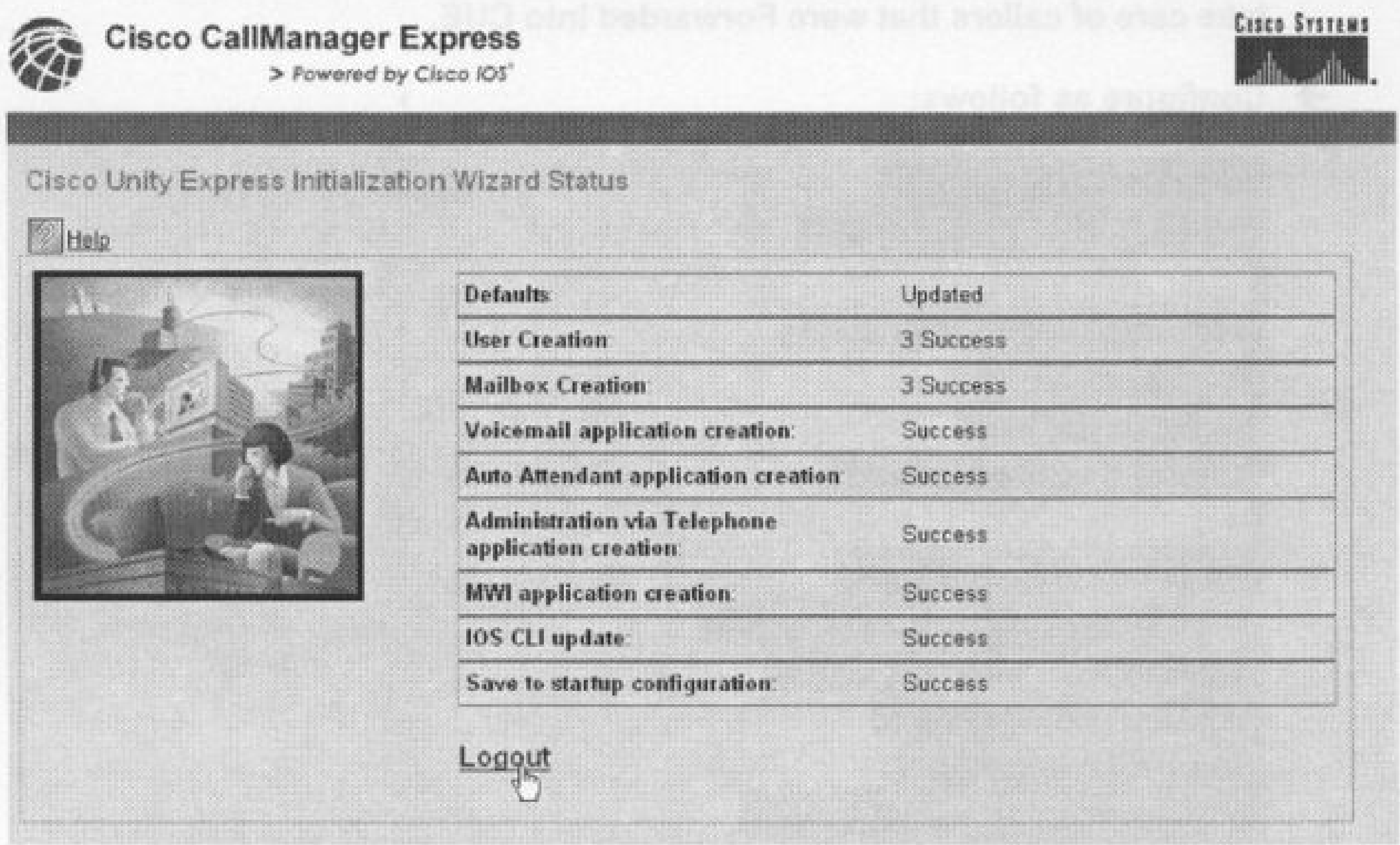





Cisco CallManager Express
> Powered by Cisco IOS
Cisco Systems
Cisco Unity Express Initialization Wizard
Steps
1 CallManager Express Login
2 Import CCME Users
3 Defaults
4 Call Handling
5 Commit
Defaults
Enter the defaults. These defaults are used while creating the users and mailboxes. The password is used for Web logins and PIN is used for telephone logins. Users will be prompted to change their password/PIN upon next login.
System Default Language: English (United States)
Password & PIN options
Generate random password
Blank password
Generate random PIN
Blank PIN
Mailbox Defaults
Mailbox Size *: 1680 seconds
Maximum Caller Message Size *: 60 seconds
Message Expiry Time *: 30 days
* indicates a mandatory field
Back
Next
Finish
Cancel
Help


Cisco CallManager Express
> Powered by Cisco IOS
Cisco Systems
Cisco Unity Express Initialization Wizard
Steps
1 CallManager Express Login
2 Import CCME Users
3 Defaults
4 Call Handling
5 Commit
Call Handling
Enter the Call in Numbers for Voice Mail, Auto Attendant and the Administration via telephone (AVT) system.
Voice Mail Number *: 3600
Voice Mail Operator Extension *: 3001
Auto Attendant Access Number: 3100
Auto Attendant Operator Extension: 3001
Administration via Telephone Number: 3199
MWI on Number: 3999
MWI off Number: 3998
* indicates a mandatory field
Back
Next
Finish
Cancel
Help


Cisco CallManager Express
> Powered by Cisco IOS
Cisco Systems
Cisco Unity Express Initialization Wizard
Steps
1 CallManager Express Login
2 Import CCME Users
3 Defaults
4 Call Handling
5 Commit
Commit
You have chosen to set/add:
Hostname 10.1.202.1
Web User Name admin
Import Users 3
Create Mailboxes 3
Administrators 0
Language English (United States)
Mailbox Size 1680
Maximum Caller Message Size 60
Message Expiry Time 30
Voice Mail Number 3600
Click on Finish to commit the initialization. Note: This operation is not reversible.
Finally, save to startup configuration (will take a few minutes more).
Back
Next
Finish
Cancel
Help


Cisco CallManager Express
> Powered by Cisco IOS
Cisco Systems
Cisco Unity Express Initialization Wizard Status
Help
Defaults: Updated
User Creation: 3 Success
Mailbox Creation: 3 Success
Voicemail application creation: Success
Auto Attendant application creation: Success
Administration via Telephone application creation: Success
MWI application creation: Success
IOS CLI update: Success
Save to startup configuration: Success
Logout

Task 15.2

Ensure that if a call is forwarded from any one of the 3 phones for reasons of No-Answer or Busy that the call goes to the appropriate mailbox

➔ **On BR2 we need to somehow avert this DDTS:**

http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_field_notice09186a008023cfe2.shtml

➔ **Which states that:**

An interoperability problem has been found between Cisco CallManager Express (CCME) or Survivable Remote Site Telephony (SRST) when using Cisco IOS® Software Release 12.3 (8)T with Cisco Unity Express (CUE) voice mail, automated attendant or Greeting Management System (GMS). CUE does not respond to Call Forwards when "dialplan-pattern" is configured on CCME.

➔ **Since we are running 12.4(3) code, which is a direct derivative of 12.3(x)T code, then we are still faced with the problem *if* we choose to use the Dialplan Pattern command – which itself does make life much easier.**

➔ **We will accomplish this using 1 Voice Translation Rule and 2 Dial-Peers. The first one will convert Ephone DNs that place calls Directly into CUE, and the second will take care of callers that were Forwarded into CUE.**

➔ **Configure as follows:**

```
voice translation-rule 1
 rule 1 /^331321\(3...\)/ /\1/
!
voice translation-profile VM
 translate calling 1
 translate called 1
 translate redirect-called 1
!
dial-peer voice 3600 voip
 translation-profile outgoing VM
 destination-pattern 3[126]00
 session protocol sipv2
 dtmf-relay sip-notify
 session target ipv4:10.1.202.2
 codec g711ulaw
 no vad
!
!
```



```
dial-peer voice 3601 voip
 translation-profile outgoing VM
 destination-pattern 3313213[126]00
 session protocol sipv2
 dtmf-relay sip-notify
 session target ipv4:10.1.202.2
 codec g711ulaw
 no vad
!
```

Task 15.3

Ensure that when users listen to their voicemail messages, that they hear the ANI announced of the phone who left them the message.

➔ **On BR2:**

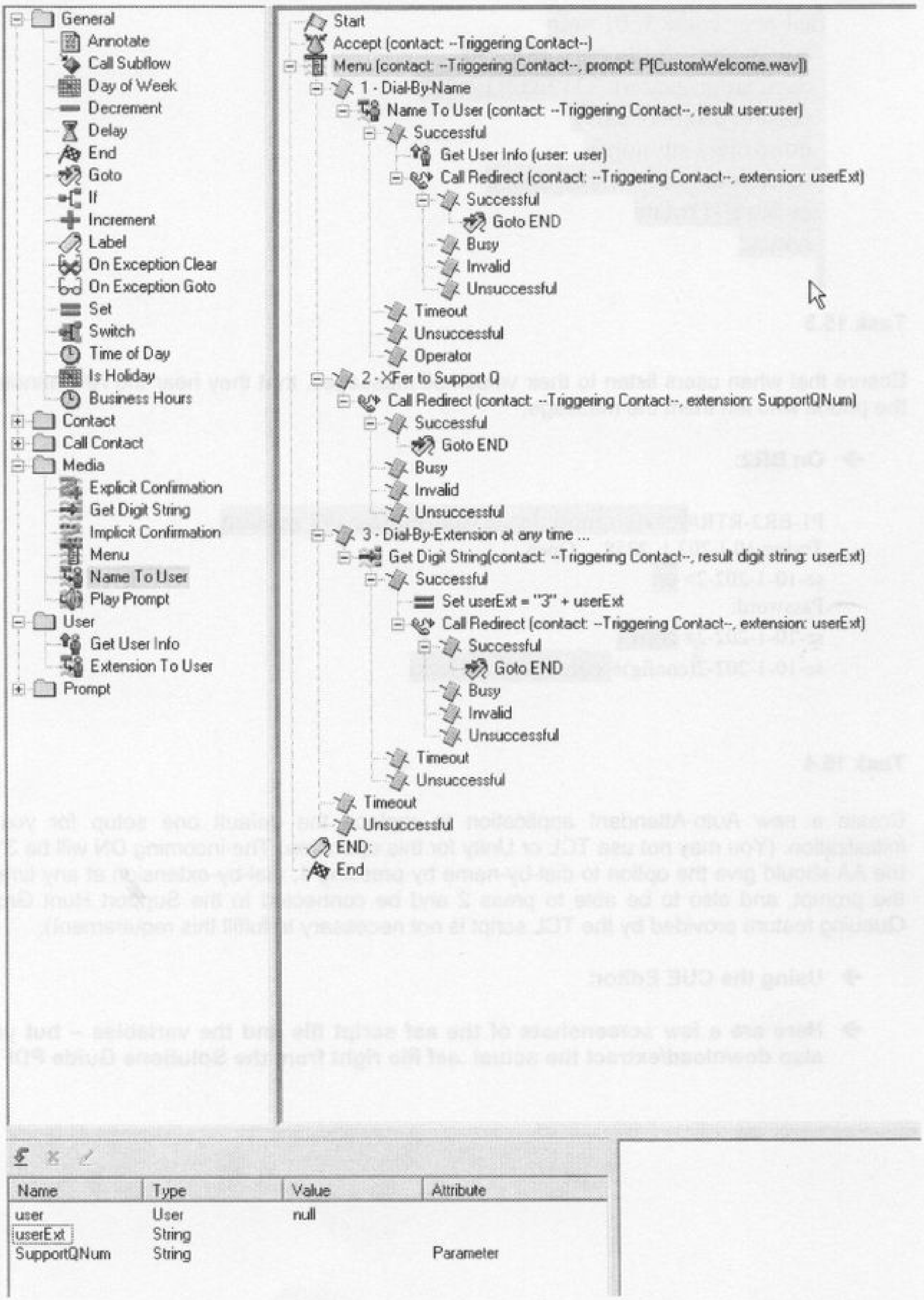
```
P1-BR2-RTR#service-module service-Engine 0/1 session
Trying 10.1.202.1, 2258 ... Open
se-10-1-202-2> en
Password:
se-10-1-202-2# conf t
se-10-1-202-2(config)# voicemail callerid
```

Task 15.4

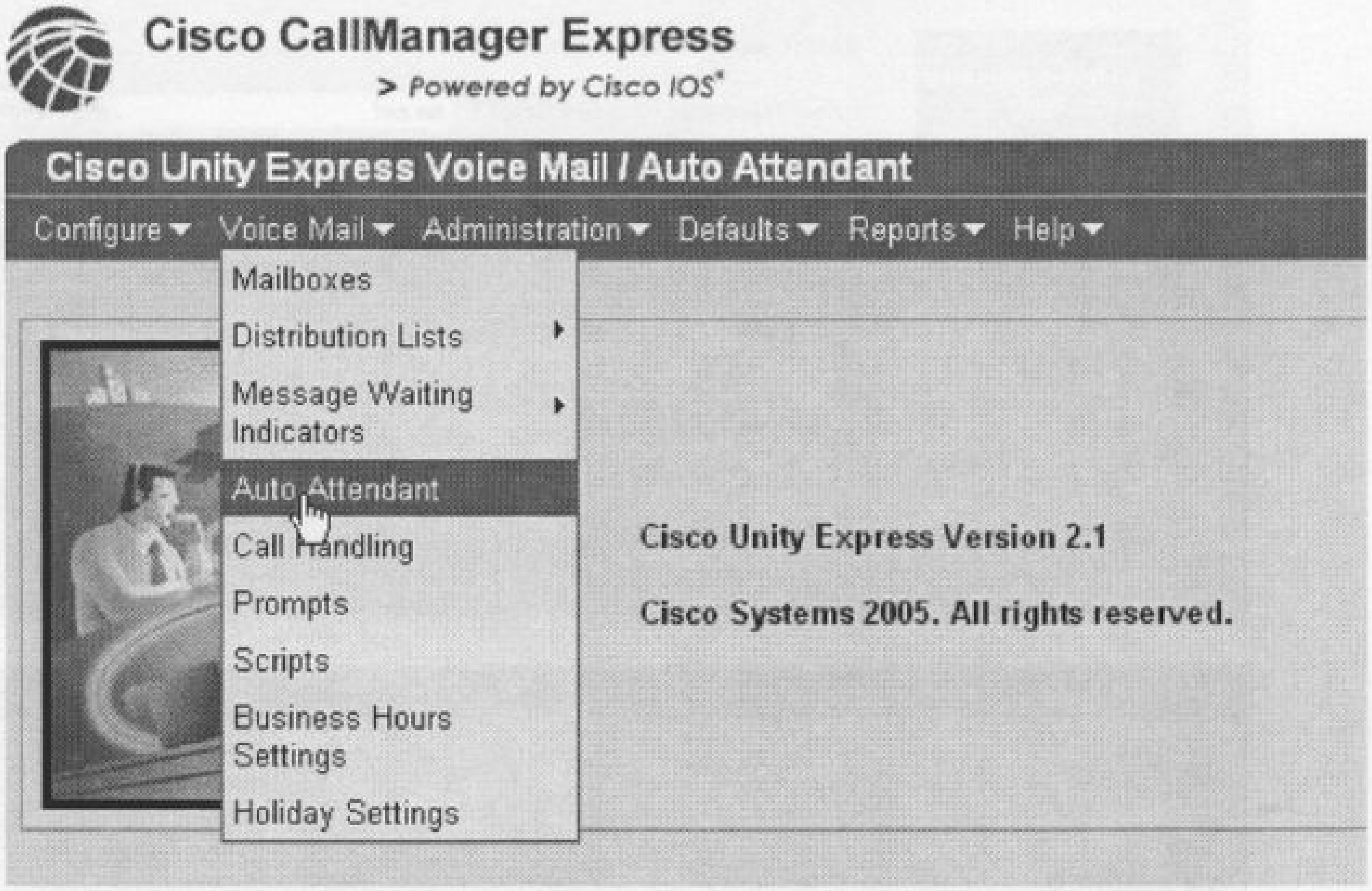
Create a new Auto-Attendant application to replace the default one setup for you during initialization. (You may not use TCL or Unity for this operation) The incoming DN will be 3100 and the AA should give the option to dial-by-name by pressing 1, dial-by-extension at any time during the prompt, and also to be able to press 2 and be connected to the Support Hunt Group (the Queuing feature provided by the TCL script is not necessary to fulfill this requirement).

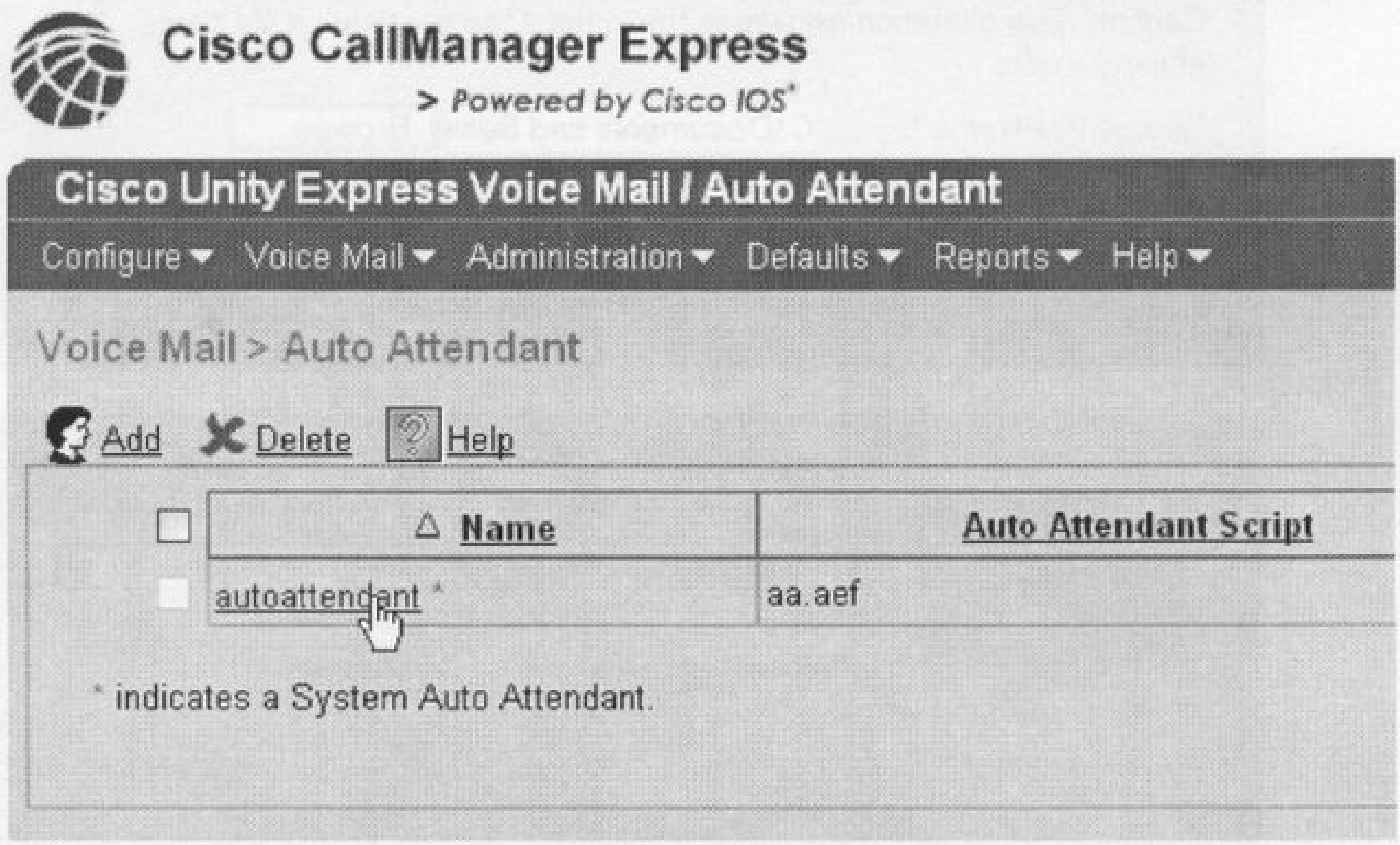
➔ **Using the CUE Editor:**

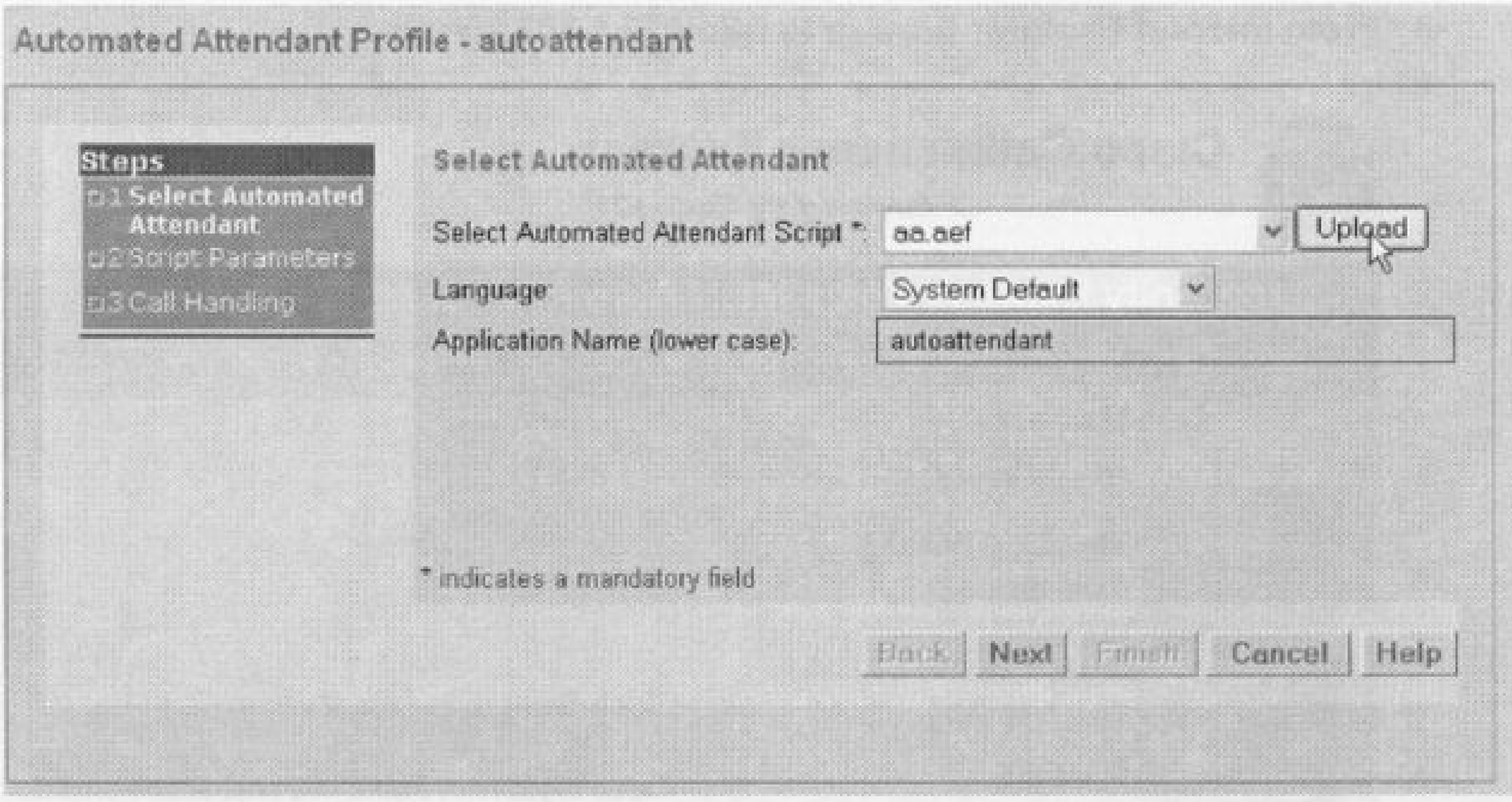
➔ **Here are a few screenshots of the aef script file and the variables – but you may also download/extract the actual .aef file right from the Solutions Guide PDF.**

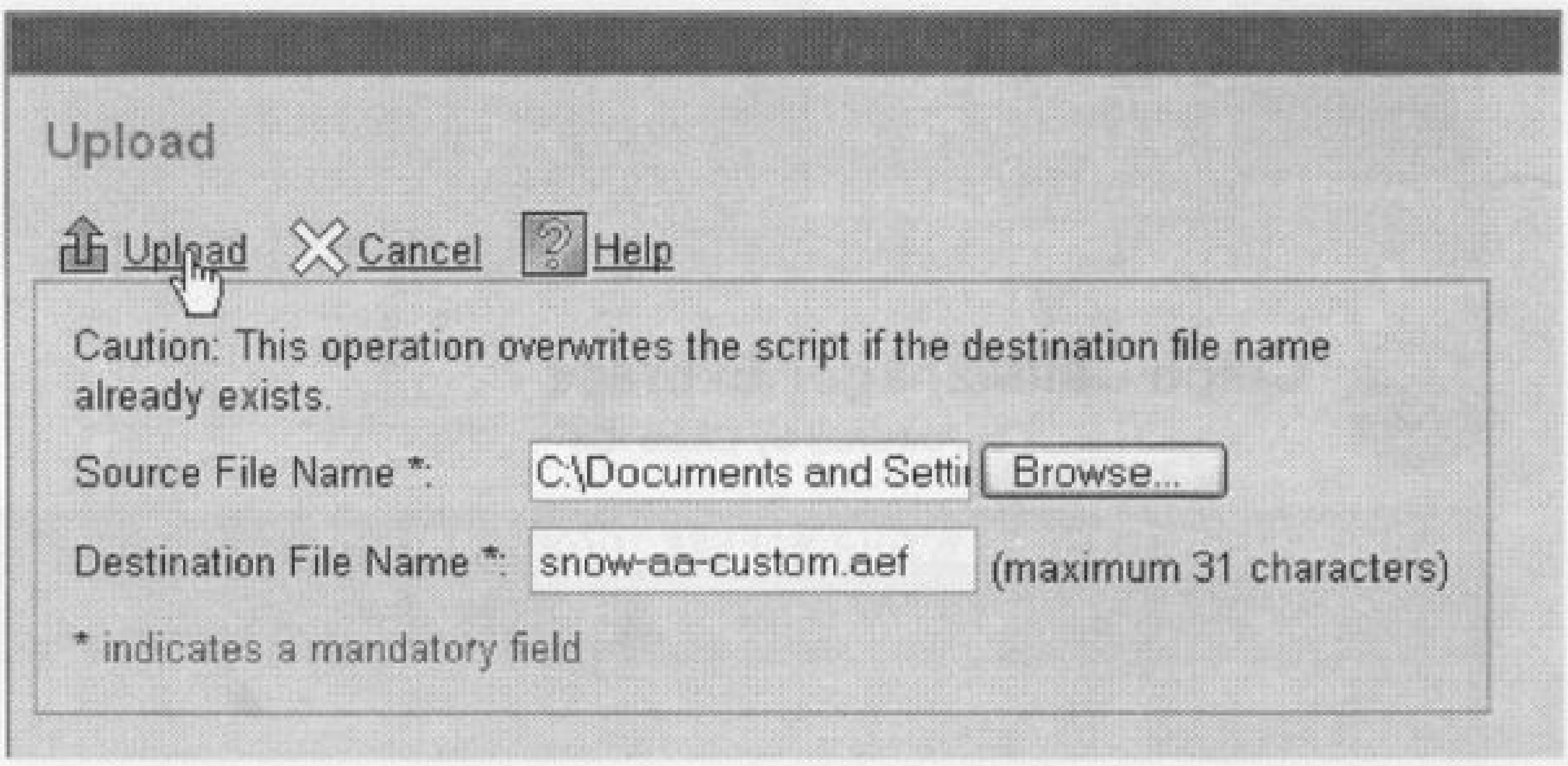

General
Annotate
Call Subflow
Day of Week
Decrement
Delay
End
Goto
If
Increment
Label
On Exception Clear
On Exception Goto
Set
Switch
Time of Day
Is Holiday
Business Hours
Contact
Call Contact
Media
Explicit Confirmation
Get Digit String
Implicit Confirmation
Menu
Name To User
Play Prompt
User
Get User Info
Extension To User
Prompt
Start
Accept (contact: --Triggering Contact--)
Menu (contact: --Triggering Contact--, prompt: P[CustomWelcome.wav])
1 - Dial-By-Name
Name To User (contact: --Triggering Contact--, result user:user)
Successful
Get User Info (user: user)
Call Redirect (contact: --Triggering Contact--, extension: userExt)
Successful
Goto END
Busy
Invalid
Unsuccessful
Timeout
Unsuccessful
Operator
2 - XFer to Support Q
Call Redirect (contact: --Triggering Contact--, extension: SupportQNum)
Successful
Goto END
Busy
Invalid
Unsuccessful
3 - Dial-By-Extension at any time ...
Get Digit String(contact: --Triggering Contact--, result digit string: userExt)
Successful
Set userExt = "3" + userExt
Call Redirect (contact: --Triggering Contact--, extension: userExt)
Successful
Goto END
Busy
Invalid
Unsuccessful
Timeout
Unsuccessful
Timeout
Unsuccessful
END
End
Name
Type
Value
Attribute
user
User
null
userExt
String
SupportQNum
String
Parameter

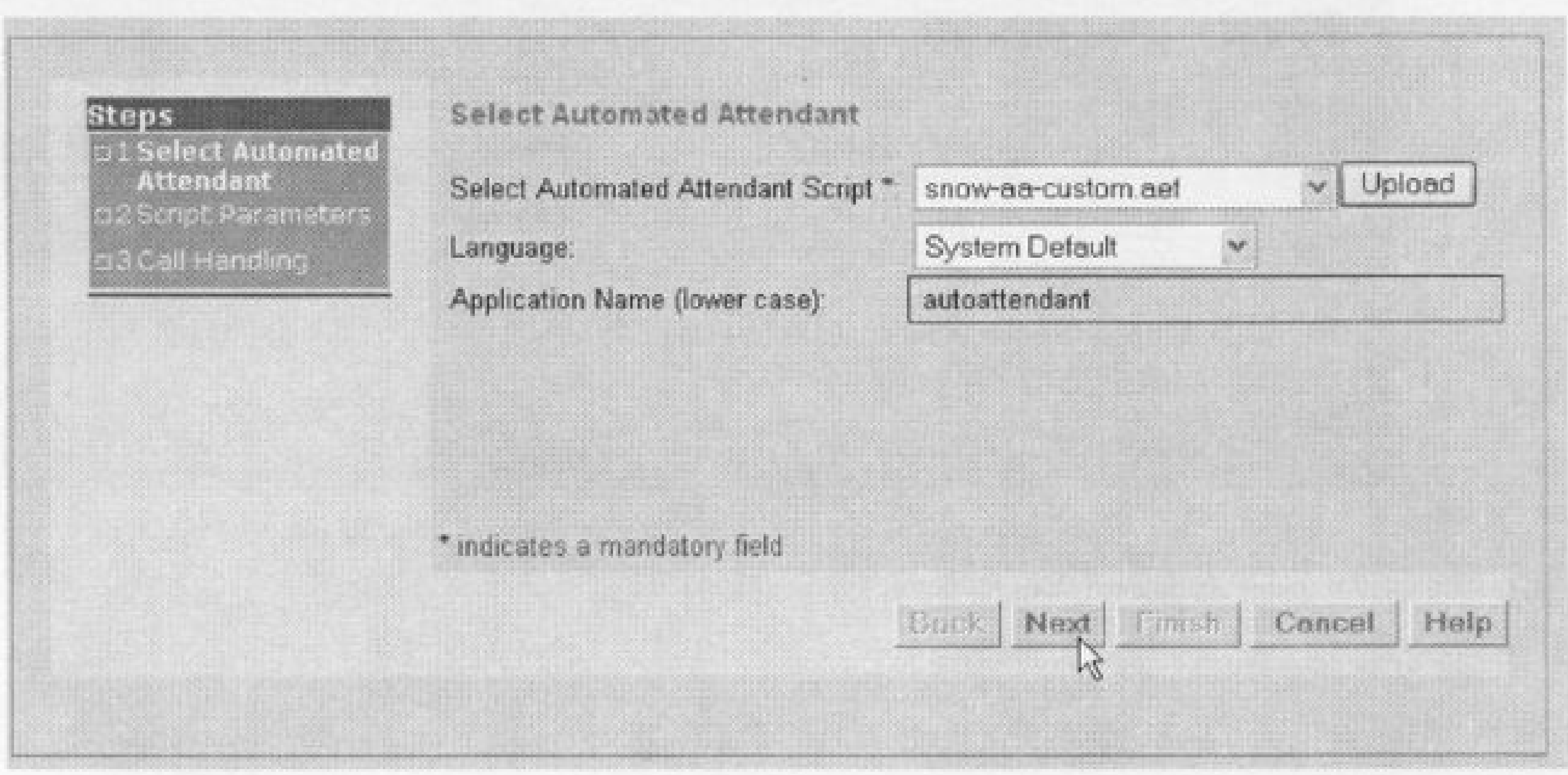
➔ **From Internet Explorer browse to http://10.1.202.2/Web.**

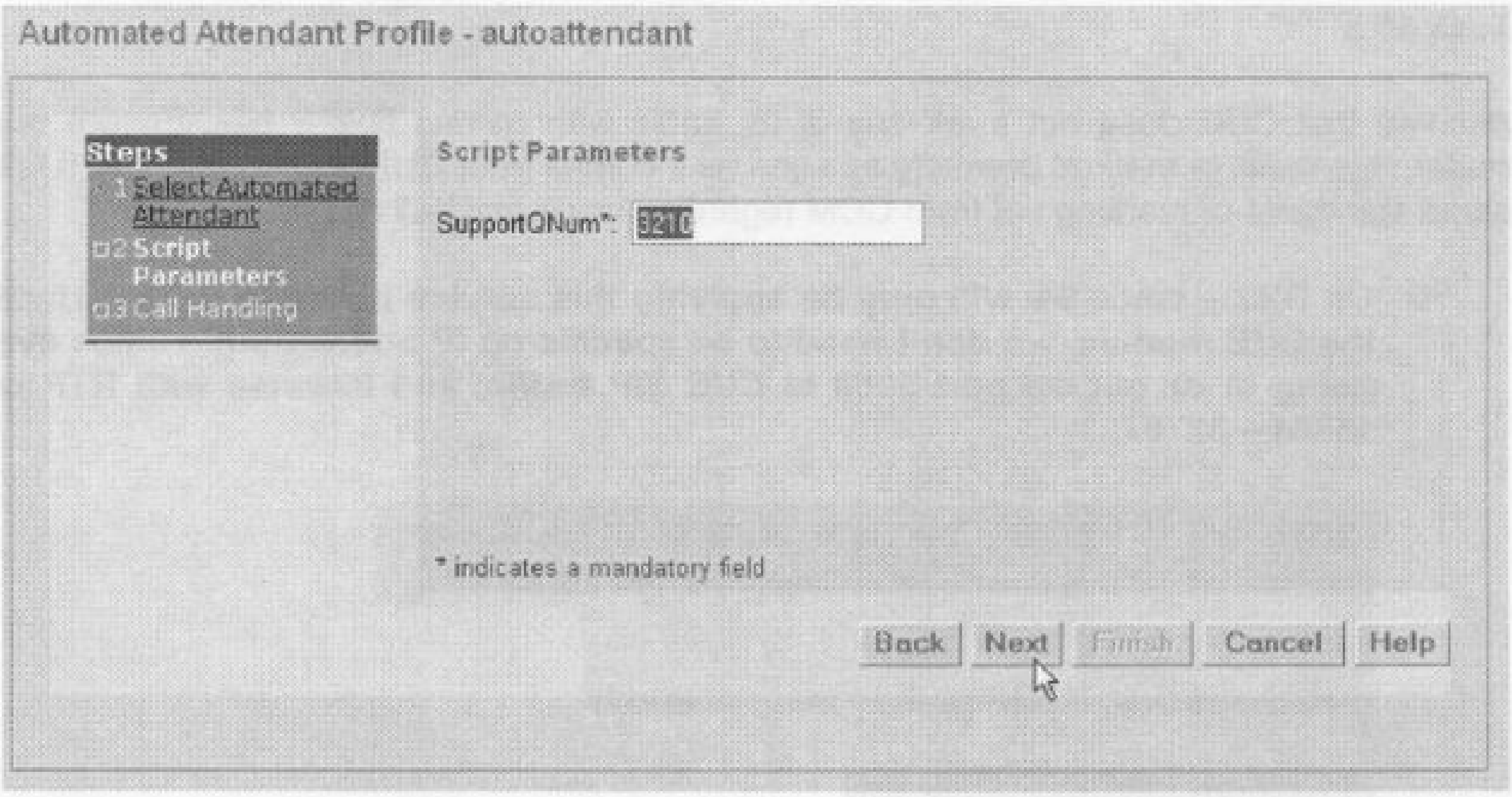





Automated Attendant Profile - autoattendant
Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Select Automated Attendant
Select Automated Attendant Script *: aa.aef
Upload
Language: System Default
Application Name (lower case): autoattendant
* indicates a mandatory field
Back
Next
Finish
Cancel
Help


Upload
Upload
Cancel
Help
Caution: This operation overwrites the script if the destination file name already exists.
Source File Name *: C:\Documents and Setti
Browse...
Destination File Name *: snow-aa-custom.aef
(maximum 31 characters)
* indicates a mandatory field


Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Select Automated Attendant
Select Automated Attendant Script *: snow-aa-custom.aef
Upload
Language: System Default
Application Name (lower case): autoattendant
* indicates a mandatory field
Back
Next
Finish
Cancel
Help


Automated Attendant Profile - autoattendant
Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Script Parameters
SupportQNum*: 3210
* indicates a mandatory field
Back
Next
Finish
Cancel
Help


Automated Attendant Profile - autoattendant
Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Call Handling
Call-in Number: 3100
Maximum Sessions *: 4
Enabled: Yes No
* indicates a mandatory field
Back
Next
Finish
Cancel
Help

Task 15.5

Assume that CUE does not mark any of its traffic with correct DSCP bits. Ensure that in the router, this traffic is marked correctly as soon as it comes from CUE and ensure that it follows the same standards of marking set from CCM regarding voice and call control.

➔ **On BR2 – since we will only be applying this service policy to the interface that is the CUE module, we don't need to be specific on IP addressing – since everything going in or out on port 5060 is CUE SIP traffic, and likewise with RTP on ports 16384 – 32767.**

```
access-list 101 permit udp any range 16384 32767 any
access-list 101 permit udp any any range 16384 32767
access-list 102 permit udp any eq 5060 any
access-list 102 permit udp any any eq 5060
!
class-map match-any cue-rtp
 match access-group 101
class-map match-any cue-sip
 match access-group 102
!
policy-map cue-traffic
 class cue-rtp
  set dscp ef
 class cue-sip
  set dscp cs3
!
interface Service-Engine0/1
 ip unnumbered FastEthernet0/0.210
 service-module ip address 10.1.202.2 255.255.255.0
 service-module ip default-gateway 10.1.202.1
 service-policy input cue-traffic
```

➔ **Why did we apply this map on the Input?**

➔ **Keep in mind how the router sees things. As far as the router is concerned, traffic is coming from the CUE module IN to the router on this interface and will be leaving OUT of the router on a different interface such as the Serial or FastEthernet.**

➔ **Verify:**

```
P1-BR2-RTR#sh policy-map interface serv0/1
 Service-Engine0/1

  Service-policy input: cue-traffic

    Class-map: cue-rtp (match-any)
      1064 packets, 226310 bytes
      5 minute offered rate 6000 bps, drop rate 0 bps
      Match: access-group 101
        1064 packets, 226310 bytes
        5 minute rate 6000 bps
      QoS Set
        dscp ef
          Packets marked 1064

    Class-map: cue-sip (match-any)
      76 packets, 31203 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 102
        76 packets, 31203 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
          Packets marked 76

    Class-map: class-default (match-any)
      3395 packets, 725678 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 16: CUE Features

Estimated Time to Complete: **3 hours**

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 16 CUE Features

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

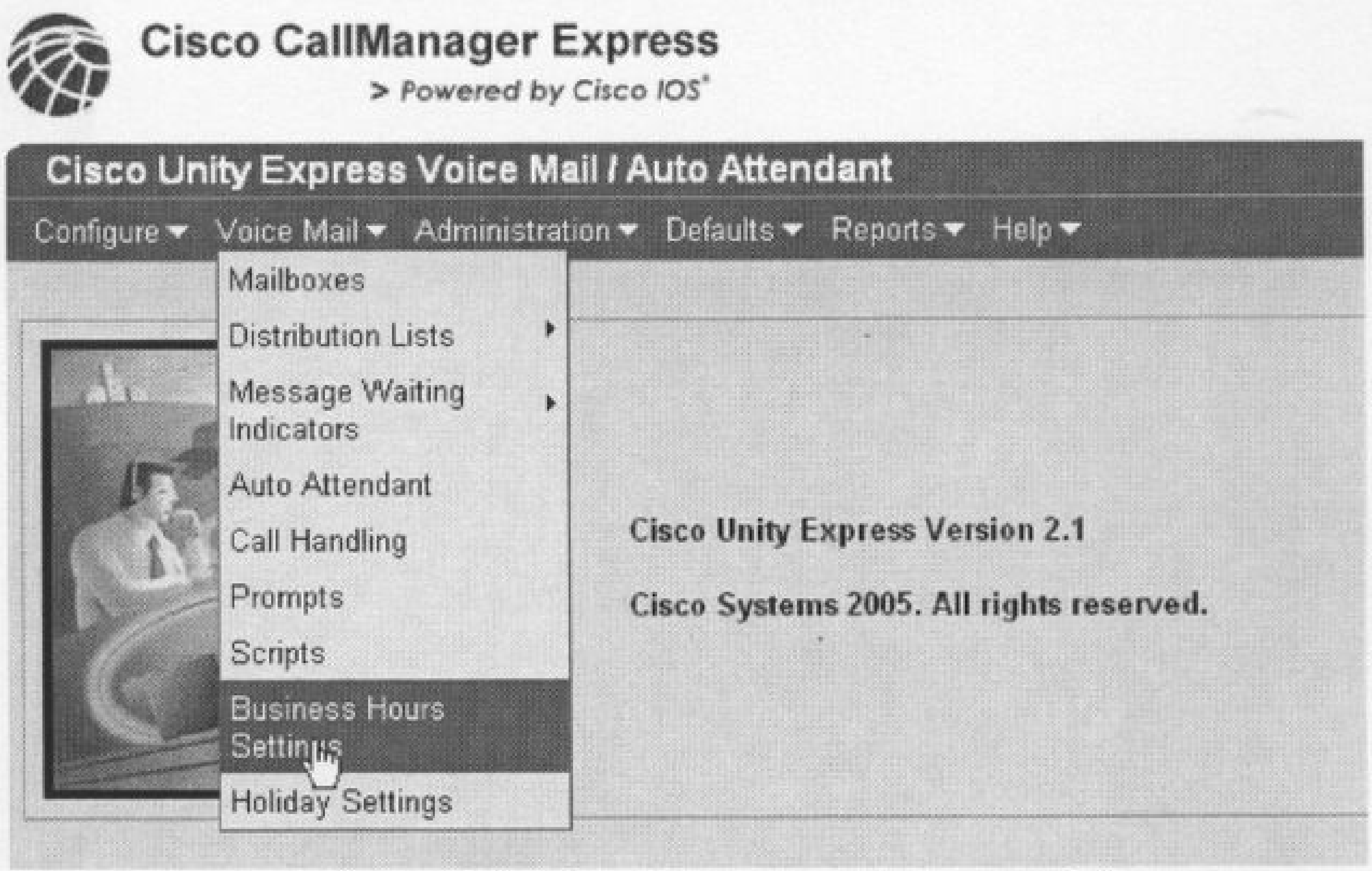
To complete this lab the infrastructure Section 1 must be completed. The Basics in Section 3 and 15 must also be completed.

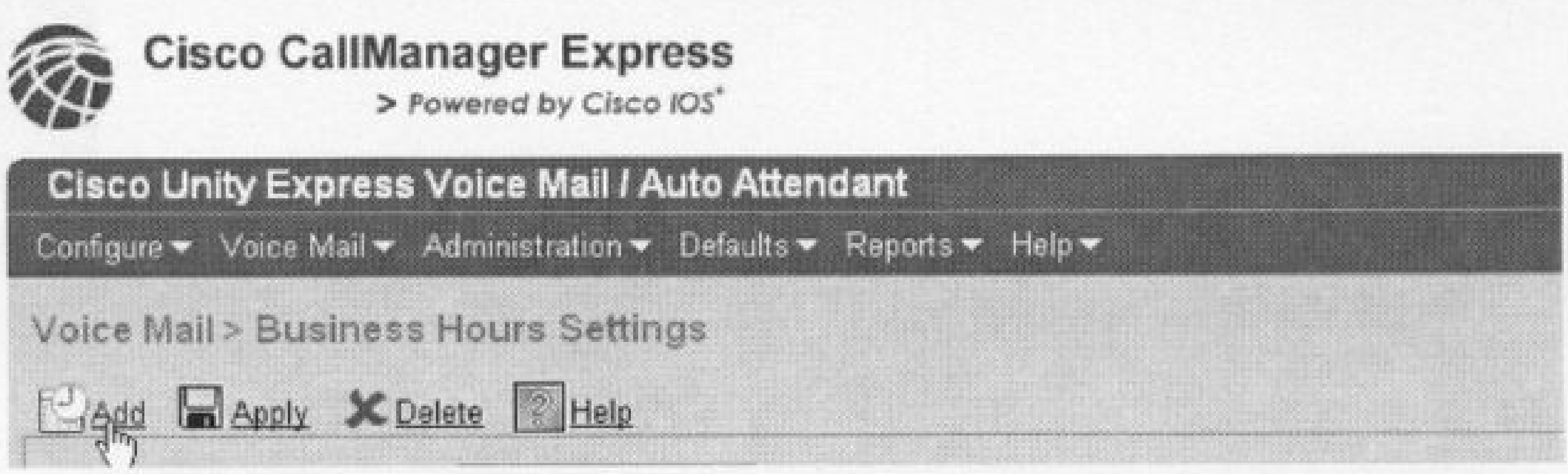
Section 16 Configuration Tasks

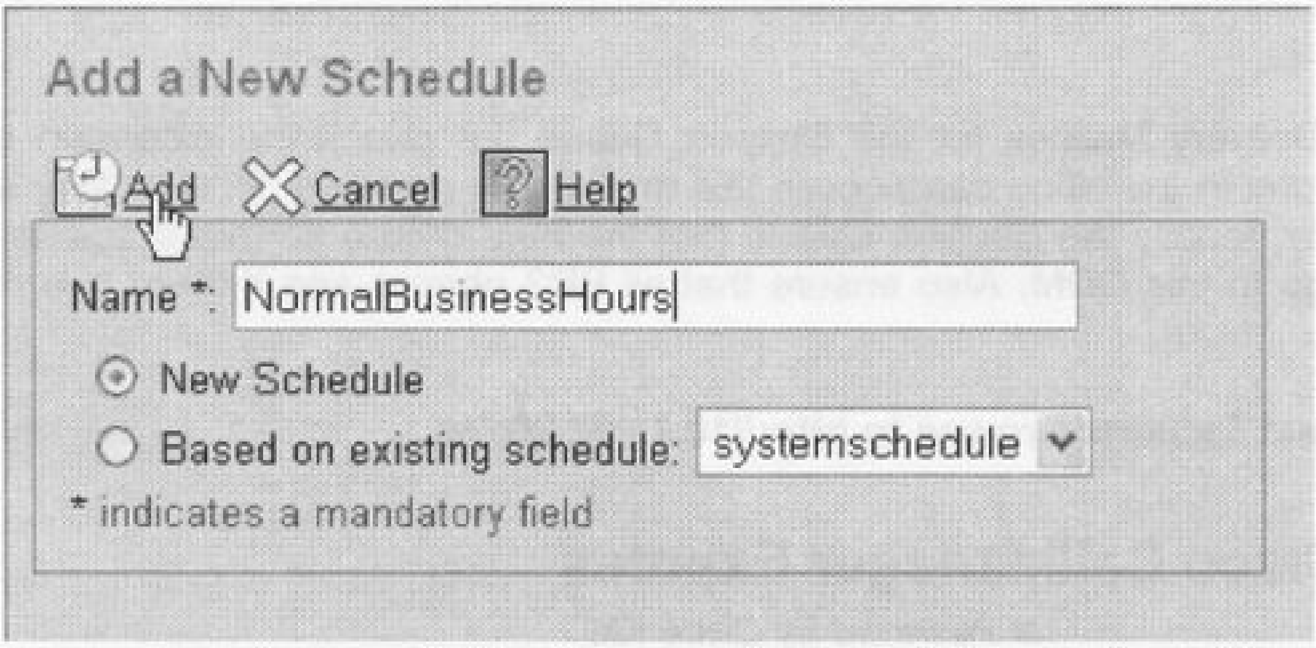
Task 16.1

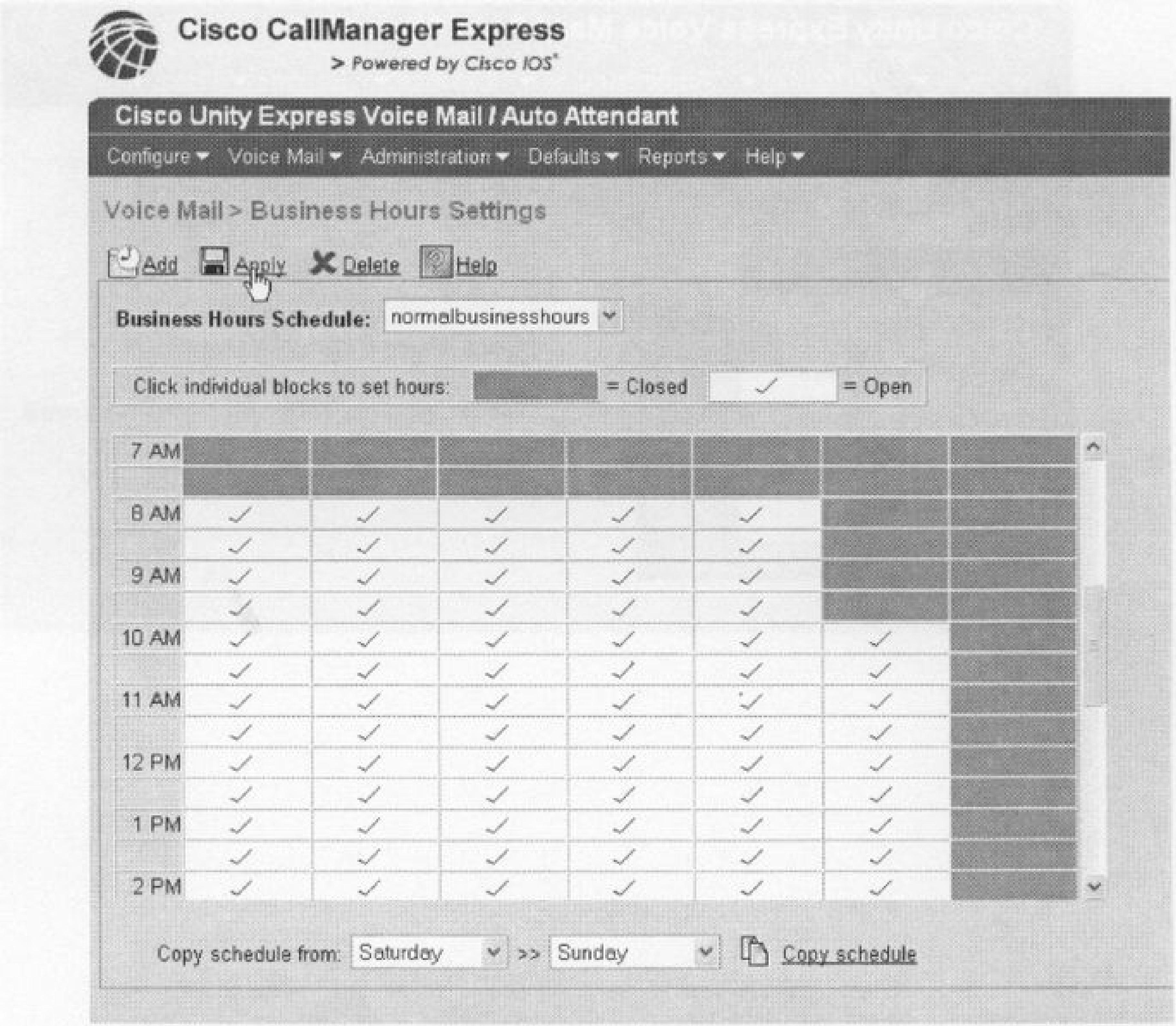
Create a schedule in CUE that defines normal business hours as Mon-Fri 8am-5pm and Saturday 10am-2pm.

➔ **From Internet Explorer browse to http://10.1.202.2/Web.**





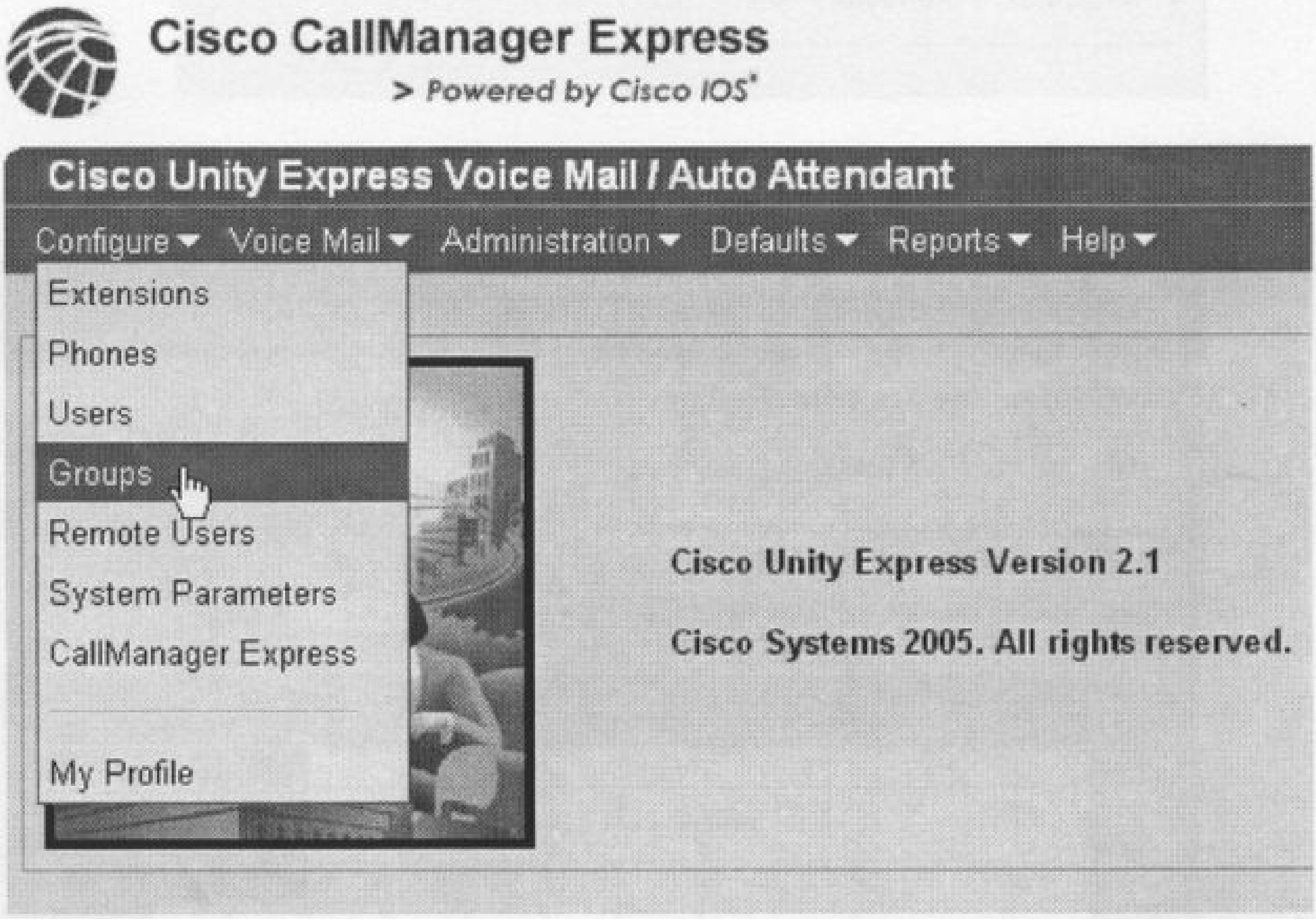

Add a New Schedule
Add
Cancel
Help
Name *: NormalBusinessHours
New Schedule
Based on existing schedule: systemschedule
* indicates a mandatory field

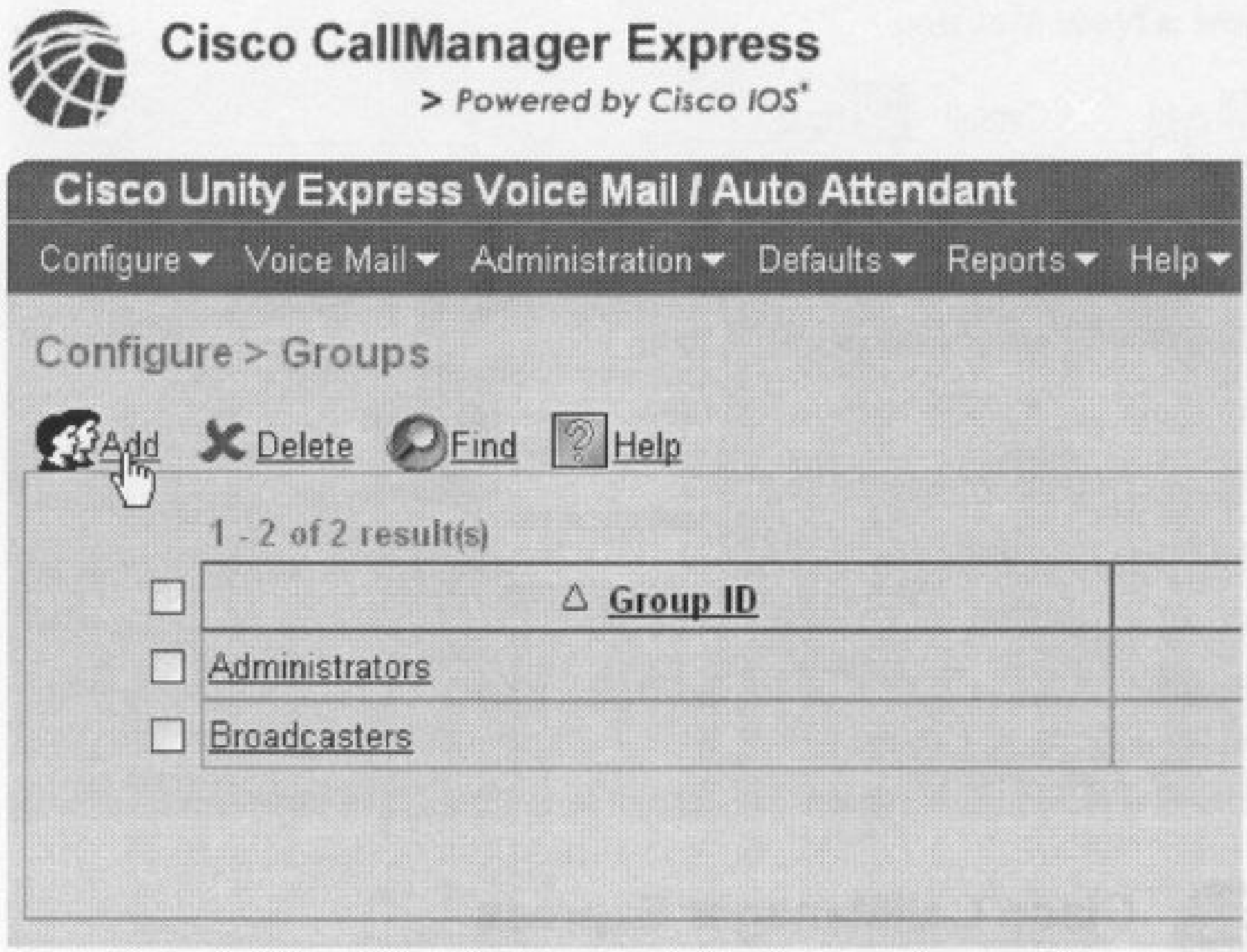

Cisco CallManager Express
> Powered by Cisco IOS
Cisco Unity Express Voice Mail / Auto Attendant
Configure
Voice Mail
Administration
Defaults
Reports
Help
Voice Mail > Business Hours Settings
Add
Apply
Delete
Help
Business Hours Schedule: normalbusinesshours
Click individual blocks to set hours:
= Closed
= Open
7 AM
8 AM
9 AM
10 AM
11 AM
12 PM
1 PM
2 PM
Copy schedule from: Saturday >> Sunday
Copy schedule

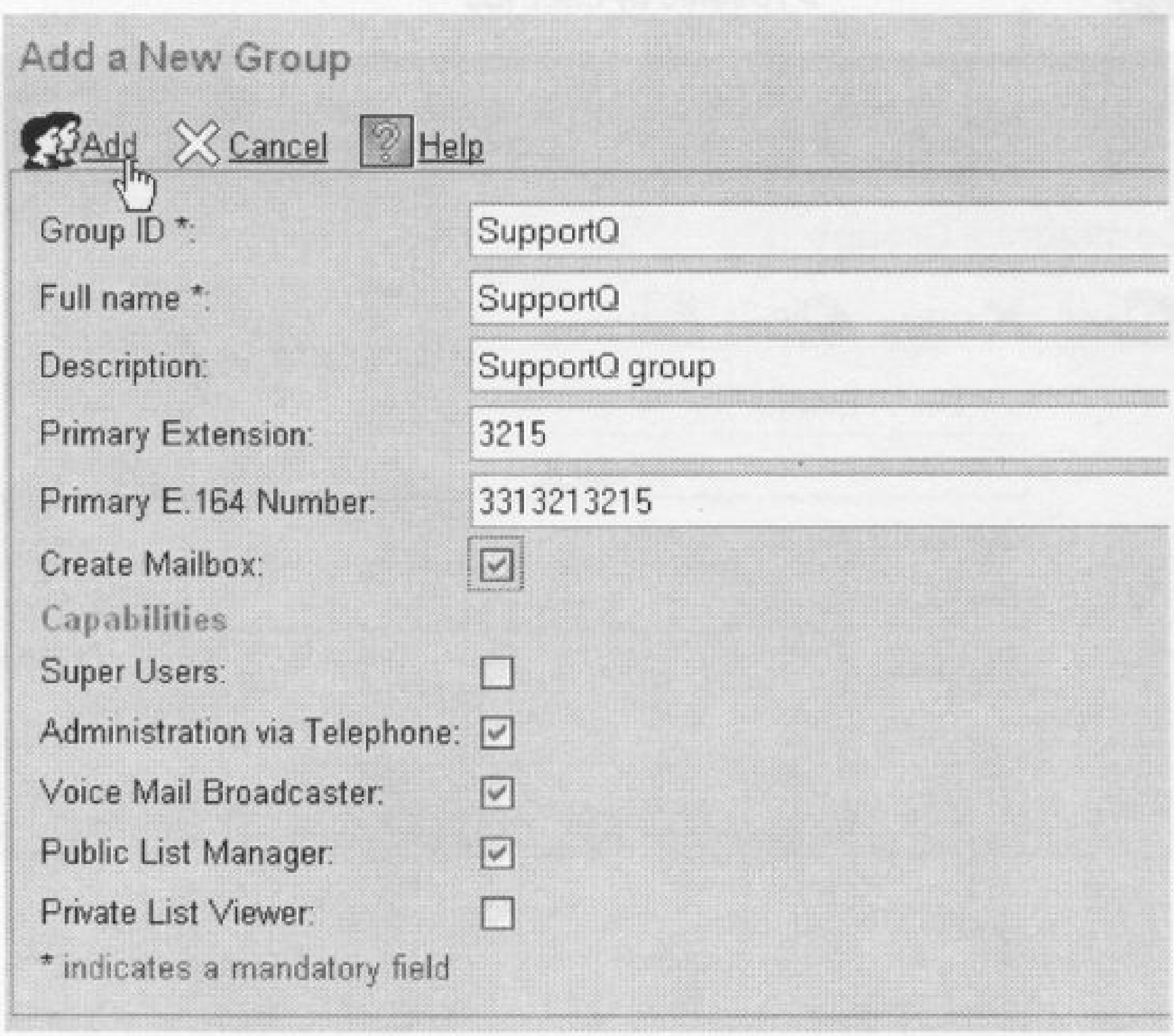
Task 16.2

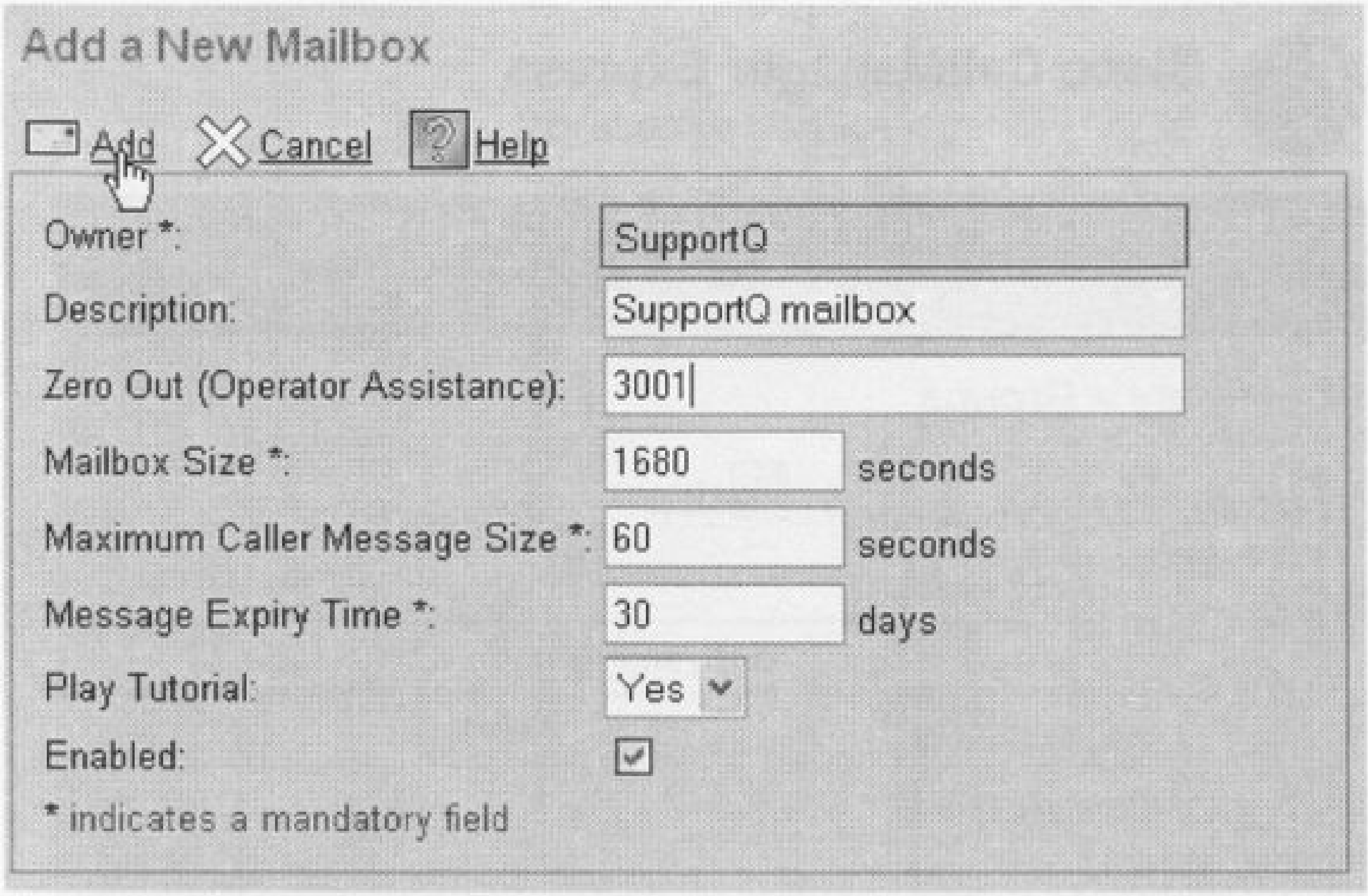
Create a General Delivery Mailbox for the Support Queue but give it the extension of 3215. Ensure that any phone in the office can access this mailbox by pressing "9" after they sign into their VM box. Finally, modify the Support Queue (not the hunt group) so that if agents are un-available they will go to this GDM. Also ensure that all BR2 phones see if there is a message waiting in the GDM.

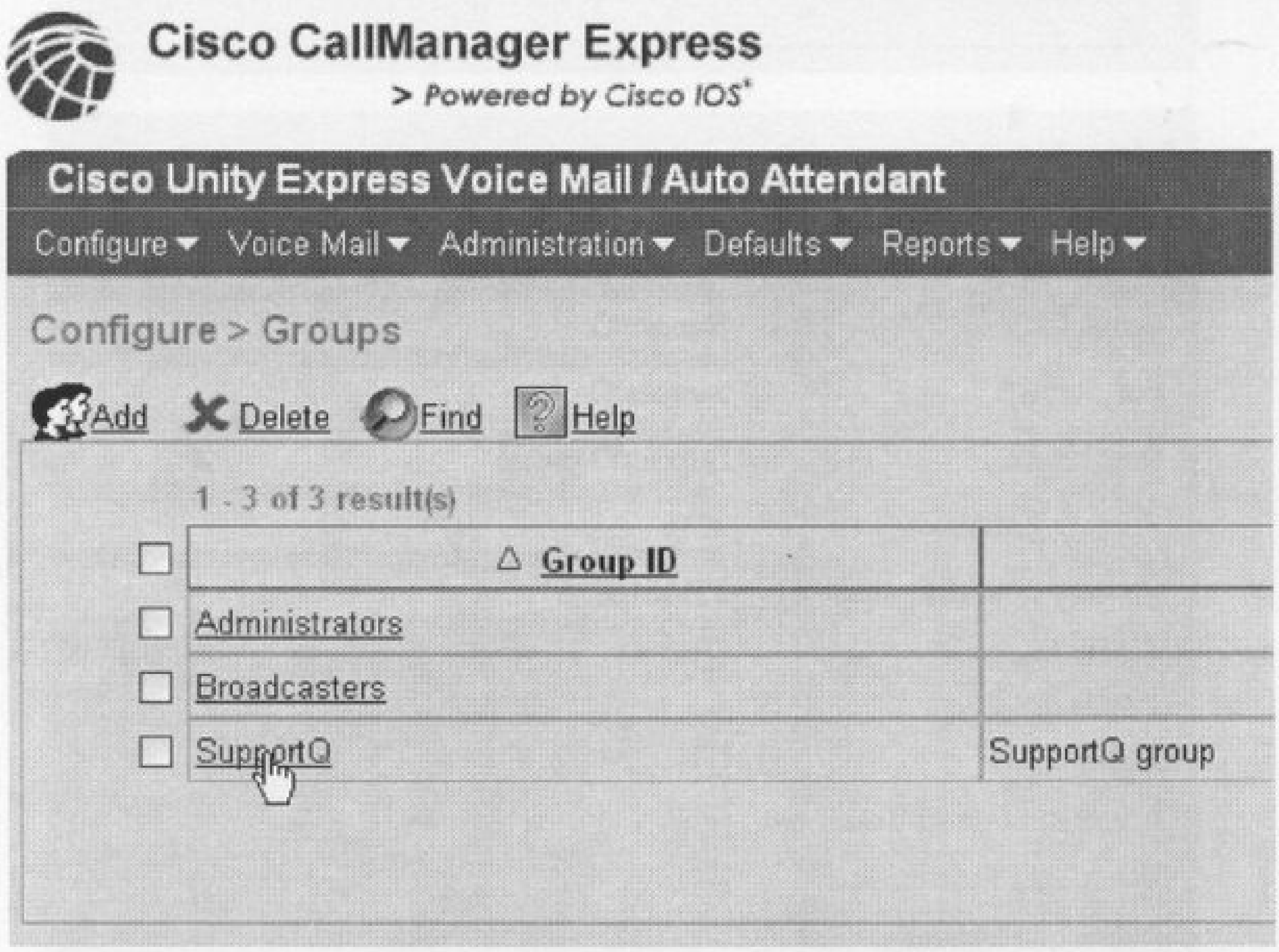
➔ **From Internet Explorer browse to http://10.1.202.2/Web.**

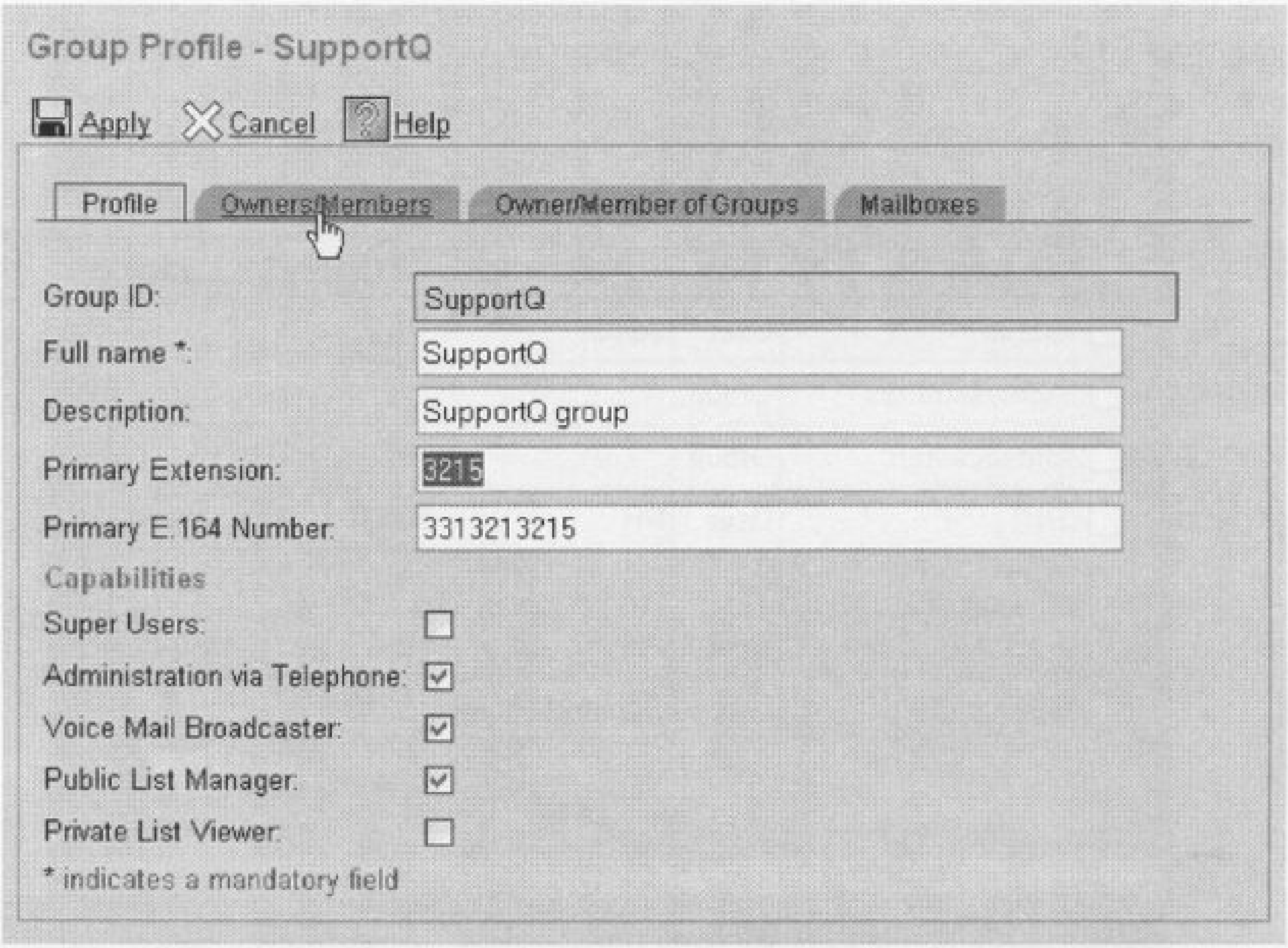


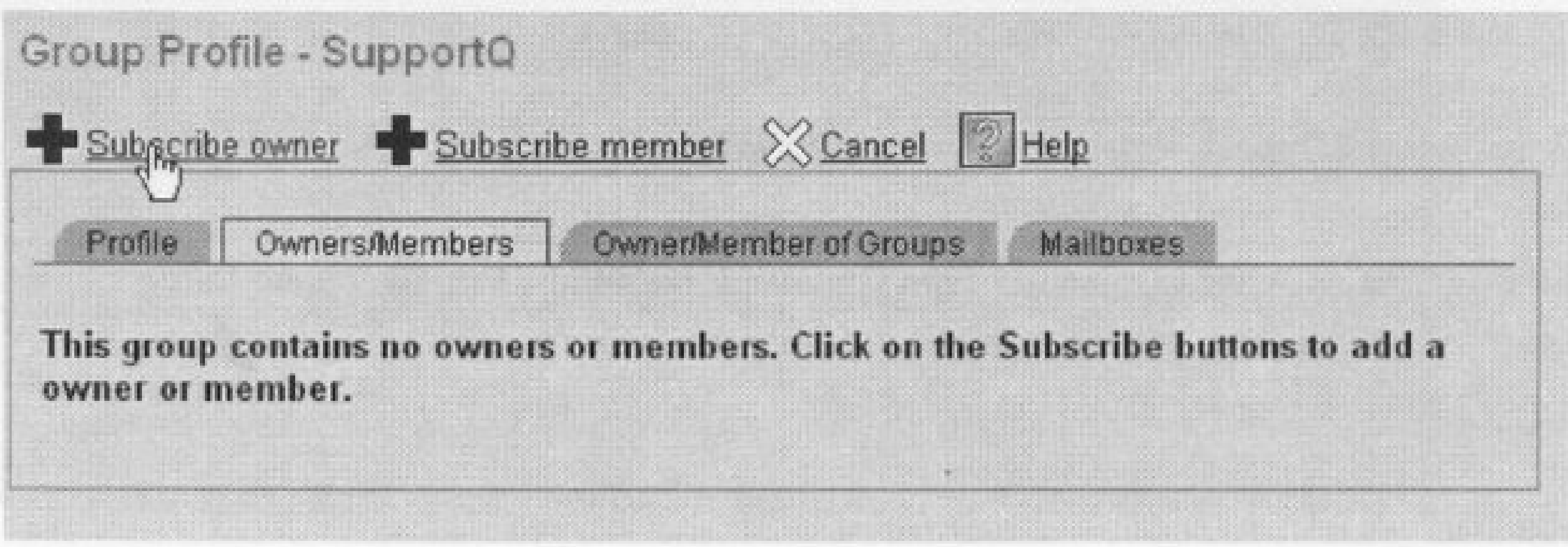

Cisco CallManager Express
> Powered by Cisco IOS
Cisco Unity Express Voice Mail / Auto Attendant
Configure Voice Mail Administration Defaults Reports Help
Configure > Groups
Add Delete Find Help
1 - 2 of 2 result(s)
Group ID
Administrators
Broadcasters

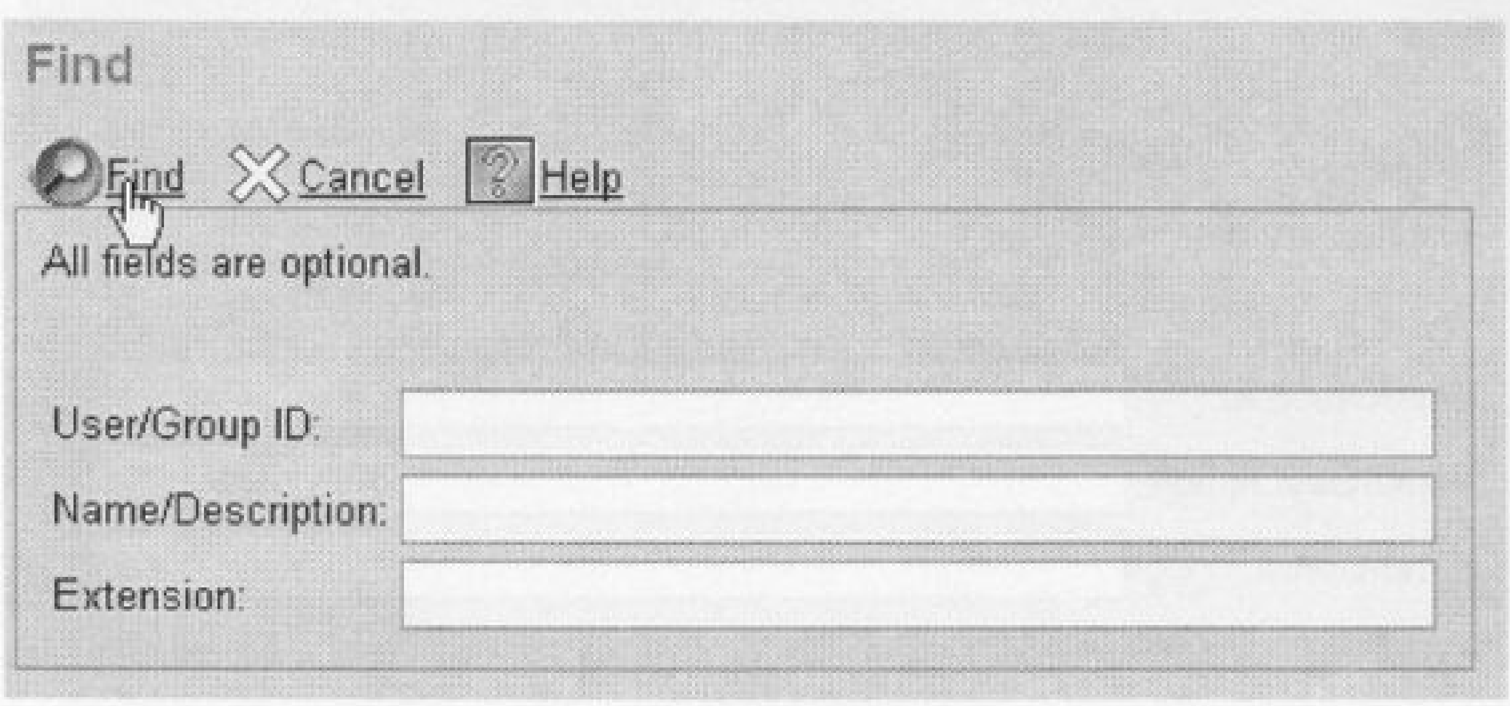

Add a New Group
Add Cancel Help
Group ID *: SupportQ
Full name *: SupportQ
Description: SupportQ group
Primary Extension: 3215
Primary E.164 Number: 3313213215
Create Mailbox:
Capabilities
Super Users:
Administration via Telephone:
Voice Mail Broadcaster:
Public List Manager:
Private List Viewer:
* indicates a mandatory field

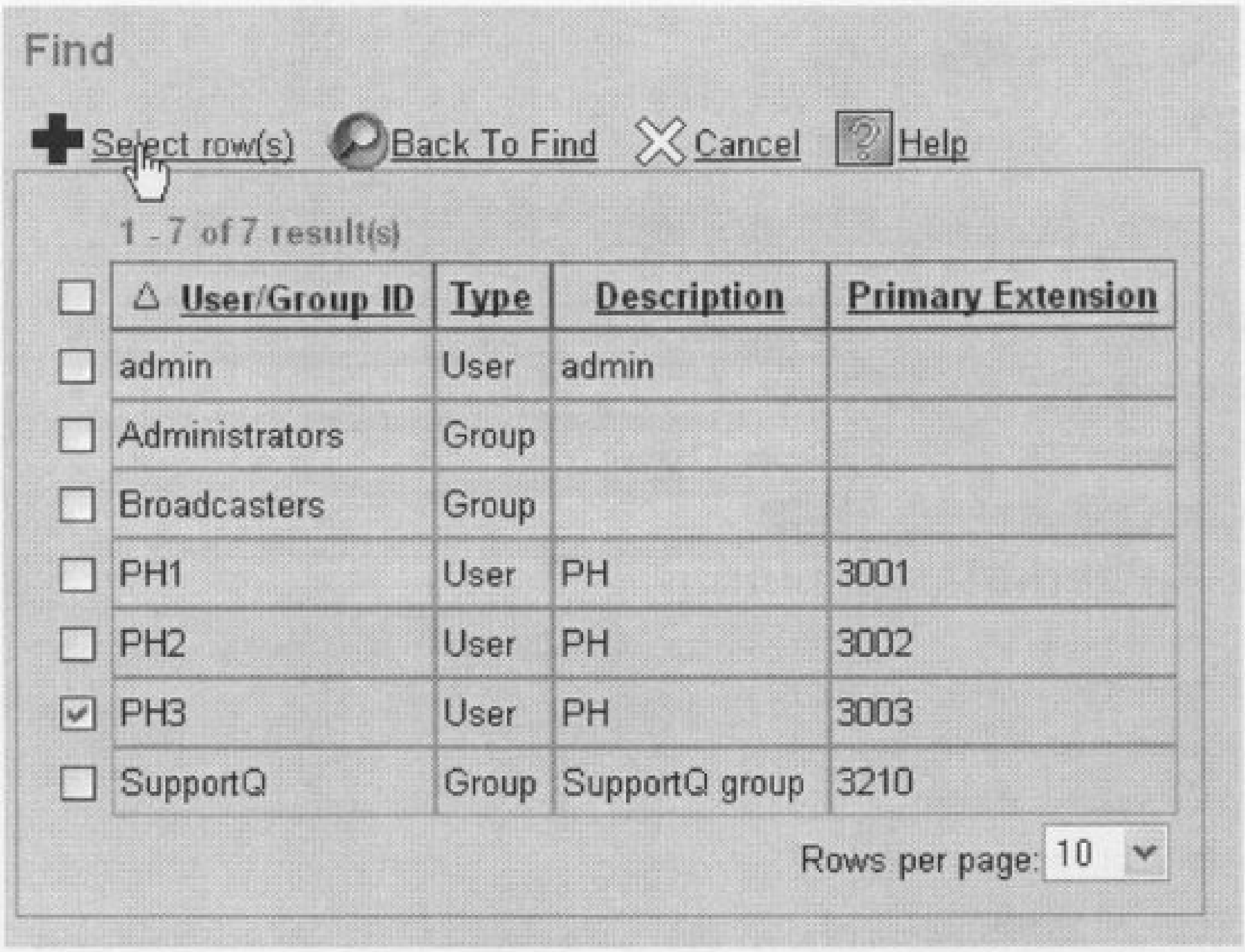

Add a New Mailbox
Add
Cancel
Help
Owner *:
SupportQ
Description:
SupportQ mailbox
Zero Out (Operator Assistance):
3001
Mailbox Size *:
1680
seconds
Maximum Caller Message Size *:
60
seconds
Message Expiry Time *:
30
days
Play Tutorial:
Yes
Enabled:
* indicates a mandatory field

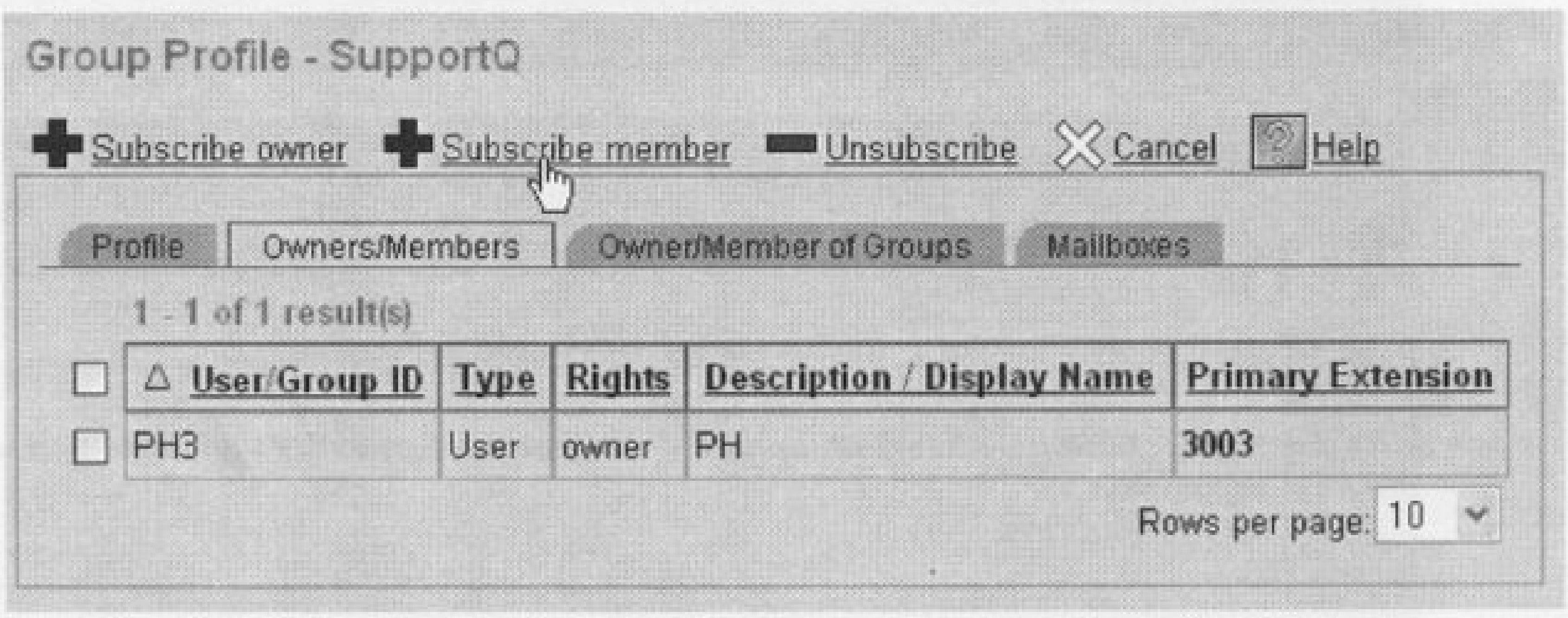

Cisco CallManager Express
> Powered by Cisco IOS
Cisco Unity Express Voice Mail / Auto Attendant
Configure
Voice Mail
Administration
Defaults
Reports
Help
Configure > Groups
Add
Delete
Find
Help
1 - 3 of 3 result(s)
Group ID
Administrators
Broadcasters
SupportQ
SupportQ group

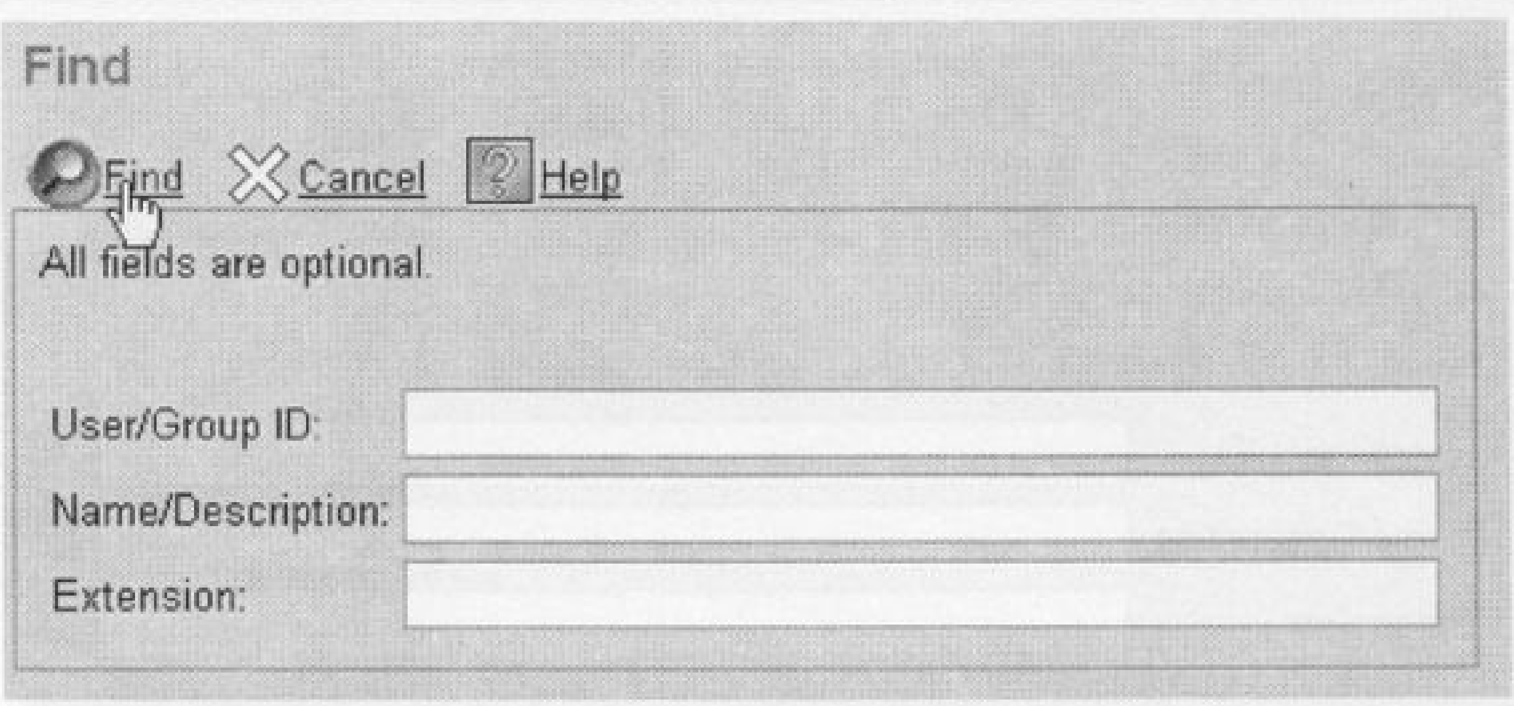

Group Profile - SupportQ
Apply
Cancel
Help
Profile
Owners/Members
Owner/Member of Groups
Mailboxes
Group ID:
SupportQ
Full name *:
SupportQ
Description:
SupportQ group
Primary Extension:
3215
Primary E.164 Number:
3313213215
Capabilities
Super Users:
Administration via Telephone:
Voice Mail Broadcaster:
Public List Manager:
Private List Viewer:
* indicates a mandatory field

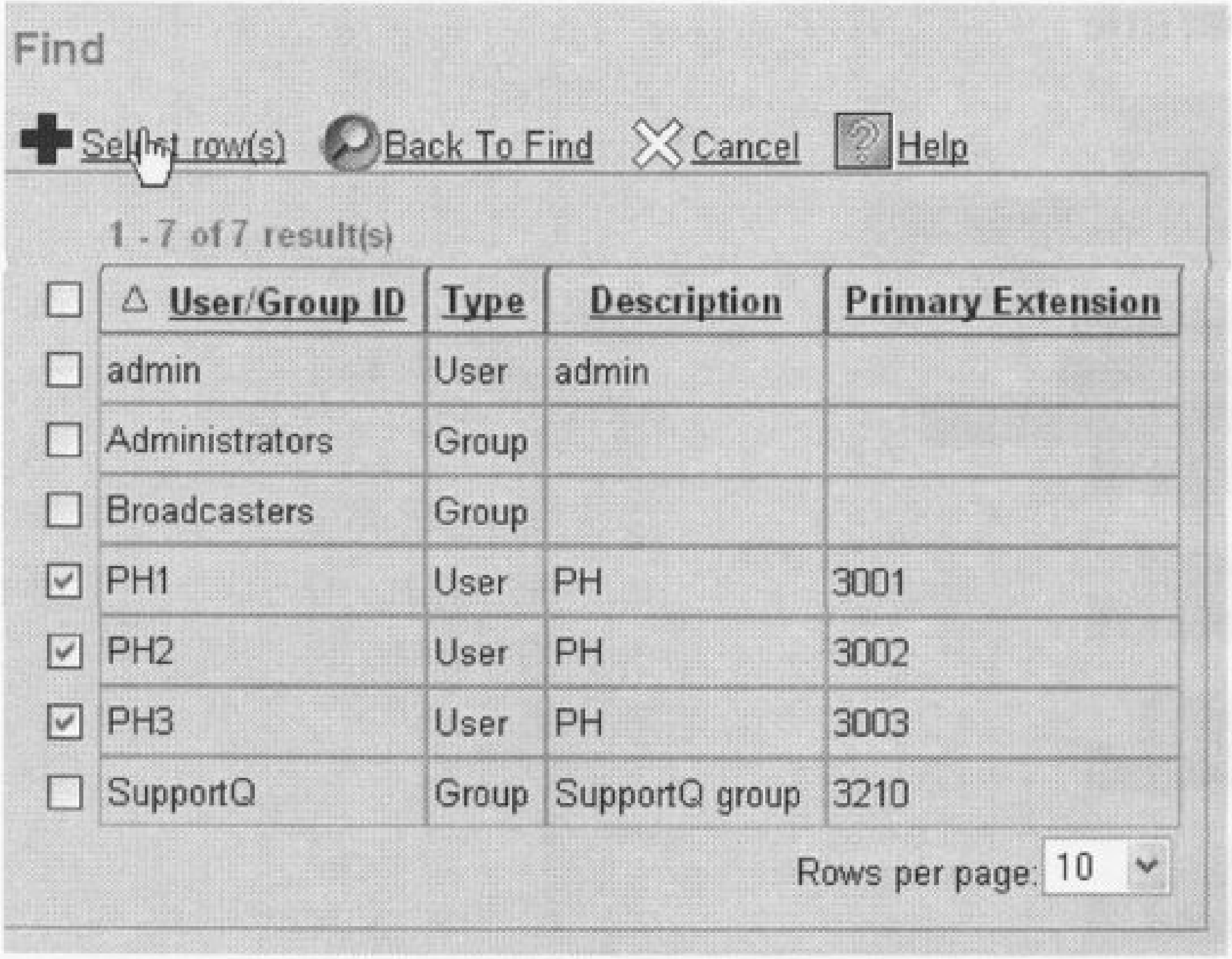

Group Profile - SupportQ
Subscribe owner
Subscribe member
Cancel
Help
Profile
Owners/Members
Owner/Member of Groups
Mailboxes
This group contains no owners or members. Click on the Subscribe buttons to add a owner or member.


Find
Find
Cancel
Help
All fields are optional.
User/Group ID:
Name/Description:
Extension:

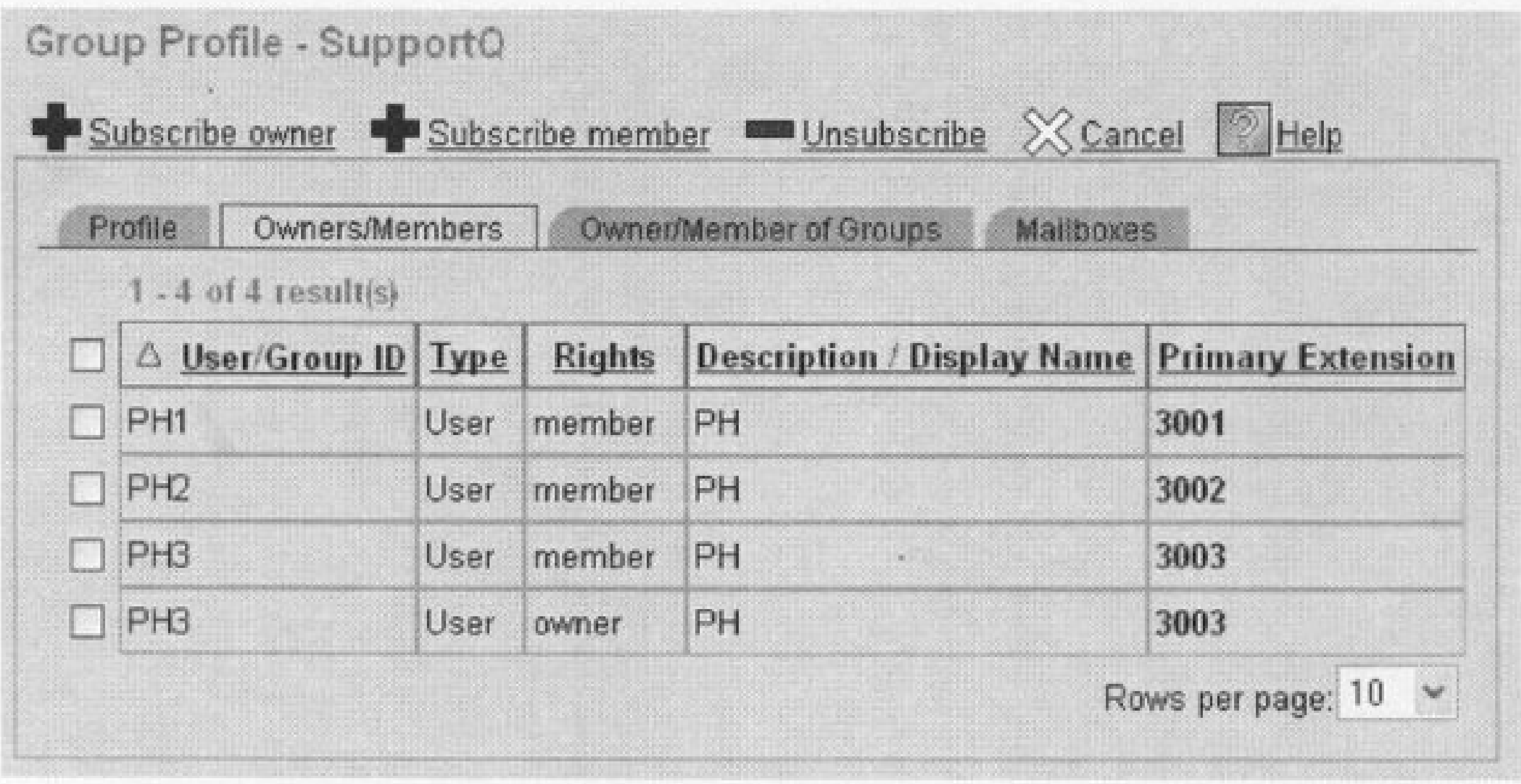

Find
Select row(s)
Back To Find
Cancel
Help
1 - 7 of 7 result(s)
User/Group ID
Type
Description
Primary Extension
admin
User
admin
Administrators
Group
Broadcasters
Group
PH1
User
PH
3001
PH2
User
PH
3002
PH3
User
PH
3003
SupportQ
Group
SupportQ group
3210
Rows per page: 10


Group Profile - SupportQ
Subscribe owner
Subscribe member
Unsubscribe
Cancel
Help
Profile
Owners/Members
Owner/Member of Groups
Mailboxes
1 - 1 of 1 result(s)
User/Group ID
Type
Rights
Description / Display Name
Primary Extension
PH3
User
owner
PH
3003
Rows per page: 10


Find
Find
Cancel
Help
All fields are optional.
User/Group ID:
Name/Description:
Extension:



	User/Group ID	Type	Description	Primary Extension
☐	admin	User	admin	
☐	Administrators	Group		
☐	Broadcasters	Group		
☑	PH1	User	PH	3001
☑	PH2	User	PH	3002
☑	PH3	User	PH	3003
☐	SupportQ	Group	SupportQ group	3210



	User/Group ID	Type	Rights	Description / Display Name	Primary Extension
☐	PH1	User	member	PH	3001
☐	PH2	User	member	PH	3002
☐	PH3	User	member	PH	3003
☐	PH3	User	owner	PH	3003

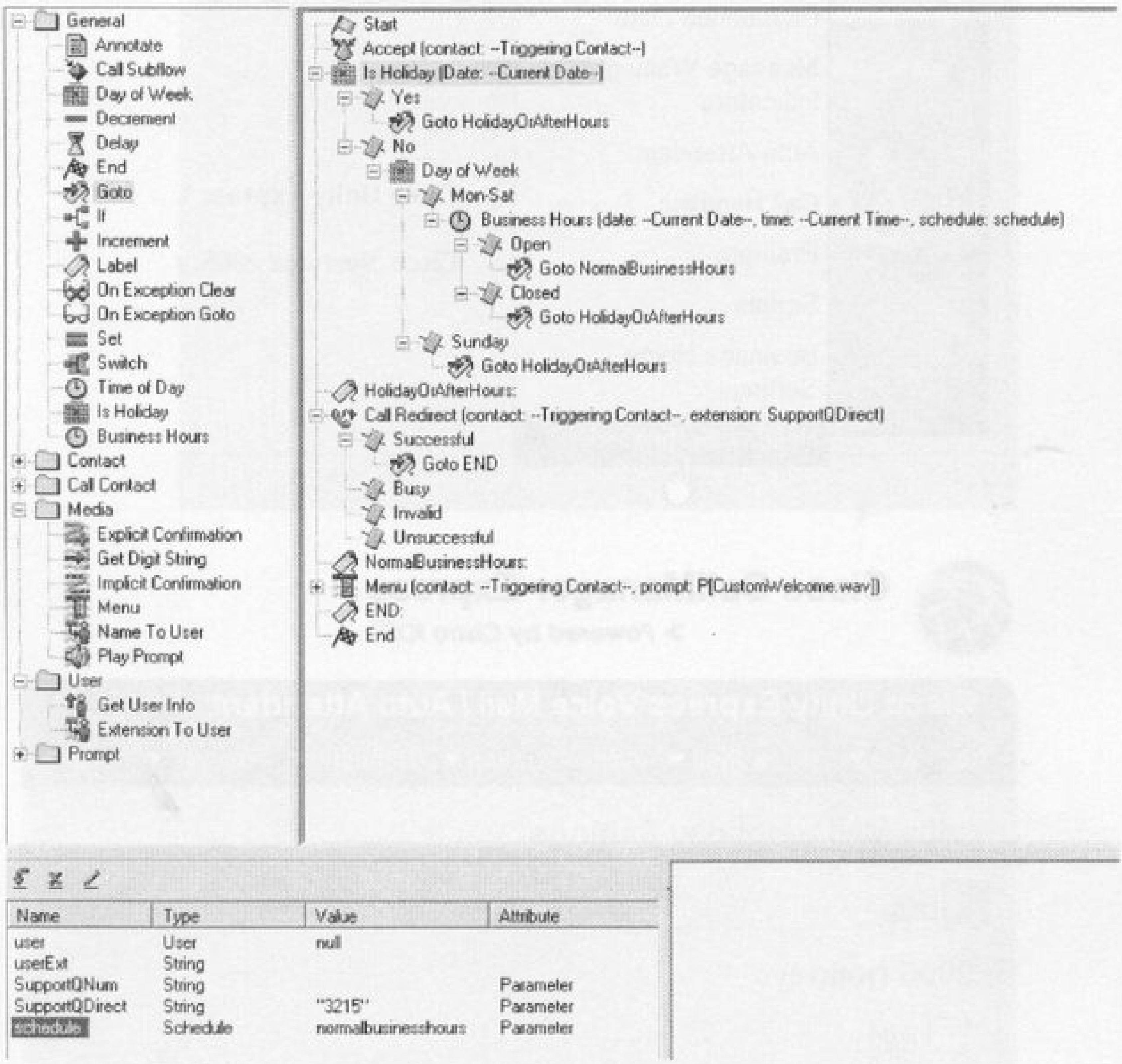
➔ **On BR2 RTR:**

```
application
 service aa
  param voice-mail 3215
!
ephone-dn 20
 number 3215
 call-forward all 3060
 label GDM
!
ephone  1
 button 4:20
!
ephone  2
 button 4:20
!
ephone  3
 button 4:20
```

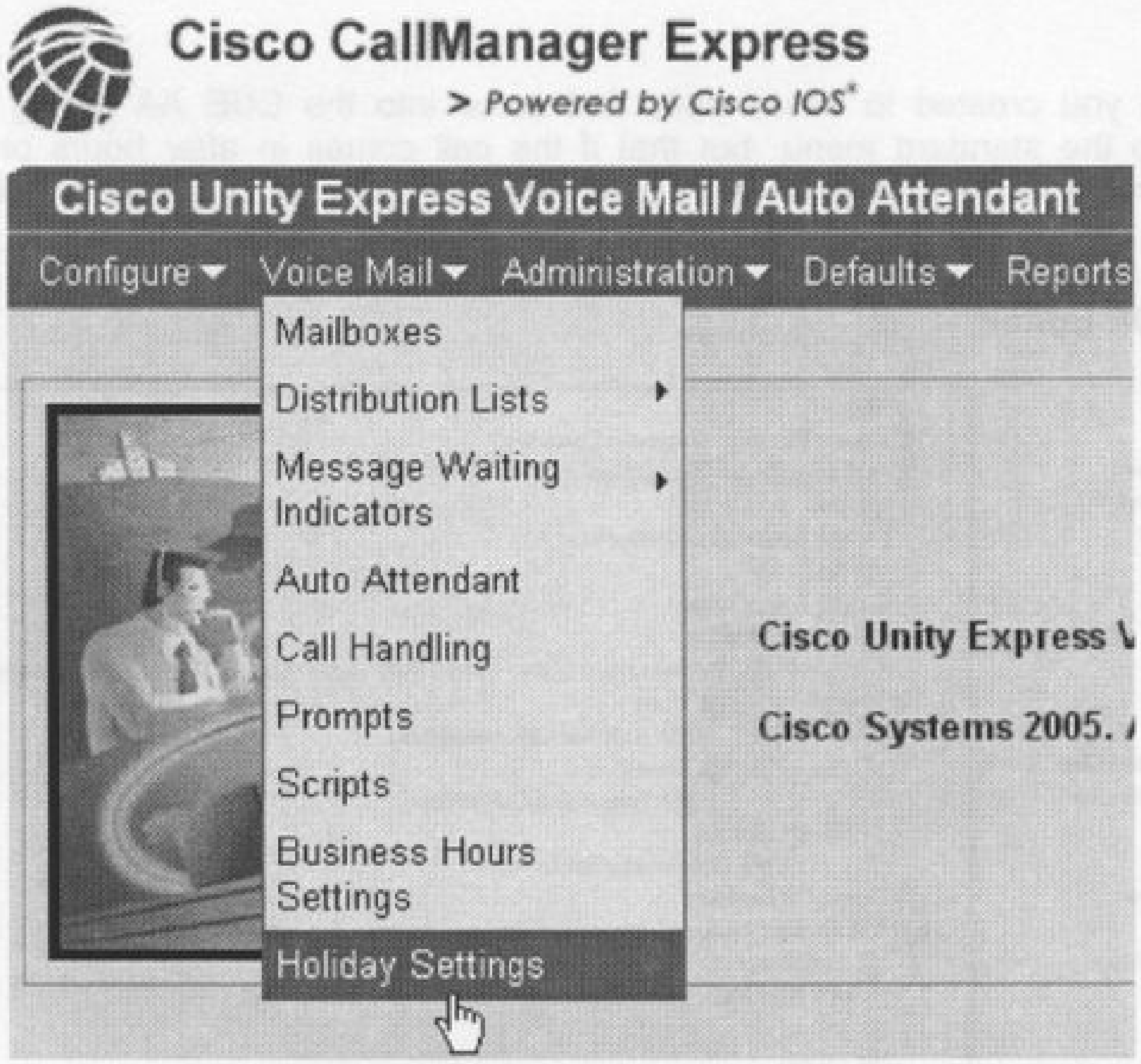
Task 16.3

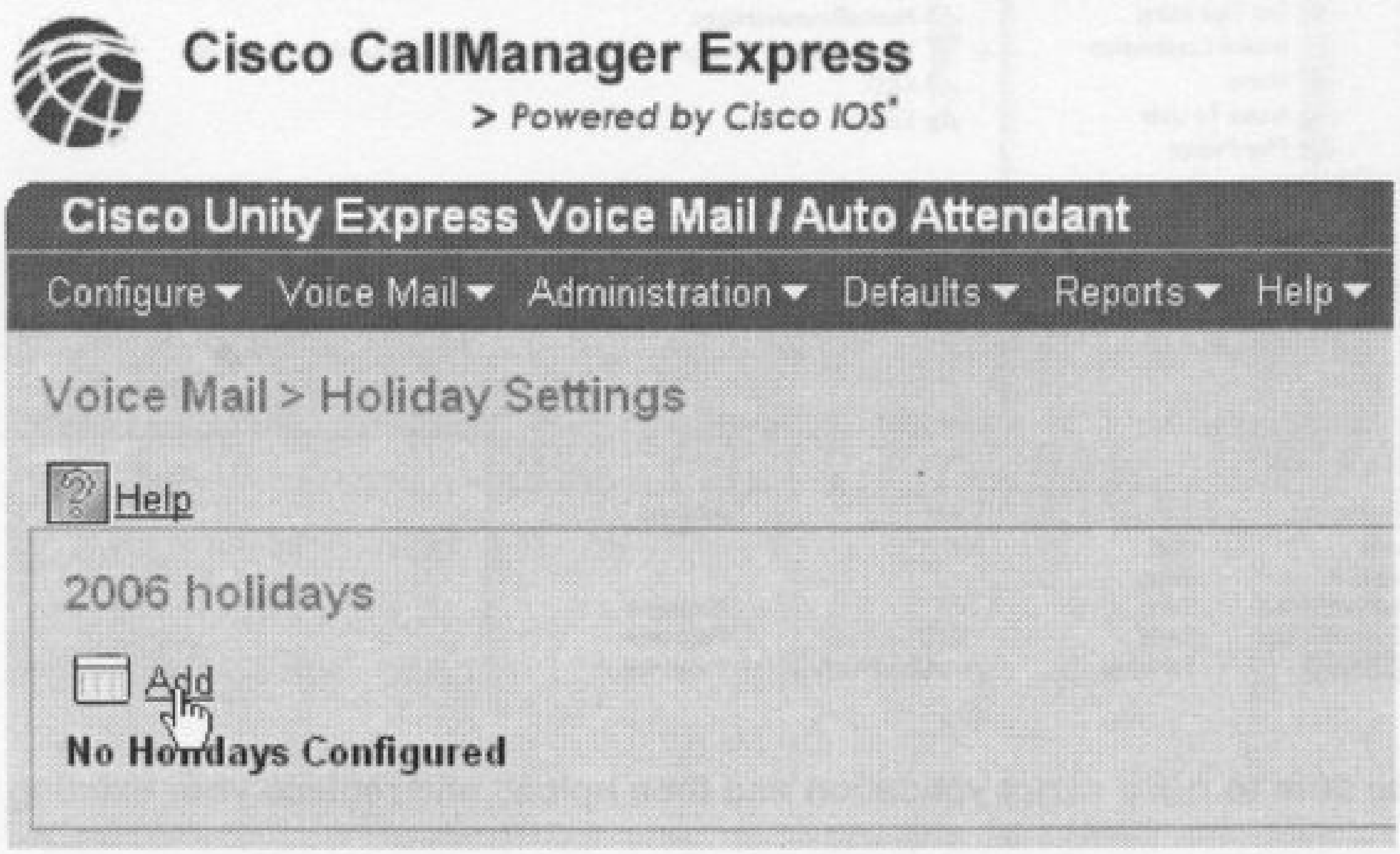
Modify the AA script you created to cause calls that come into the CUE AA during normal business hours go to the standard menu, but that if the call comes in after hours or during holidays, to send it directly to the general delivery mailbox for the Support Q. Create a holiday for Dec 25.

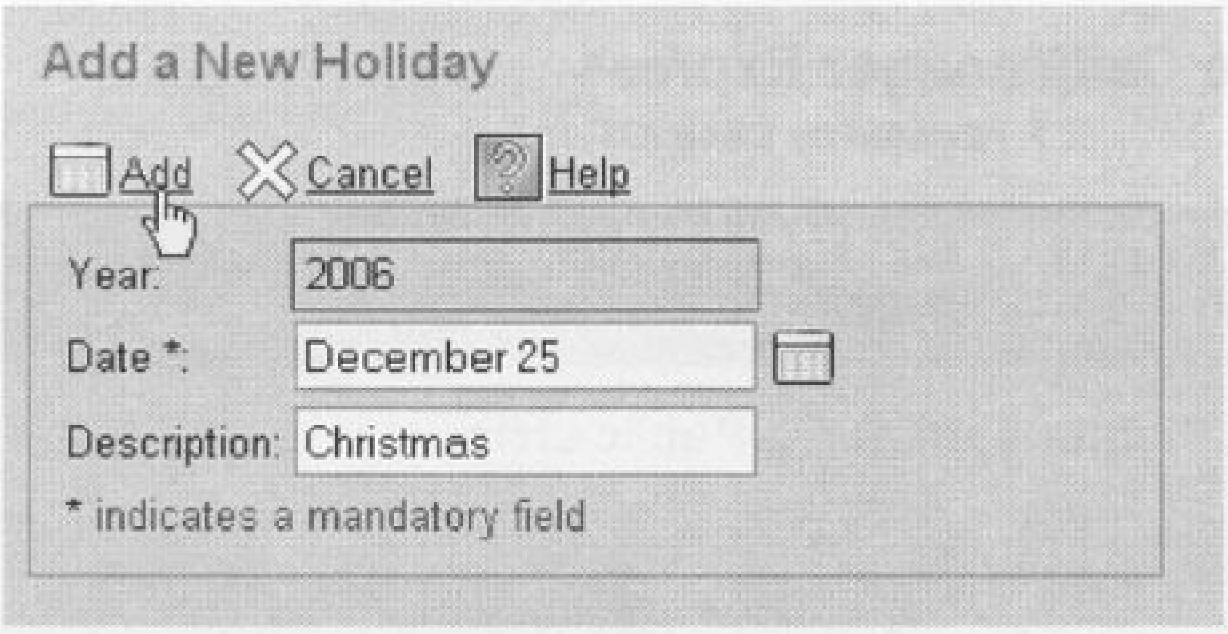
➔ **Using the CUE Editor:**



➔ **Be sure to run a script validation and then upload and replace your existing script.**


Cisco CallManager Express
> Powered by Cisco IOS
Cisco Unity Express Voice Mail / Auto Attendant
Configure Voice Mail Administration Defaults Reports
Mailboxes
Distribution Lists
Message Waiting Indicators
Auto Attendant
Call Handling
Prompts
Scripts
Business Hours Settings
Holiday Settings
Cisco Unity Express V
Cisco Systems 2005.


Cisco CallManager Express
> Powered by Cisco IOS
Cisco Unity Express Voice Mail / Auto Attendant
Configure Voice Mail Administration Defaults Reports Help
Voice Mail > Holiday Settings
Help
2006 holidays
Add
No Holidays Configured

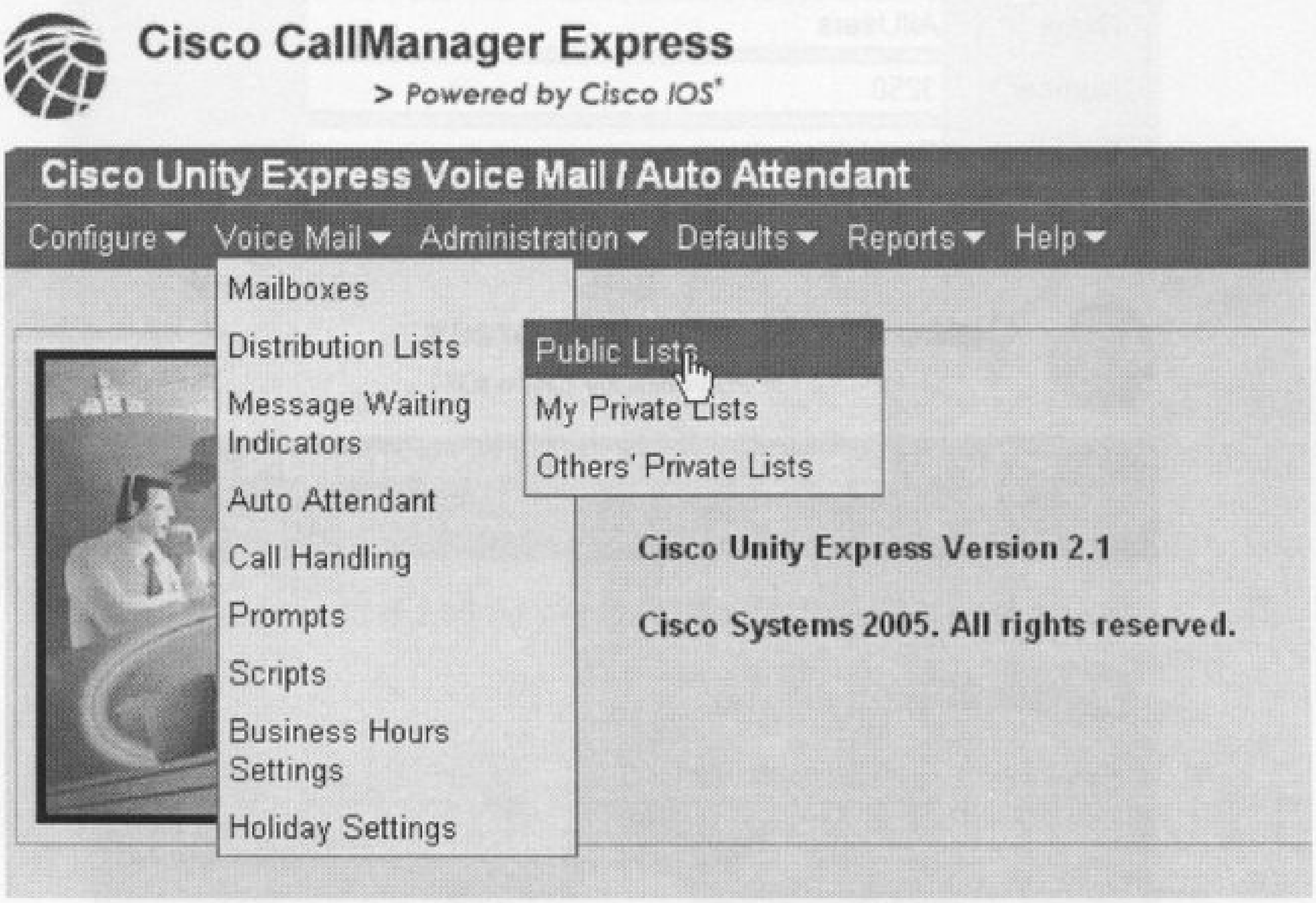


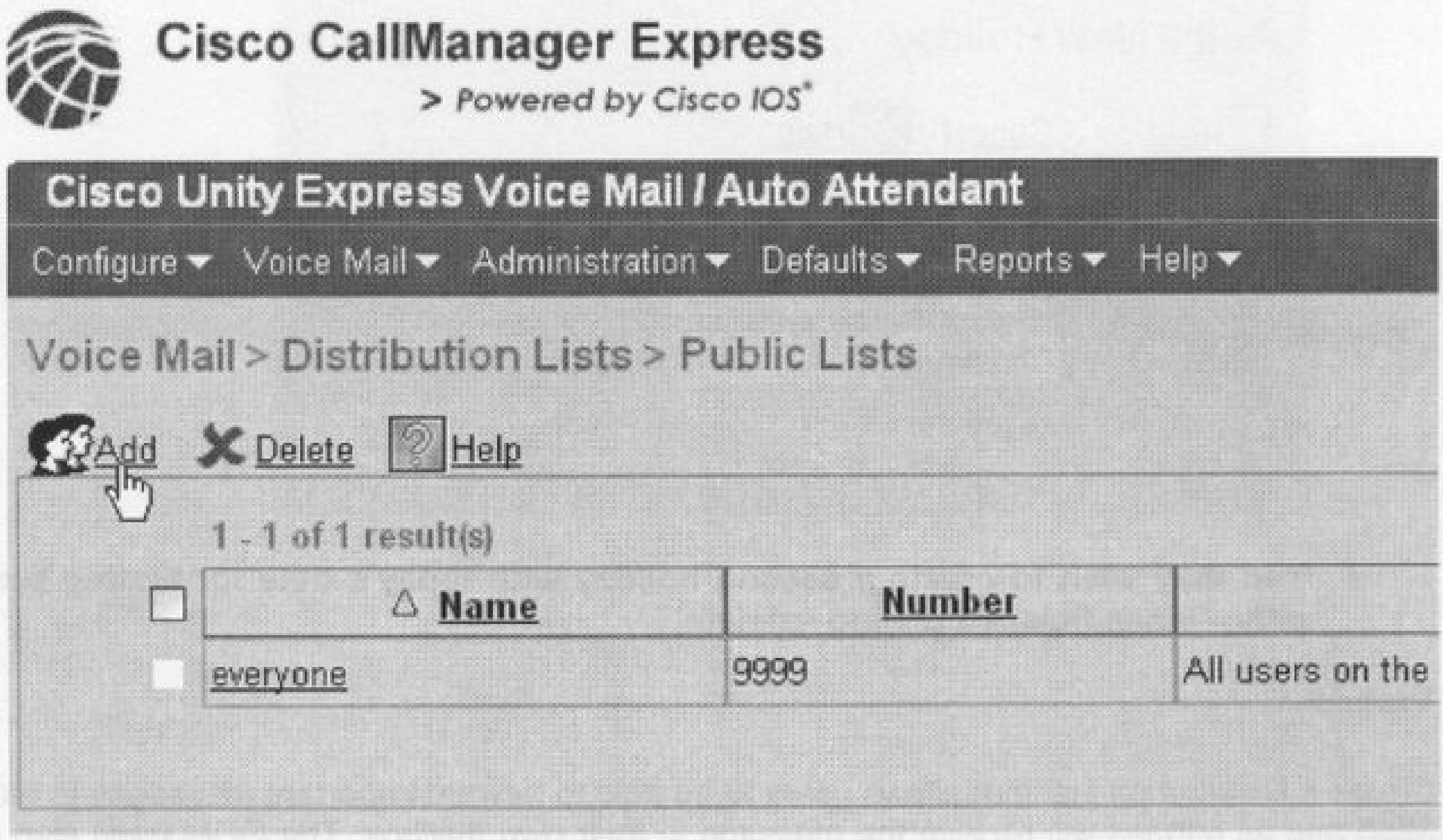
➔ **You may wish to create a second holiday with today's date for testing purposes only – when finished testing – delete.**

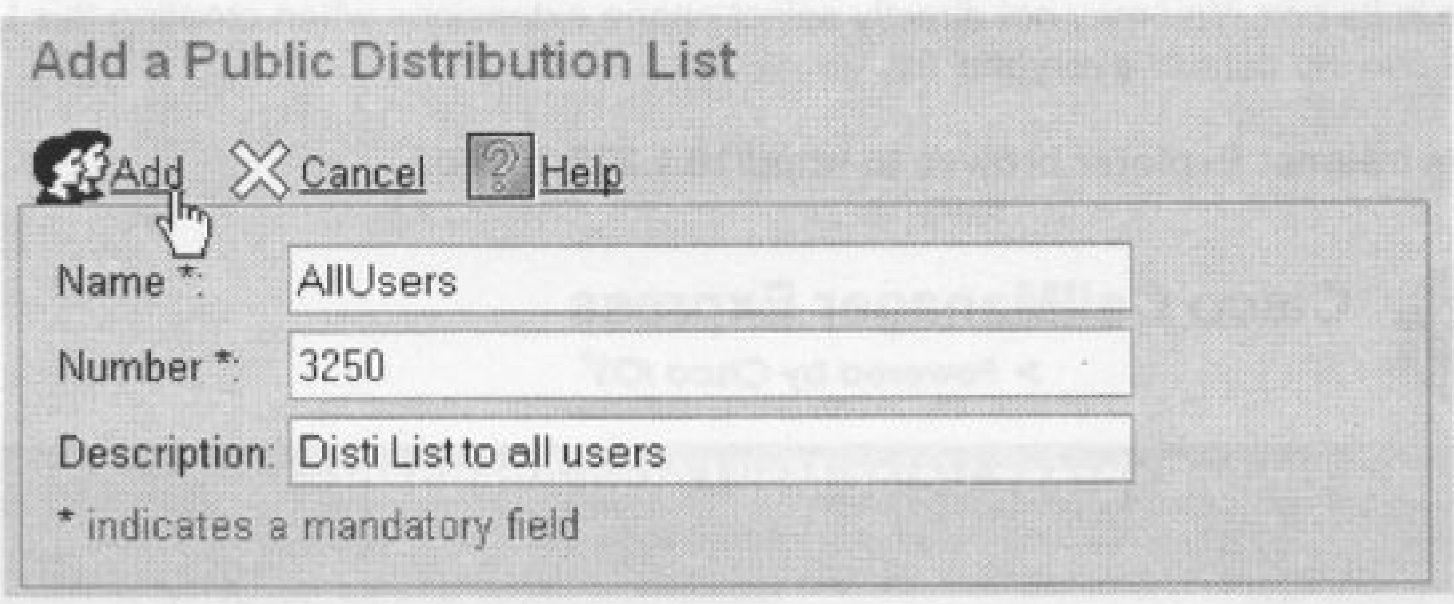
Task 16.4

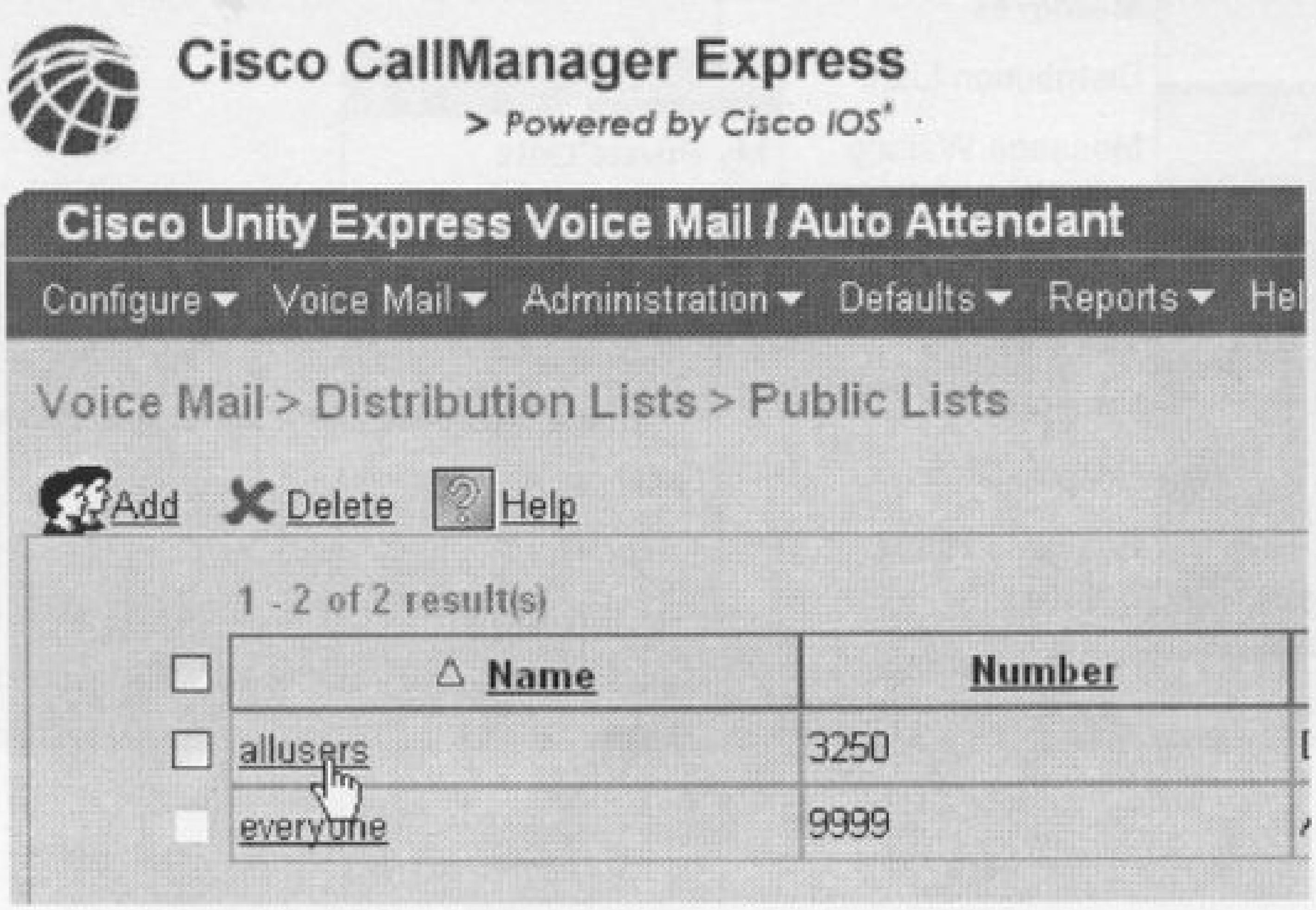
Create a Distribution List that allows users to be able to forward important messages to extension 3250 and all phones will receive the message in their own mailbox. The GDM must also receive the message in its box. You may not directly select phone extensions when creating this List. You also may not use the default 'everyone' list.

➔ **From Internet Explorer browse to http://10.1.202.2/Web.**

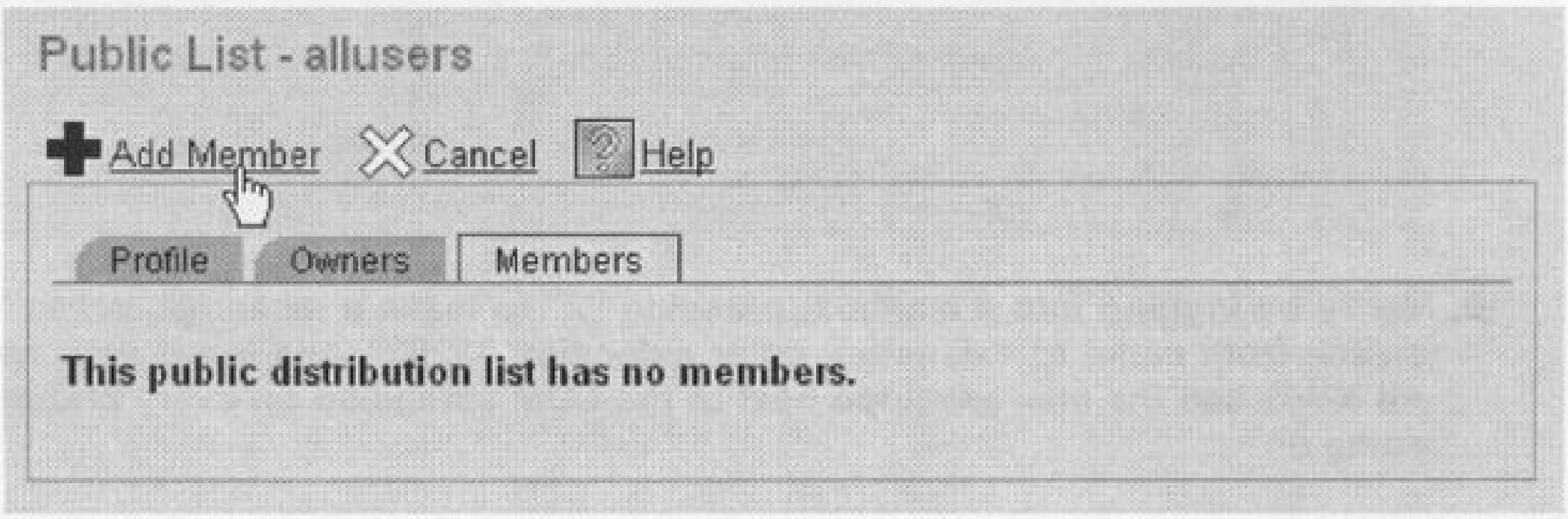


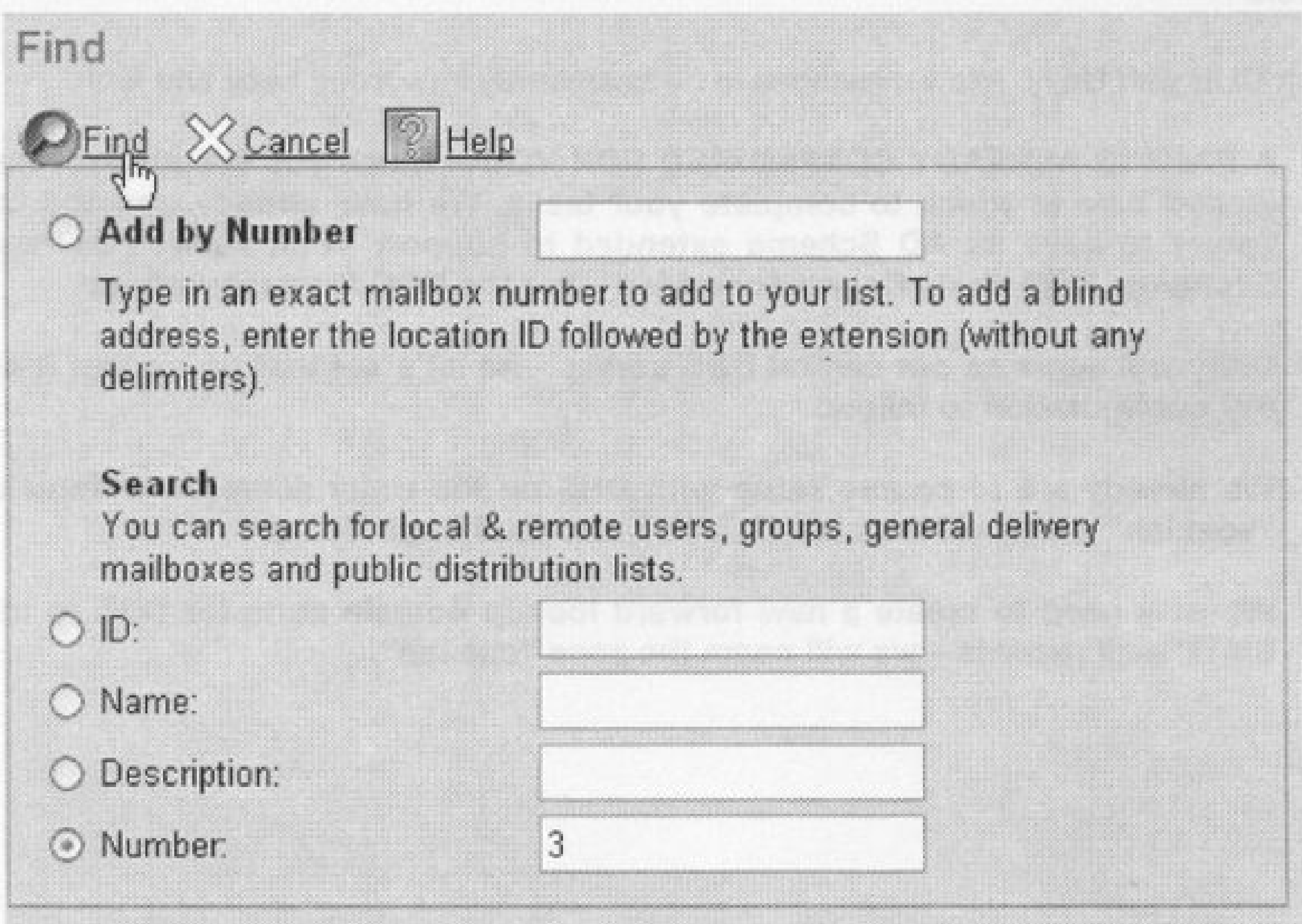

Cisco CallManager Express
> Powered by Cisco IOS
Cisco Unity Express Voice Mail / Auto Attendant
Configure Voice Mail Administration Defaults Reports Help
Voice Mail > Distribution Lists > Public Lists
Add Delete Help
1 - 1 of 1 result(s)
Name
Number
everyone
9999
All users on the

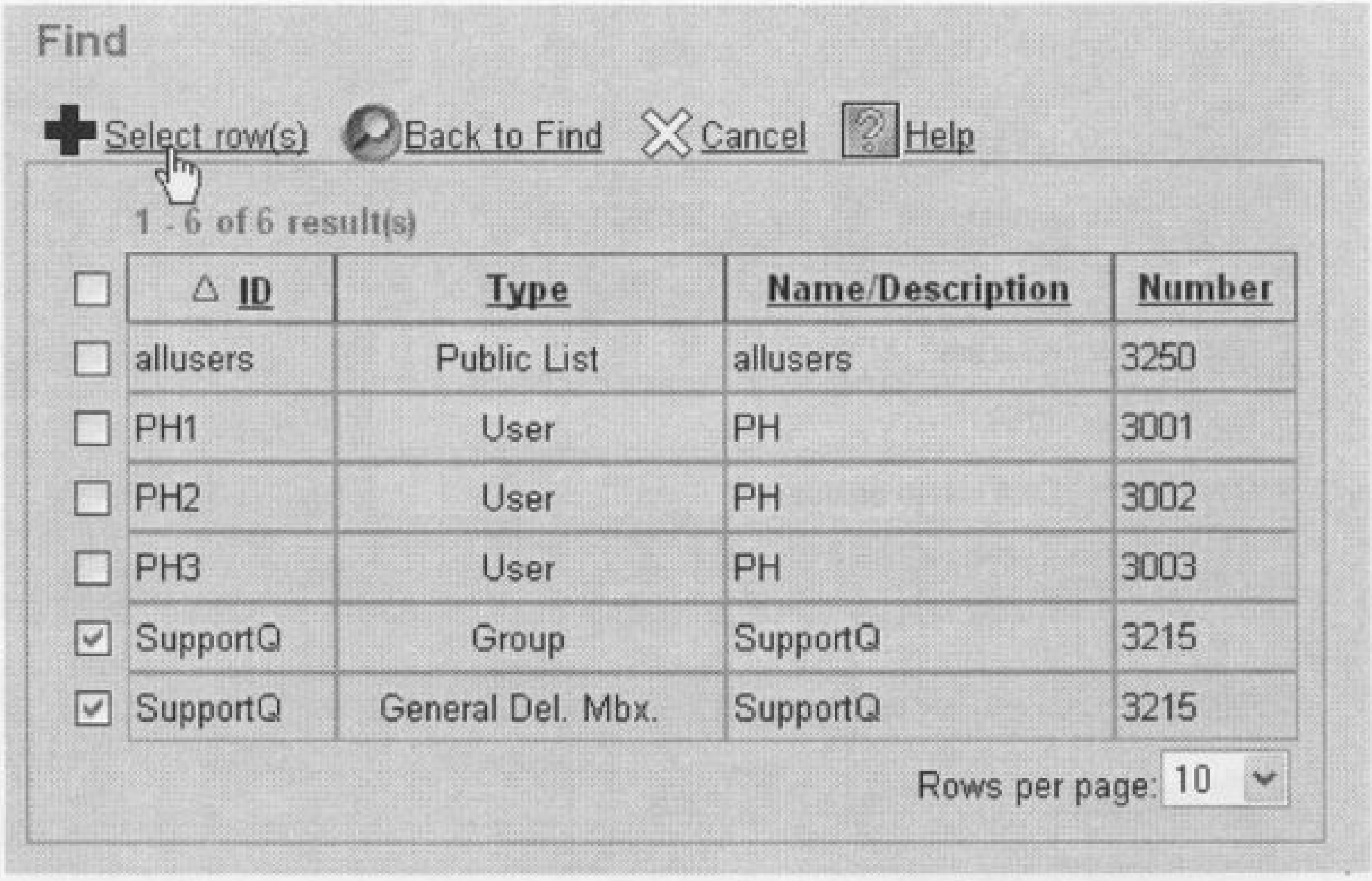

Add a Public Distribution List
Add Cancel Help
Name *: AllUsers
Number *: 3250
Description: Disti List to all users
* indicates a mandatory field


Cisco CallManager Express
> Powered by Cisco IOS
Cisco Unity Express Voice Mail / Auto Attendant
Configure Voice Mail Administration Defaults Reports Hel
Voice Mail > Distribution Lists > Public Lists
Add Delete Help
1 - 2 of 2 result(s)
Name
Number
allusers
3250
everyone
9999


Public List - allusers
Apply
Cancel
Help
Profile
Owners
Members
Name *:
allusers
Number *:
3250
Description:
Disti List to all users
* indicates a mandatory field


Public List - allusers
Add Member
Cancel
Help
Profile
Owners
Members
This public distribution list has no members.


Find
Find
Cancel
Help
Add by Number
Type in an exact mailbox number to add to your list. To add a blind address, enter the location ID followed by the extension (without any delimiters).
Search
You can search for local & remote users, groups, general delivery mailboxes and public distribution lists.
ID:
Name:
Description:
Number:
3



	ID	Type	Name/Description	Number
☐	allusers	Public List	allusers	3250
☐	PH1	User	PH	3001
☐	PH2	User	PH	3002
☐	PH3	User	PH	3003
☑	SupportQ	Group	SupportQ	3215
☑	SupportQ	General Del. Mbx.	SupportQ	3215

➔ **Verify by logging into a mailbox, pressing "2" to leave a message, press "# #" to switch from name to extension, enter extension "3250", and leave your message. All MWIs and the mail envelope next to the GDM extension on every phone should come on.**

Task 16.5

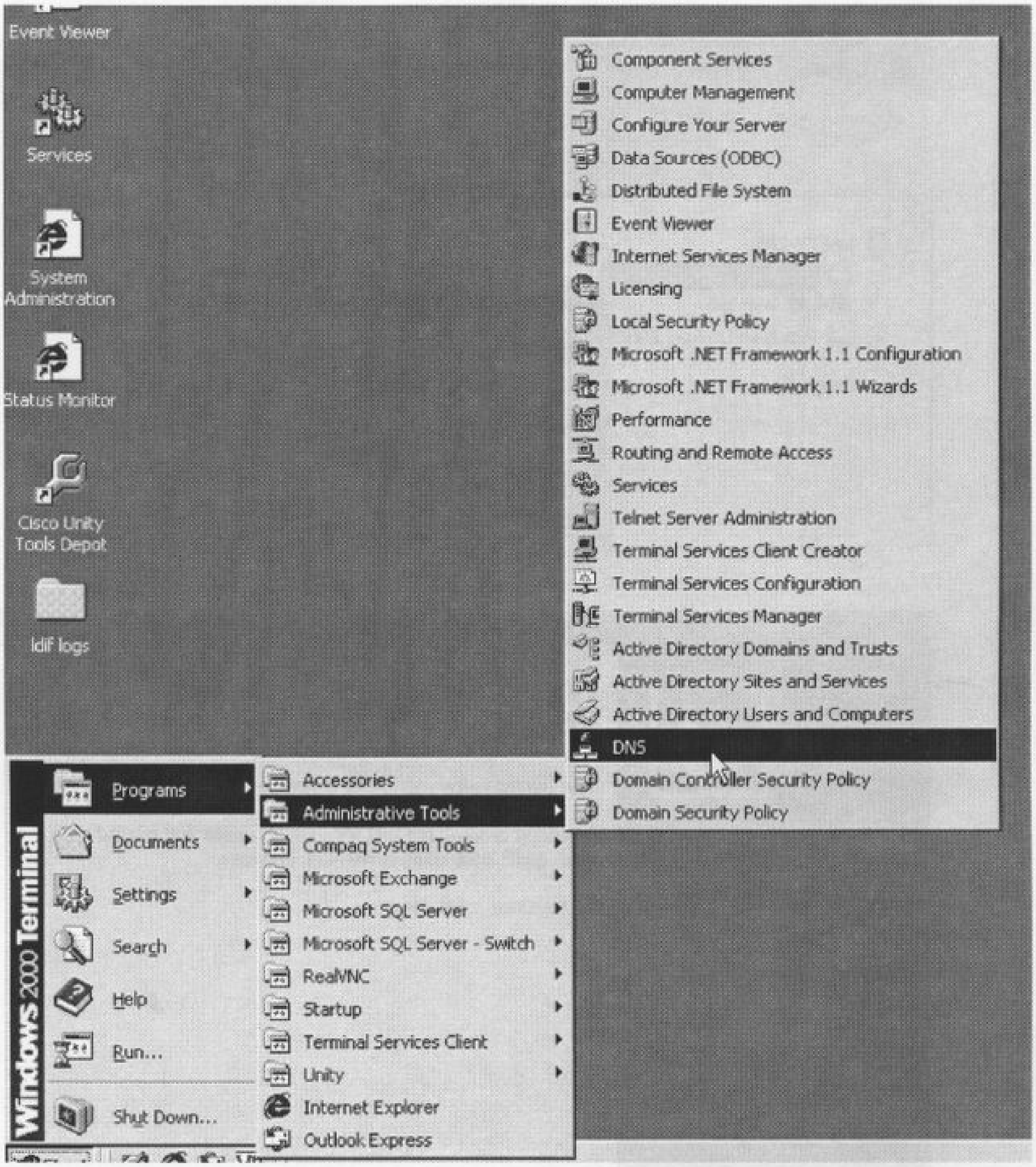
Network CUE with Unity. Allow messages to be seamlessly forwarded back and forth.

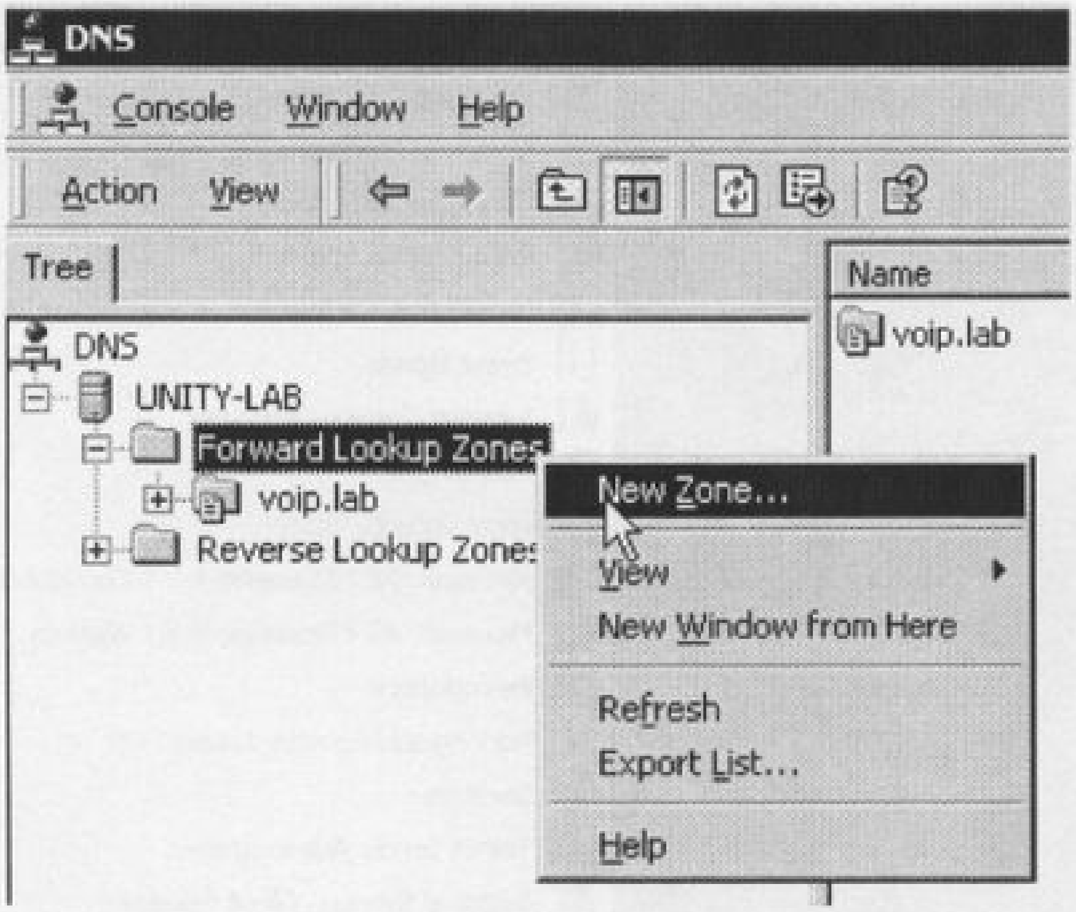
➔ **A PART IS ALREADY CONFIGURED FOR YOU – Since you the student have very limited time in which to complete your tasks, We have already updated the Unity server to have its AD Schema extended to support VPIM as well as having the Exchange 2000 Voice Connector added – per the CCO Documentation.**

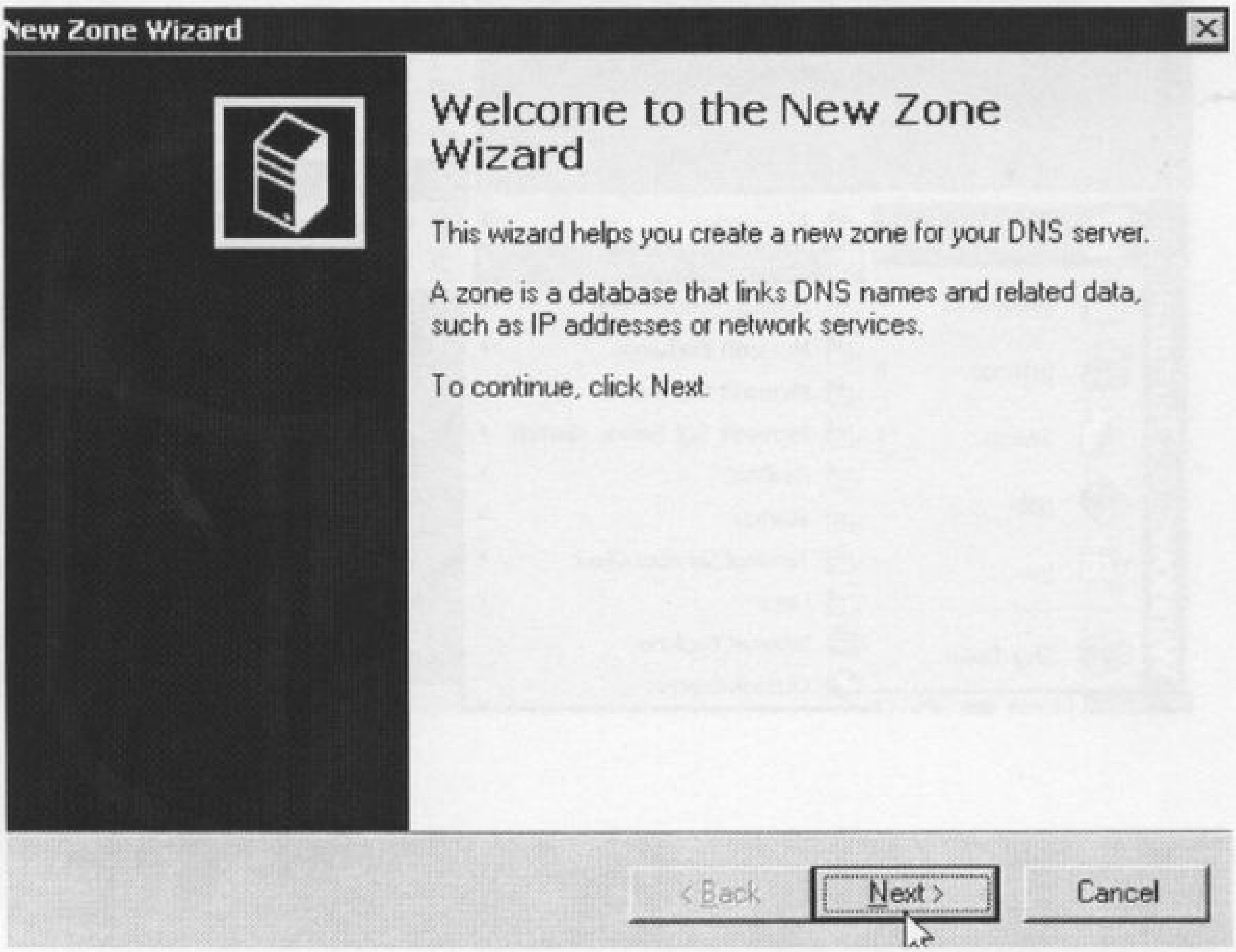
➔ **Unity will serve as our central DNS server – so let's set that up so that it supports our configuration to follow.**

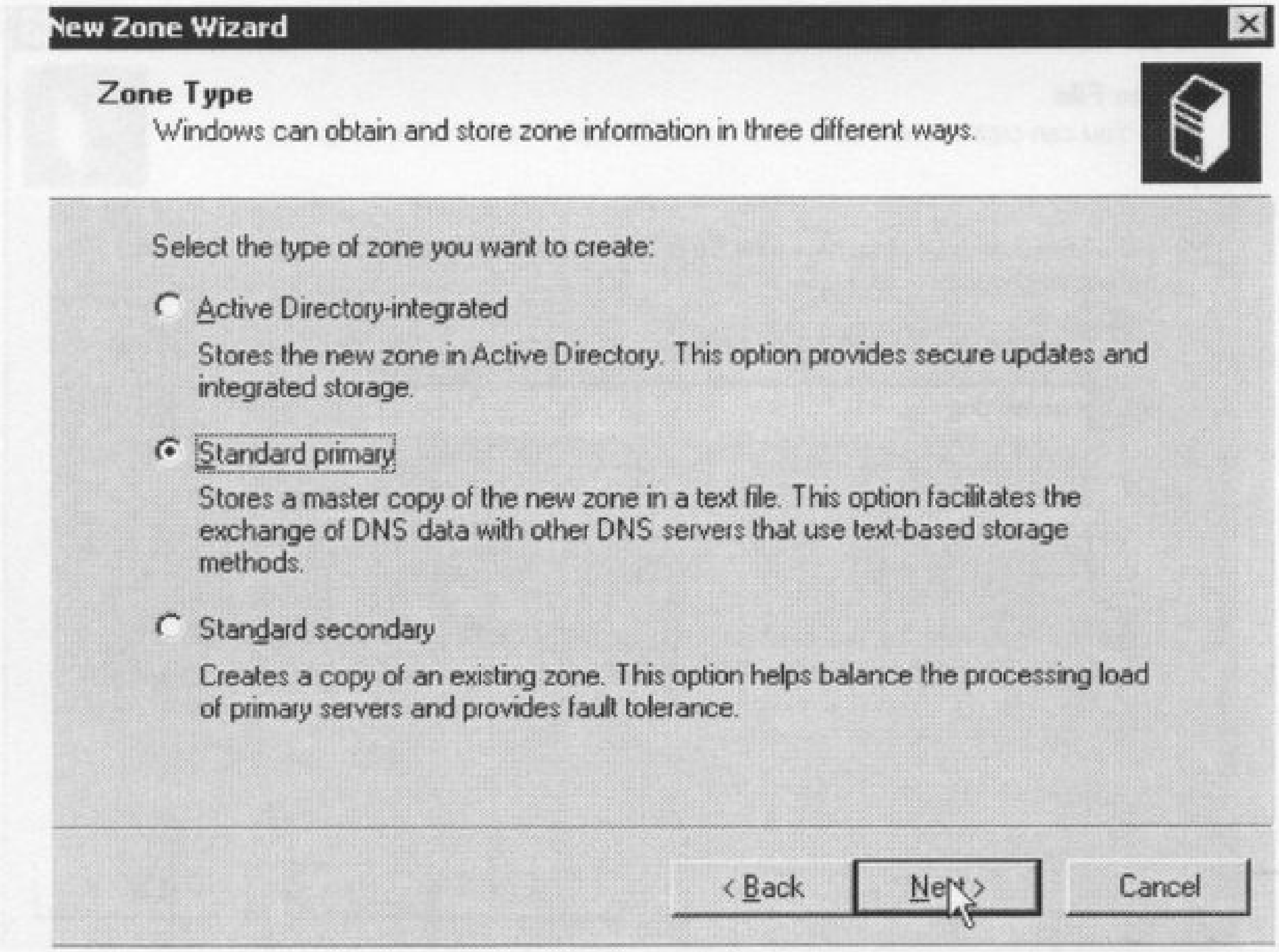
➔ **We already are of course setup with DNS on the Unity server in a domain called "voip.lab" which serves our AD, Unity, and Exchange Server.**

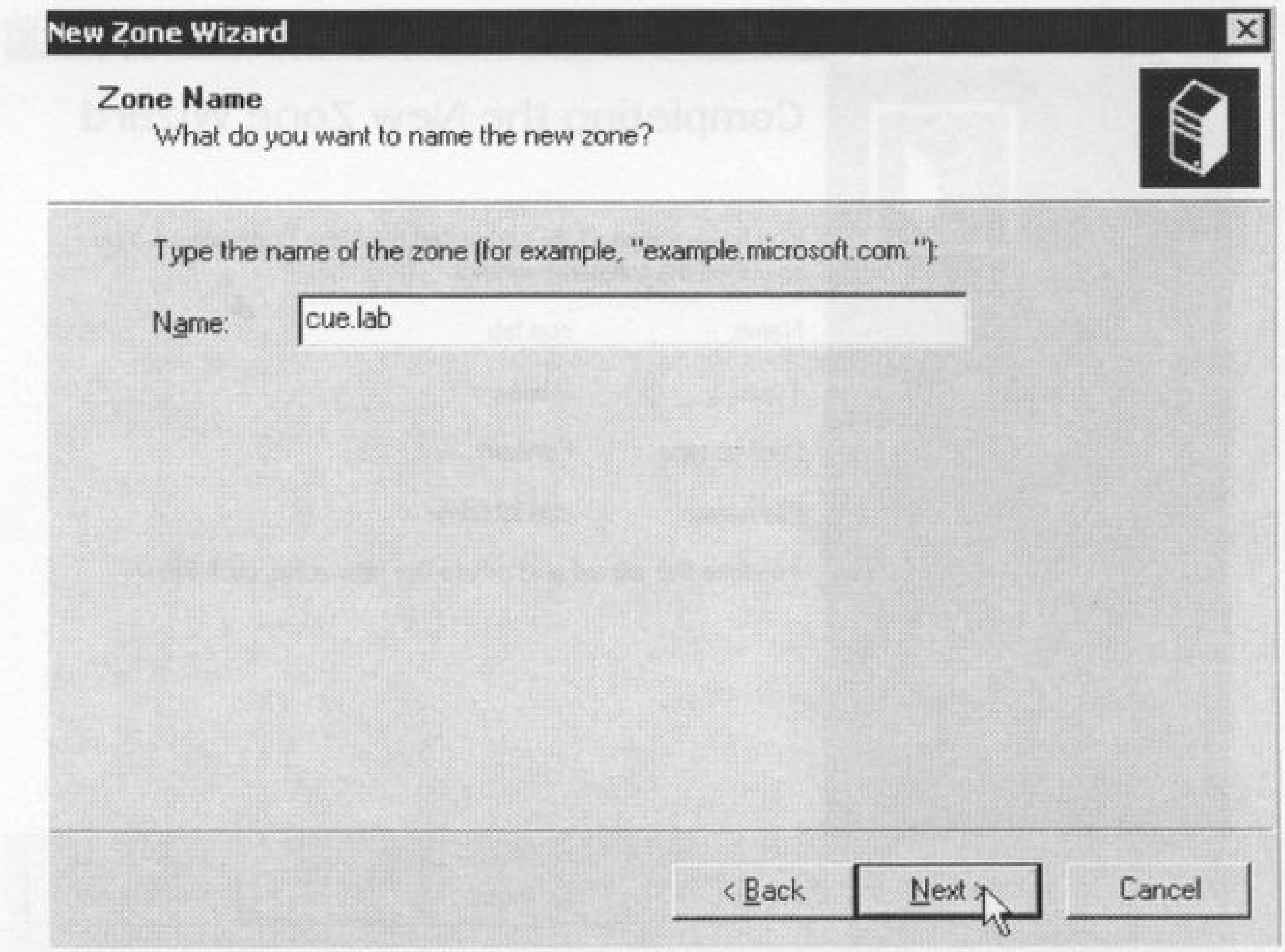
➔ **We now need to create a new forward lookup domain zone for CUE to utilize for SMTP mail records – we will name the zone "cue.lab".**

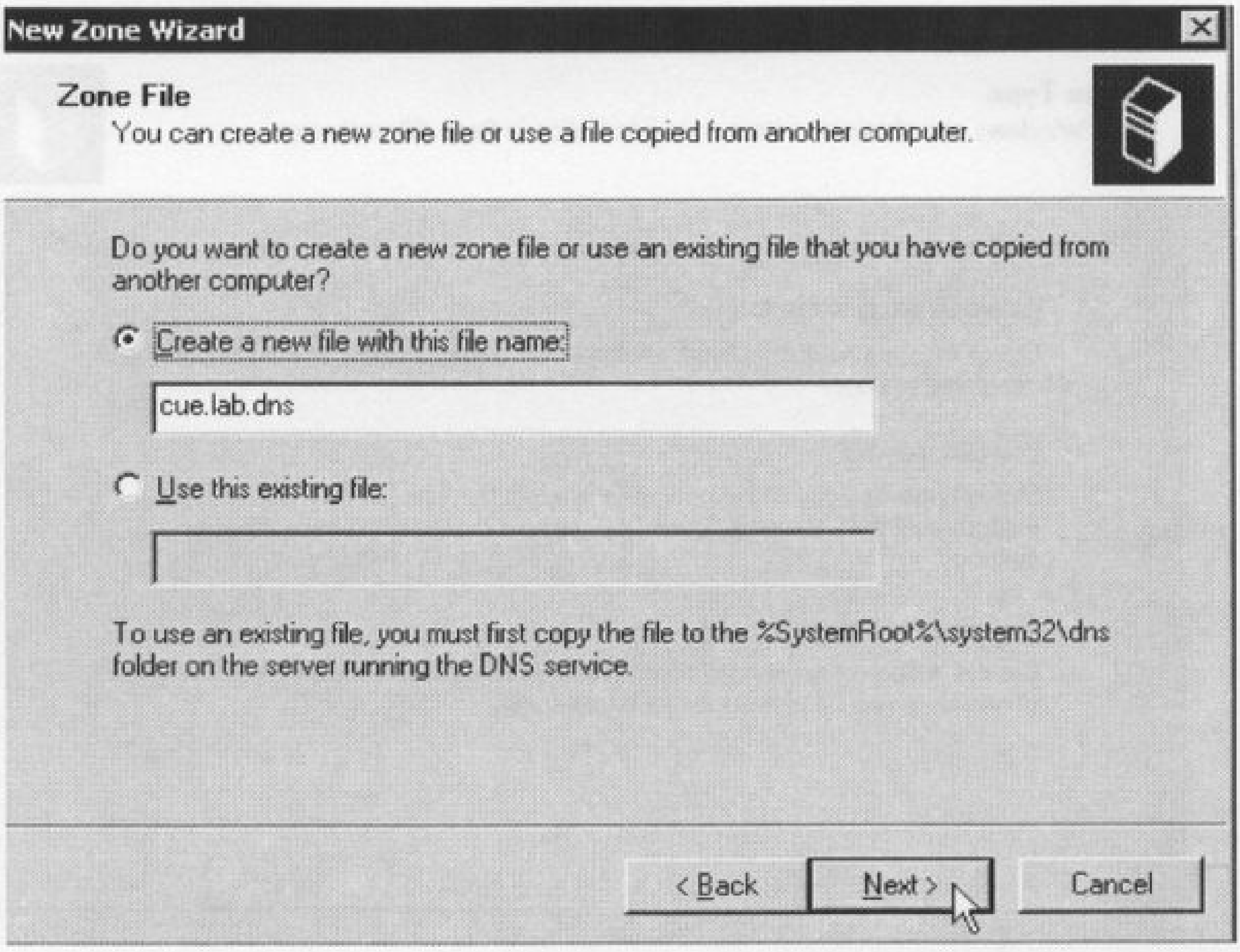

Event Viewer
Services
System Administration
Status Monitor
Cisco Unity Tools Depot
ldif logs
Component Services
Computer Management
Configure Your Server
Data Sources (ODBC)
Distributed File System
Event Viewer
Internet Services Manager
Licensing
Local Security Policy
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Performance
Routing and Remote Access
Services
Telnet Server Administration
Terminal Services Client Creator
Terminal Services Configuration
Terminal Services Manager
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
DNS
Domain Controller Security Policy
Domain Security Policy
Programs
Documents
Settings
Search
Help
Run...
Shut Down...
Windows 2000 Terminal
Accessories
Administrative Tools
Compaq System Tools
Microsoft Exchange
Microsoft SQL Server
Microsoft SQL Server - Switch
RealVNC
Startup
Terminal Services Client
Unity
Internet Explorer
Outlook Express

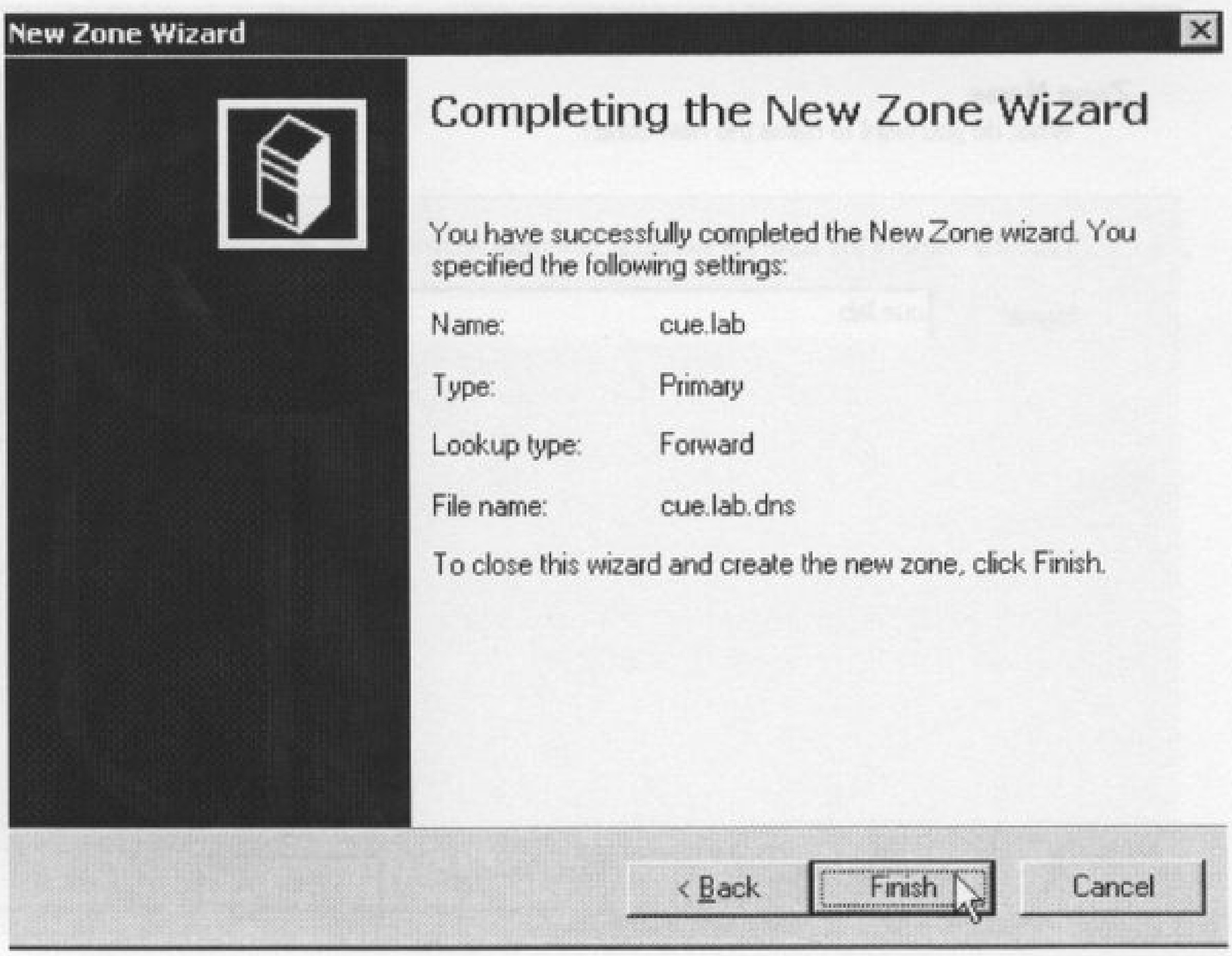

DNS
Console Window Help
Action View
Tree
Name
voip.lab
DNS
UNITY-LAB
Forward Lookup Zones
voip.lab
Reverse Lookup Zones
New Zone...
View
New Window from Here
Refresh
Export List...
Help


New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone is a database that links DNS names and related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel

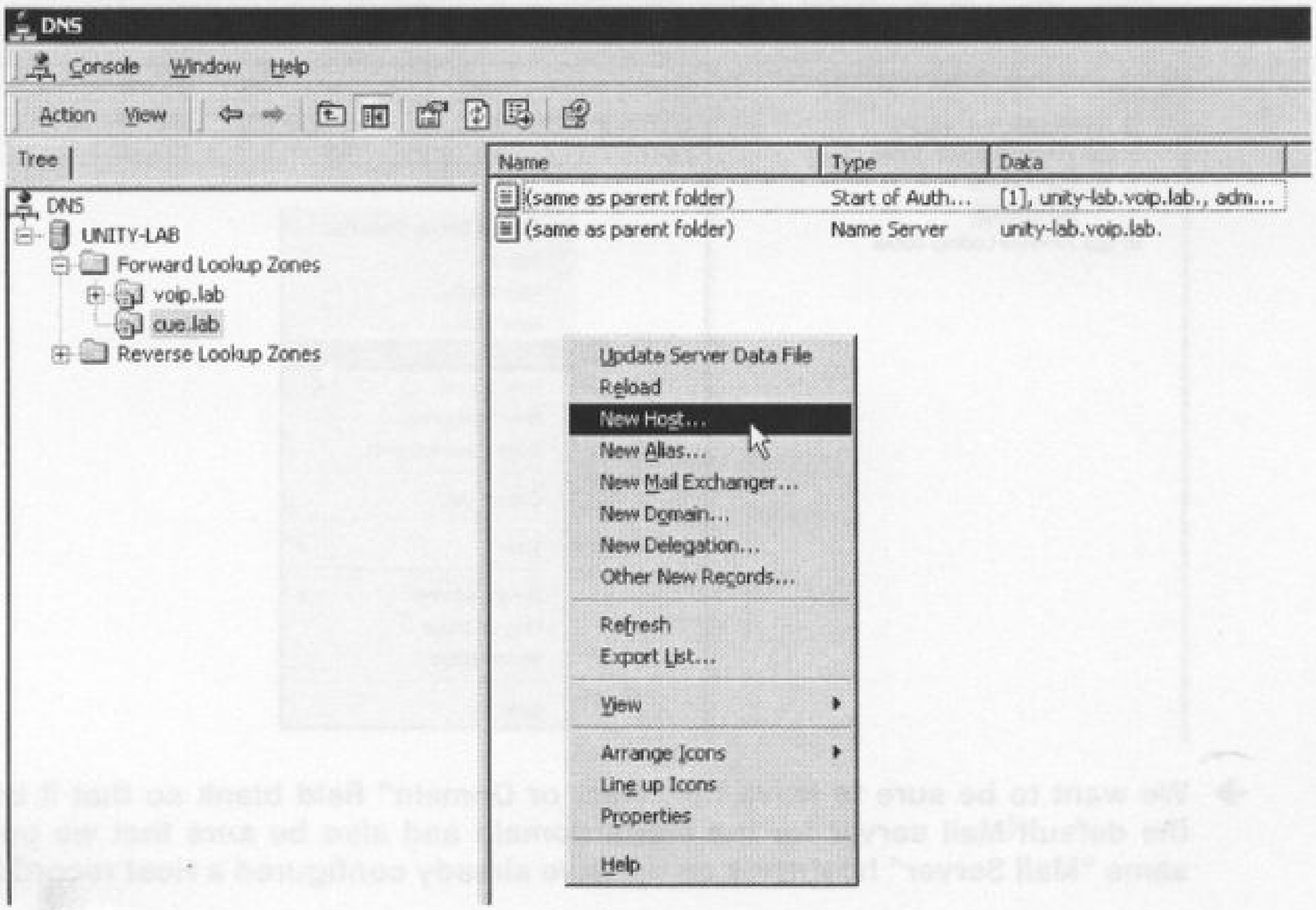

New Zone Wizard
Zone Type
Windows can obtain and store zone information in three different ways.
Select the type of zone you want to create:
Active Directory-integrated
Stores the new zone in Active Directory. This option provides secure updates and integrated storage.
Standard primary
Stores a master copy of the new zone in a text file. This option facilitates the exchange of DNS data with other DNS servers that use text-based storage methods.
Standard secondary
Creates a copy of an existing zone. This option helps balance the processing load of primary servers and provides fault tolerance.
< Back
Next >
Cancel


New Zone Wizard
Zone Name
What do you want to name the new zone?
Type the name of the zone (for example, "example.microsoft.com."):
Name:
cue.lab
< Back
Next >
Cancel

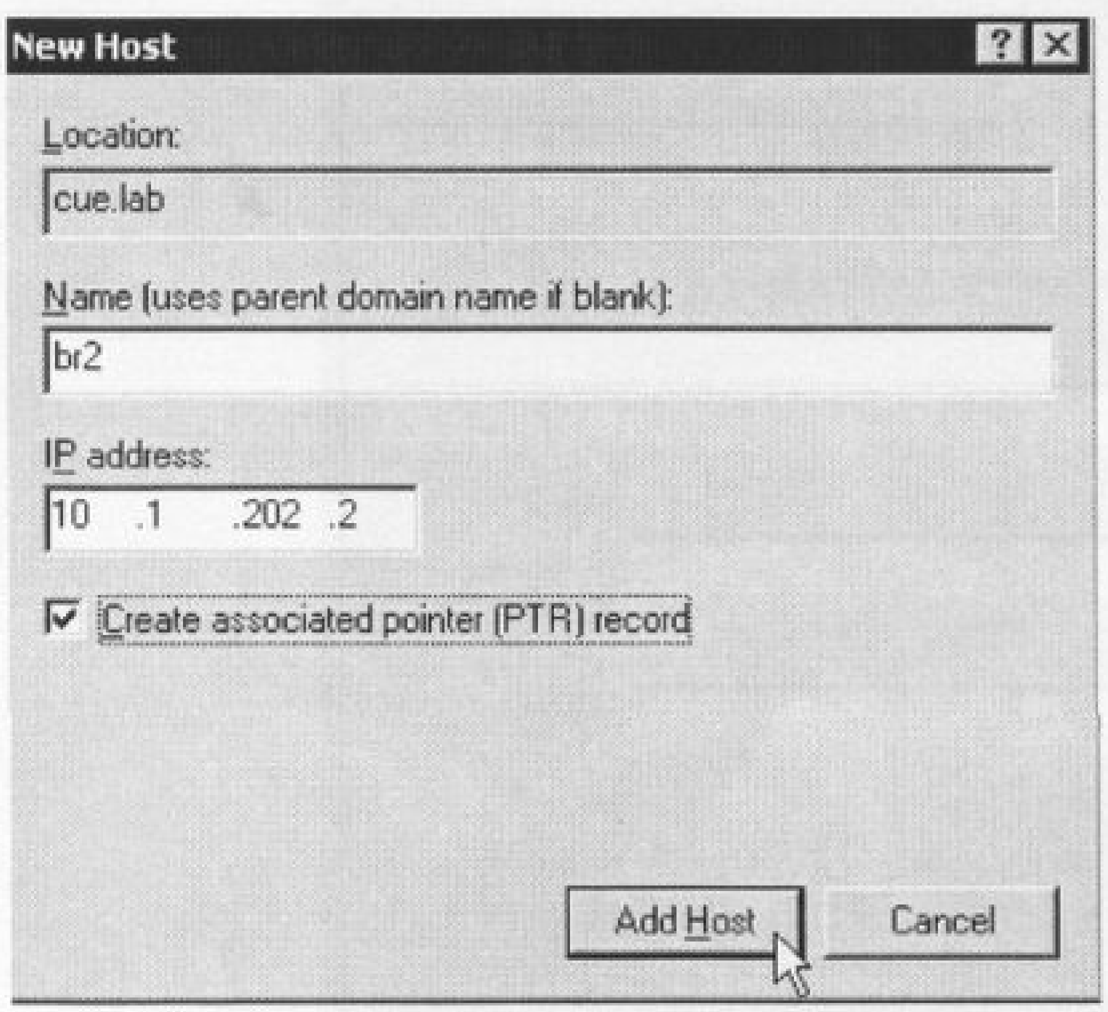

New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another computer.
Do you want to create a new zone file or use an existing file that you have copied from another computer?
Create a new file with this file name:
cue.lab.dns
Use this existing file:
To use an existing file, you must first copy the file to the %SystemRoot%\system32\dns folder on the server running the DNS service.
< Back
Next >
Cancel

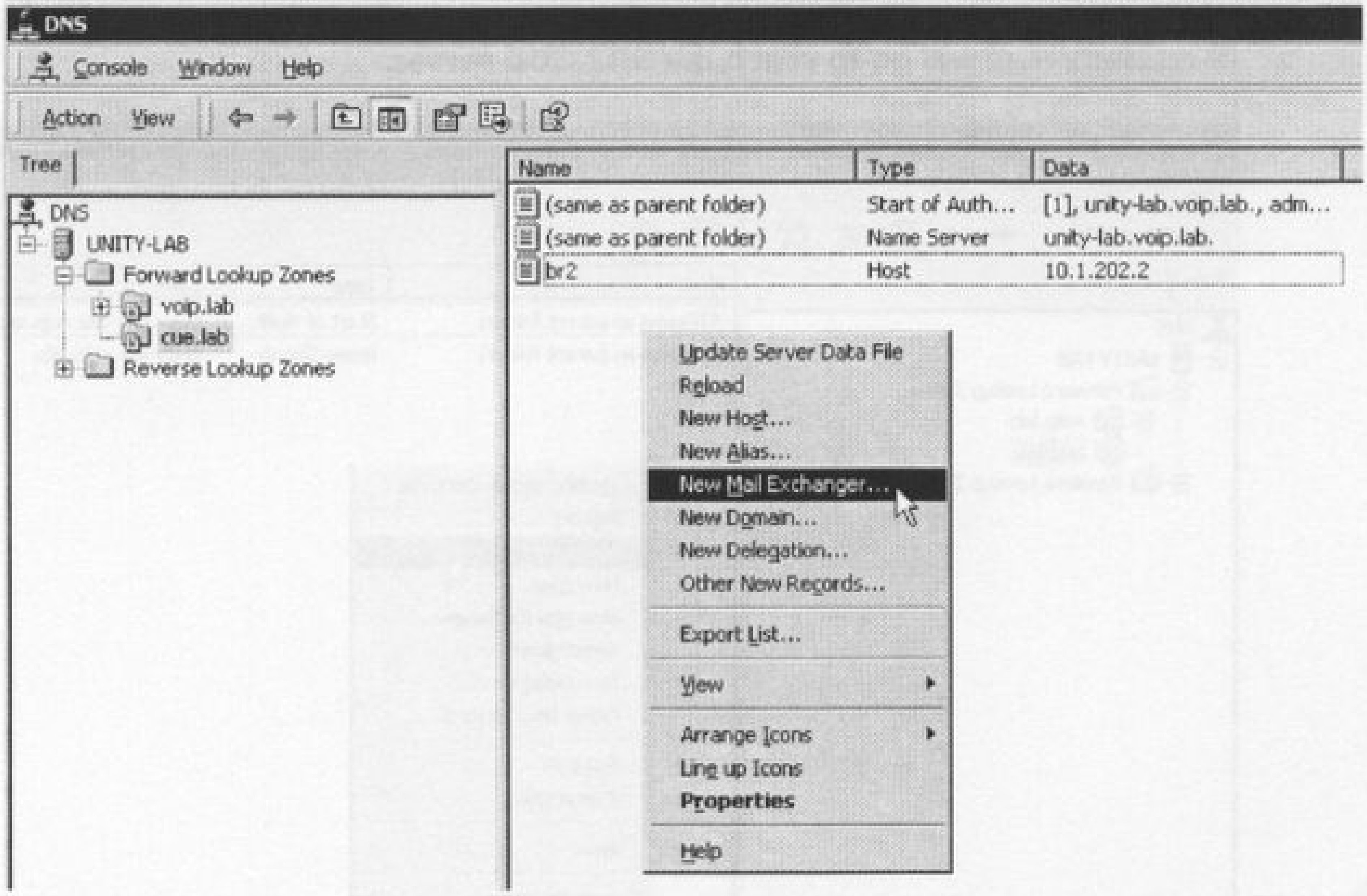

New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone wizard. You specified the following settings:
Name: cue.lab
Type: Primary
Lookup type: Forward
File name: cue.lab.dns
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel

➔ **Now we will need to create a new Host record and a MX record to decipher at what IP address mail will go to reach the BR2 CUE server.**

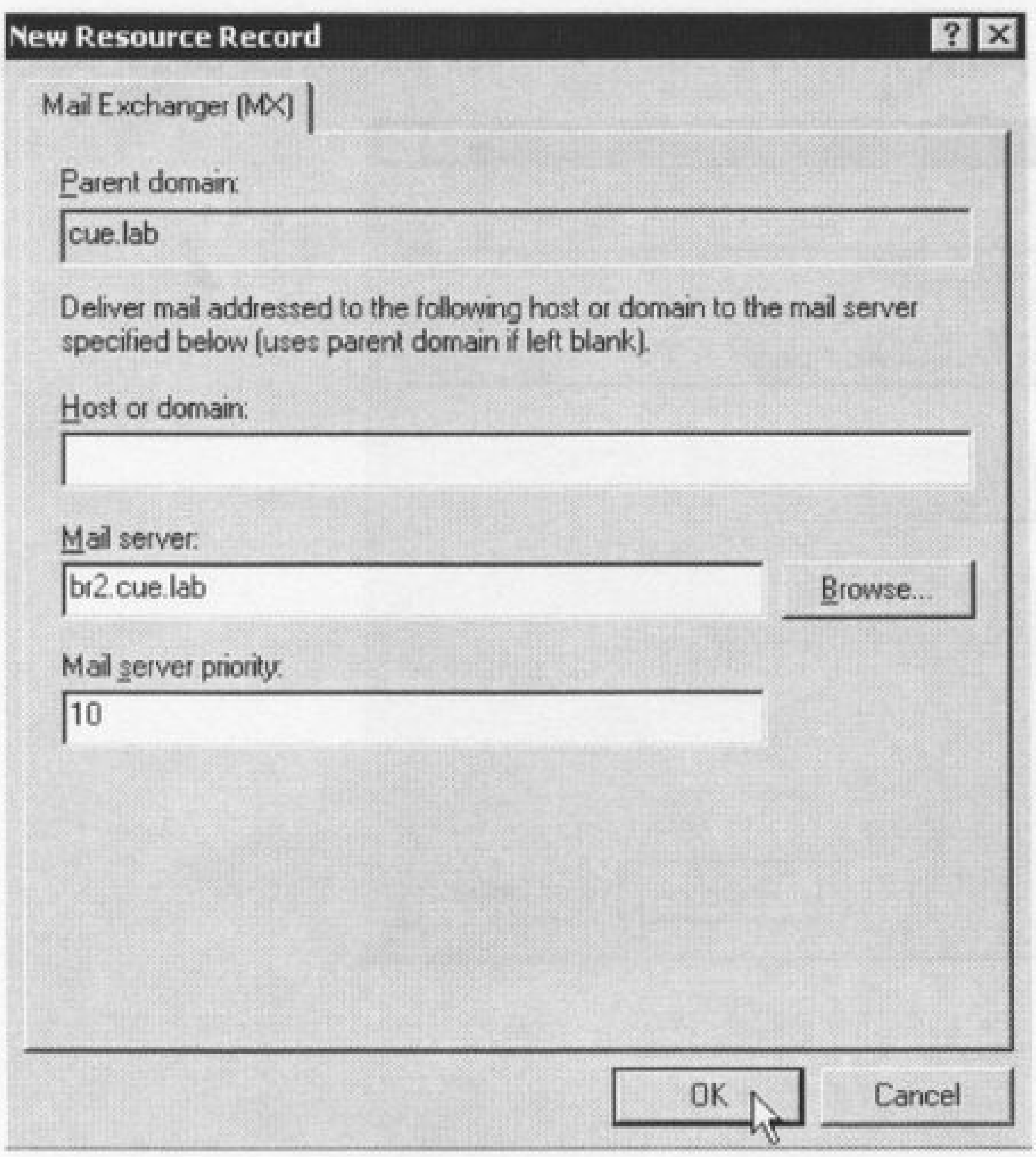


➔ **Make sure that you point it to the CUE IP Address and not the CME IP Address.**

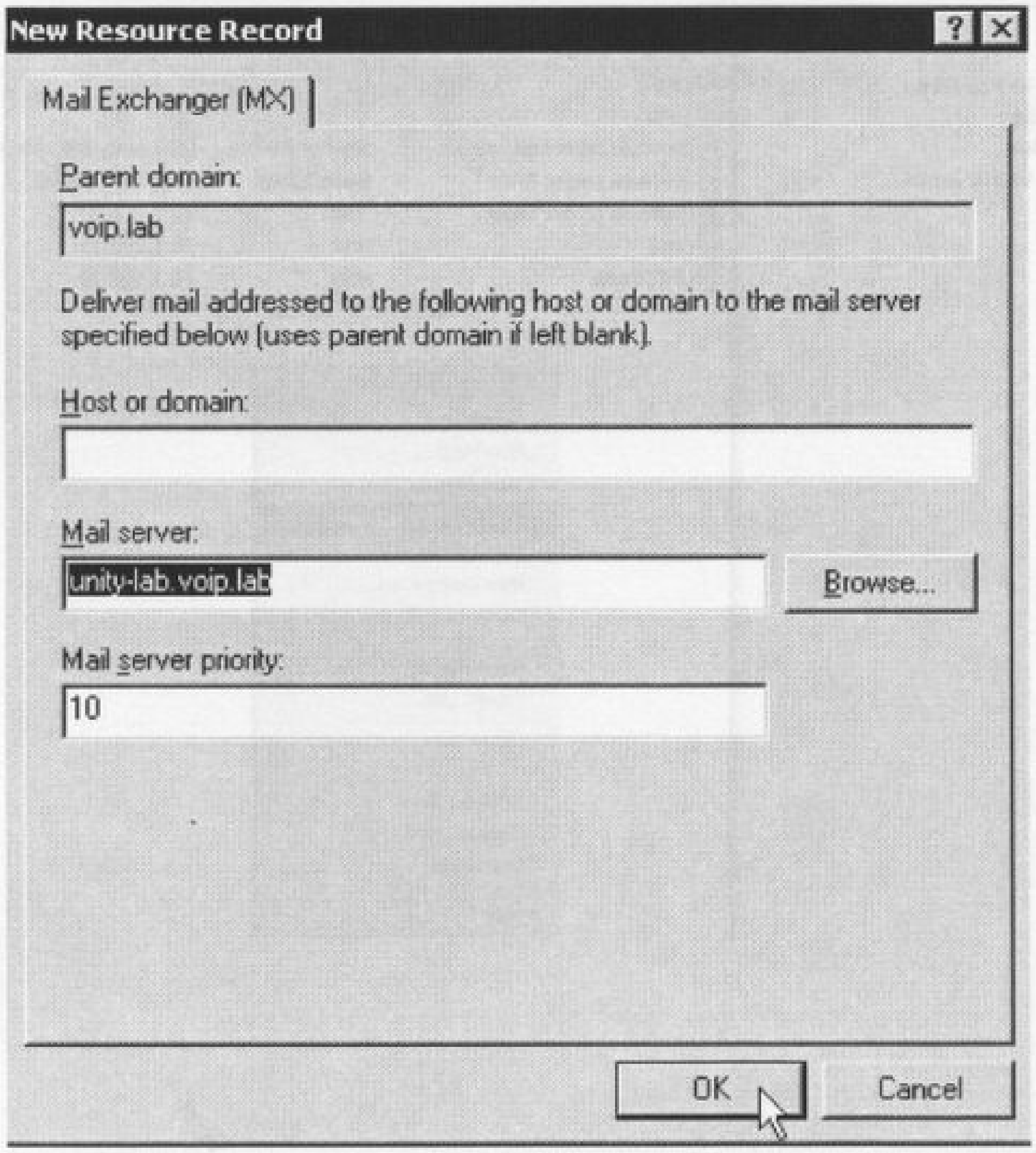




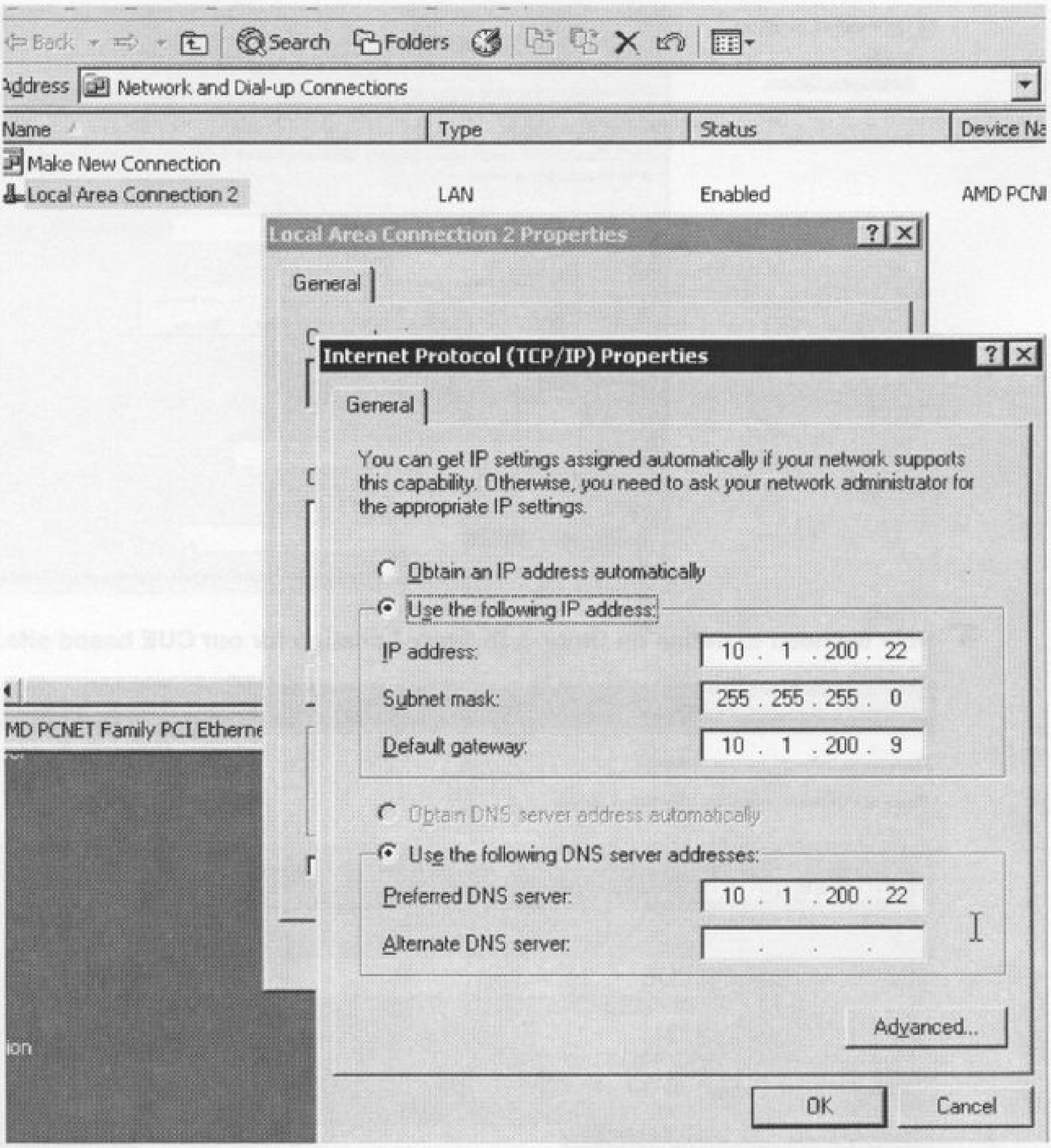
➔ **We want to be sure to leave the "Host or Domain" field blank so that it becomes the default Mail server for the entire domain and also be sure that we put in the same "Mail Server" hostname as we have already configured a Host record for.**



➔ **We want to be sure to leave the "Host or Domain" field blank so that it becomes the default Mail server for the entire domain and also be sure that we put in the same "Mail Server" hostname as we have already configured a Host record for – in this case, "UNITY-LAB" was already a host record.**

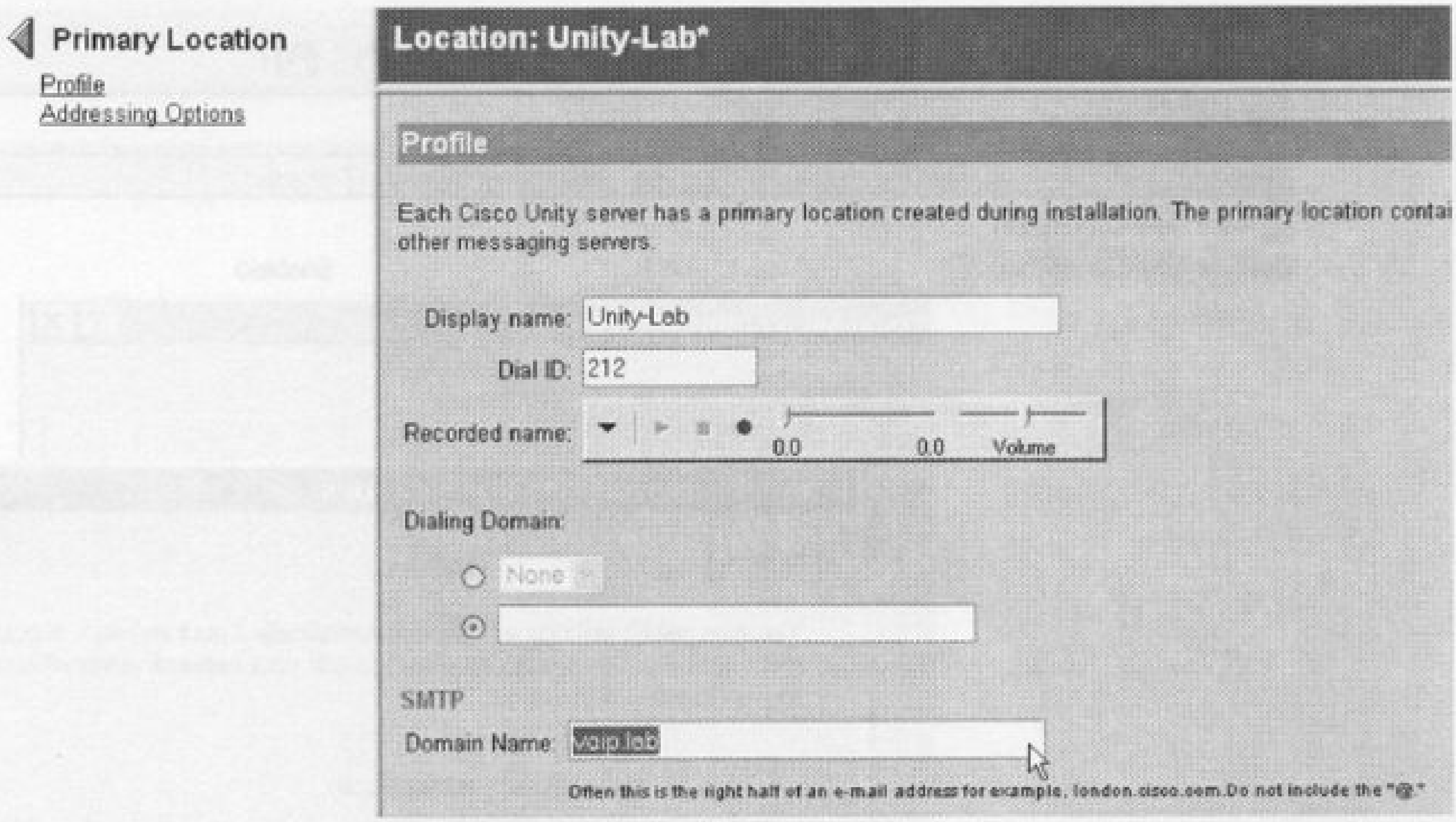


➔ **Now we need to ensure that Unity looks to itself as a DNS provider.**

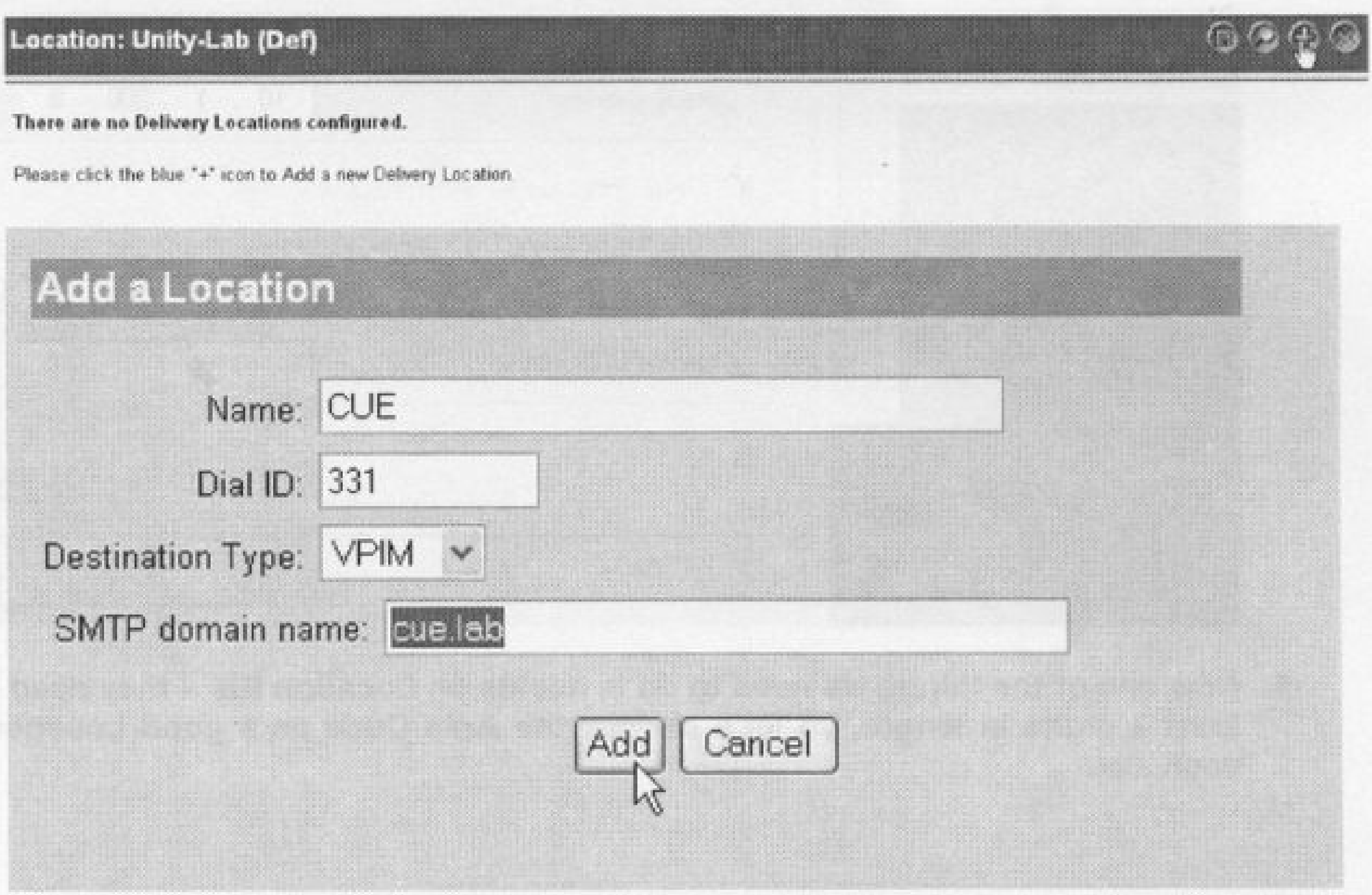


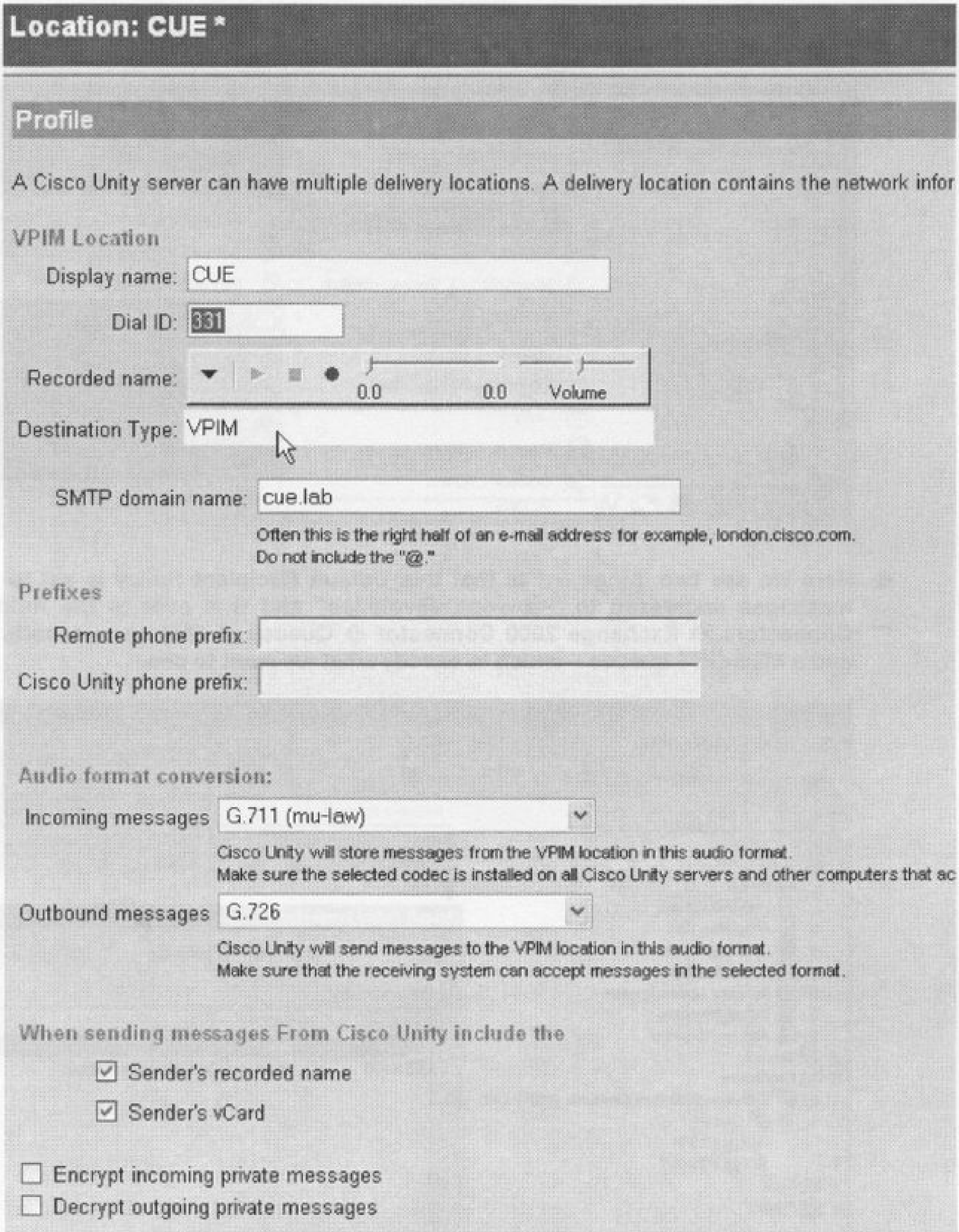
➔ **Now one of the things we need to do is decide on Location IDs – they need to be at least 3 digits in length, so let's choose the Area Code as a good Location ID for each site.**

➔ **In Unity we must first configure our Primary location (our own location).**

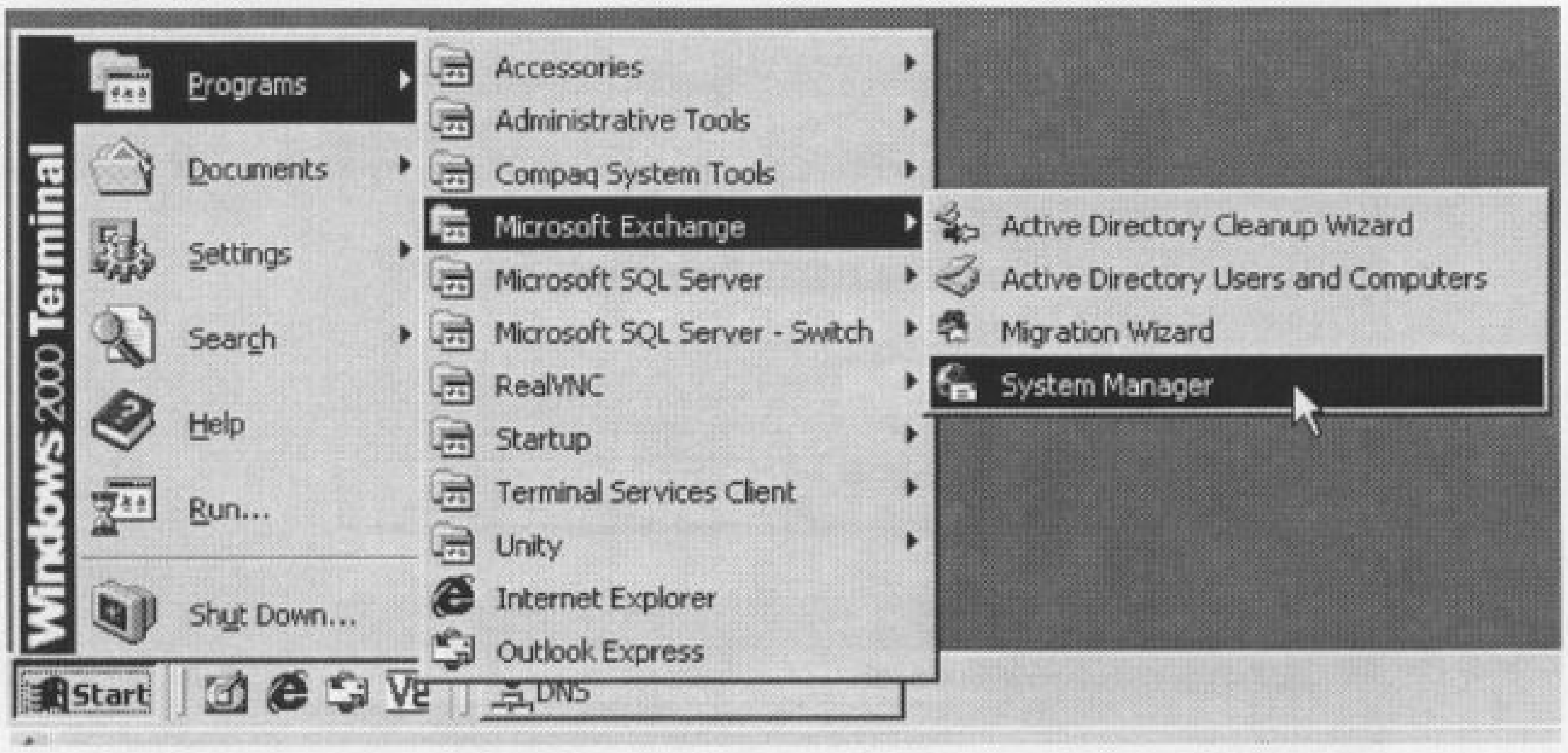


➔ **Now we need to define on Unity, a Delivery Location for our CUE based site.**

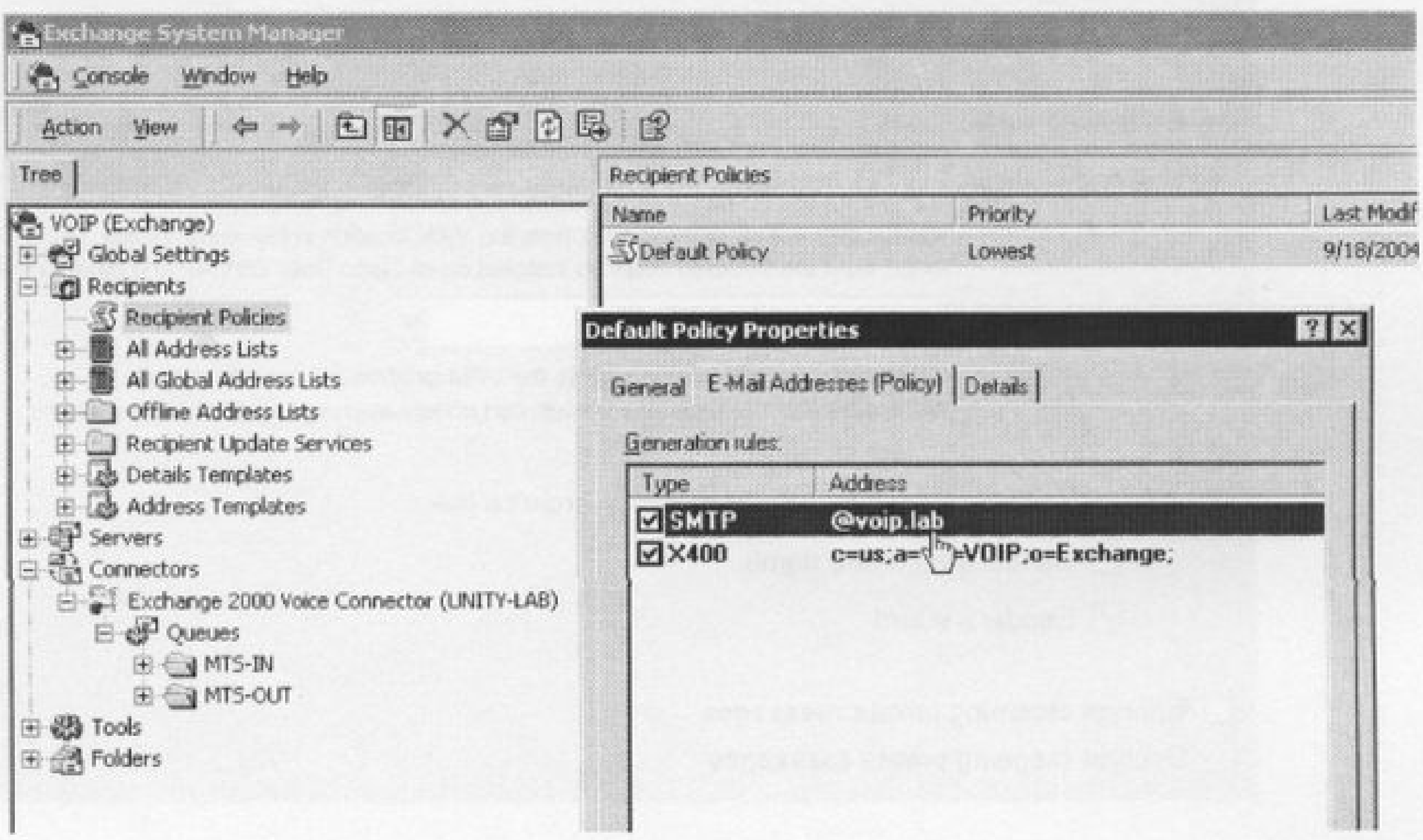



Location: CUE *
Profile
A Cisco Unity server can have multiple delivery locations. A delivery location contains the network infor
VPIM Location
Display name: CUE
Dial ID: 331
Recorded name:
0.0
0.0
Volume
Destination Type: VPIM
SMTP domain name: cue.lab
Often this is the right half of an e-mail address for example, london.cisco.com.
Do not include the "@."
Prefixes
Remote phone prefix:
Cisco Unity phone prefix:
Audio format conversion:
Incoming messages G.711 (mu-law)
Cisco Unity will store messages from the VPIM location in this audio format.
Make sure the selected codec is installed on all Cisco Unity servers and other computers that ac
Outbound messages G.726
Cisco Unity will send messages to the VPIM location in this audio format.
Make sure that the receiving system can accept messages in the selected format.
When sending messages From Cisco Unity include the
Sender's recorded name
Sender's vCard
Encrypt incoming private messages
Decrypt outgoing private messages

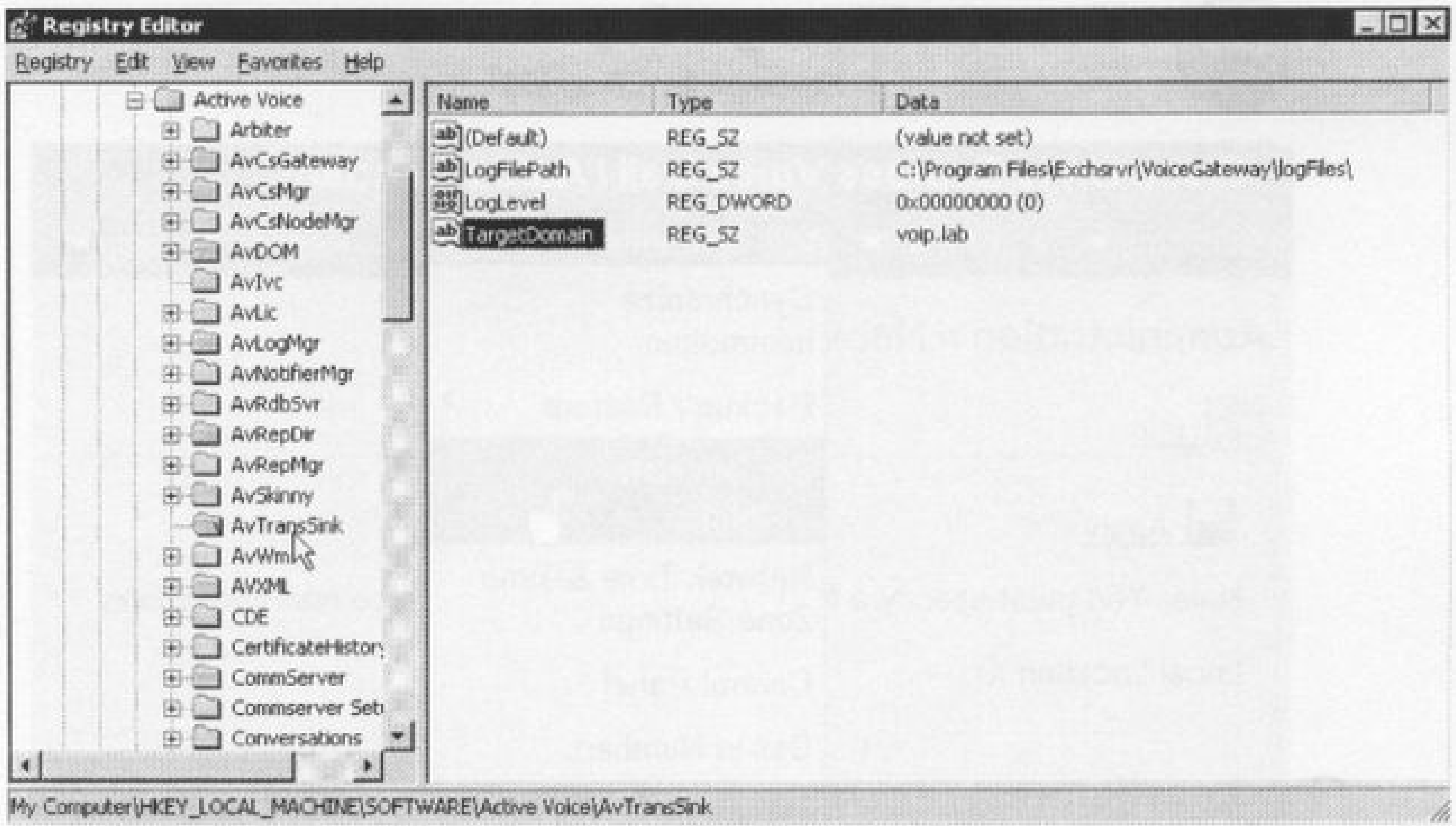
➔ **Now we need to ensure that MS Exchange is setup properly to receive and deliver the necessary messages.**



➔ **Here we see two things – 1 is that this Default Recipient Policy is set to receive messages addressed to "<anyone>@voip.lab" and that over to the right under Connectors ➔ Exchange 2000 Connector ➔ Queues ➔ that we see both MTS-IN and a MTS-OUT queues – which is exactly what we want to see.**



➔ **We also need to ensure that in the MS registry under "HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\AvTransSink" that our Target Domain is set correctly to voip.lab.**

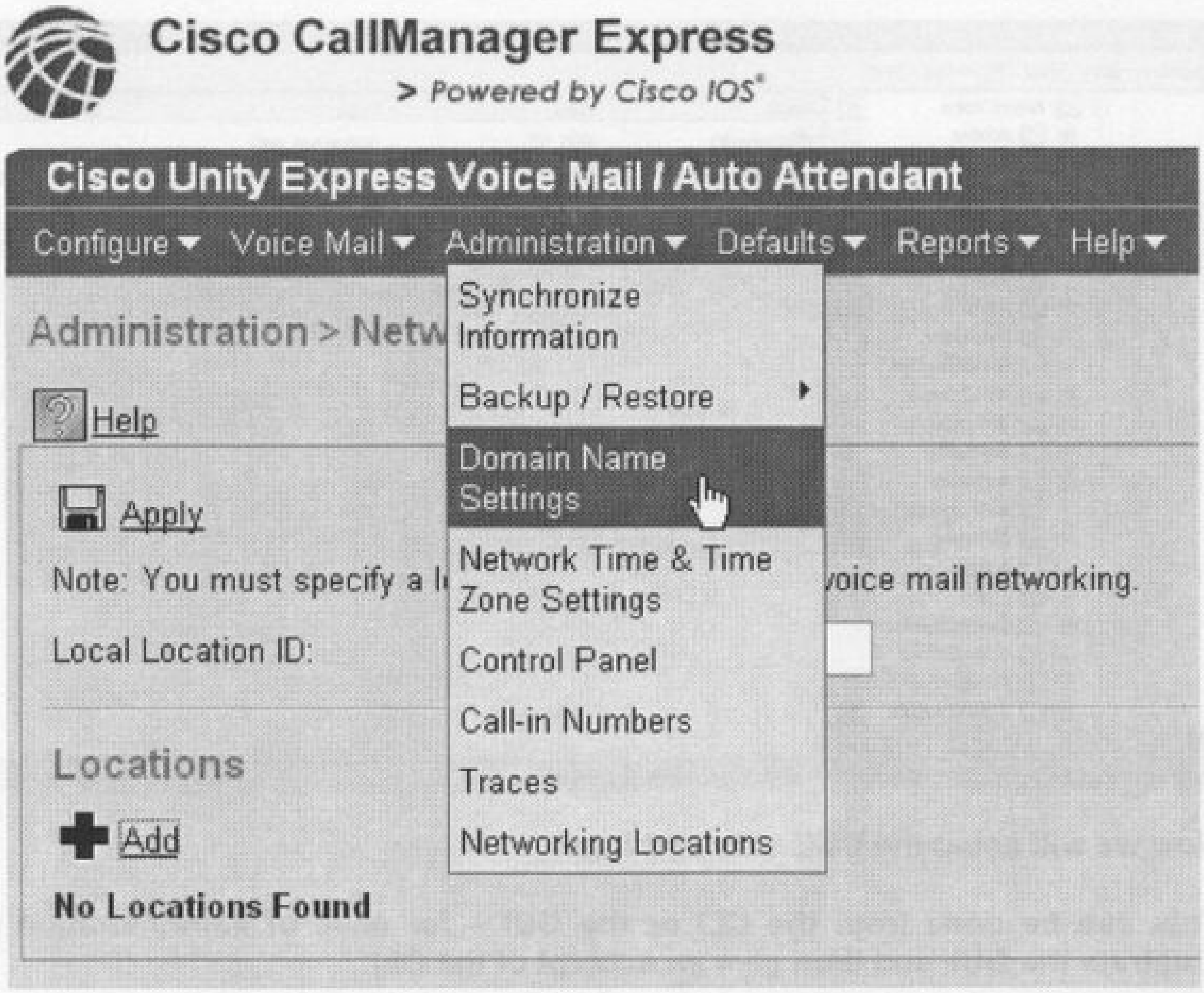


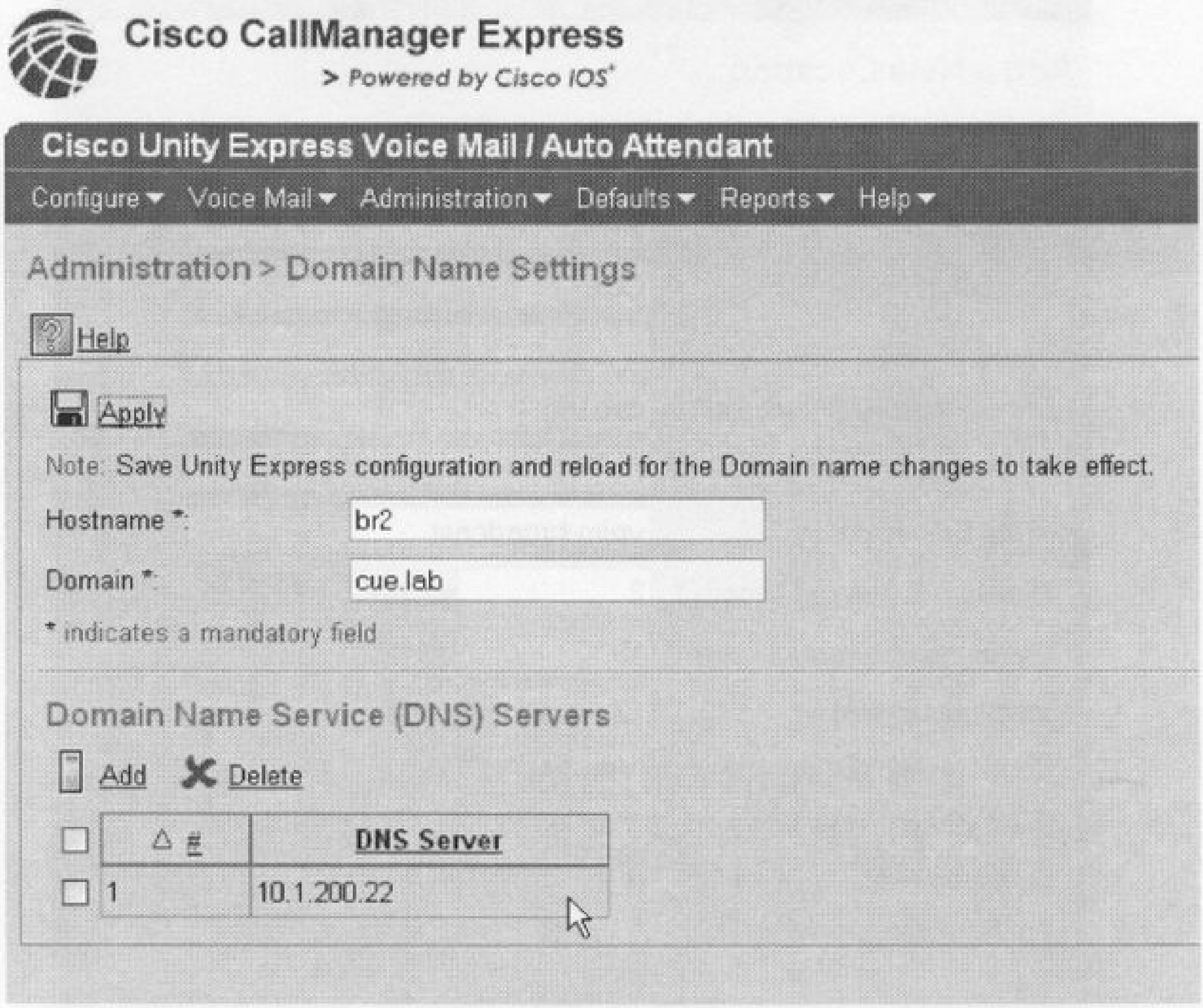
➔ **Now we will setup the CUE side of things.**

➔ **This can be done from the CLI or the GUI – for ease of demonstration we will illustrate the GUI, and then give an excerpt of the CLI.**

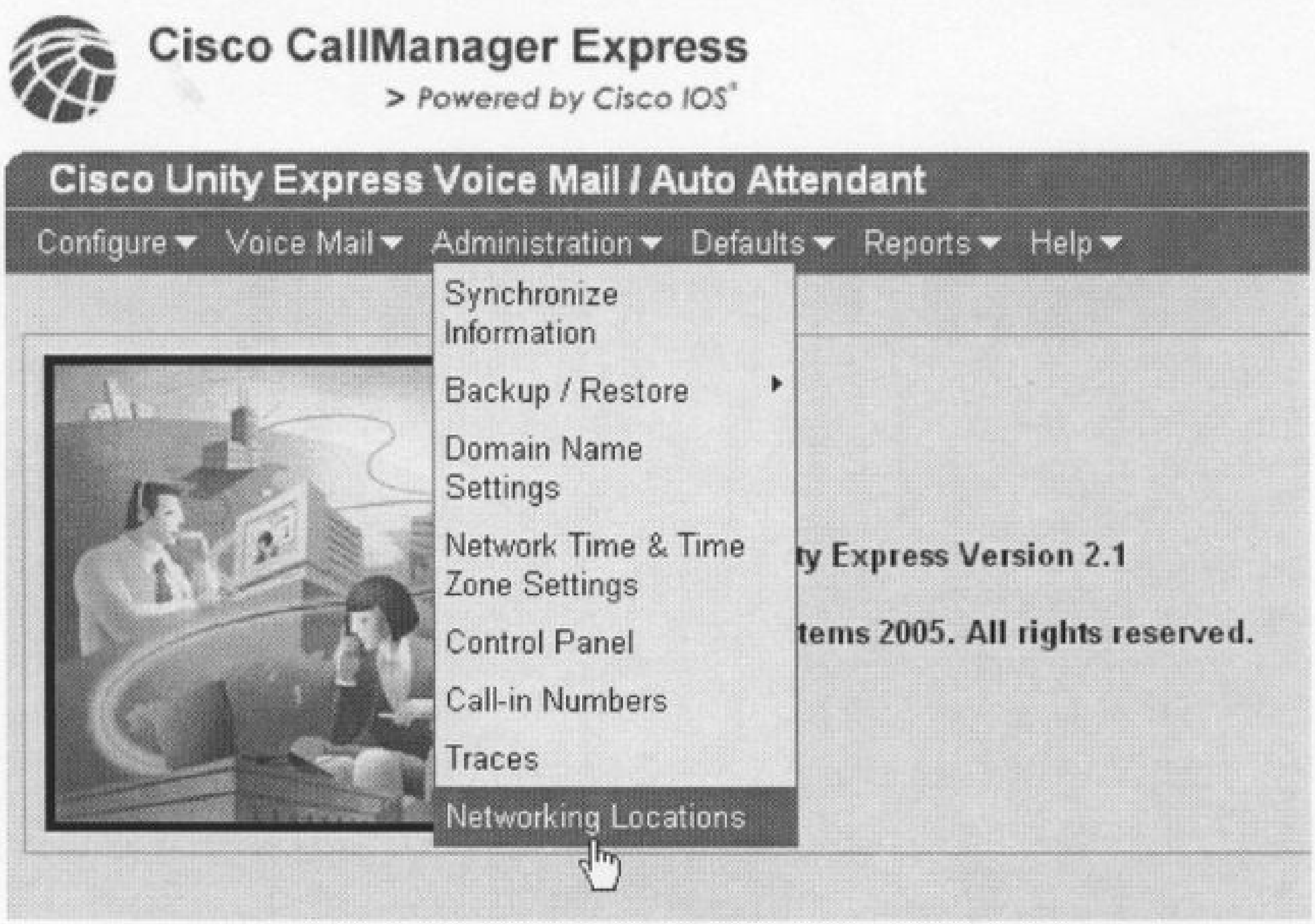
➔ **From Internet Explorer browse to http://10.1.202.2/Web.**

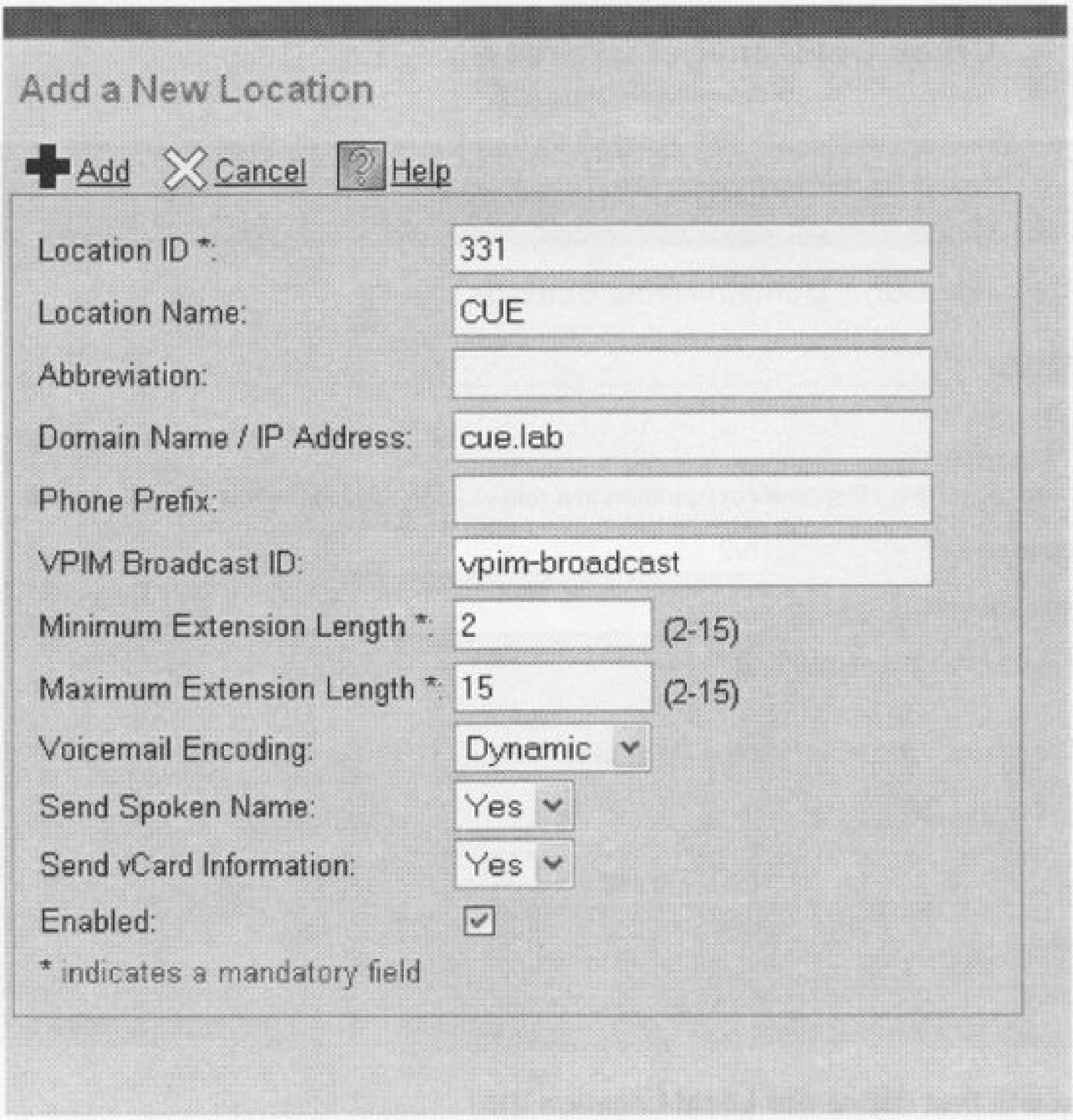
➔ **We will start by ensuring that we tell CUE to use the Unity server as its DNS resolver and that we define our proper Host and Domain Name.**





➔ **Next will first define our Local Location ID.**



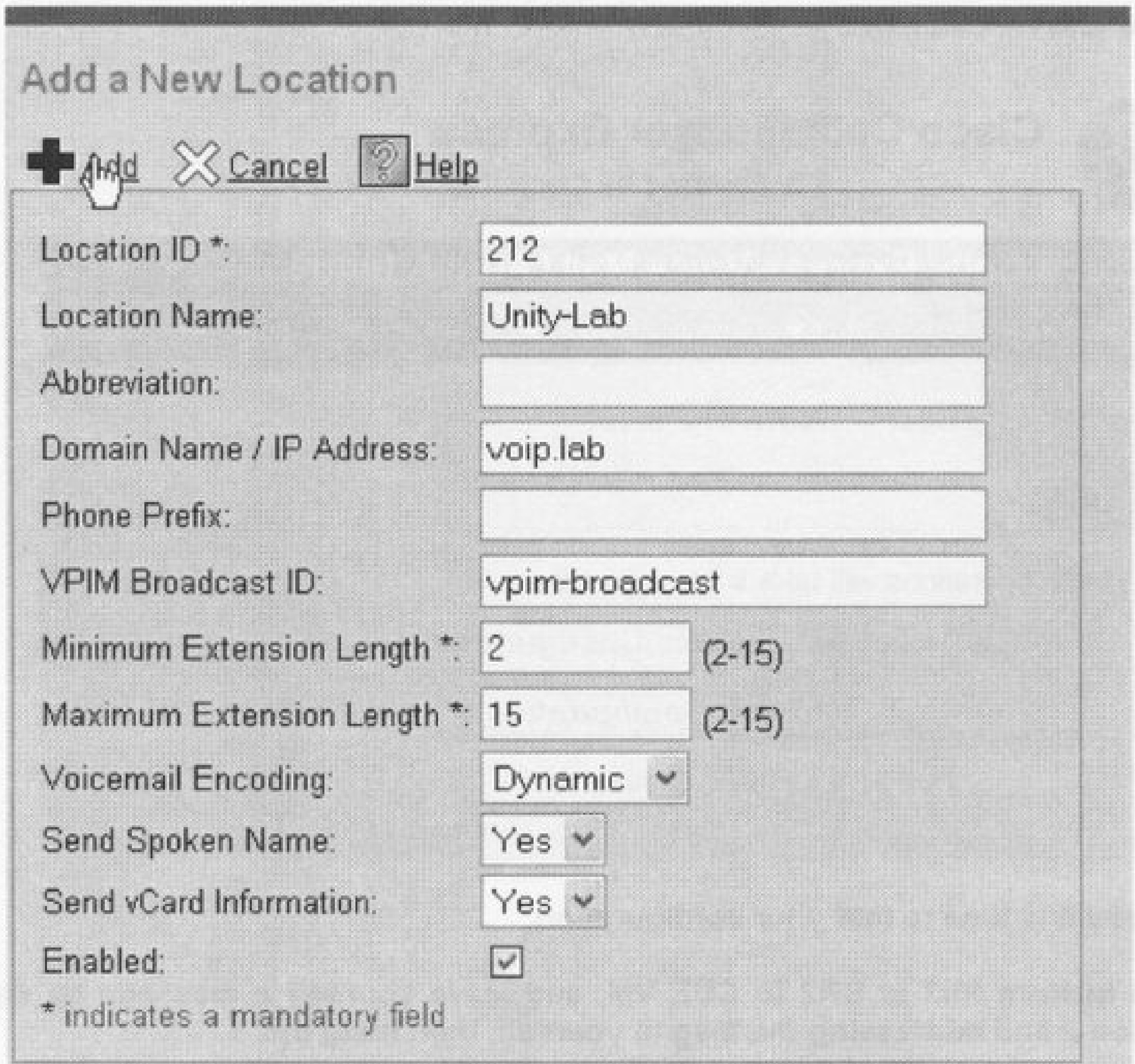


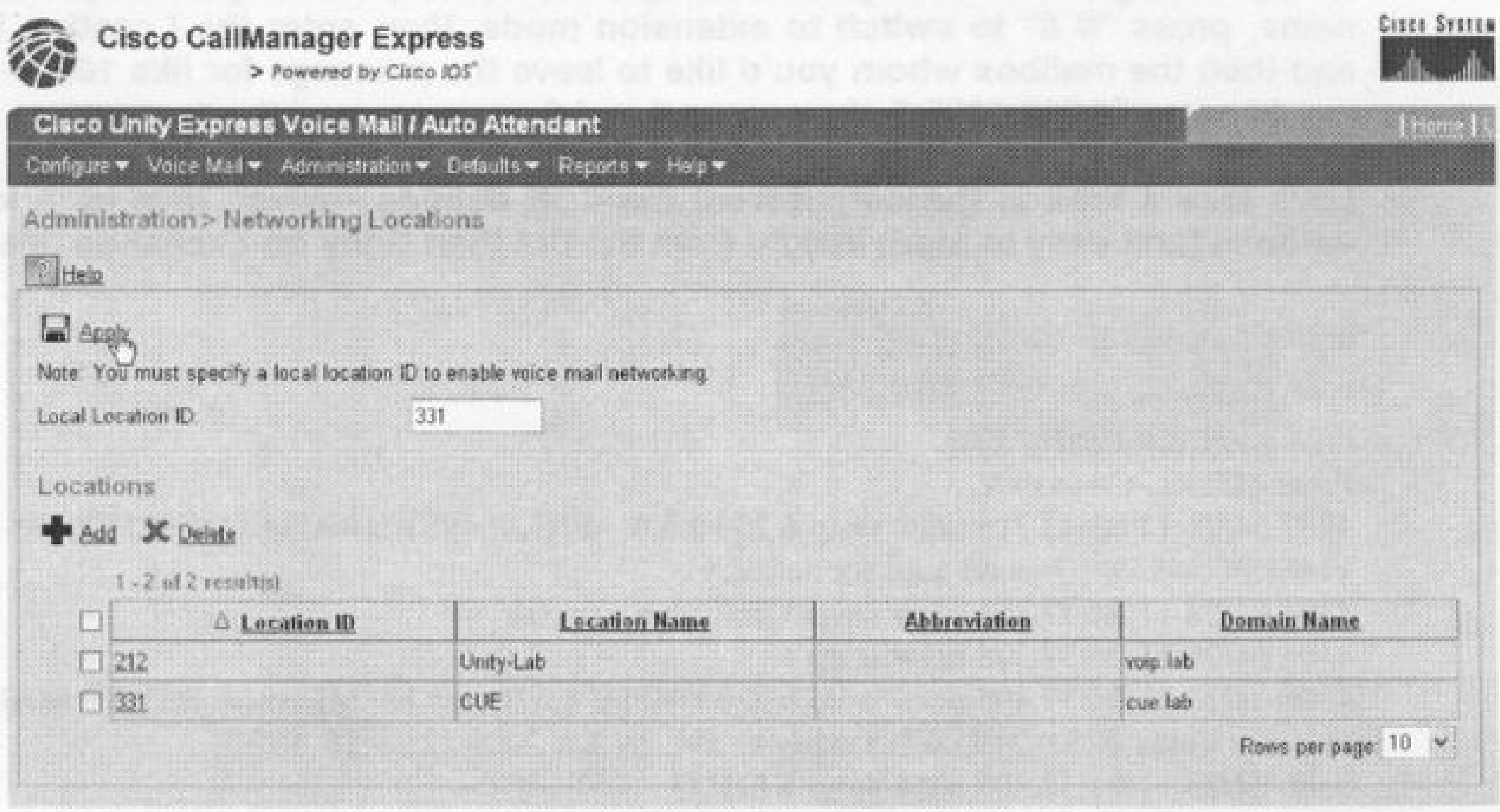
Add a New Location

Add | Cancel | Help

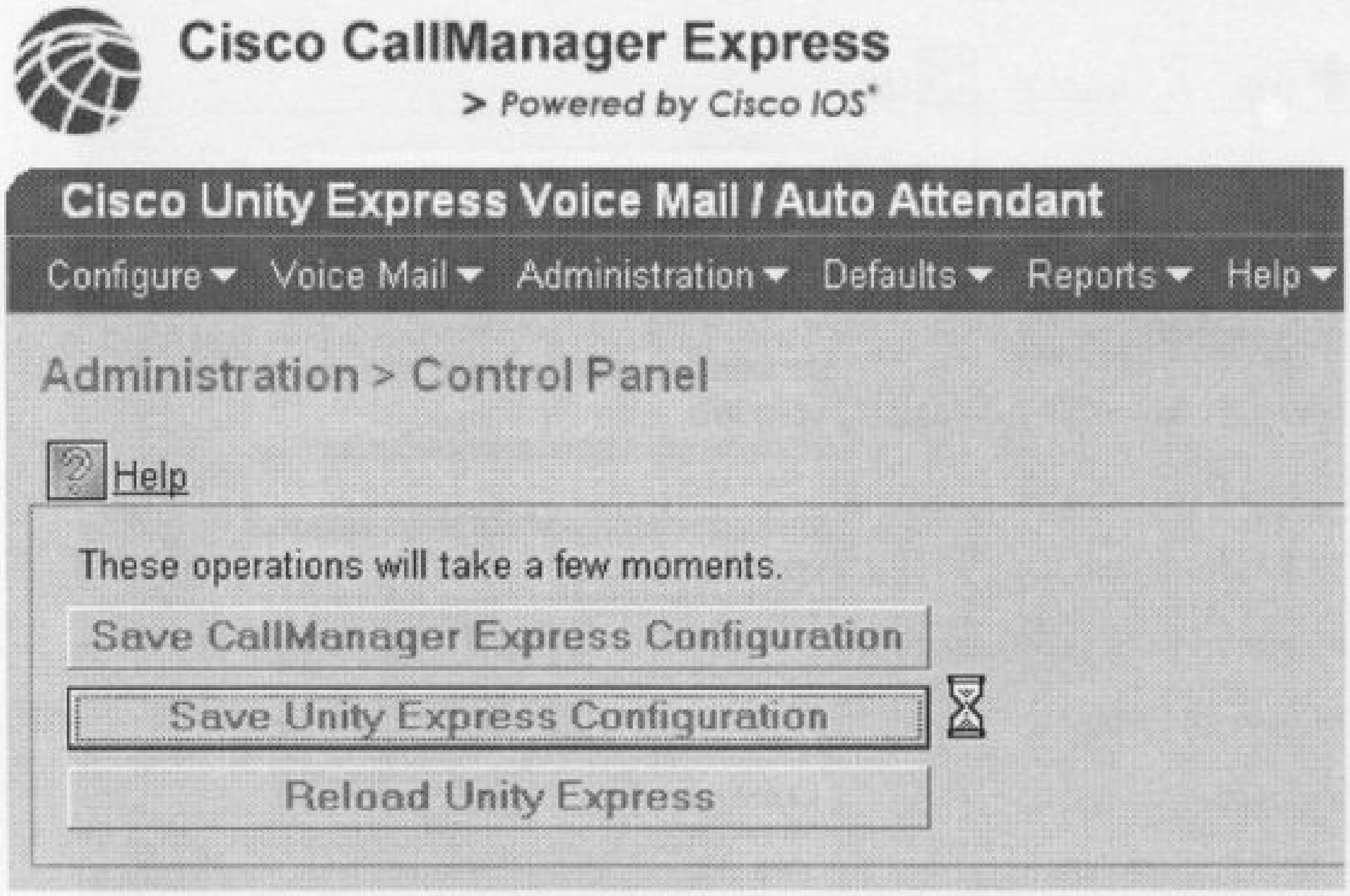
Location ID *:	331
Location Name:	CUE
Abbreviation:	
Domain Name / IP Address:	cue.lab
Phone Prefix:	
VPIM Broadcast ID:	vpim-broadcast
Minimum Extension Length *:	2 (2-15)
Maximum Extension Length *:	15 (2-15)
Voicemail Encoding:	Dynamic
Send Spoken Name:	Yes
Send vCard Information:	Yes
Enabled:	☑

* indicates a mandatory field


Add a New Location
Add
Cancel
Help
Location ID *:
212
Location Name:
Unity-Lab
Abbreviation:
Domain Name / IP Address:
voip.lab
Phone Prefix:
VPIM Broadcast ID:
vpim-broadcast
Minimum Extension Length *:
2
(2-15)
Maximum Extension Length *:
15
(2-15)
Voicemail Encoding:
Dynamic
Send Spoken Name:
Yes
Send vCard Information:
Yes
Enabled:
* indicates a mandatory field


Cisco CallManager Express
> Powered by Cisco IOS
Cisco Systems
Cisco Unity Express Voice Mail / Auto Attendant
Home
Configure
Voice Mail
Administration
Defaults
Reports
Help
Administration > Networking Locations
Help
Apply
Note: You must specify a local location ID to enable voice mail networking.
Local Location ID:
331
Locations
Add
Delete
1 - 2 of 2 result(s)
Location ID
Location Name
Abbreviation
Domain Name
212
Unity-Lab
voip.lab
331
CUE
cue.lab
Rows per page:
10

➔ **Save and Reload CUE.**



➔ **Finally it is time to test your configuration.**

➔ **Call in from Ph3 at BR2 to CUE VM, and leave yourself a message by choosing option 2 and addressing the msg to yourself, then hang up.**

➔ **Now call back to CUE VM again from BR2 Ph3, and listen to your message, this time pressing 5 to forward your message, when prompted to spell the person's last name, press "# #" to switch to extension mode, then enter the Location ID (212) and then the mailbox whom you'd like to leave the message for like 1003 – so you would enter ## 212 1003 #, then press # and # again to send the message.**

➔ **Let's take a look at the output from the CUE debugs - which give us a lot more verbose (and easy to read) insight from the CLI than Unity on Exchange does:**

```
br2# trace networking smtp send
br2# trace networking vpim send
br2# sh trace buffer tail
Press <CTRL-C> to exit...
4287 04/28 11:03:45.715 netw smtp 6 250 2.6.0 <FHK0849F1CU-AIM-FOC081829KP-
1146186254269> Queued mail for delivery
4306 04/28 11:04:37.365 netw smtp 3 unity-lab.voip.lab
4306 04/28 11:04:37.395 netw smtp 4
4306 04/28 11:04:37.405 netw smtp 6 220 UNITY-LAB.voip.lab Microsoft ESMTP MAIL
Service, Version: 5.0.2195.6713 ready at  Fri, 28 Apr 2006 12:39:28 -0230
4306 04/28 11:04:37.405 netw smtp 5 EHLO
4306 04/28 11:04:37.429 netw smtp 6 250-UNITY-LAB.voip.lab Hello [10.1.202.2]
4306 04/28 11:04:37.429 netw smtp 6 250-TURN
4306 04/28 11:04:37.429 netw smtp 6 250-ATRN
4306 04/28 11:04:37.430 netw smtp 6 250-SIZE
4306 04/28 11:04:37.430 netw smtp 6 250-ETRN
4306 04/28 11:04:37.430 netw smtp 6 250-PIPELINING
4306 04/28 11:04:37.430 netw smtp 6 250-DSN
```


4306 04/28 11:04:37.431 netw smtp 6 250-ENHANCEDSTATUSCODES
4306 04/28 11:04:37.431 netw smtp 6 250-8bitmime
4306 04/28 11:04:37.431 netw smtp 6 250-BINARYMIME
4306 04/28 11:04:37.432 netw smtp 6 250-CHUNKING
4306 04/28 11:04:37.432 netw smtp 6 250-VRFY
4306 04/28 11:04:37.432 netw smtp 6 250-X-EXPS GSSAPI NTLM LOGIN
4306 04/28 11:04:37.433 netw smtp 6 250-X-EXPS=LOGIN
4306 04/28 11:04:37.433 netw smtp 6 250-AUTH GSSAPI NTLM LOGIN
4306 04/28 11:04:37.433 netw smtp 6 250-AUTH=LOGIN
4306 04/28 11:04:37.434 netw smtp 6 250-X-LINK2STATE
4306 04/28 11:04:37.434 netw smtp 6 250-XEXCH50
4306 04/28 11:04:37.434 netw smtp 6 250 OK
4306 04/28 11:04:37.926 netw smtp 5 MAIL FROM 3003@cue.lab
4306 04/28 11:04:37.937 netw smtp 6 250 2.1.0 3003@cue.lab....Sender OK
4306 04/28 11:04:37.938 netw smtp 5 RCPT TO 1003@voip.lab
4306 04/28 11:04:37.946 netw smtp 6 250 2.1.5 1003@voip.lab
4306 04/28 11:04:37.946 netw smtp 5 DATA
4306 04/28 11:04:37.960 netw smtp 6 354 Start mail input; end with <CRLF>.<CRLF>
4306 04/28 11:04:37.962 netw vpim 3 VPIM
4306 04/28 11:04:37.992 netw vpim 3 VPIM: To: <1003@voip.lab>
4306 04/28 11:04:37.995 netw vpim 3 VPIM: From: PH<3003@cue.lab>
4306 04/28 11:04:37.999 netw vpim 3 VPIM: Date: Fri, 28 Apr 2006 11:04:37 -0400 (EDT)
4306 04/28 11:04:38.000 netw vpim 3 VPIM: MIME-Version: 1.0 (Voice 2.0)
4306 04/28 11:04:38.000 netw vpim 3 VPIM: Content-Type: Multipart/Voice-Message; Version=2.0;
4306 04/28 11:04:38.000 netw vpim 3 VPIM: Boundary="==VpimMsg==1146236677960"
4306 04/28 11:04:38.001 netw vpim 3 VPIM: Content-Transfer-Encoding: 7bit
4306 04/28 11:04:38.001 netw vpim 3 VPIM: Message-ID: <FHK0849F1CU-AIM-FOC081829KP-1146186254270>
4306 04/28 11:04:38.001 netw vpim 3 VPIM:
4306 04/28 11:04:38.002 netw vpim 3 VPIM: --==VpimMsg==1146236677960
4306 04/28 11:04:38.002 netw vpim 3 VPIM: Content-Type: text/directory; charset=us-ascii; profile=vCard
4306 04/28 11:04:38.002 netw vpim 3 VPIM: Content-Transfer-Encoding: 7bit
4306 04/28 11:04:38.003 netw vpim 3 VPIM: Content-Disposition: attachment; filename="PH.vcf"
4306 04/28 11:04:38.003 netw vpim 3 VPIM:
4306 04/28 11:04:38.003 netw vpim 3 VPIM: BEGIN:vCard
4306 04/28 11:04:38.004 netw vpim 3 VPIM: FN:PH
4306 04/28 11:04:38.004 netw vpim 3 VPIM: EMAIL;TYPE=INTERNET;TYPE=VPIM:3003@cue.lab
4306 04/28 11:04:38.004 netw vpim 3 VPIM: TEL:3003
4306 04/28 11:04:38.005 netw vpim 3 VPIM: VERSION: 3.0
4306 04/28 11:04:38.005 netw vpim 3 VPIM: END:vCard
4306 04/28 11:04:38.005 netw vpim 3 VPIM:
4306 04/28 11:04:38.065 netw vpim 3 VPIM: --==VpimMsg==1146236677960
4306 04/28 11:04:38.065 netw vpim 3 VPIM: Content-Type: Audio/32KADPCM
4306 04/28 11:04:38.066 netw vpim 3 VPIM: Content-Transfer-Encoding: Base64
4306 04/28 11:04:38.066 netw vpim 3 VPIM: Content-Disposition: inline; voice=Originator-Spoken-Name
4306 04/28 11:04:38.066 netw vpim 3 VPIM:
4306 04/28 11:04:38.066 netw vpim 7
4306 04/28 11:04:38.176 netw vpim 3 VPIM:
4306 04/28 11:04:38.201 netw vpim 3 VPIM: --==VpimMsg==1146236677960
4306 04/28 11:04:38.202 netw vpim 3 VPIM: Content-type: Message/RFC822
4306 04/28 11:04:38.202 netw vpim 3 VPIM: Content-Transfer-Encoding: 7bit

4306 04/28 11:04:38.202 netw vpim 3 VPIM: To: <3003@cue.lab>
4306 04/28 11:04:38.205 netw vpim 3 VPIM: From: PH<3003@cue.lab>
4306 04/28 11:04:38.209 netw vpim 3 VPIM: Date: Thu, 20 Apr 2006 19:41:50 -0400 (EDT)
4306 04/28 11:04:38.210 netw vpim 3 VPIM: MIME-Version: 1.0 (Voice 2.0)
4306 04/28 11:04:38.210 netw vpim 3 VPIM: Content-Type: Multipart/Voice-Message; Version=2.0;
4306 04/28 11:04:38.210 netw vpim 3 VPIM: Boundary="==VpimMsg==11462366779601"
4306 04/28 11:04:38.211 netw vpim 3 VPIM: Content-Transfer-Encoding: 7bit
4306 04/28 11:04:38.211 netw vpim 3 VPIM:
4306 04/28 11:04:38.269 netw vpim 3 VPIM: --==VpimMsg==1146236779601
4306 04/28 11:04:38.269 netw vpim 3 VPIM: Content-Type: Audio/32KADPCM
4306 04/28 11:04:38.270 netw vpim 3 VPIM: Content-Transfer-Encoding: Base64
4306 04/28 11:04:38.270 netw vpim 3 VPIM: Content-Disposition: inline; voice=Originator-Spoken-Name
4306 04/28 11:04:38.270 netw vpim 3 VPIM:
4306 04/28 11:04:38.270 netw vpim 7
4306 04/28 11:04:38.375 netw vpim 3 VPIM:
4306 04/28 11:04:38.376 netw vpim 3 VPIM: --==VpimMsg==1146236779601
4306 04/28 11:04:38.376 netw vpim 3 VPIM: Content-Type: Audio/32KADPCM
4306 04/28 11:04:38.376 netw vpim 3 VPIM: Content-Transfer-Encoding: Base64
4306 04/28 11:04:38.377 netw vpim 3 VPIM: Content-Description: VPIM Message
4306 04/28 11:04:38.377 netw vpim 3 VPIM: Content-Disposition: inline; voice=Voice-Message
4306 04/28 11:04:38.377 netw vpim 3 VPIM: Content-ID: FHK0849F1CU-AIM-FOC081829KP-1145558083318
4306 04/28 11:04:38.378 netw vpim 3 VPIM:
4306 04/28 11:04:38.386 netw vpim 7
4306 04/28 11:04:38.857 netw vpim 3 VPIM:
4306 04/28 11:04:38.857 netw vpim 3 VPIM: --==VpimMsg==1146236779601--
4306 04/28 11:04:38.858 netw vpim 3 VPIM: --==VpimMsg==1146236677960--
4306 04/28 11:04:38.860 netw smtp 5 End of DATA
4306 04/28 11:04:39.377 netw smtp 6 250 2.6.0 <FHK0849F1CU-AIM-FOC081829KP-1146186254270> Queued mail for delivery

➔ **Now call into Unity from Ph3 1003 at HQ and see if the message arrived properly.**

➔ **Next try to reply to that message by pressing 4, record an intro, press # and # again – now your message has been send back to the CUE site (Location ID 331) to mailbox 3003.**

➔ **Place a call from BR2 Ph3 into its mailbox to ensure the message arrived properly.**

➔ **Now let's try a call in the opposite direction beginning with a new message (not a reply) from Unity Ph3 (3003) targeted to CUE Ph 1 (1003) and let's take a look at the debug in CUE CLI:**

br2# no trace all
br2# trace networking smtp receive
br2# trace networking vpim receive
br2# sh trace buffer tail
Press <CTRL-C> to exit...
4306 04/28 11:04:39.377 netw smtp 6 250 2.6.0 <FHK0849F1CU-AIM-FOC081829KP-1146186254270> Queued mail for delivery
3636 04/28 11:12:53.248 netw smtp 2
3636 04/28 11:12:53.254 netw smtp 3 socket hostName: 10.1.200.22, hostAddress: 10.1.200.22

3636 04/28 11:12:53.254 netw smtp 3 hostname: 10.1.200.22 found in good address cache
4349 04/28 11:12:53.264 netw smtp 5 Initial connection message
3636 04/28 11:12:53.267 netw smtp 1
4349 04/28 11:12:53.284 netw smtp 6 UNKNOWN: EHLO UNITY-LAB.voip.lab
4349 04/28 11:12:53.285 netw smtp 5 250-cue.lab
4349 04/28 11:12:53.294 netw smtp 6 EHLO : MAIL FROM:<1003@voip.lab>
4349 04/28 11:12:53.295 netw smtp 5 250 ok
4349 04/28 11:12:53.301 netw smtp 6 MAIL FROM:: RCPT TO:<3001@cue.lab>
4349 04/28 11:12:53.301 netw smtp 5 250 ok
4349 04/28 11:12:53.307 netw smtp 6 RCPT TO:: DATA
4349 04/28 11:12:53.307 netw smtp 5 354 Start data
4349 04/28 11:12:53.346 netw vpim 4 VPIM: Received: from mail pickup service by UNITY-LAB.voip.lab with Microsoft SMTPSVC;Fri, 28 Apr 2006 12:47:44 -0230
4349 04/28 11:12:53.347 netw vpim 4 VPIM: Date: Fri, 28 Apr 2006 15:17:43 GMT
4349 04/28 11:12:53.351 netw vpim 4 VPIM: From: "HQ Ph3" <1003@voip.lab>
4349 04/28 11:12:53.351 netw vpim 4 VPIM: To: 3001@cue.lab
4349 04/28 11:12:53.352 netw vpim 4 VPIM: MIME-Version: 1.0 (Voice 2.0)
4349 04/28 11:12:53.353 netw vpim 4 VPIM: Content-Type: multipart/Voice-Message; boundary="==AvVoice==3510ab46-4eff-4dee-8440-2ca7b006c23d"
4349 04/28 11:12:53.355 netw vpim 4 VPIM: Message-ID: 741ae5b9-63dc-4970-ad4e-afc8b5e8dcc7
4349 04/28 11:12:53.355 netw vpim 4 VPIM: Content-Transfer-Encoding: 7bit
4349 04/28 11:12:53.356 netw vpim 4 VPIM: Subject: Message from 1003
4349 04/28 11:12:53.357 netw vpim 4 VPIM: X-OriginalArrivalTime: 28 Apr 2006 15:17:44.0312 (UTC) FILETIME=[E6213780:01C66AD6]
4349 04/28 11:12:53.358 netw vpim 4 VPIM:
4349 04/28 11:12:53.359 netw vpim 4 VPIM:
4349 04/28 11:12:53.360 netw vpim 4 VPIM: --==AvVoice==3510ab46-4eff-4dee-8440-2ca7b006c23d
4349 04/28 11:12:53.373 netw vpim 4 VPIM: Content-Type: text/directory; charset=us-ascii; profile=vCard
4349 04/28 11:12:53.374 netw vpim 4 vCard: Content-Transfer-Encoding: 7bit
4349 04/28 11:12:53.374 netw vpim 4 vCard: Content-Disposition: attachment;filename="HQ Ph3.vcf"
4349 04/28 11:12:53.375 netw vpim 4 vCard:
4349 04/28 11:12:53.375 netw vpim 4 vCard: BEGIN:vCard
4349 04/28 11:12:53.376 netw vpim 4 vCard: FN:HQ Ph3
4349 04/28 11:12:53.376 netw vpim 4 vCard: N:Ph3;HQ;;;
4349 04/28 11:12:53.377 netw vpim 4 vCard: EMAIL;TYPE=INTERNET;TYPE=VPIM:1003@voip.lab
4349 04/28 11:12:53.378 netw vpim 4 vCard: TEL:1003
4349 04/28 11:12:53.378 netw vpim 4 vCard: VERSION: 3.0
4349 04/28 11:12:53.379 netw vpim 4 vCard: END:vCard
4349 04/28 11:12:53.379 netw vpim 4 vCard:
4349 04/28 11:12:53.380 netw vpim 4 vCard: --==AvVoice==3510ab46-4eff-4dee-8440-2ca7b006c23d
4349 04/28 11:12:53.380 netw vpim 4 VPIM: Content-Type: Audio/32KADPCM
4349 04/28 11:12:53.381 netw vpim 4 VPIM: Content-Transfer-Encoding: base64
4349 04/28 11:12:53.382 netw vpim 4 VPIM: Content-Description: VPIM Message
4349 04/28 11:12:53.382 netw vpim 4 VPIM: Content-Disposition: inline; voice=Voice-Message
4349 04/28 11:12:53.383 netw vpim 4 VPIM: Content-ID: a54d1816-01fb-4317-b327-21dc4aa6e856
4349 04/28 11:12:53.394 netw vpim 5 33783
4349 04/28 11:12:53.394 netw vpim 8
4349 04/28 11:12:53.858 netw vpim 6 16074
4349 04/28 11:12:54.298 netw vpim 6 16074

```
4349 04/28 11:12:54.844 netw vpim 6 16074
4349 04/28 11:12:55.244 netw vpim 6 16074
4349 04/28 11:12:55.577 netw vpim 6 12184
4349 04/28 11:12:55.621 netw vpim 10
4349 04/28 11:12:55.665 netw vpim 4 VPIM: --==AvVoice==3510ab46-4eff-4dee-8440-
2ca7b006c23d--
4349 04/28 11:12:55.665 netw vpim 4 VPIM: .
4349 04/28 11:12:55.919 netw smtp 5 260 Message queued
4349 04/28 11:12:55.968 netw smtp 6 DATA: QUIT
4349 04/28 11:12:55.969 netw smtp 5 221 closing channel
```

➔ **Finally place a call into CUE from Ph1 3001 at BR1 and see if the message arrived properly.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 17: Security

Estimated Time to Complete: 5 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 17 Voice Security

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

To complete this lab the infrastructure Section 1 must be completed along with the CCME Gateway section. The Basics in Section 2, 4, 8, and 9 must also be completed.

Section 17 Configuration Tasks

This lab begins with a critical step that, due to your lack of physical access to the Proctor Labs hardware, you will not be able to perform, but has instead been done for you and documented here for your education – as this is still a testable topic.

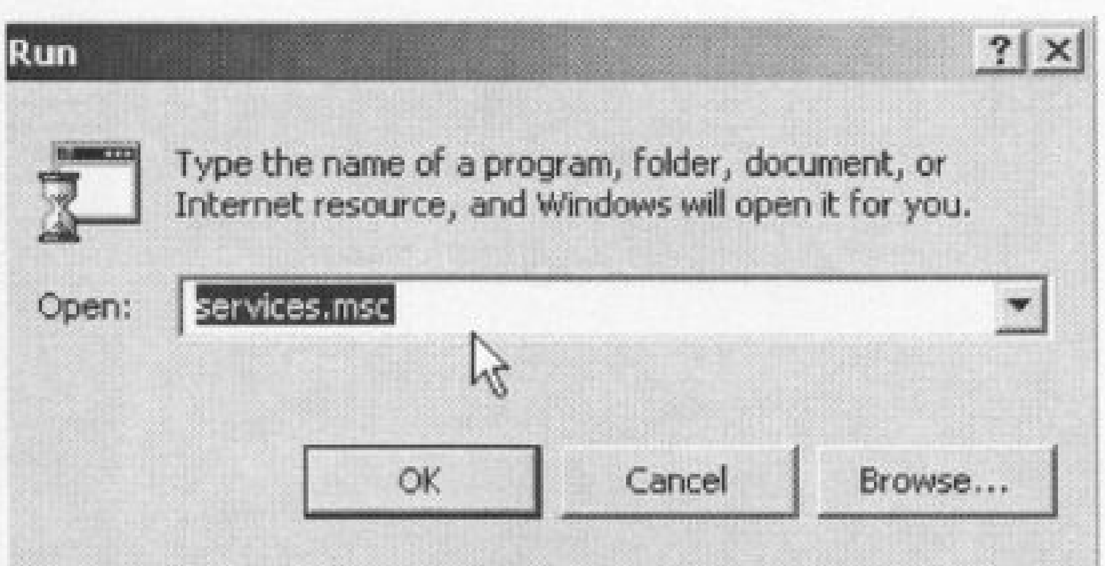
PLEASE NOTE: Although we ask you to enable SRTP and write security certificates to the phones for SRTP and S-SRST, you will unfortunately not be able to receive your certificates on your IP Blue or CIPC clients. You *will* still be able to perform the tasks and write the Certificates to the physical 79xx series phones that *are housed at Proctor Labs' facilities* and *verify* using inbound calls from one site through the PSTN in to another site – and verify the SRTP from the GW to the 79xx phone using the IOS commands and the HTTP server on the 79xx phone.

Also, you may want to consider signing up for one of IPexpert's CCIE Voice Boot Camps – where *you will* have access to physical 7940 and 7960 series IP Phones in order to complete and better verify your security configurations.

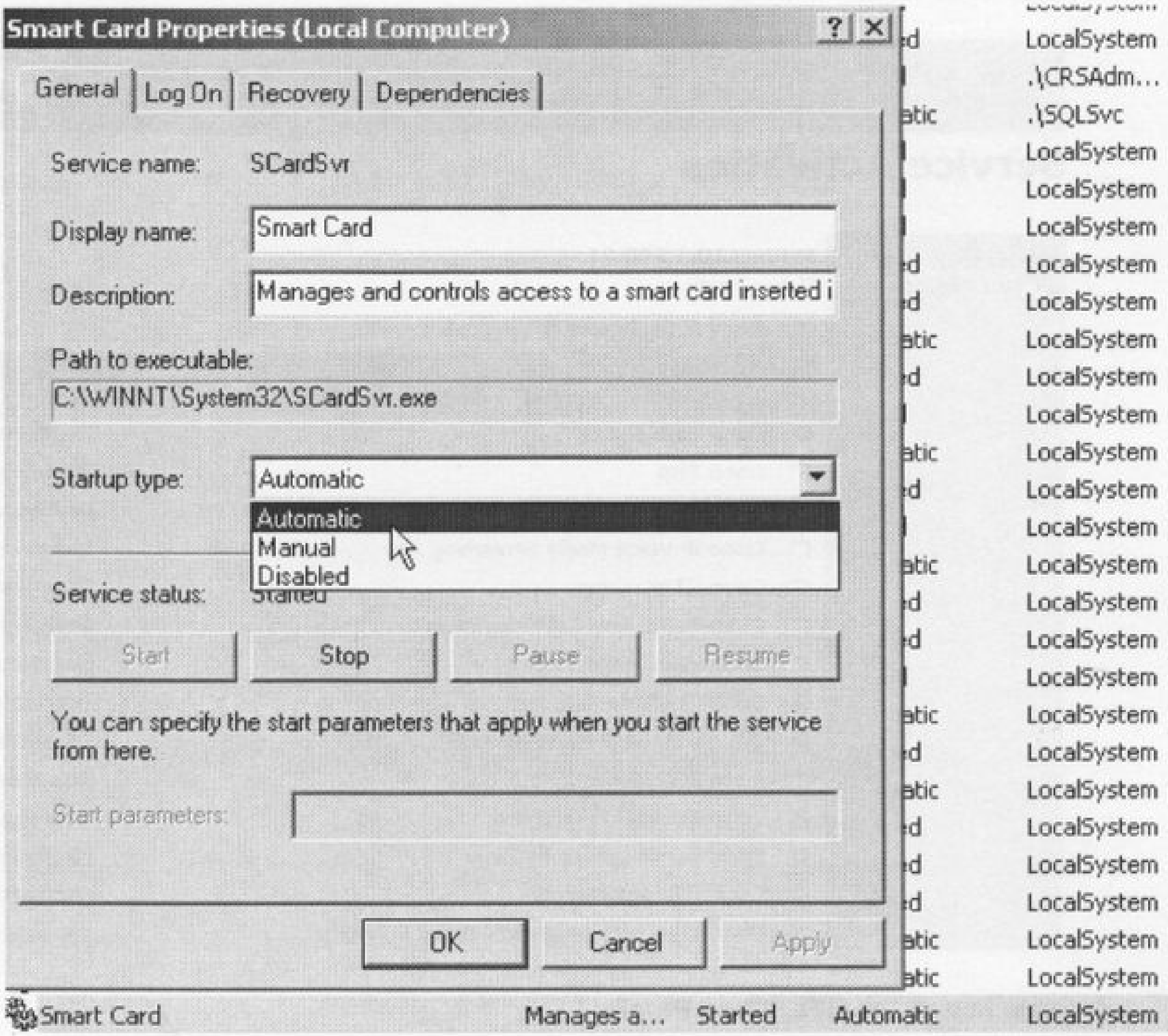
Pre-Task 17.1

(This task already been done for you because of your lack of physical access to the (2) USB slots for Token usage on the Server – since only 1 Token can be inserted at any time.)

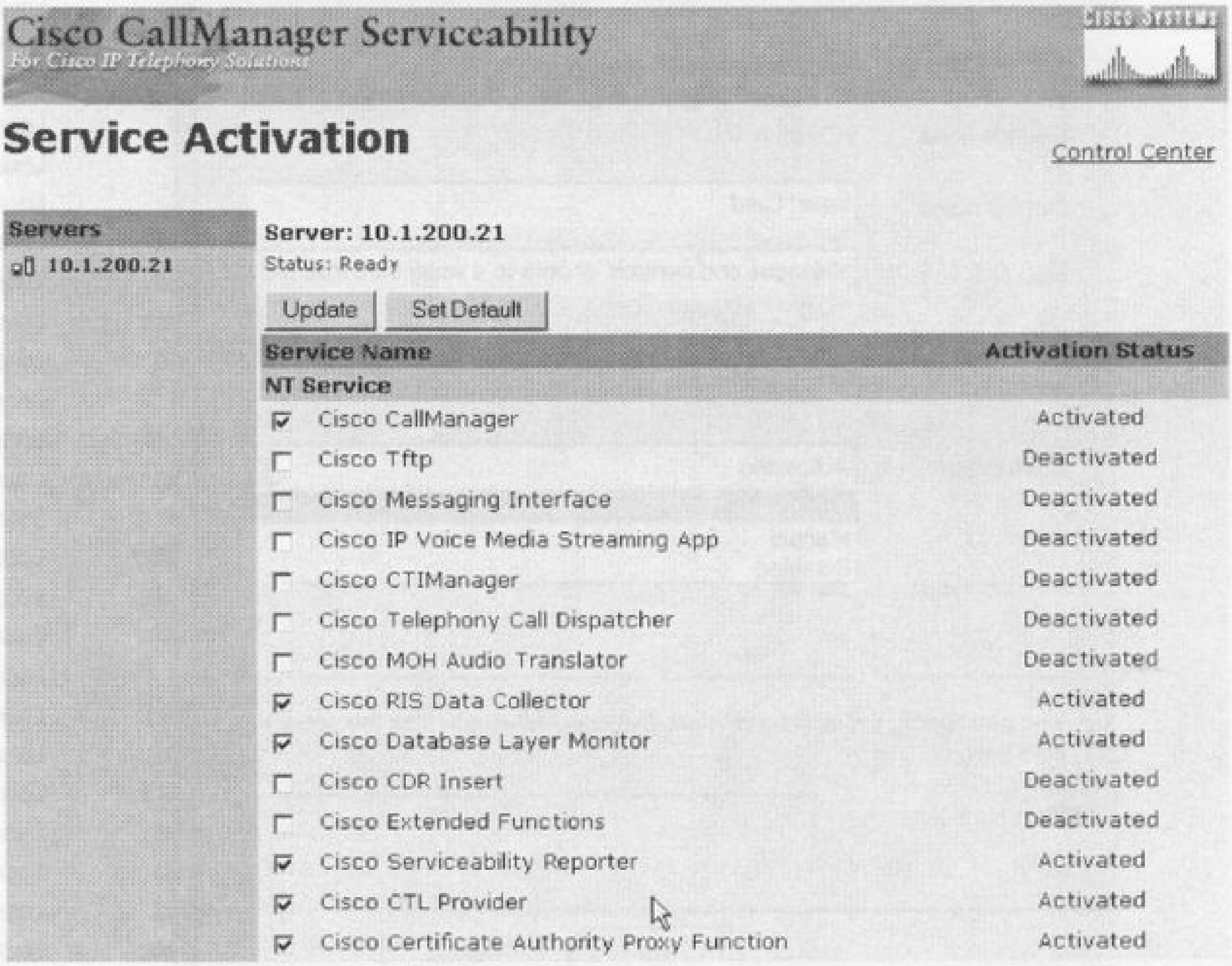
➔ **Start the Services MSC:**



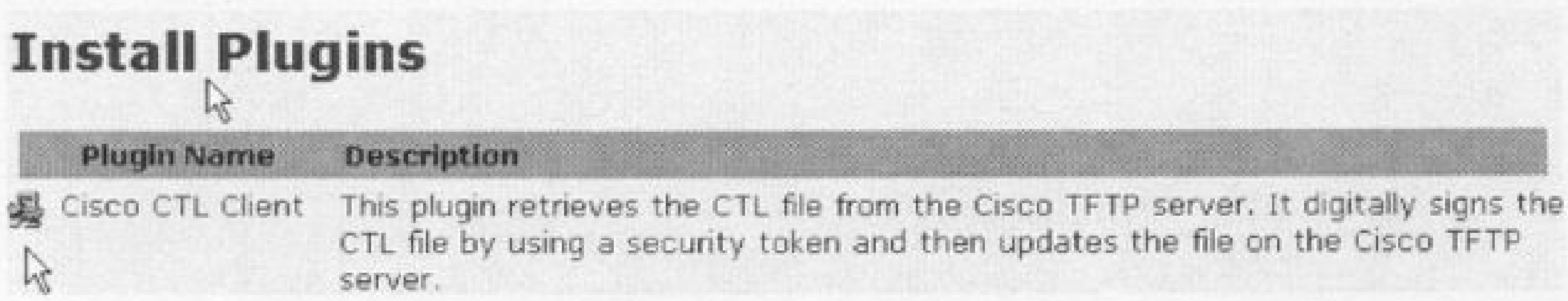
➔ **Change the "Smart Card" Service from Disabled, to Automatic, and start the service.**



➔ **Activate two Services in the CallManager Serviceability Page, namely the "Cisco CTL Provider" service and the "Cisco Certificate Authority Proxy Function" service and make sure that they are started:**

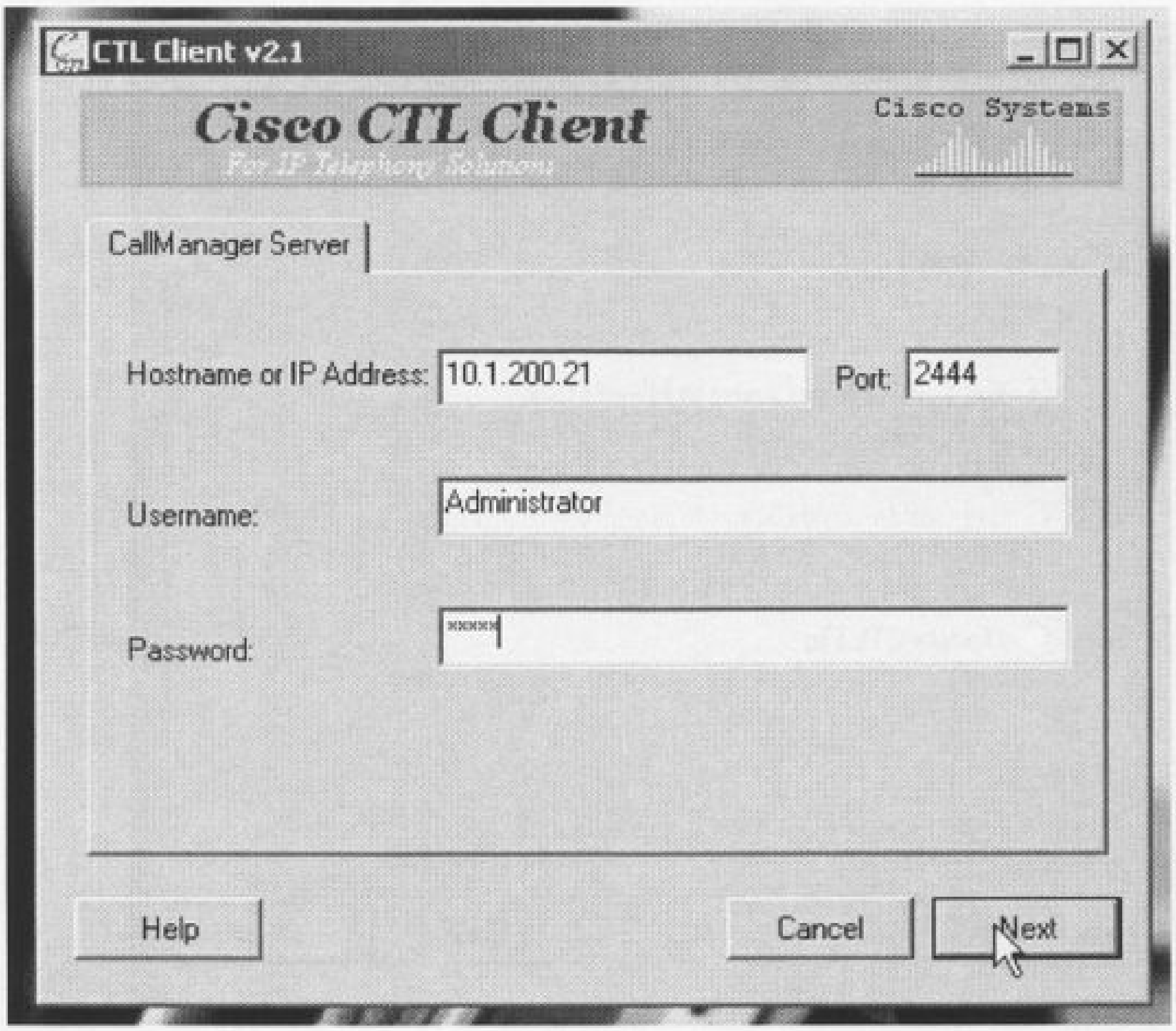


➔ **Now install the CTL Client Plugin:**

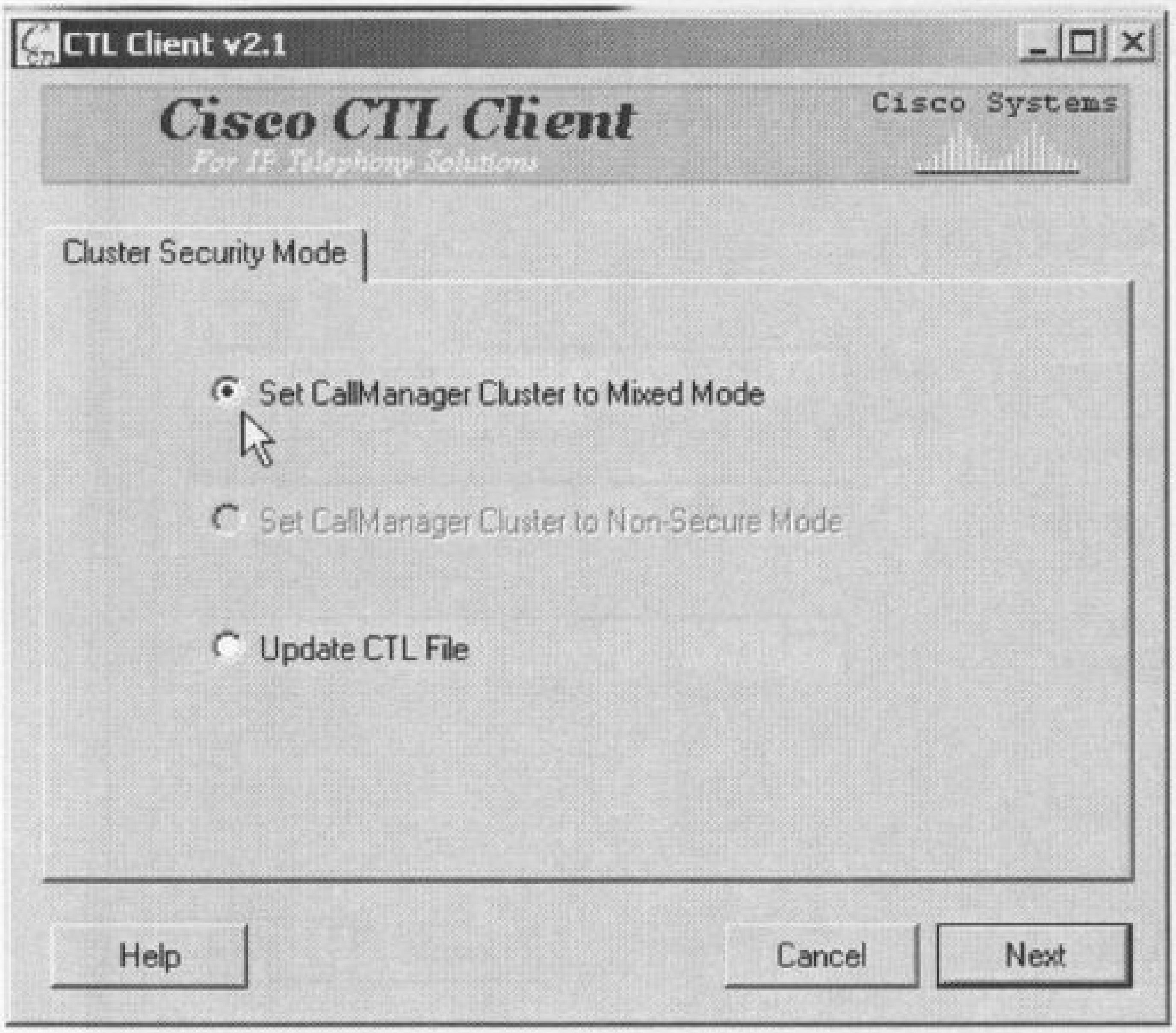


➔ **Launch the CTL Client:**

➔ **Fill in the correct info for the CCM Pub Server you wish to connect with:**

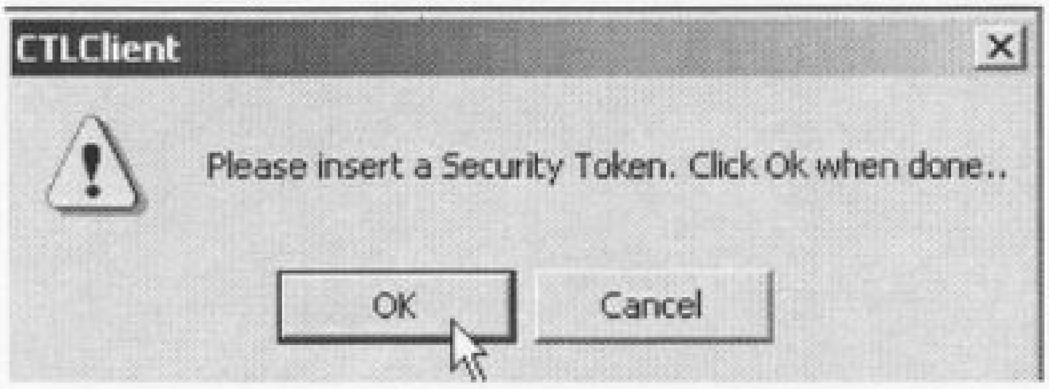


➔ **Next check the radio button to "Set CallManager Cluster to Mixed Mode".**

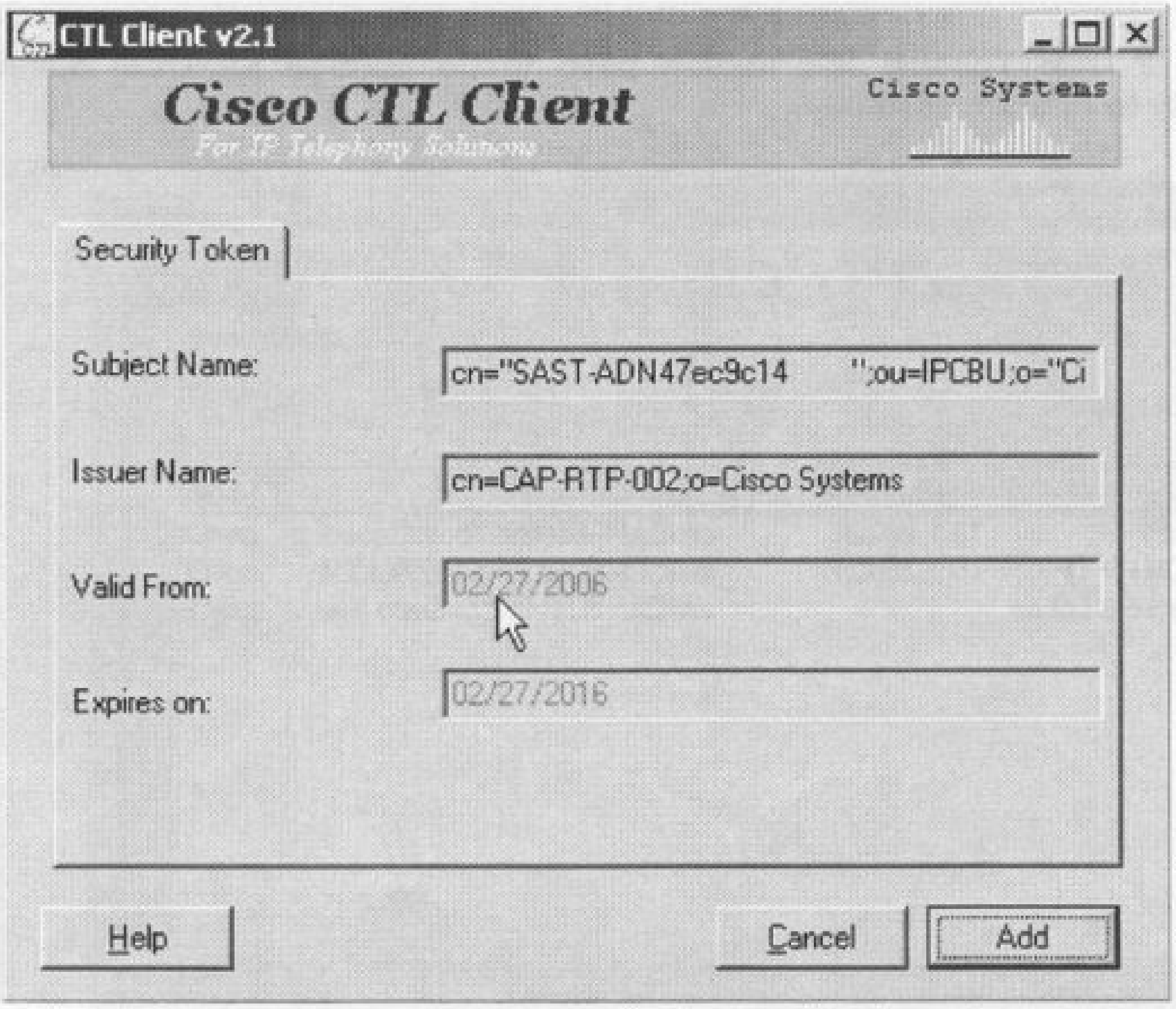


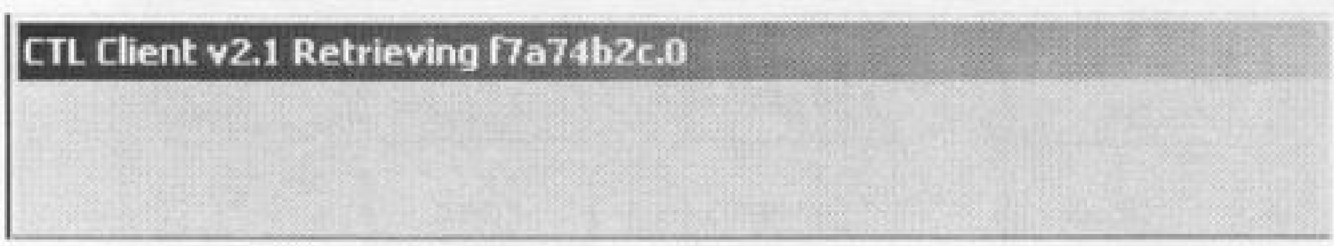
➔ **Now you need to physically insert a Cisco USB Security Token into an available USB slot on the Server (or whatever machine you are running this application from):**

WARNING: DO NOT INSERT 2 USB TOKENS AT ONE TIME!



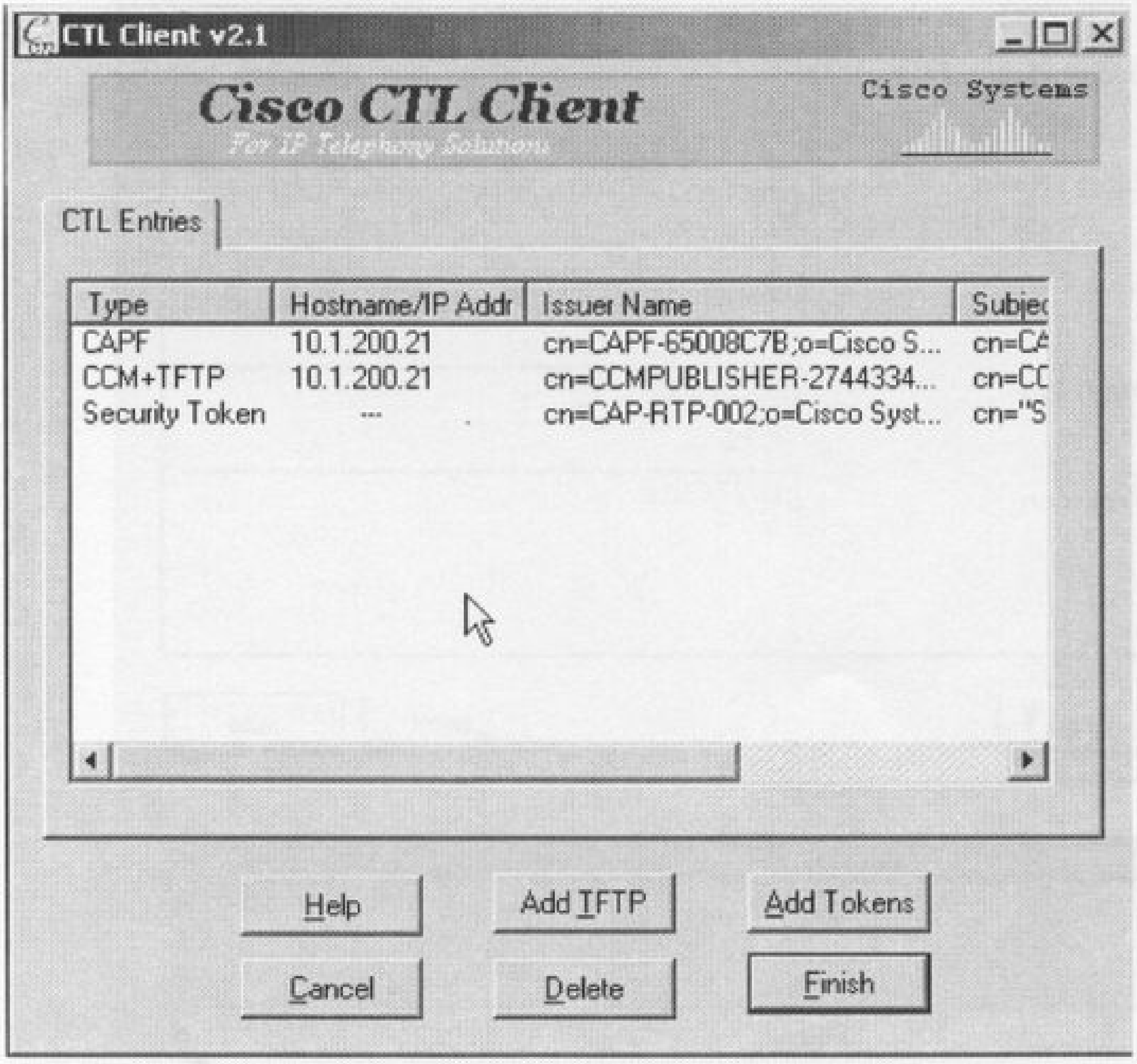
➔ **Information about the Token is provided, click Add:**



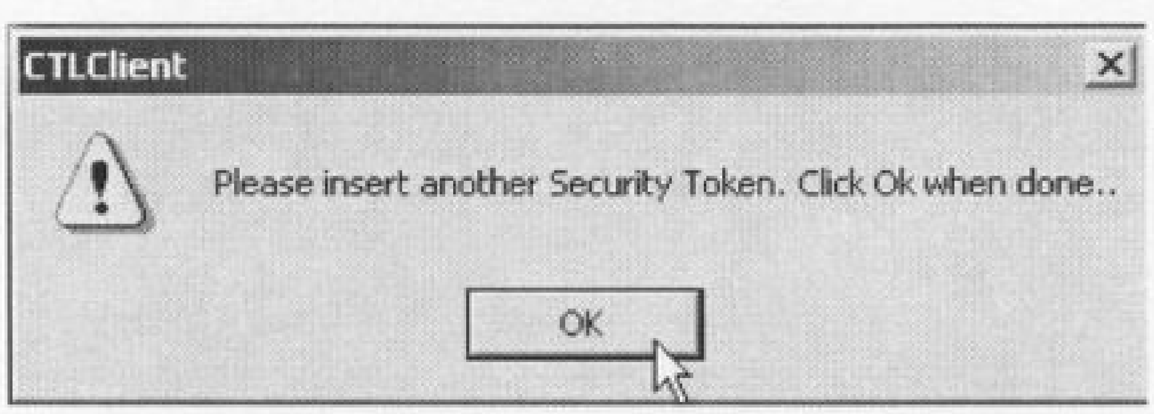


➔ **Now the CTL Client shows information regarding the CCM Pub Server, the CCM Cluster's TFTP Server, and the 1 Token that has been added.**

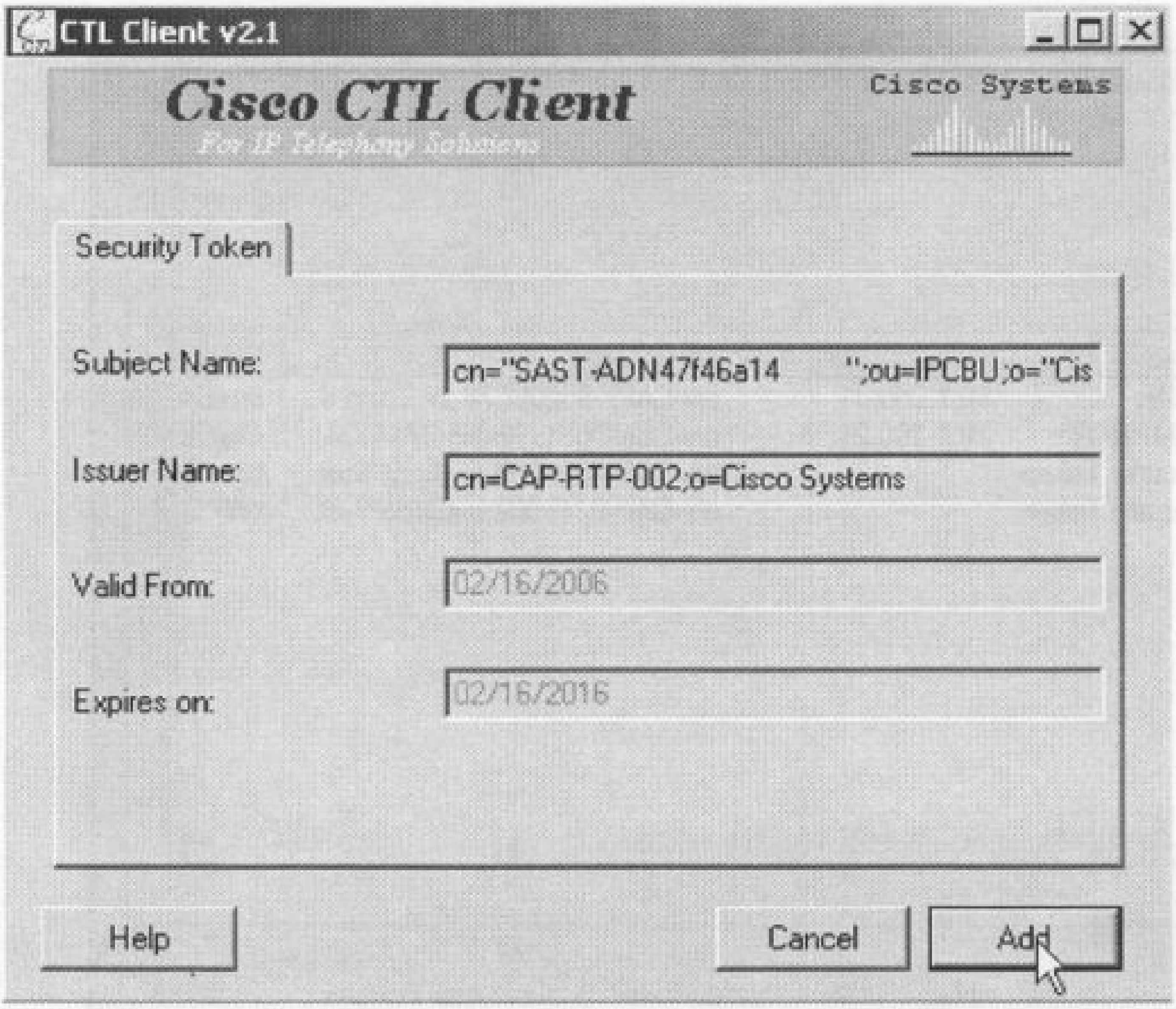
NOTE: 2 USB Tokens' information have to be entered for CCM Mixed Mode Security to operate correctly.



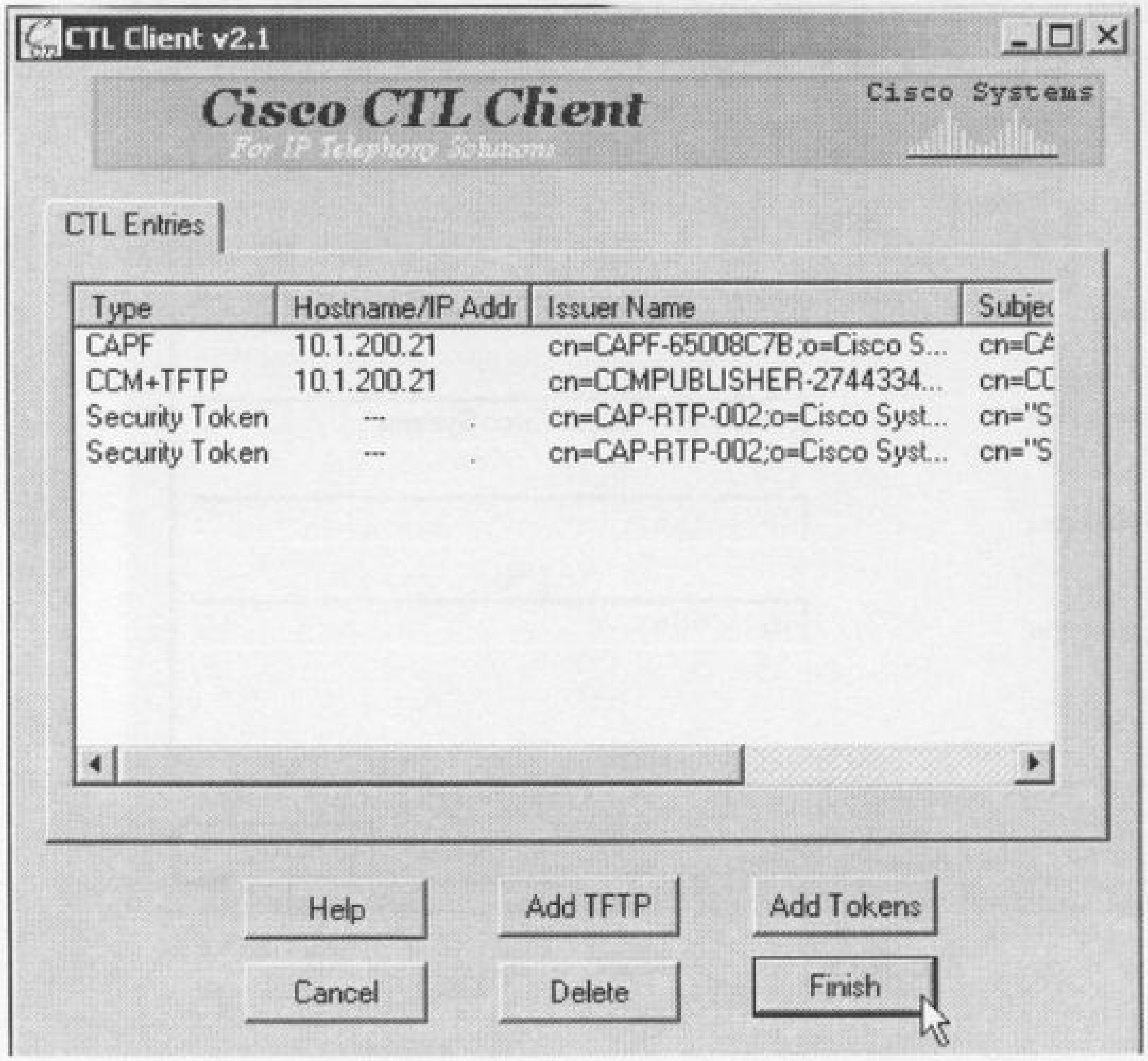
➔ **Now click the "Add Tokens" button to add your second token (*remove the first USB token BEFORE adding the second*).**



➔ **A window appears giving information about the 2nd USB Token:**

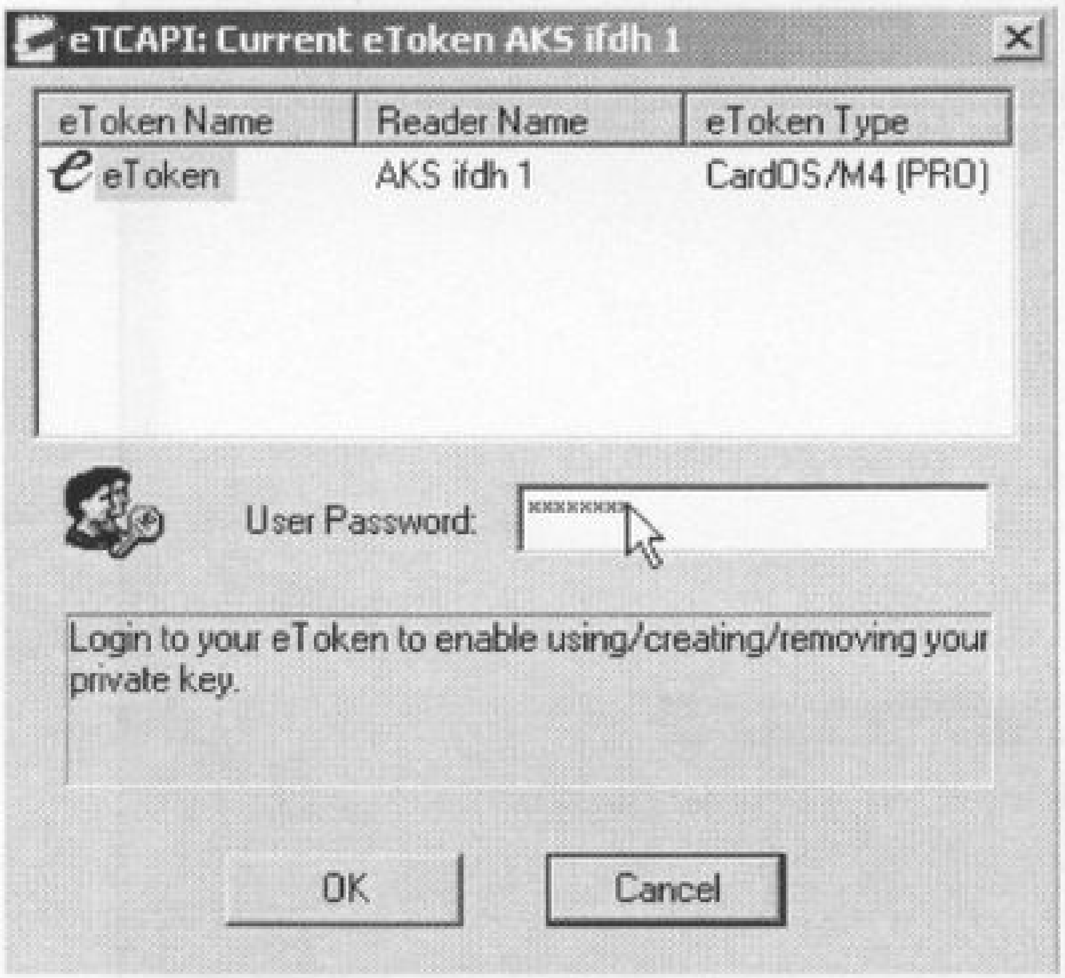


➔ **The CTL Client now shows information about the CCM Server, the TFTP Server, and both USB Tokens.**

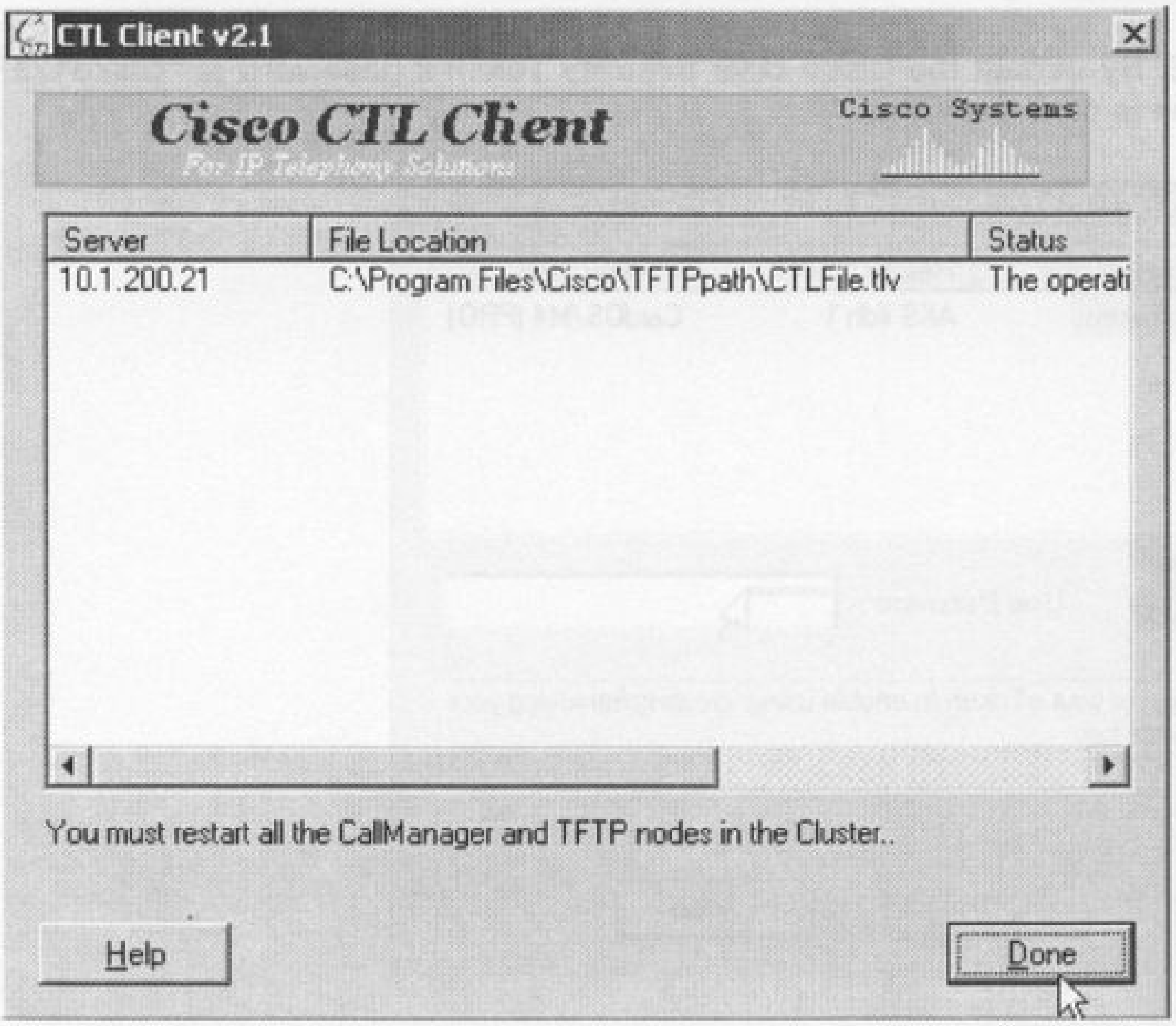


➔ **Finally a window appears asking you to authenticate the token which is presently in the machine's USB slot in order to digitally sign the CTL file about to be written to all CallManagers and TFTP Servers listed in the previous screen.**

NOTE: By default the Cisco USB Security Token's password is "Cisco123" and of course is case-sensitive.



➔ **And now the client finishes, telling us where the new TLV security file has been stored, and that we must reboot every CallManager and TFTP Server in the Cluster.**



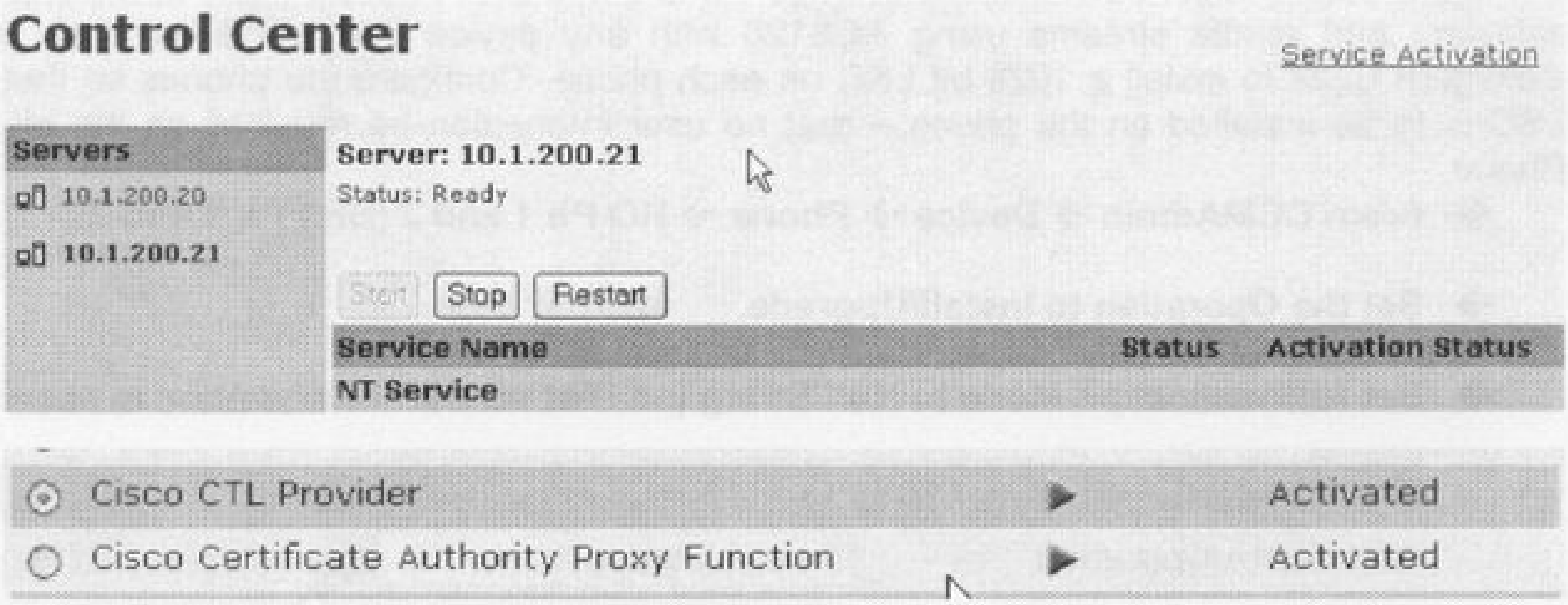
➔ **Once you have begun your reboot process, you may remove both of your USB tokens and save them in a very safe place – as you will be able to make no changes to this server's security file without them!**

Task 17.1

CallManager has already been converted to Mixed Mode and has 2 USB Security Tokens installed in the CTL. Ensure that the proper Services in CallManager are activated and running in order to allow the CTL and CAPF functions to operate correctly (DO NOT change their status – this may break security without physical access to the USB ports and Tokens – which you do not have).

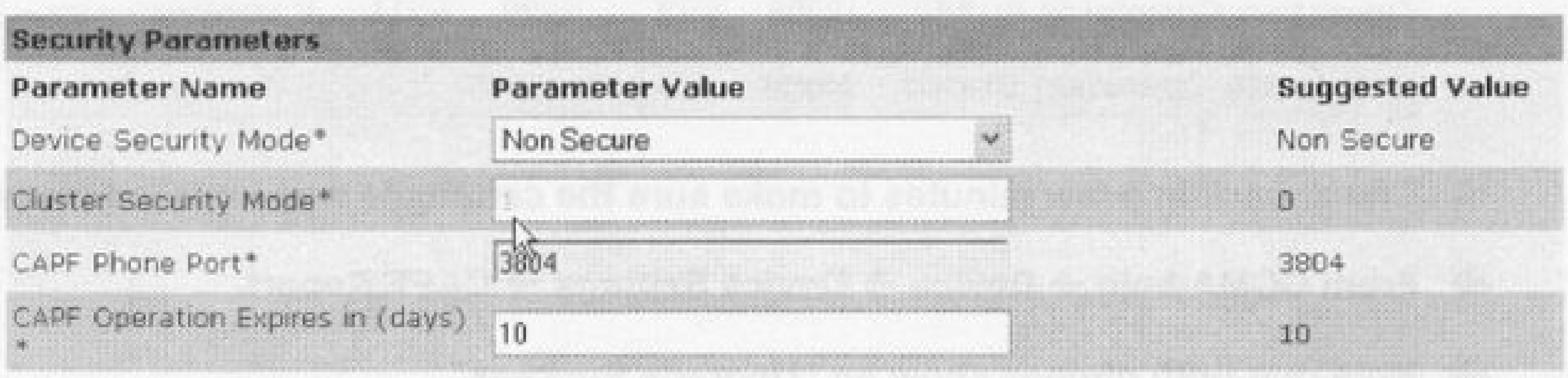
➔ **From CCMAdmin ➔ Application ➔ CallManager Serviceability ➔ Service Activation.**

➔ **Ensure that the CTL Provider and the Cert Authority Proxy Function are activated and running.**



➔ **From CCMAdmin ➔ System ➔ Enterprise Parameters.**

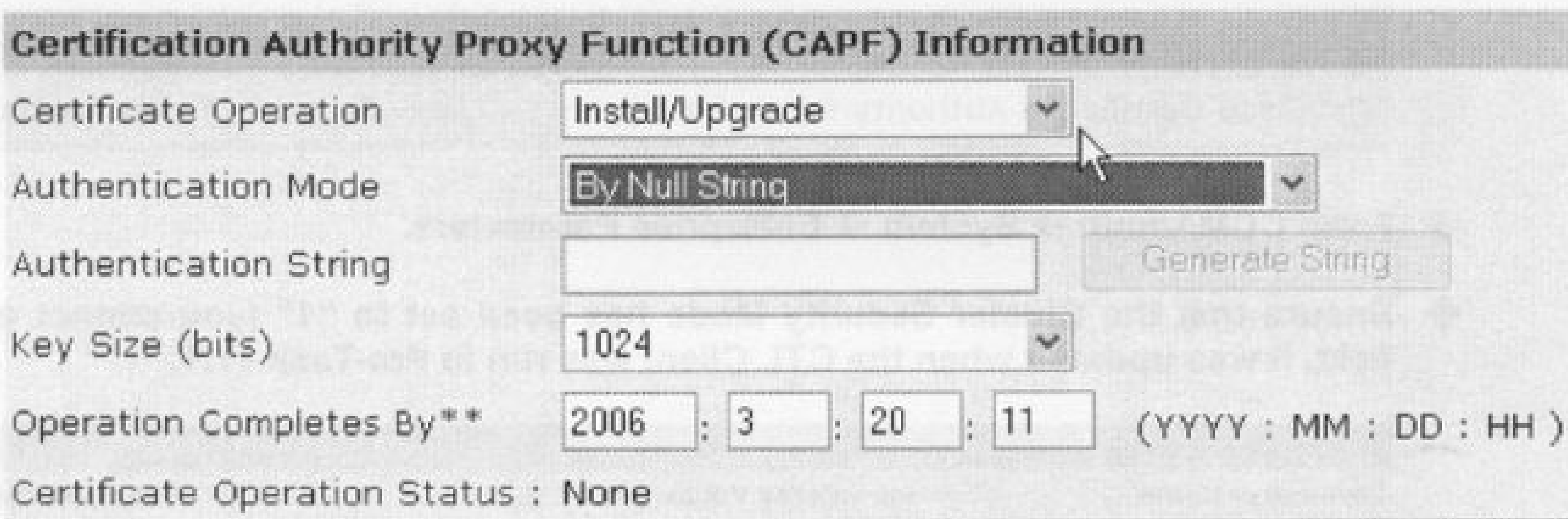
➔ **Ensure that the Cluster Security Mode has been set to "1" (you cannot edit this field, it was updated when the CTL Client was run in Pre-Task 17.1.**



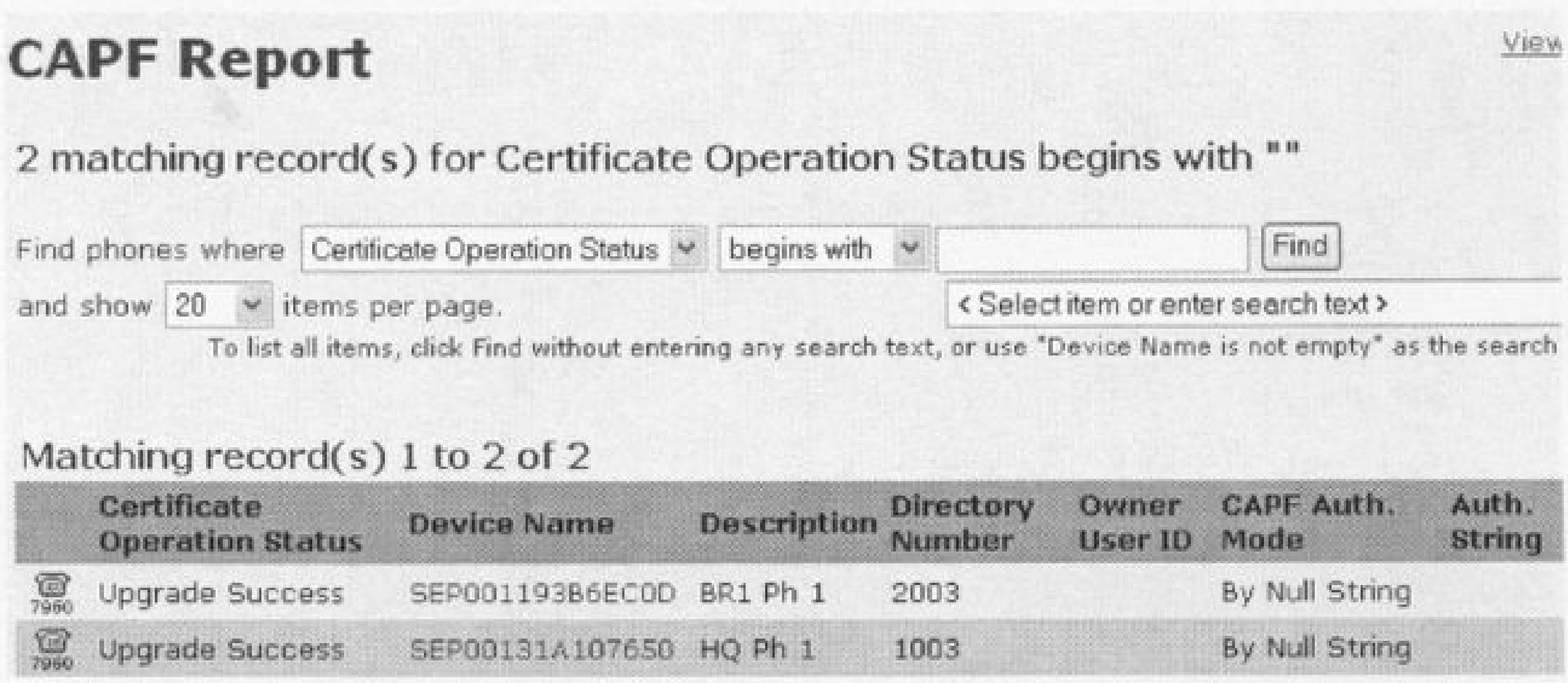
Task 17.2

Configure CallManager such that HQ Phones 1 and 2 and BR1 Phones 1 and 2, will encrypt their signaling and media streams using AES128 with any device that will allow such to occur. Configure CCM to install a 1028 bit LSC on each phone. Configure the phones so that when a LSC is to be installed on the phone – that no user interaction be required on the physical IP Phone.

- ➔ **From CCMAdmin → Device → Phone → HQ Ph 1 and 2 (BR1 Ph 1 and 2).**
- ➔ **Set the Operation to Install/Upgrade.**
- ➔ **Set Authentication Mode to Null String (so that no user intervention is required).**

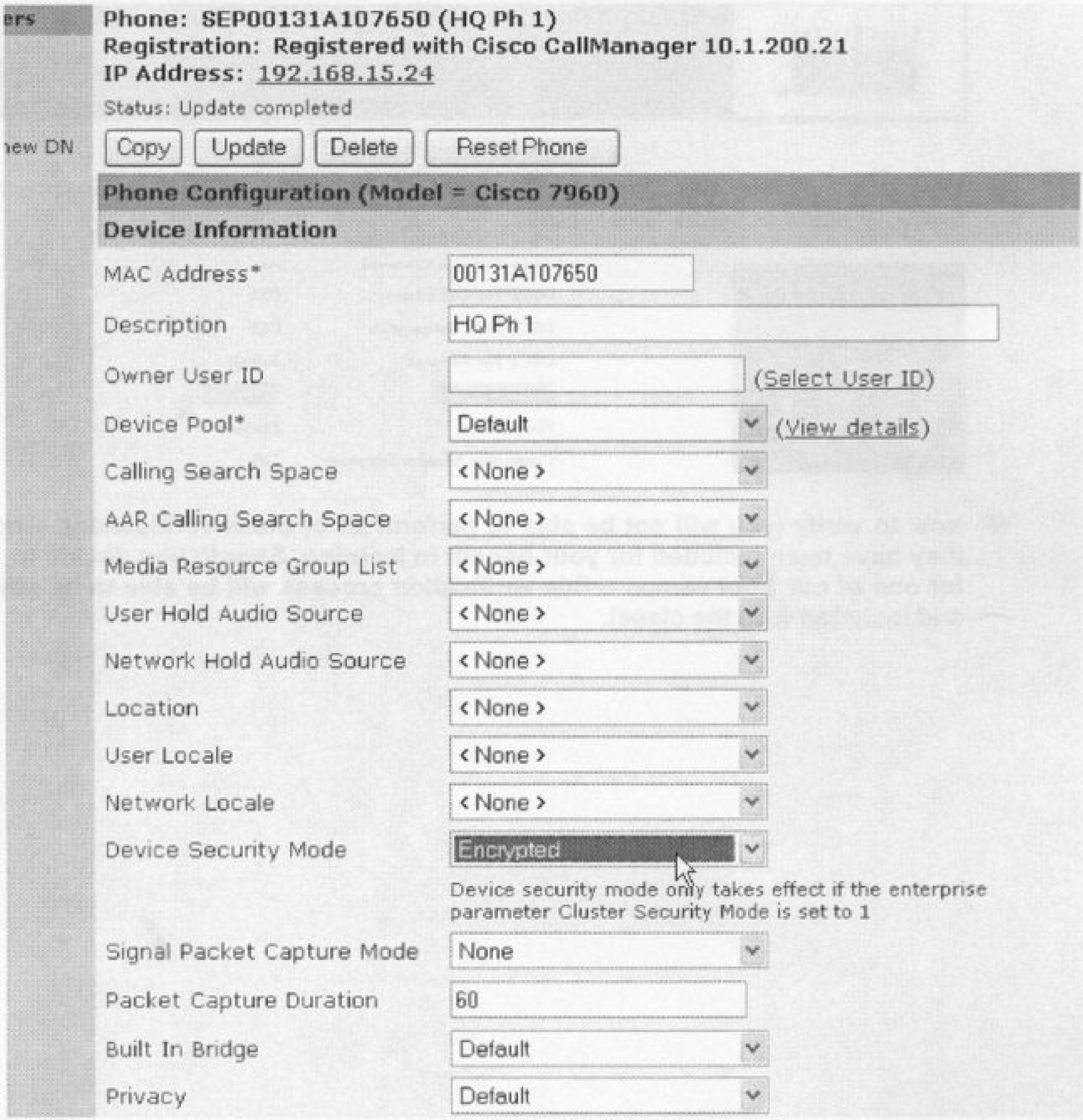


- ➔ **Check back in a few minutes to make sure the certificate was installed properly.**
- ➔ **From CCMAdmin → Device → Device Settings → CAPF Report.**
- ➔ **Note that both phones show an "Upgrade Success".**

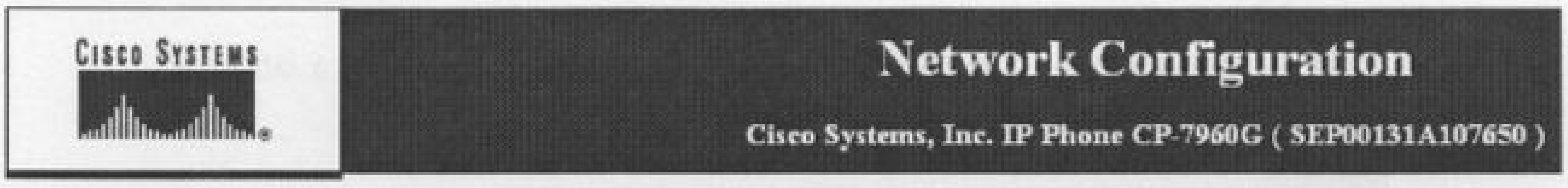


Certificate Operation Status	Device Name	Description	Directory Number	Owner User ID	CAPF Auth. Mode	Auth. String
Upgrade Success	SEP001193B6EC0D	BR1 Ph 1	2003		By Null String	
Upgrade Success	SEP00131A107650	HQ Ph 1	1003		By Null String	

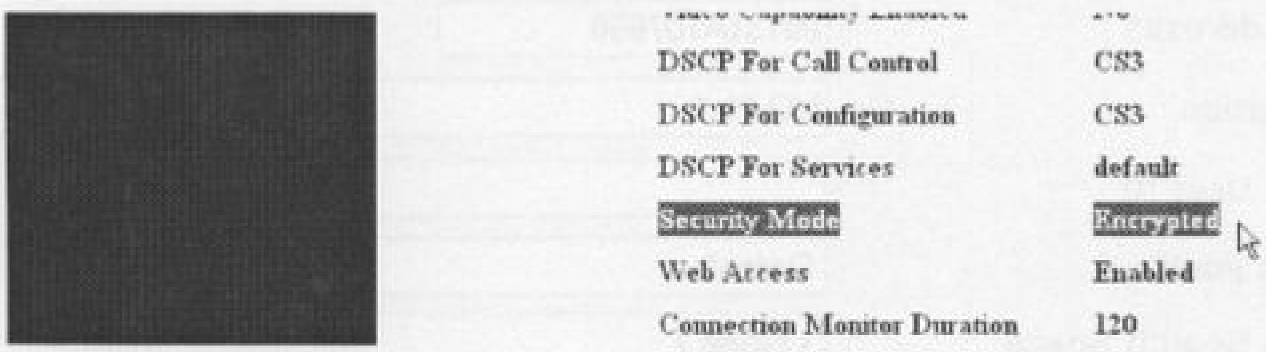
➔ **Now that we know the phones successfully have their LSCs, we need to set them to Encrypt their Signaling and RTP traffic.**



➔ **Now pull up the Phone's HTTP server by clicking on the IP Address in the CCMAdmin window above.**



➔ **Now click on Network Configuration and scroll to the bottom to ensure that the Security Mode is set to "Encrypted".**



➔ **Now to verify (you will not be able to perform all of these verifications – however, they have been included for your benefit in learning. Should you decide to sign up for one of our boot camps – this verification process will be able to be performed and included with the class).**

➔ **This is how an Ethereal capture would look when both IP Phones are in a normal, Non-Secure status: (Note that you see both Skinny and RTP packets in the Capture window, and a Skinny packet in the Decoder window:**

```
47 3.494943  10.1.200.21    192.168.15.24  SKINNY  CallStateMessage
48 3.495693  10.1.200.21    192.168.15.24  SKINNY  SelectSoftKeysMessage
49 3.496372  10.1.200.21    192.168.15.24  SKINNY  DisplayPromptStatusMessage
50 3.497393  10.1.200.21    192.168.15.24  SKINNY  CallInfoMessage
51 3.497651  10.1.200.21    192.168.15.24  SKINNY  StopToneMessage
52 3.499775  192.168.15.24  10.1.200.21    TCP     49224 > 2000 [ACK] Seq=148 Ack=1964 Win=984 Len=0
53 3.518719  192.168.15.24  10.1.200.21    TCP     [TCP Window Update] 49224 > 2000 [ACK] Seq=148 Ack=1964 Win=1400 Len=0
54 3.555676  10.1.200.21    192.168.15.24  SKINNY  StartMediaTransmission
55 3.557513  192.168.15.27  Broadcast      ARP     Who has 192.168.15.24?  Tell 192.168.15.27
56 3.558927  192.168.15.24  192.168.15.27  ARP     192.168.15.24 is at 00:13:1a:10:76:50
57 3.559269  192.168.15.24  10.1.200.21    TCP     49224 > 2000 [ACK] Seq=148 Ack=2060 Win=1400 Len=0
58 3.560198  192.168.15.24  Broadcast      ARP     Who has 192.168.15.27?  Tell 192.168.15.24
59 3.560760  192.168.15.27  192.168.15.24  ARP     192.168.15.27 is at 00:11:93:b6:ec:0d
60 3.595665  192.168.15.27  192.168.15.24  RTP     Payload type=ITU-T G.711 PCMU, SSRC=233617052, Seq=2899, Time=482544, Mark
61 3.600049  192.168.15.24  192.168.15.27  RTP     Payload type=ITU-T G.711 PCMU, SSRC=1349914665, Seq=56527, Time=9136864, Mark
62 3.615596  192.168.15.27  192.168.15.24  RTP     Payload type=ITU-T G.711 PCMU, SSRC=233617052, Seq=2900, Time=482704
63 3.620053  192.168.15.24  192.168.15.27  RTP     Payload type=ITU-T G.711 PCMU, SSRC=1349914665, Seq=56528, Time=9137024
64 3.636552  192.168.15.27  192.168.15.24  RTP     Payload type=ITU-T G.711 PCMU, SSRC=233617052, Seq=2901, Time=482864
```

```
⊞ Frame 50 (450 bytes on wire, 450 bytes captured)
⊞ Ethernet II, Src: 192.168.15.1 (00:d0:58:7d:4b:80), Dst: 192.168.15.24 (00:13:1a:10:76:50)
⊞ Internet Protocol, Src: 10.1.200.21 (10.1.200.21), Dst: 192.168.15.24 (192.168.15.24)
⊟ Transmission Control Protocol, Src Port: 2000 (2000), Dst Port: 49224 (49224), Seq: 1548, Ack: 116, Len: 396
    Source port: 2000 (2000)
    Destination port: 49224 (49224)
    Sequence number: 1548    (relative sequence number)
    [Next sequence number: 1944    (relative sequence number)]
    Acknowledgement number: 116    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 64016
    Checksum: 0x0f89 [correct]
⊟ Skinny Client Control Protocol
    Data Length: 388
    Reserved: 0x00000000
    Message ID: CallInfoMessage (0x0000008f)
    Calling Party Name:
    Calling Party: 1003
    Called Party Name:
    CalledParty: 2003
    Line Instance: 1
    Call Identifier: 16777247
    Call Type: OutBoundCall (2)
    Original Called Party Name:
    Original Called Party: 2003
    LastRedirectingPartyName:
    LastRedirectingParty: 2003
    OriginalCdpnRedirectReason: 0
    LastRedirectingReason: 0
```

➔ **This is how an Ethereal capture would look when both IP Phones have been set to a Secure Encrypted status: (Note that the Skinny and RTP packets are no longer distinguishable as such – but instead are just TCP and UDP packets – and while the encrypted RTP packets still use ports 16384 – 32767, the Skinny packets no longer user port 2000 but port 2443 instead.**

```
48 2.774281  10.1.200.21    192.168.15.24  TCP  2443 > 49228 [PSH, ACK] Seq=3312 Ack=265 Win=64135 Len=474
49 2.774423  10.1.200.21    192.168.15.24  TCP  2443 > 49228 [PSH, ACK] Seq=3786 Ack=265 Win=64135 Len=90
50 2.779527  192.168.15.24  10.1.200.21    TCP  49228 > 2443 [ACK] Seq=265 Ack=3876 Win=1400 Len=0
51 2.892913  192.168.15.24  10.1.200.21    TCP  49228 > 2443 [PSH, ACK] Seq=265 Ack=3876 Win=1400 Len=69
52 3.008792  10.1.200.21    192.168.15.24  TCP  2443 > 49228 [PSH, ACK] Seq=3876 Ack=334 Win=64066 Len=170
53 3.014400  192.168.15.27  Broadcast      ARP  Who has 192.168.15.24?  Tell 192.168.15.27
54 3.015729  192.168.15.24  192.168.15.27  ARP  192.168.15.24 is at 00:13:1a:10:76:50
55 3.019424  192.168.15.24  10.1.200.21    TCP  49228 > 2443 [ACK] Seq=334 Ack=4046 Win=1400 Len=0
56 3.030325  192.168.15.24  Broadcast      ARP  Who has 192.168.15.27?  Tell 192.168.15.24
57 3.030948  192.168.15.27  192.168.15.24  ARP  192.168.15.27 is at 00:11:93:b6:ec:0d
58 3.070196  192.168.15.27  192.168.15.24  UDP  Source port: 29126  Destination port: 30140
59 3.080323  192.168.15.24  192.168.15.27  UDP  Source port: 30140  Destination port: 29126
60 3.090858  192.168.15.27  192.168.15.24  UDP  Source port: 29126  Destination port: 30140
61 3.098706  192.168.15.24  192.168.15.27  UDP  Source port: 30140  Destination port: 29126
62 3.110362  192.168.15.27  192.168.15.24  UDP  Source port: 29126  Destination port: 30140
63 3.118351  192.168.15.24  192.168.15.27  UDP  Source port: 30140  Destination port: 29126
64 3.131115  192.168.15.27  192.168.15.24  UDP  Source port: 29126  Destination port: 30140
65 3.139615  192.168.15.24  192.168.15.27  UDP  Source port: 30140  Destination port: 29126
66 3.151100  192.168.15.27  192.168.15.24  UDP  Source port: 29126  Destination port: 30140
67 3.159406  192.168.15.24  192.168.15.27  UDP  Source port: 30140  Destination port: 29126
68 3.171151  192.168.15.27  192.168.15.24  UDP  Source port: 29126  Destination port: 30140
```

```
⊞ Frame 49 (144 bytes on wire, 144 bytes captured)
⊞ Ethernet II, Src: 192.168.15.1 (00:d0:58:7d:4b:80), Dst: 192.168.15.24 (00:13:1a:10:76:50)
⊞ Internet Protocol, Src: 10.1.200.21 (10.1.200.21), Dst: 192.168.15.24 (192.168.15.24)
⊟ Transmission Control Protocol, Src Port: 2443 (2443), Dst Port: 49228 (49228), Seq: 3786, Ack: 265, Len: 90
    Source port: 2443 (2443)
    Destination port: 49228 (49228)
    Sequence number: 3786    (relative sequence number)
    [Next sequence number: 3876    (relative sequence number)]
    Acknowledgement number: 265    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 64135
    Checksum: 0x75f7 [correct]
  Data (90 bytes)
```

```
0000  00 13 1a 10 76 50 00 d0  58 7d 4b 80 08 00 45 00   ....vP.. X}K...E.
0010  00 82 8f 23 00 00 7e 06  0b 7c 0a 01 c8 15 c0 a8   ...#..~. .|......
0020  0f 18 09 8b c0 4c 3f d0  9a a5 28 fb eb 38 50 18   .....L?. ..(..8P.
0030  fa 87 75 f7 00 00 17 03  01 00 20 75 d2 b3 e7 ec   ..u..... .. u....
0040  96 28 b9 53 bd 8f 90 b2  4d 55 ae c3 ec 23 f1 f5   .(.S.... MU...#..
0050  b5 87 69 4e a9 15 70 c7  95 36 7e 17 03 01 00 30   ..iN..p. .6~....0
0060  bc 9e 0c 63 72 1c e1 5c  1f 8d 14 30 be 26 10 3e   ...cr..\ ...0.&.>
0070  ad d6 4c 64 83 96 81 28  1e 26 8f 21 29 b3 53 64   ..Ld...( .&.!).Sd
0080  b2 bf ec 37 83 2d bd f4  fa 4b 90 1f 2c e8 ea f9   ...7.-.. .K......
```

Task 17.3

Ensure that if BR1 gateway goes into fallback mode, that it has already created its own certificate, forwarded that certificate to CallManager and that CallManager in turn has installed that certificate into the IP Phones at BR1, so that signaling and media continue to be encrypted during any fallback occurrence.

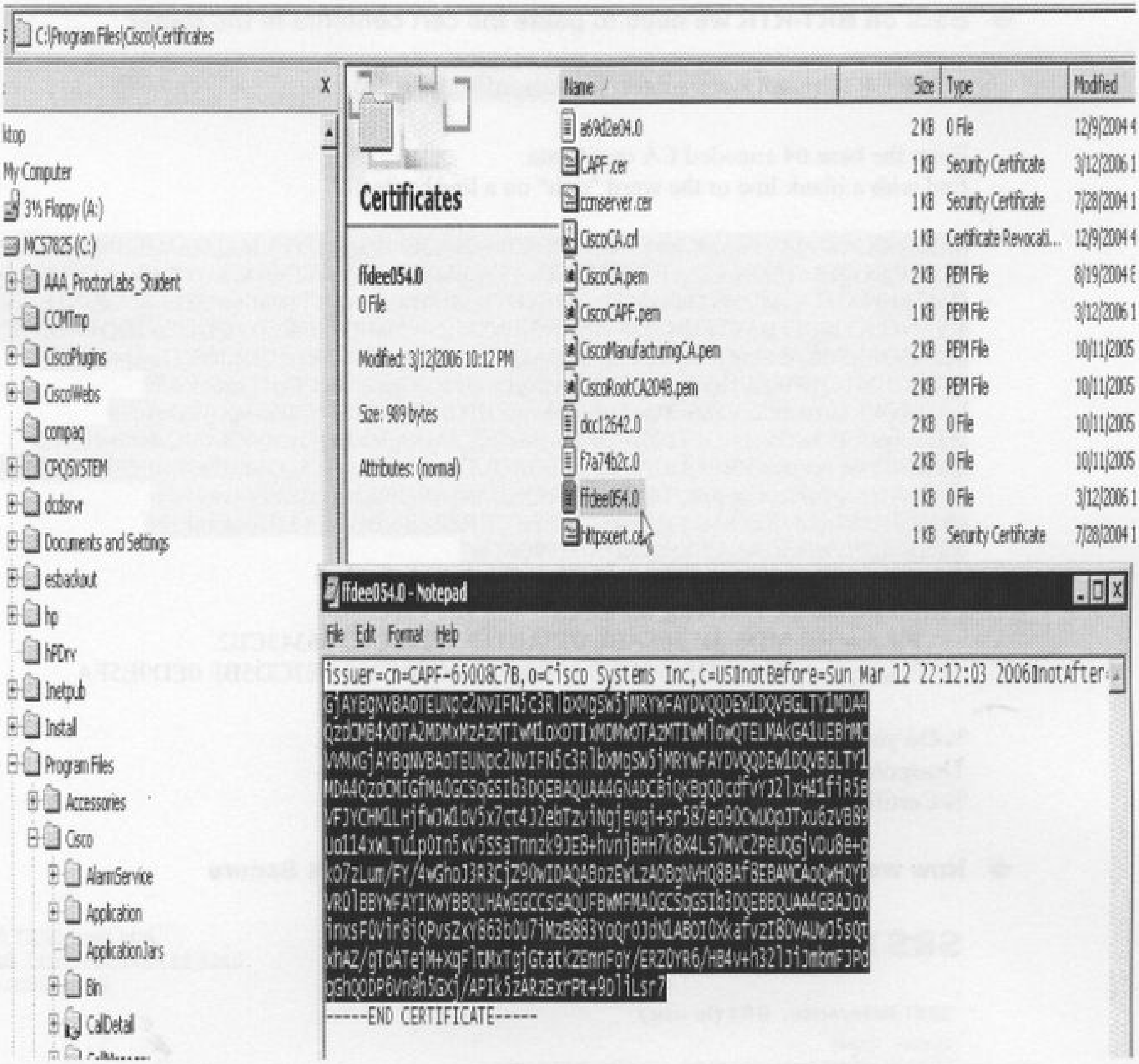
➔ **On BR1 GW:**

```
P1-BR1-RTR(config)#ntp server 10.1.200.3

P1-BR1-RTR(config)#ip http server

P1-BR1-RTR(config)#no call-manager-fallback

P1-BR1-RTR(config)#crypto pki server S-SRST
P1-BR1-RTR(config)# database level complete
P1-BR1-RTR(config)# database url nvram
P1-BR1-RTR(config)# issuer-name CN=S-SRST
P1-BR1-RTR(config)# grant auto
Mar 21 15:40:47.057: %PKI-6-CS_GRANT_AUTO: All enrollment requests will be
automatically granted.
P1-BR1-RTR(config)# no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: (cisco123)
Re-enter password: (cisco123)
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.
P1-BR1-RTR(cs-server)#
Mar 21 15:41:33.313: %SSH-5-ENABLED: SSH 1.99 has been enabled
P1-BR1-RTR(cs-server)#
P1-BR1-RTR(config)#crypto pki trustpoint S-SRST-CA
P1-BR1-RTR(ca-trustpoint)#enrollment url http://10.1.201.1
P1-BR1-RTR(ca-trustpoint)#revocation-check none
P1-BR1-RTR(ca-trustpoint)#exit
P1-BR1-RTR(config)#crypto pki authenticate S-SRST-CA
Certificate has the following attributes:
       Fingerprint MD5: A987B5A1 2786F7B0 912A1A21 CE826700
      Fingerprint SHA1: 13C4E038 E8B2568A 23239E30 1F86858B D140774B
```

```
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
P1-BR1-RTR(config)#
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: (cisco)
Mar 20 21:35:29.195: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password: (cisco)

% The subject name in the certificate will include: P1-BR1-RTR.voip.lab
% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: 8F6291BA
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate S-SRST-CA verbose' command will show the fingerprint.
P1-BR1-RTR(config)#
Mar 20 21:36:12.589: CRYPTO_PKI: Certificate Request Fingerprint MD5: C59F35FA
60E51A04 E46BC3F5 FA3D7156
Mar 20 21:36:12.589: CRYPTO_PKI: Certificate Request Fingerprint SHA1: C57A0A60
B82F64F0 99269E0B 186BB3C9 D01F3FAB
P1-BR1-RTR(config)#
Mar 20 21:36:14.265: %PKI-6-CERTRET: Certificate received from Certificate Authority
P1-BR1-RTR(config)#credentials
P1-BR1-RTR(config-credentials)#ip source-address 10.1.201.1 port 2445
P1-BR1-RTR(config-credentials)#trustpoint S-SRST-CA
P1-BR1-RTR(config-credentials)#

P1-BR1-RTR(config)#crypto pki trustpoint 7960-A
P1-BR1-RTR(ca-trustpoint)#revocation-check none
P1-BR1-RTR(ca-trustpoint)#enrollment terminal
P1-BR1-RTR(ca-trustpoint)#exit
```

➔ **Before our next step – we need to switch over to the CCM server, and navigate to the C:\Program Files\Cisco\Certificates directory, and open with Notepad the files ending in ".0". We need to copy the contents of these files between the words " -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" manually into the router in the next step**

➔ **NOTE: This step needs to be performed for every .0 file. This would also require the .pem files if we were using the 7970 phone which uses MICs (Manufacturer Installed Certificates) instead of LSCs (Locally Significant Certificates).**


C:\Program Files\Cisco\Certificates
Certificates
ffdee054.0
0 File
Modified: 3/12/2006 10:12 PM
Size: 909 bytes
Attributes: (normal)
Name
Size
Type
Modified
a69d2e04.0
CAPF.cer
ccmserver.cer
CiscoCA.crl
CiscoCA.pem
CiscoCAPF.pem
CiscoManufacturingCA.pem
CiscoRootCA2048.pem
dcc12642.0
f7a74b2c.0
ffdee054.0
httpscert.cer
ffdee054.0 - Notepad
File Edit Format Help
-----END CERTIFICATE-----

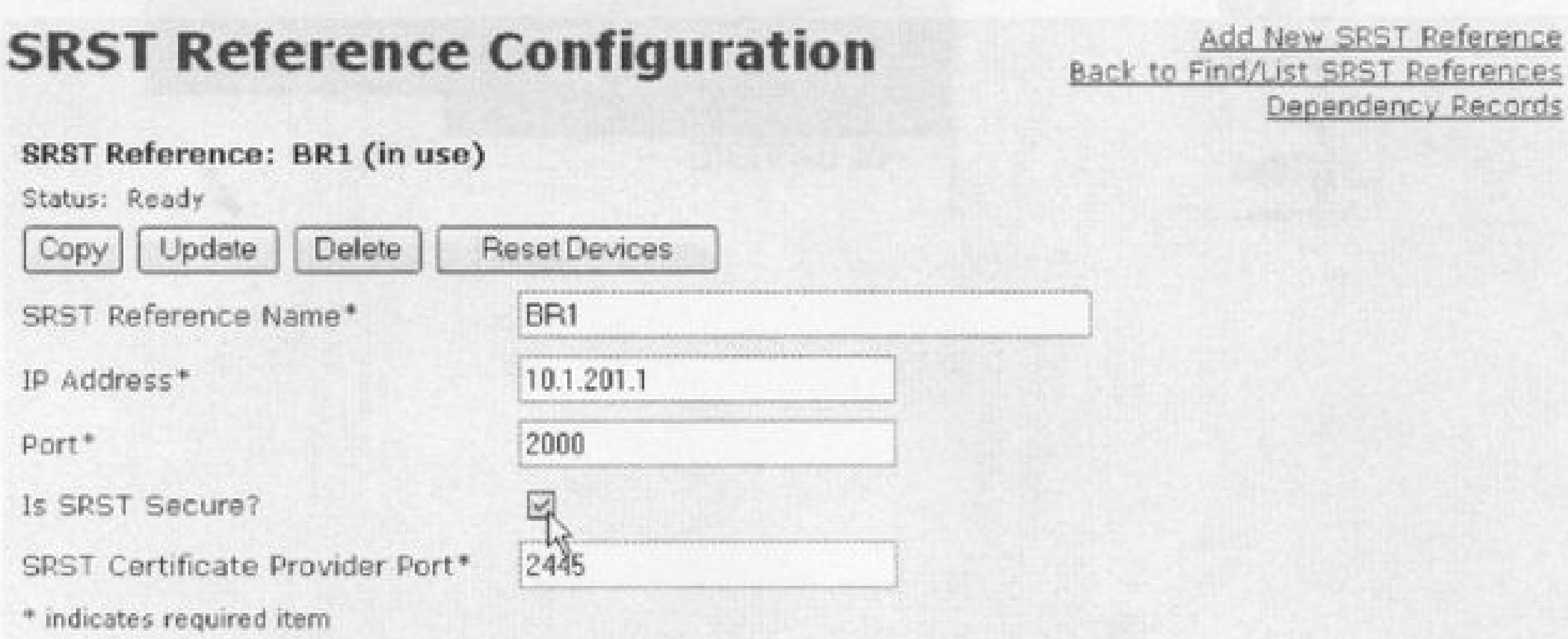
➔ **Back on BR1-RTR we need to paste the cert contents in the router.**

```
P1-BR1-RTR(config)#crypto pki authenticate 7960

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

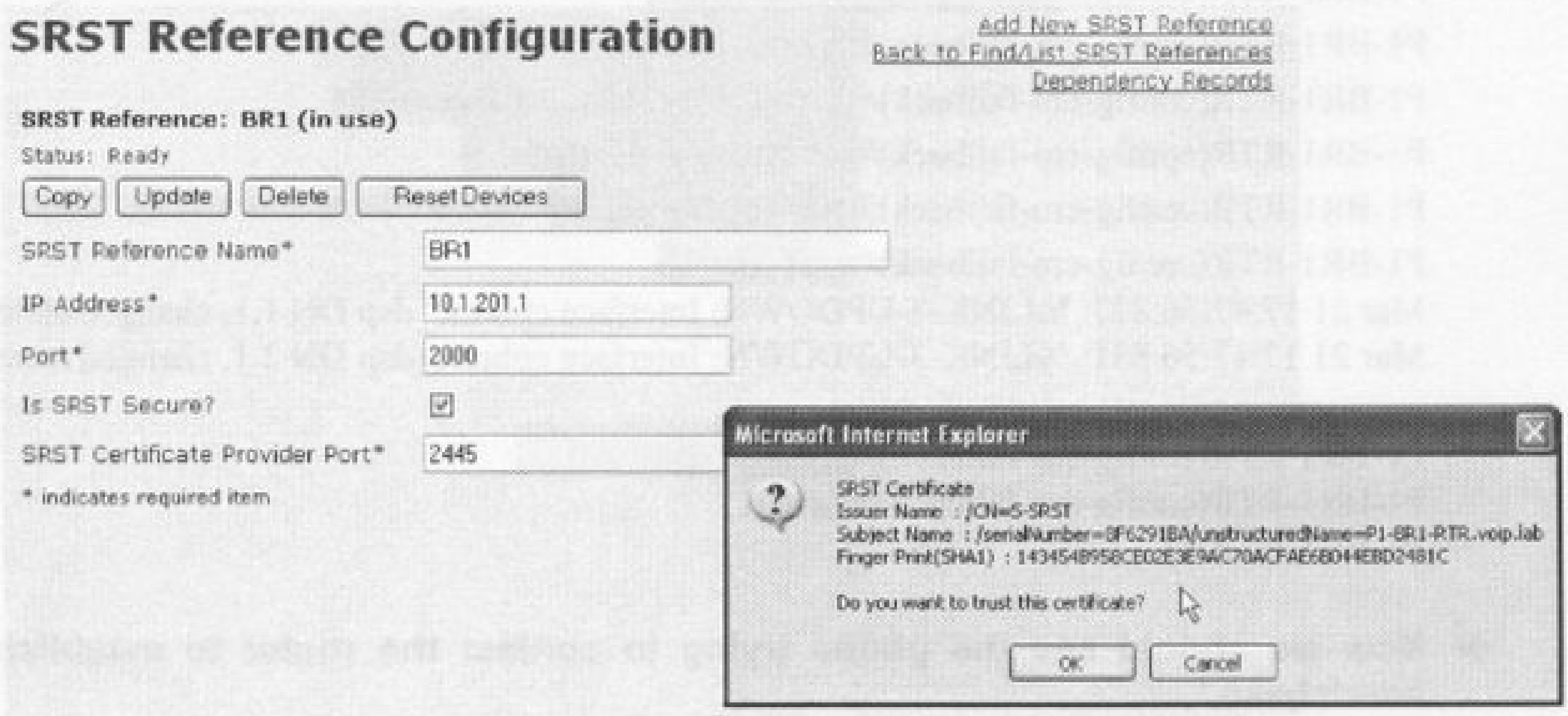

MIICKjCCAZOgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQTELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTY1MDA4
QzdCMB4XDTA2MDMxMzAzMTIwM1oXDTIxMDMwOTAzMTIwMlowQTELMAkGA1UEBhMC
VVMxGjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTY1
MDA4QzdCMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcdfvYJ2lxH41fiR5B
VFJYCHM1LHjfWJW1bV5x7ct4J2ebTzviNgjevqi+sr587eo90CwUOpJTxu6zVB89
Uo114xWLTu1p0In5xV5SSaTnnzk9JE8+hvnjBHH7k8X4LS7MVC2PeUQGjVDu8e+g
kO7zLum/FY/4wGhoJ3R3CjZ90wIDAQABozEwLzAOBgNVHQ8BAf8EBAMCAoQwHQYD
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMFMA0GCSqGSIb3DQEBBQUAA4GBAJox
inxsF0Vir8iQPvsZxY863b0U7iMzB883YoQrOJdN1ABOI0XkafvzI80VAUwJ5sQt
xhAZ/gTdATejM+XqFltMxTgjGtatkZEmnFoY/ERZ0YR6/HB4v+h32lJiJmbmFJPd
qGhQODP6Vn9h5GXj/APIk5zARzExrPt+9DliLsr7


```
Certificate has the following attributes:
    Fingerprint MD5: BE395ABE 078AB112 1725CC1D 46343CB2
   Fingerprint SHA1: DE990CED 99E0431F 60EDC393 7E7CD5BF 0ED9E5FA

% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

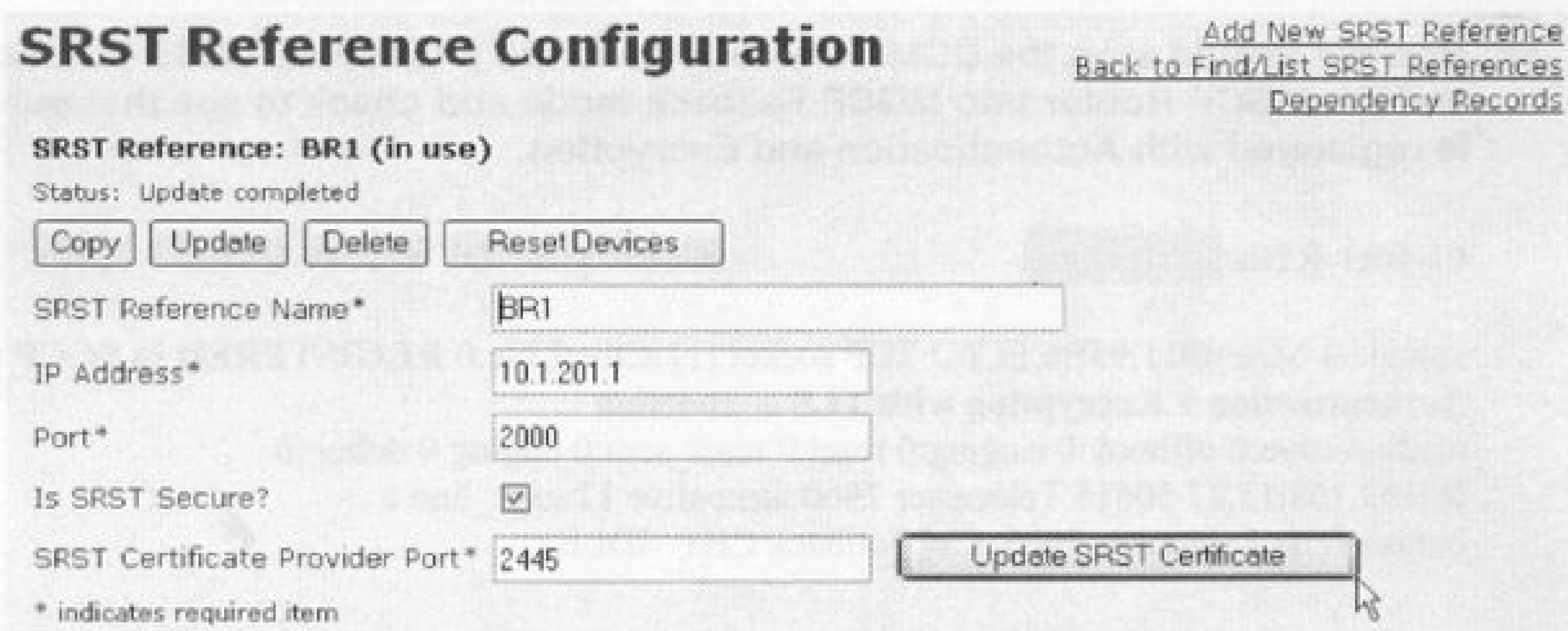
➔ **Now we need to tell CCM that our SRST reference is Secure**



➔ **And CCM will go out to the router and try to retrieve a SRST certificate to install in the IP Phones from the CA that we just setup on the BR1-RTR**



➔ **Now the CCM–SRST page should look like this if the certificate was properly installed from the BR1-RTR CA:**



➔ **Finally we need to turn SRST back on in the router.**

```
P1-BR1-RTR(config)#call-manager-fallback
P1-BR1-RTR(config-cm-fallback)#ip source-address 10.1.202.1
P1-BR1-RTR(config-cm-fallback)#transfer-system full-consult
P1-BR1-RTR(config-cm-fallback)#secondary-dialtone 9
P1-BR1-RTR(config-cm-fallback)#max-ephones 24
P1-BR1-RTR(config-cm-fallback)#max-dn 48
Mar 21 17:47:56.827: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
Mar 21 17:47:56.831: %LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up
....
P1-BR1-RTR(config-cm-fallback)#transfer-pattern ....
P1-BR1-RTR(config-cm-fallback)#end
P1-BR1-RTR#
```

➔ **Now we should see the phone trying to contact the router to establish a TLS handshake.**

```
P1-BR1-RTR(config)#
Mar 21 18:19:11.674: CRYPTO_PKI_OPSSL - Verifying 1 Certs
```

➔ **Now we should stop the CCM Service to send the phone into SRST Fallback mode and the MGCP Router into MGCP Fallback mode and check to see that our ephone is registered with Authentication and Encryption.**

```
P1-BR1-RTR#sh ephone
```

ephone-1 Mac:0011.93B6.EC0D TCP socket:[1] activeLine:0 **REGISTERED in SCCP ver 6 + Authentication + Encryption with TLS connection**
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:192.168.15.27 50615 Telecaster 7960 keepalive 12 max_line 6
button 1: dn 1 number 2003 CM Fallback CH1 IDLE

➔ **Now we will place a call over the PSTN to 911 to check for a secure transport.**

P1-BR1-RTR#sh ephone

ephone-1 Mac:0011.93B6.EC0D TCP socket:[1] activeLine:1 REGISTERED in SCCP ver 6 + Authentication + Encryption with TLS connection
mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:192.168.15.27 50615 Telecaster 7960 keepalive 2 max_line 6
button 1: dn 1 number 2003 CM Fallback CH1 CONNECTED
Active Secure Call on DN 1 chan 1 :2003 192.168.15.27 30232 to 10.1.201.1 2000 via 162.1.101.1
G711Ulaw64k 160 bytes no vad
Tx Pkts 691 bytes 121616 Rx Pkts 694 bytes 122144 Lost 0
Jitter 0 Latency 0 callingDn -1 calledDn -1 (media path callID 7 srcCallID 8)

Task 17.4

Ensure that RTP traffic between the any capable IP Phone and the BR1 MGCP gateway is encrypted with AES128.

➔ **On BR1-RTR:**

P1-BR1-RTR(config)#no mgcp
Mar 22 15:24:55.058: %MGCP_APP-6-MGCP_SHUTDOWN_COMPLETE: MGCP Shutdown has completed
P1-BR1-RTR(config)#mgcp package-capability srtp-package
Reminder: To have a secure voice solution using SRTP,
be sure to configure IPsec. Configuring an IPsec tunnel
(a symmetrical set of IPsec security associations for ESP
transport mode) protects MGCP signaling messages to and
from the Call Agent.
P1-BR1-RTR(config)#mgcp validate call-agent source-ipaddr ← **optional – (not required to complete task) this authenticates or validates CCM to be who it says it is**
P1-BR1-RTR(config)#mgcp
P1-BR1-RTR(config)#

➔ **Verify – Place a call from an Encrypted IP Phone and verify that the Lock symbol is seen on the IP Phone.**

➔ **Verify on BR1-RTR:**

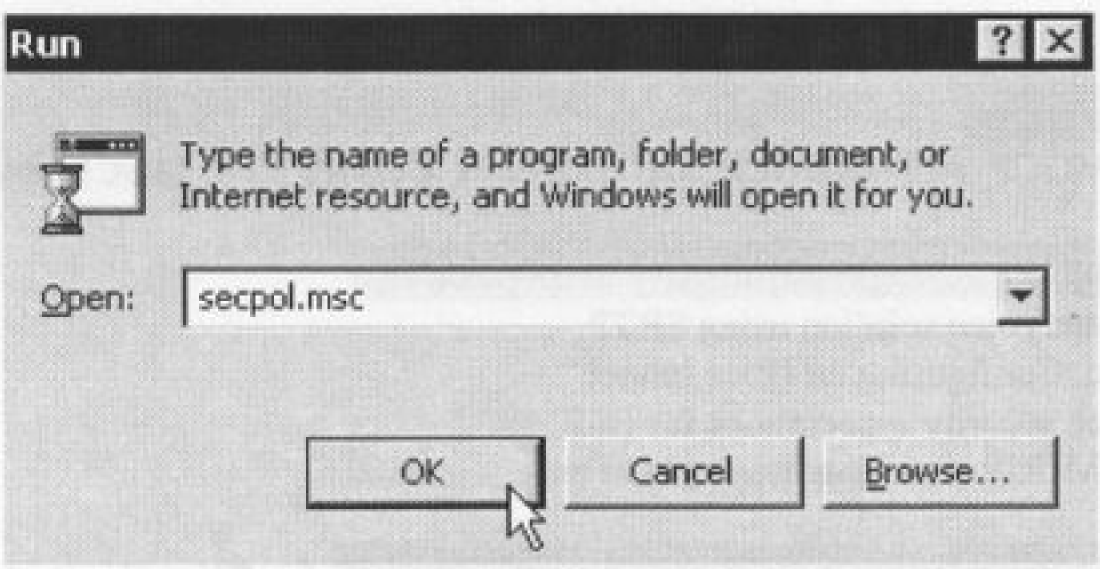
```
P1-BR1-RTR#sh mgcp srtp sum
MGCP SRTP Connection Summary
Endpoint        Conn Id   Crypto Suite
S2/SU0/DS1-0/3     4      AES_CM_128_HMAC_SHA1_32

1 SRTP connections active
```

Task 17.5

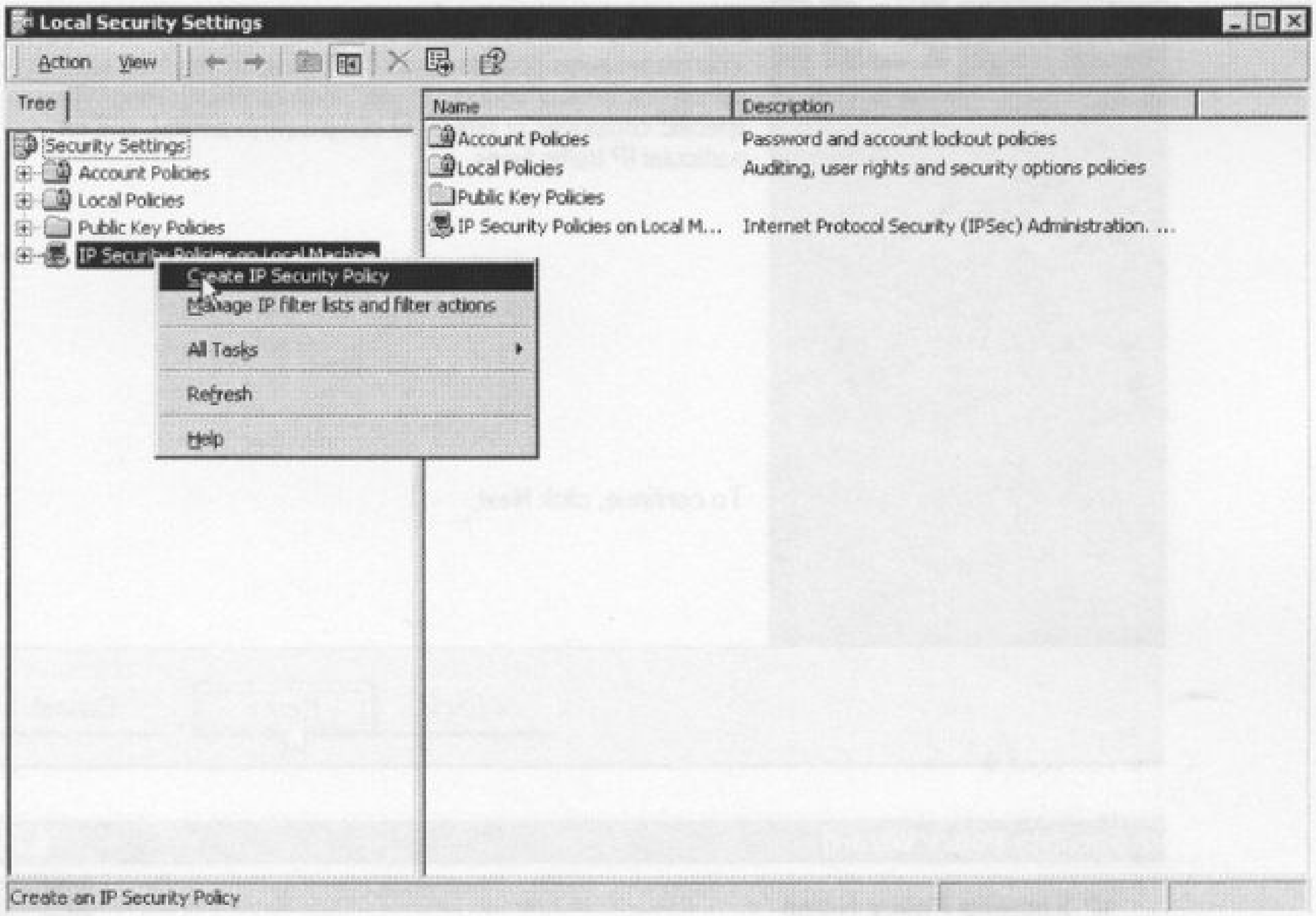
Ensure that all MGCP signaling between CallManager and BR1 gateway is encrypted with 3DES 168bit encryption using a SHA hashing algorithm.

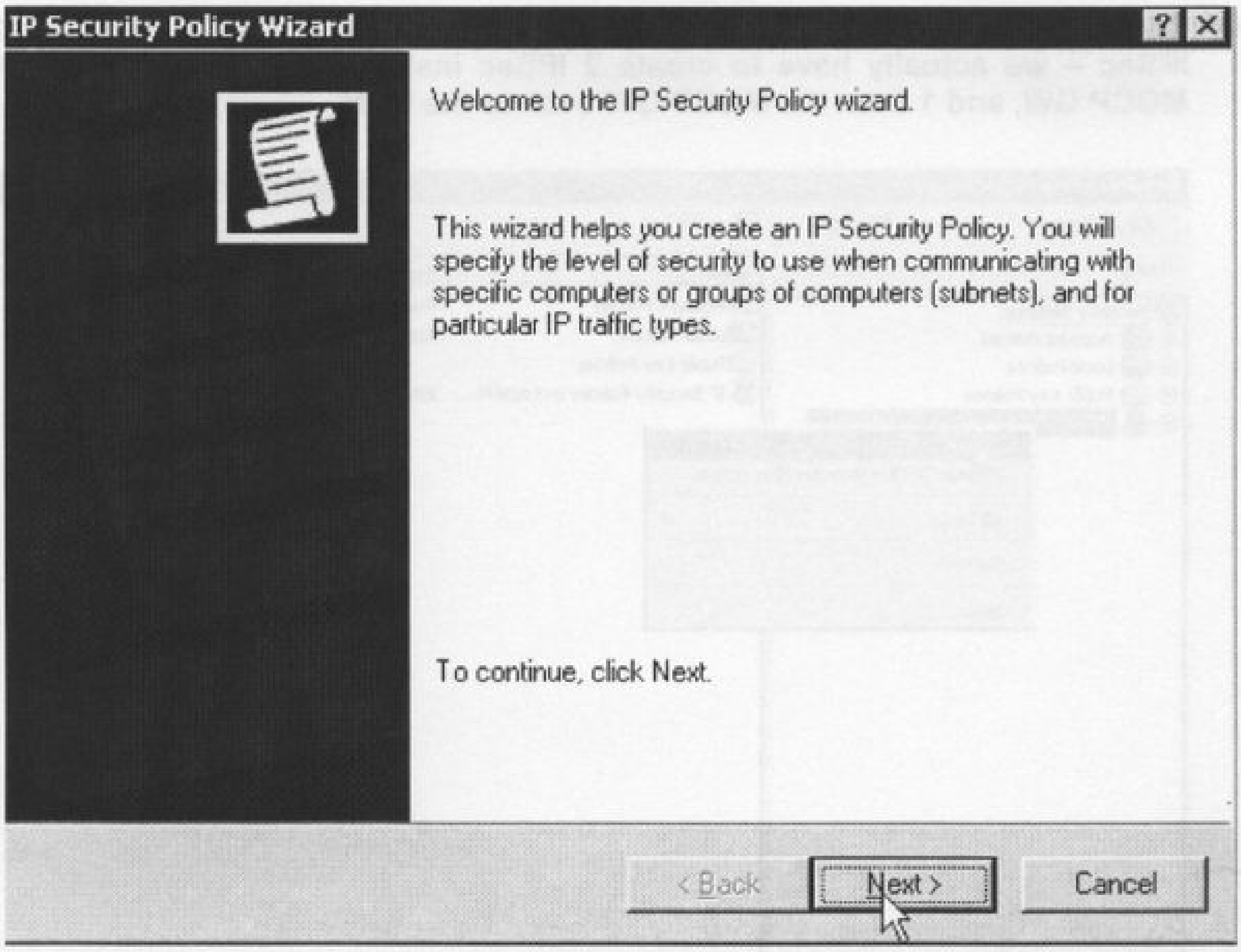
➔ **On CCM we need to setup an IPSec Tunnel to the MGCP GW (This would need to be performed on BOTH Pub and Sub although here we only demonstrate the Pub server).**

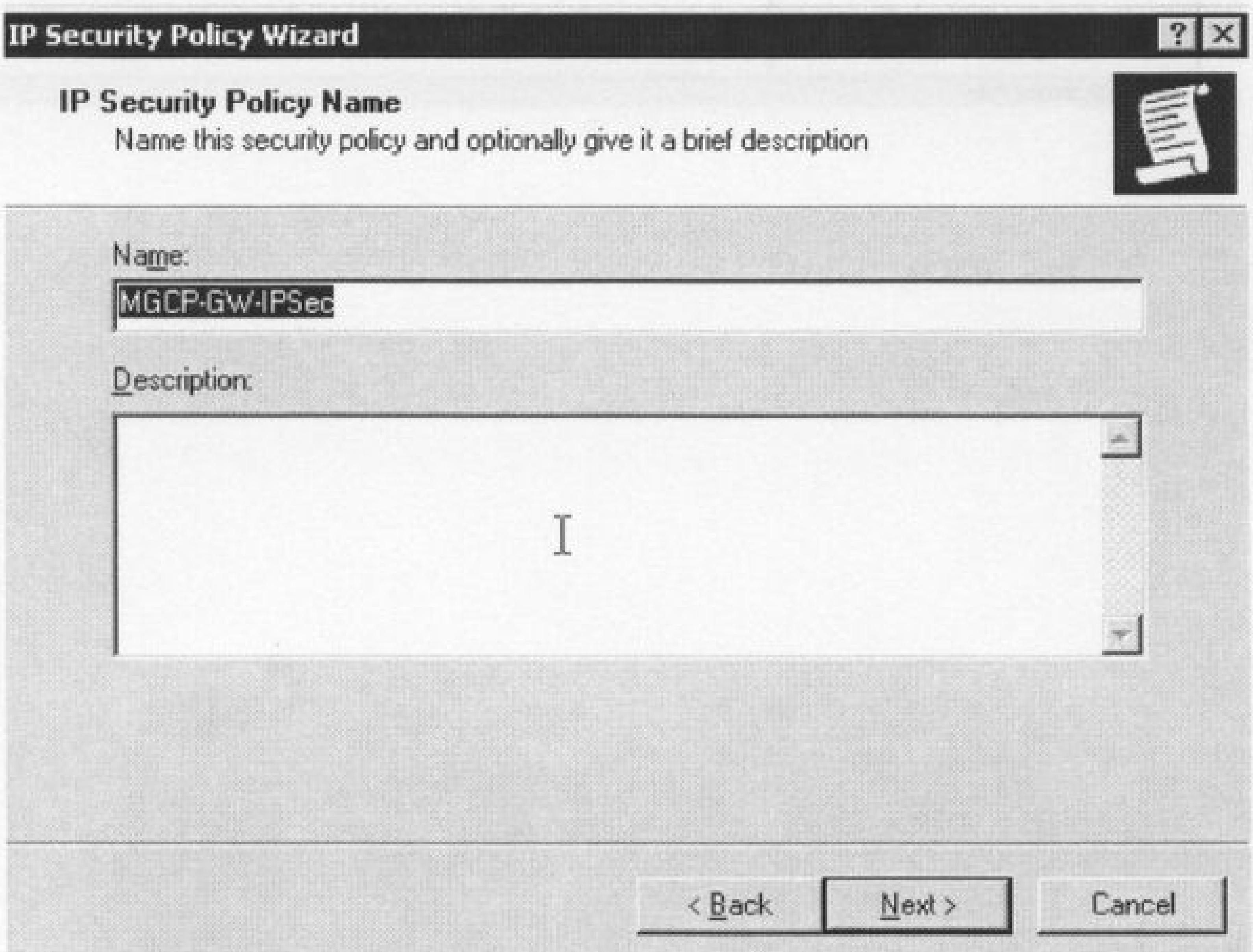
➔ **Go to Start >Run >and enter 'secpol.msc'.**

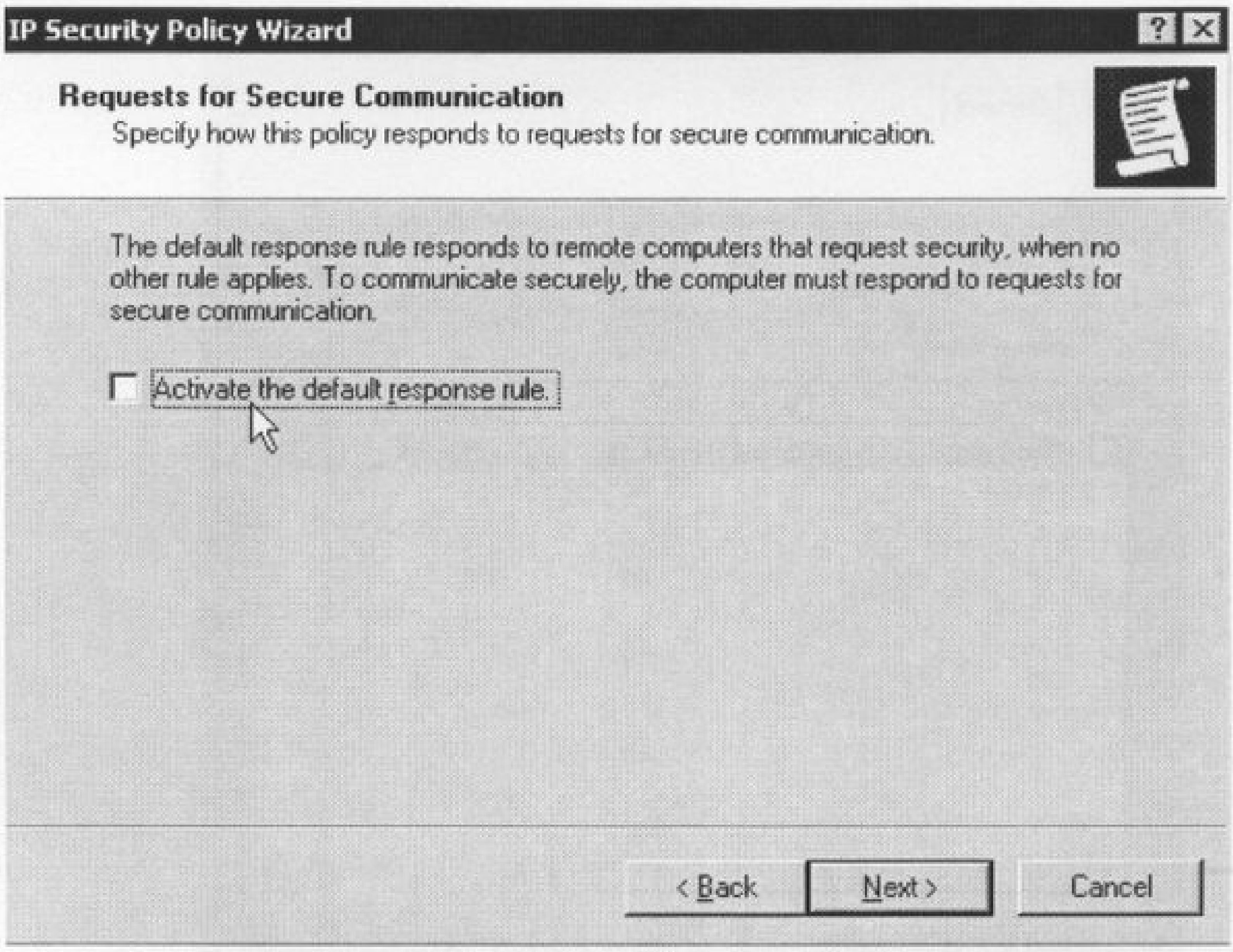


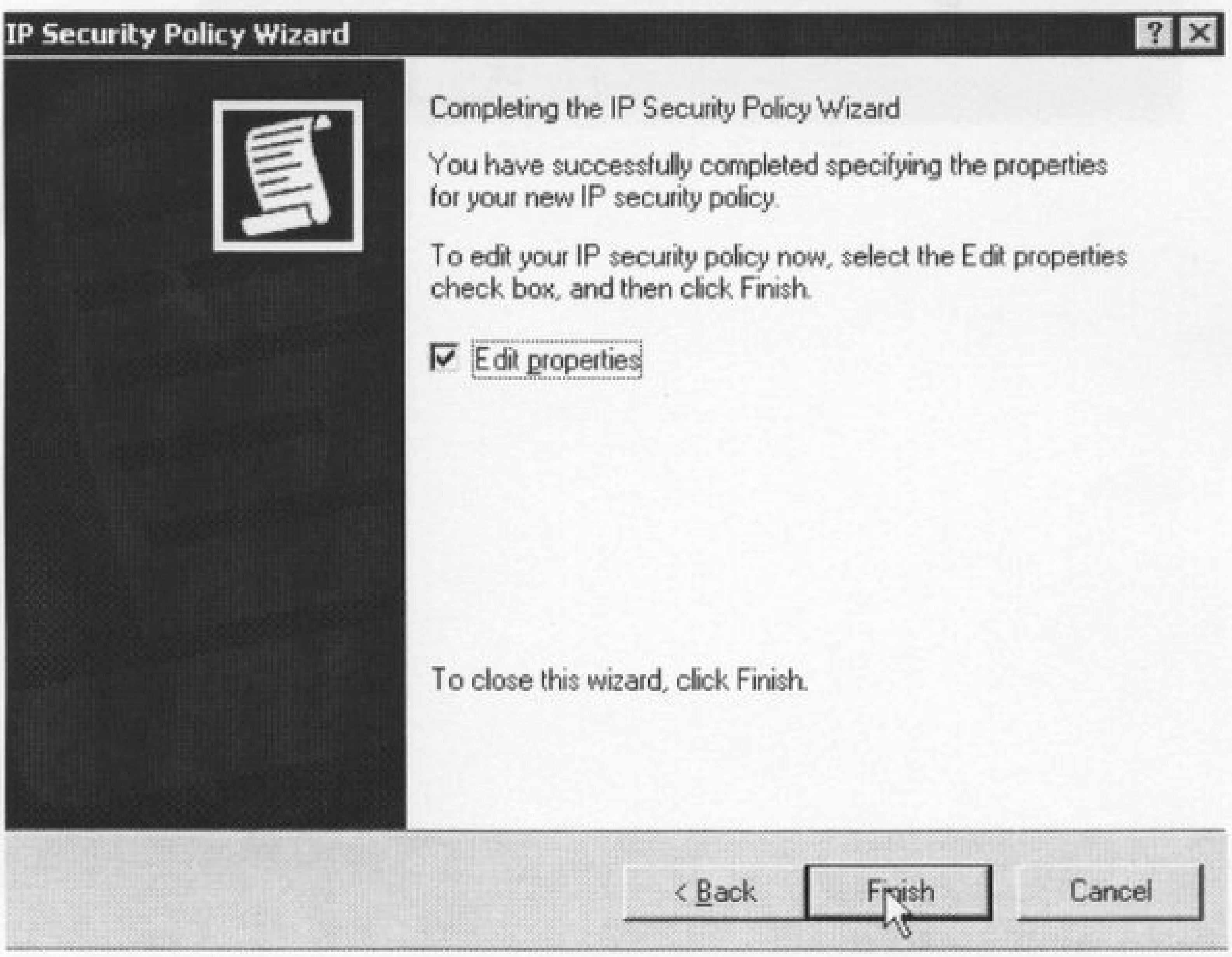
➔ **Now we need to setup an IPSec connection – because MS is a little weird about its IPSec – we actually have to create 2 IPSec instances – 1 from the CCM to the MGCP GW, and 1 from the MGCP GW back to the CCM.**

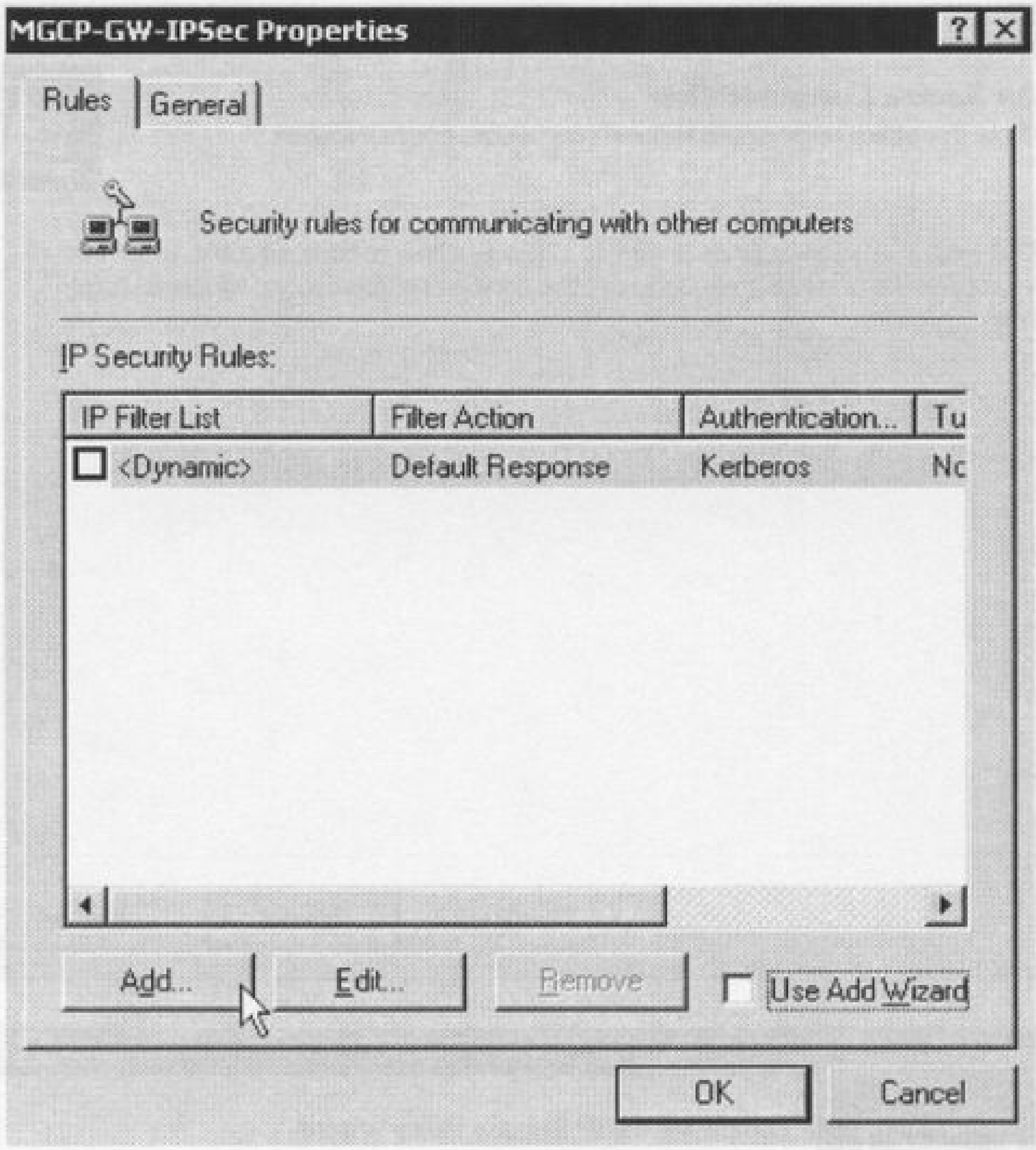


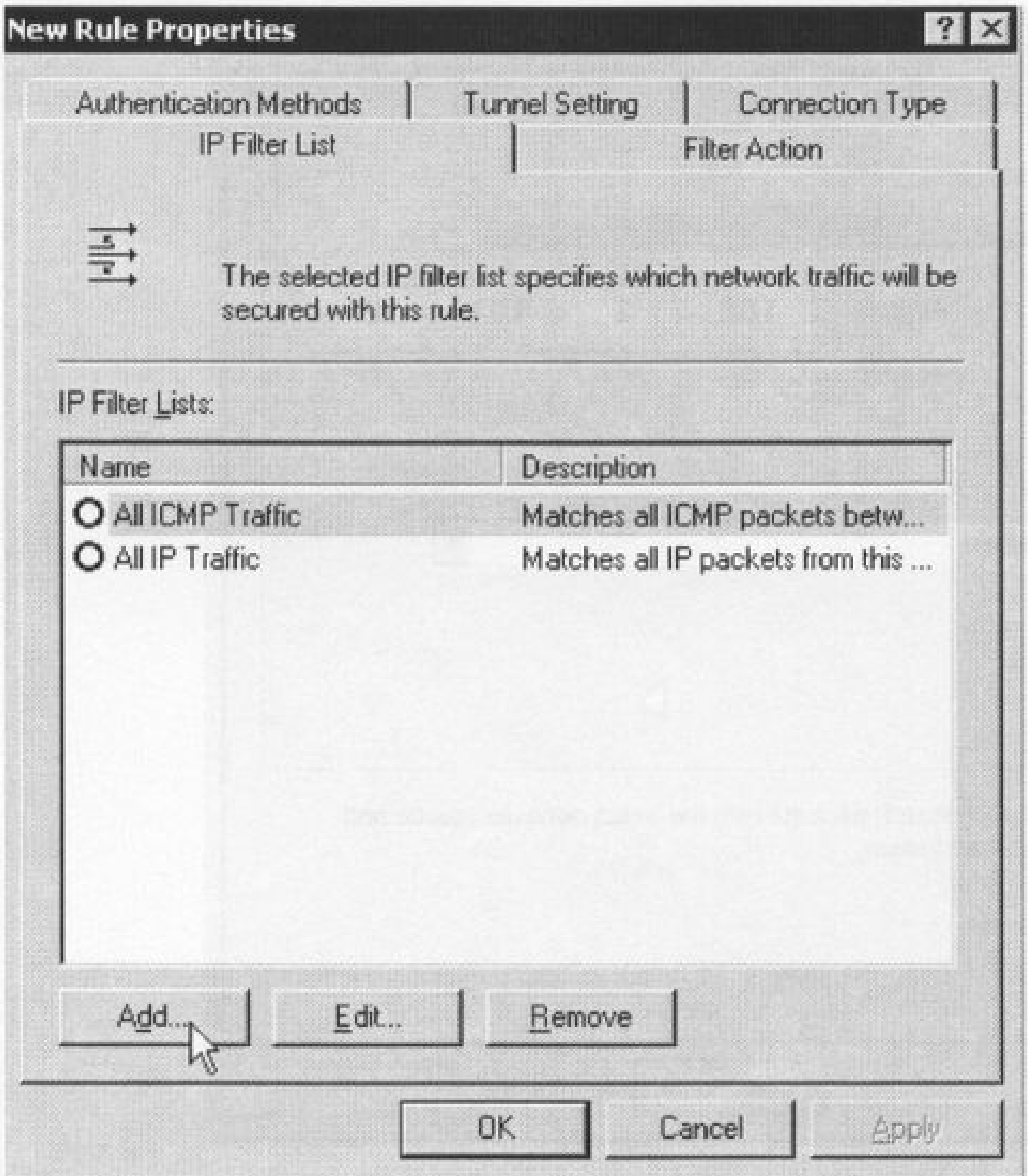

IP Security Policy Wizard
Welcome to the IP Security Policy wizard.
This wizard helps you create an IP Security Policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.
To continue, click Next.
< Back
Next >
Cancel

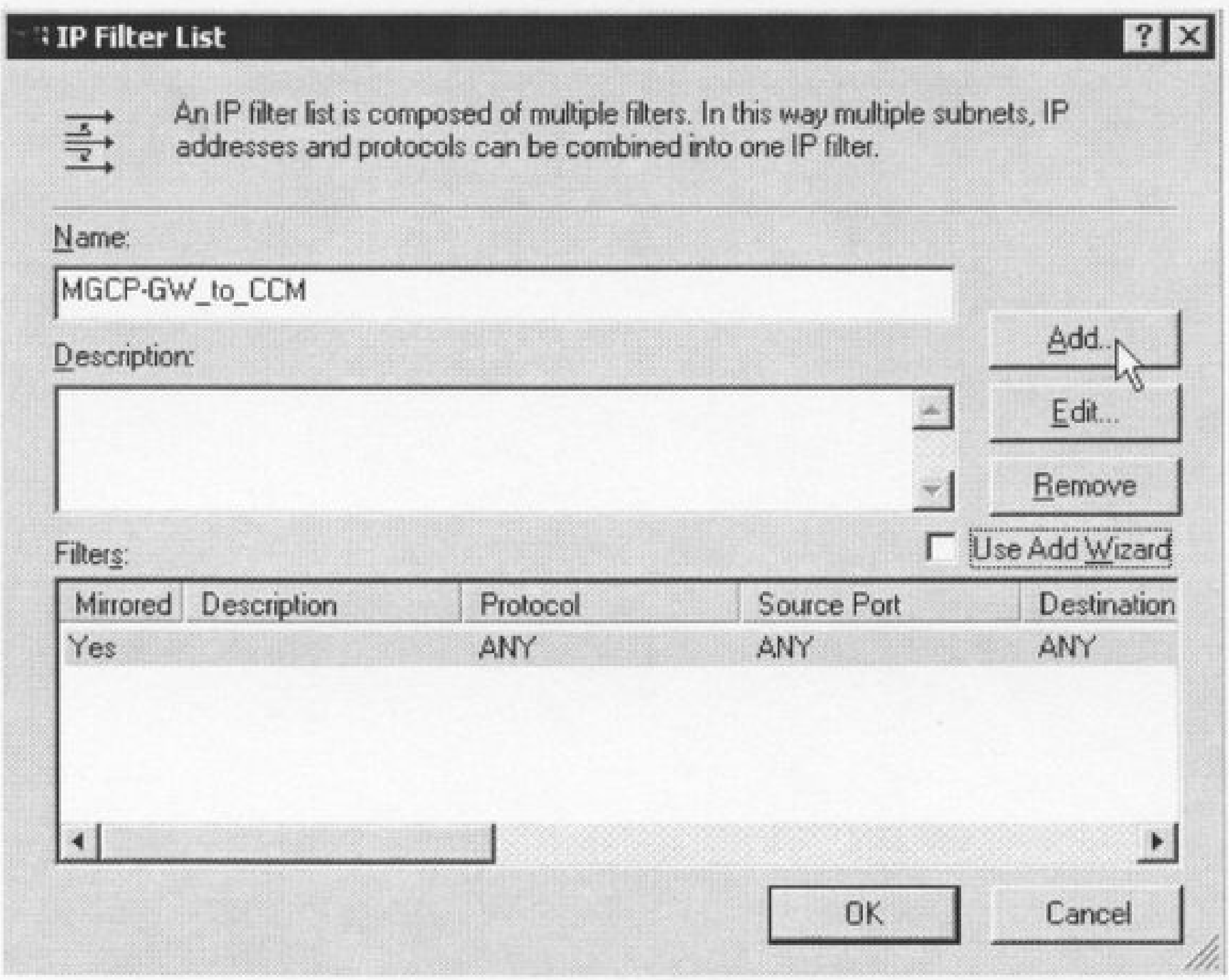

IP Security Policy Wizard
IP Security Policy Name
Name this security policy and optionally give it a brief description
Name:
MGCP-GW-IPSec
Description:
< Back
Next >
Cancel

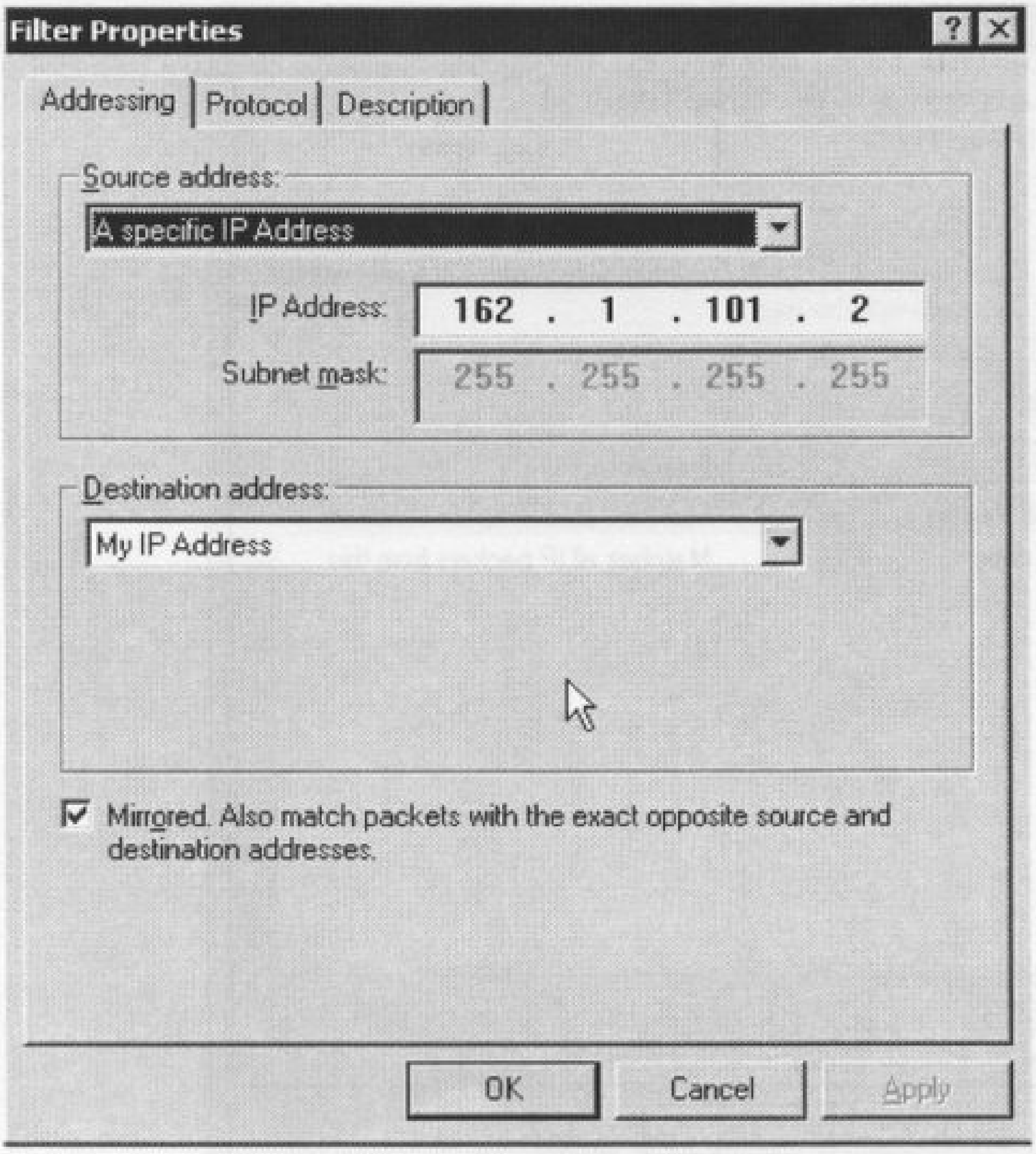

IP Security Policy Wizard
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
Activate the default response rule.
< Back
Next >
Cancel

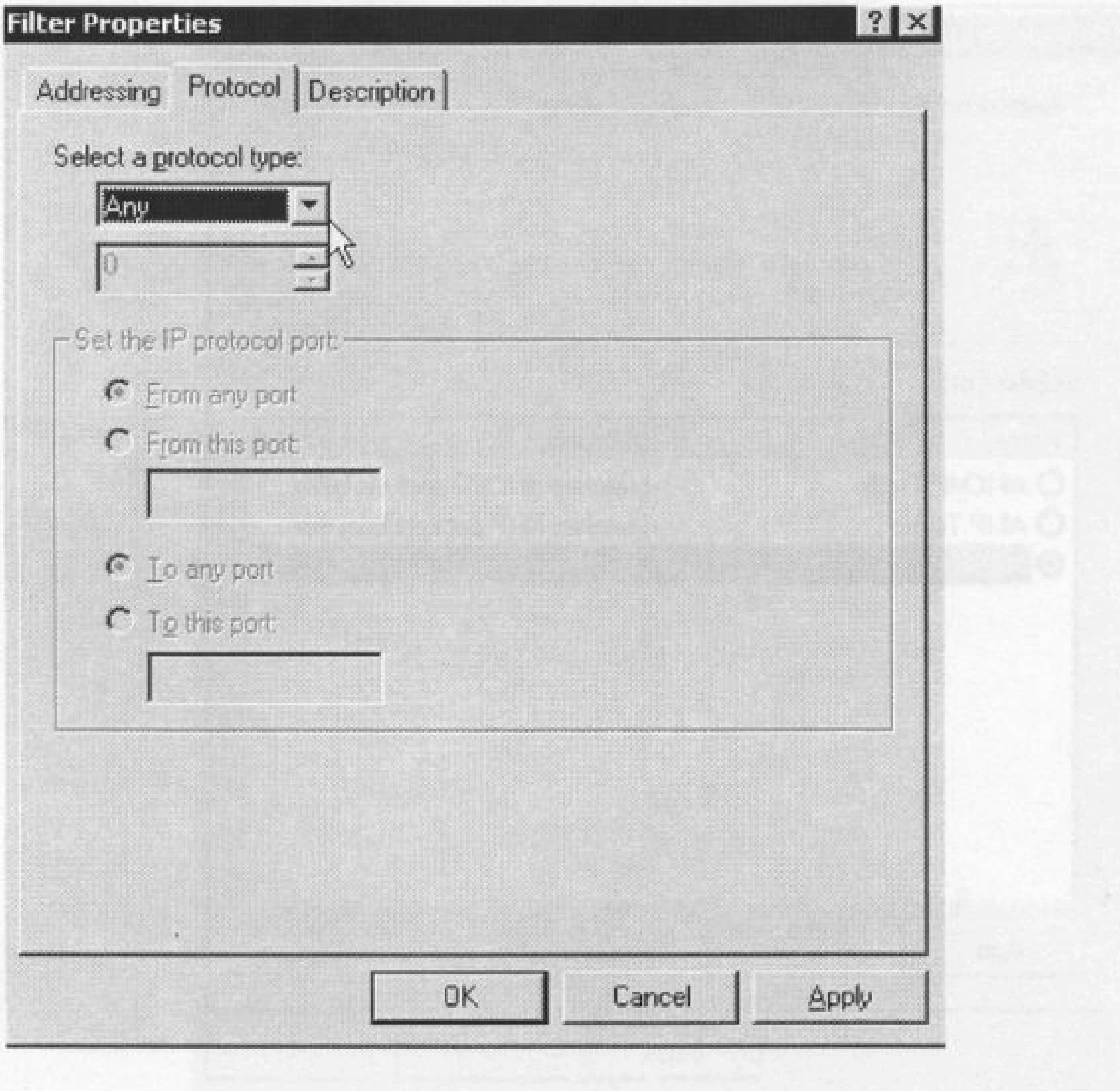

IP Security Policy Wizard
Completing the IP Security Policy Wizard
You have successfully completed specifying the properties for your new IP security policy.
To edit your IP security policy now, select the Edit properties check box, and then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

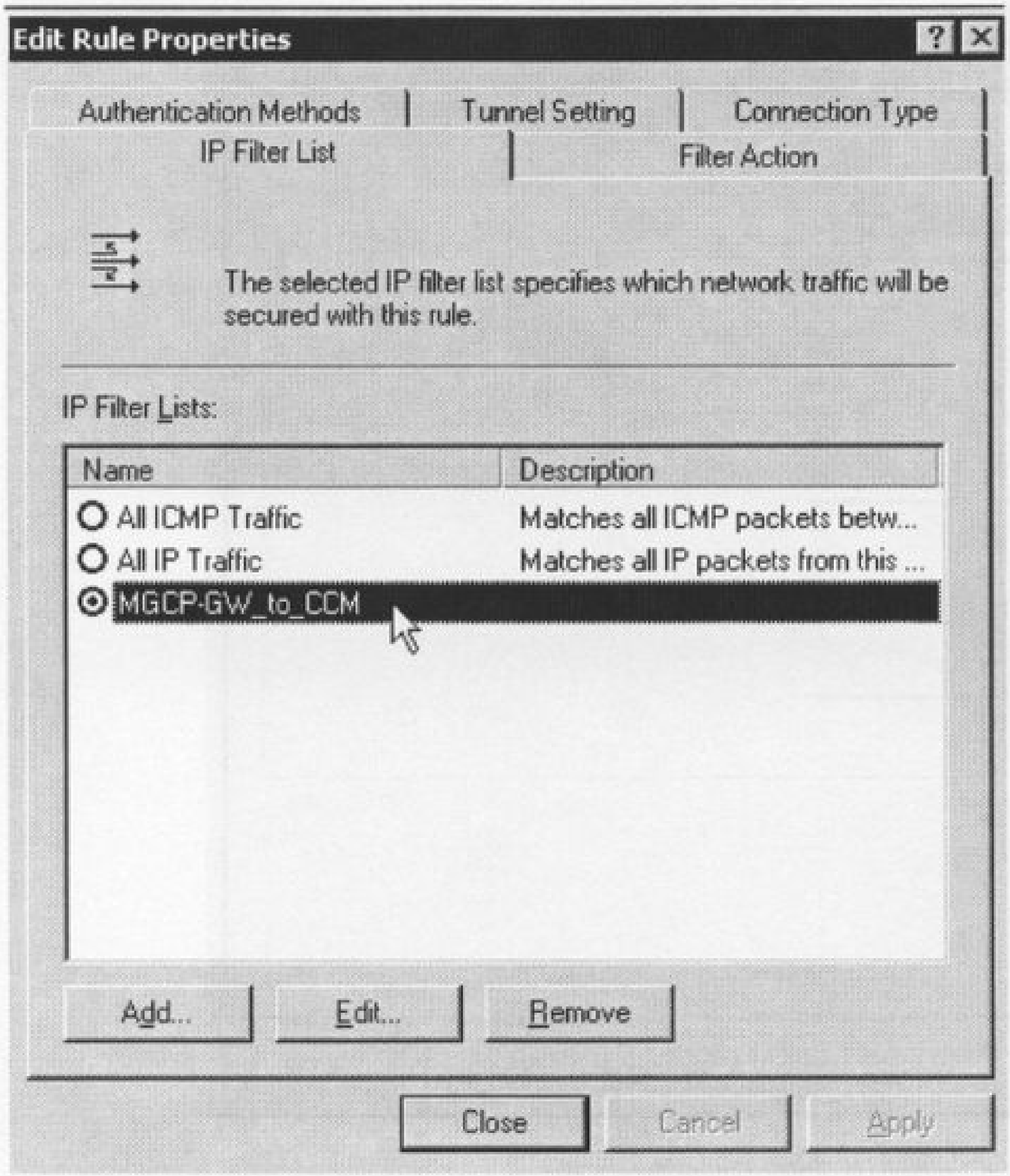

MGCP-GW-IPSec Properties
Rules
General
Security rules for communicating with other computers
IP Security Rules:
IP Filter List
Filter Action
Authentication...
Tu
<Dynamic>
Default Response
Kerberos
Nc
Add...
Edit...
Remove
Use Add Wizard
OK
Cancel

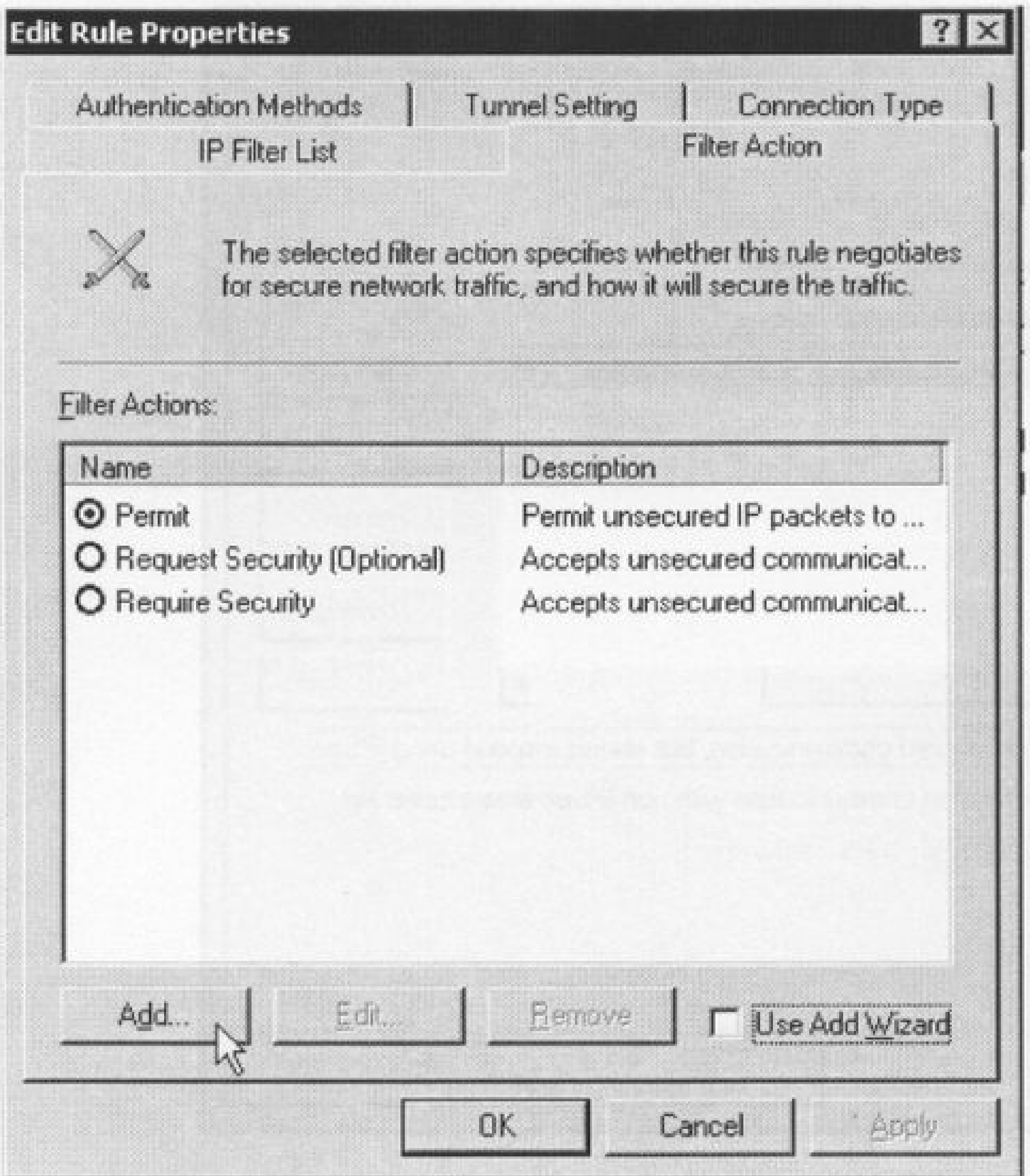

New Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected IP filter list specifies which network traffic will be secured with this rule.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
Add...
Edit...
Remove
OK
Cancel
Apply

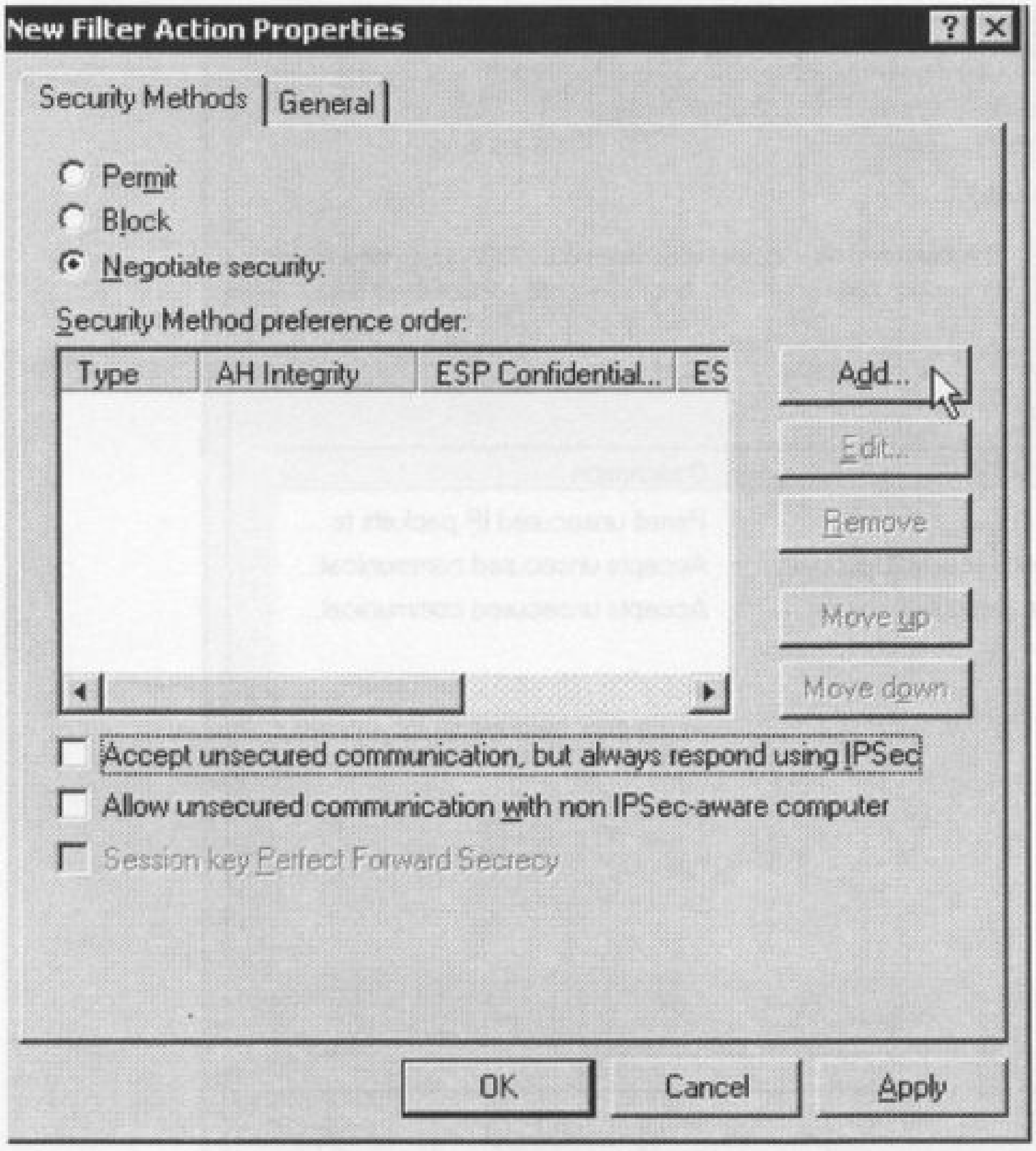

IP Filter List
An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
MGCP-GW_to_CCM
Description:
Add...
Edit...
Remove
Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
Yes
ANY
ANY
ANY
OK
Cancel


Filter Properties
Addressing
Protocol
Description
Source address:
A specific IP Address
IP Address: 162 . 1 . 101 . 2
Subnet mask: 255 . 255 . 255 . 255
Destination address:
My IP Address
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK
Cancel
Apply

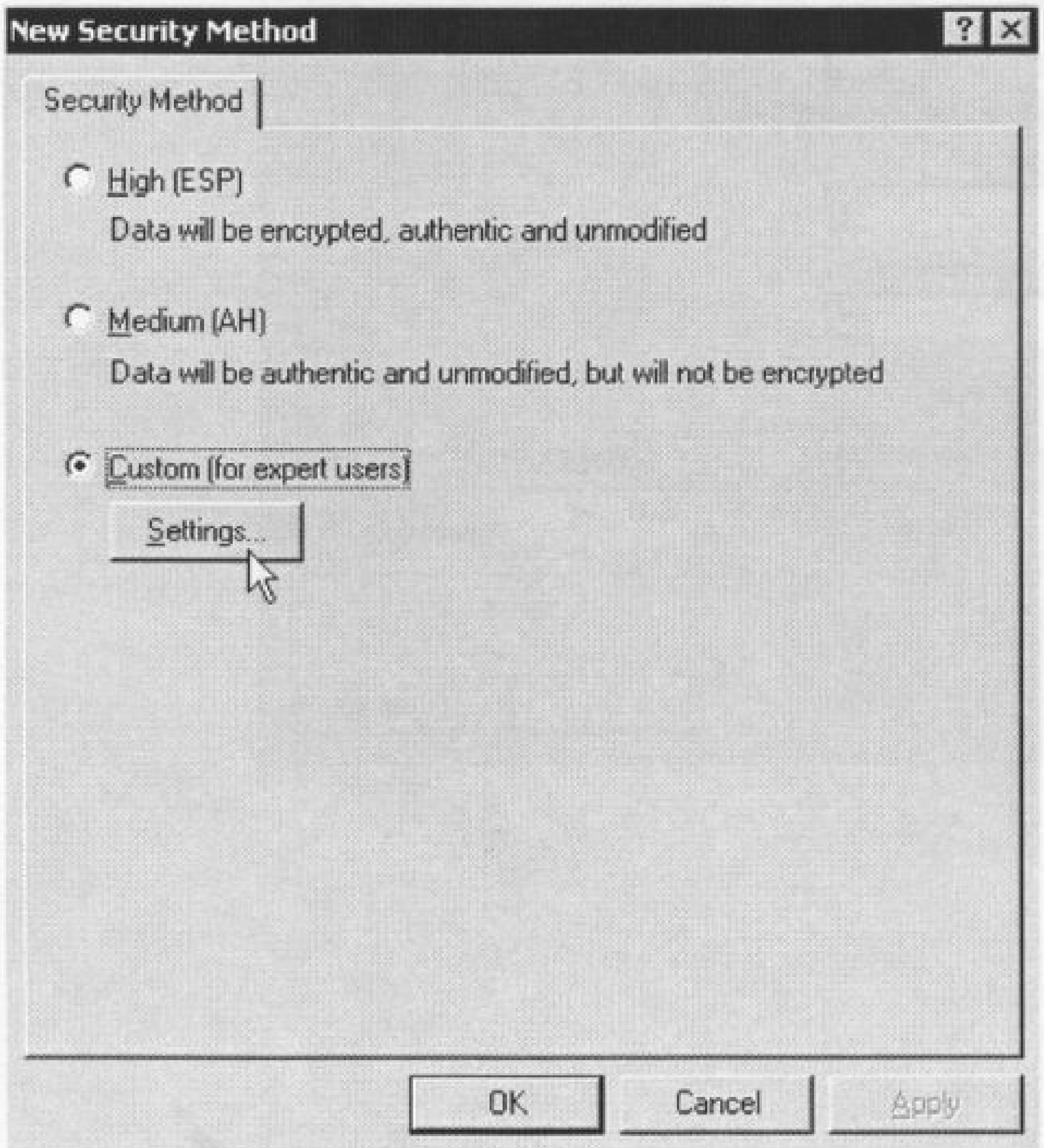

Filter Properties
Addressing
Protocol
Description
Select a protocol type:
Any
0
Set the IP protocol port:
From any port
From this port:
To any port
To this port:
OK
Cancel
Apply

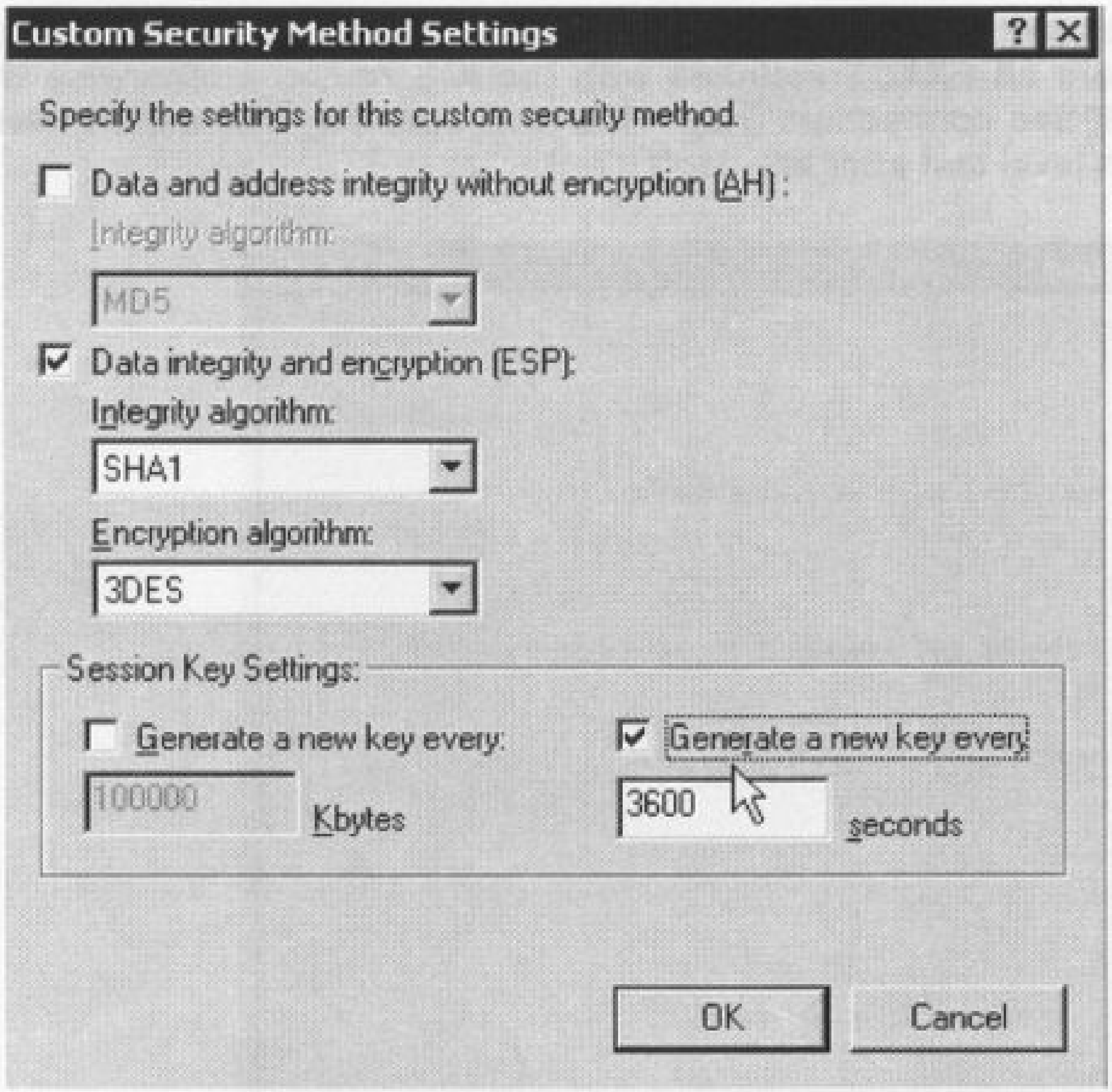

Edit Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected IP filter list specifies which network traffic will be secured with this rule.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
MGCP-GW_to_CCM
Add...
Edit...
Remove
Close
Cancel
Apply

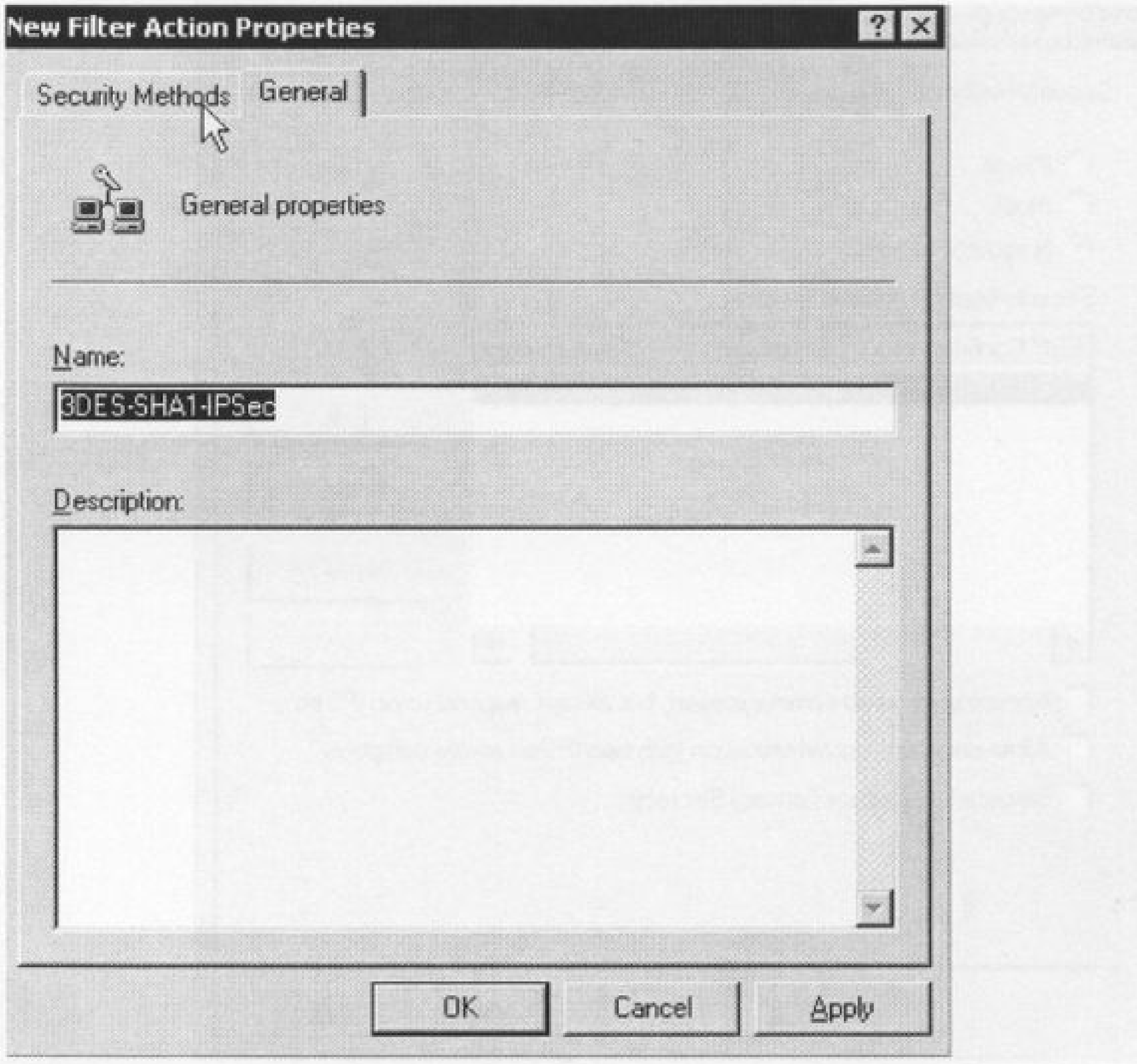

Edit Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.
Filter Actions:
Name
Description
Permit
Permit unsecured IP packets to ...
Request Security (Optional)
Accepts unsecured communicat...
Require Security
Accepts unsecured communicat...
Add...
Edit...
Remove
Use Add Wizard
OK
Cancel
Apply

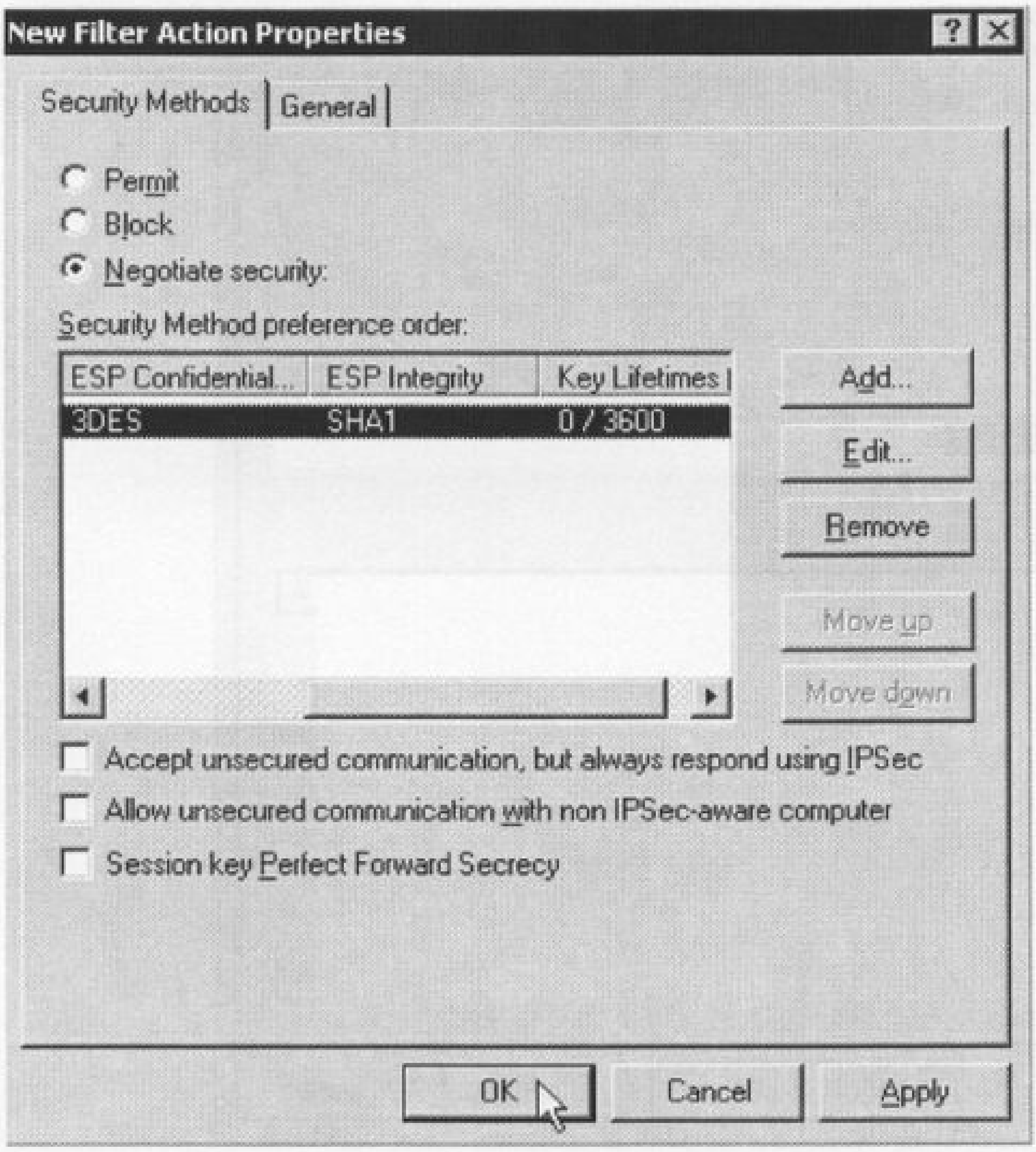

New Filter Action Properties
Security Methods
General
Permit
Block
Negotiate security:
Security Method preference order:
Type
AH Integrity
ESP Confidential...
ES
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non IPSec-aware computer
Session key Perfect Forward Secrecy
OK
Cancel
Apply

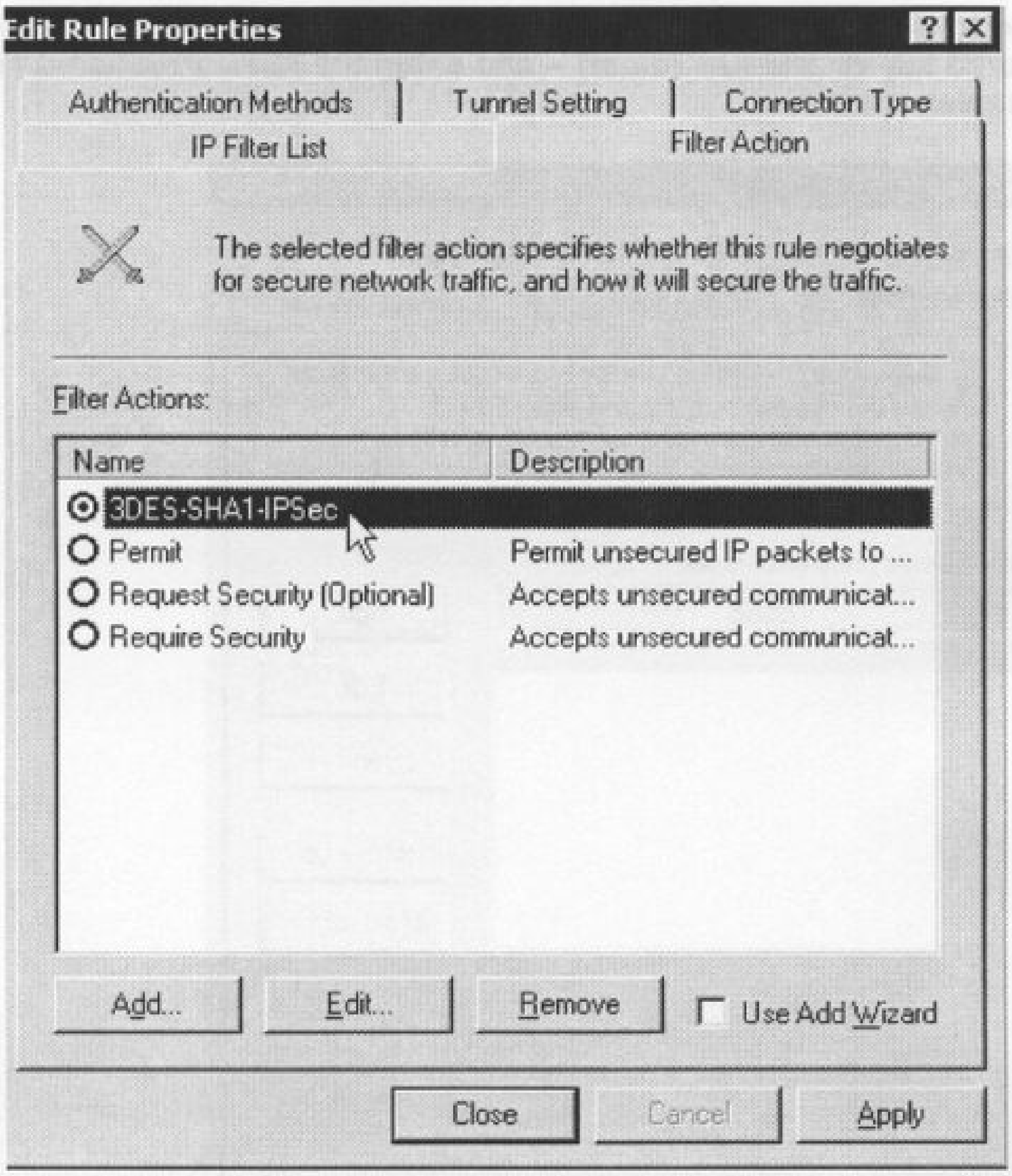
➔ **Here we need to set very specific options so that our Hash, Encryption, and Key timer settings are all EXACT matches with the IOS router – otherwise they will never create a IPSec connection. (Hey – the icon does say "for expert users" and this is an Expert level test after all – isn't it? ;)**



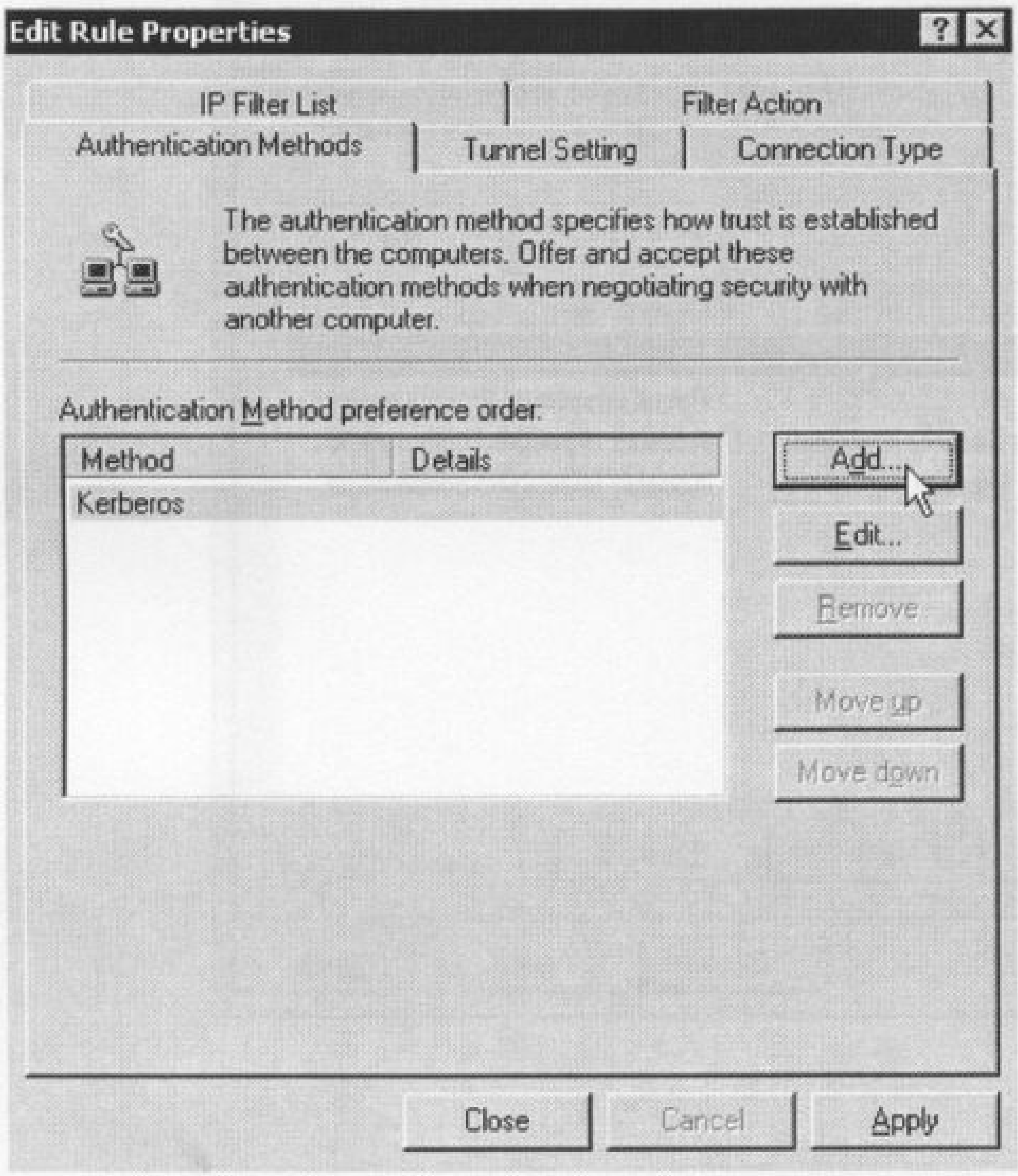

Custom Security Method Settings
Specify the settings for this custom security method.
Data and address integrity without encryption (AH) :
Integrity algorithm:
MD5
Data integrity and encryption (ESP):
Integrity algorithm:
SHA1
Encryption algorithm:
3DES
Session Key Settings:
Generate a new key every:
100000
Kbytes
Generate a new key every
3600
seconds
OK
Cancel

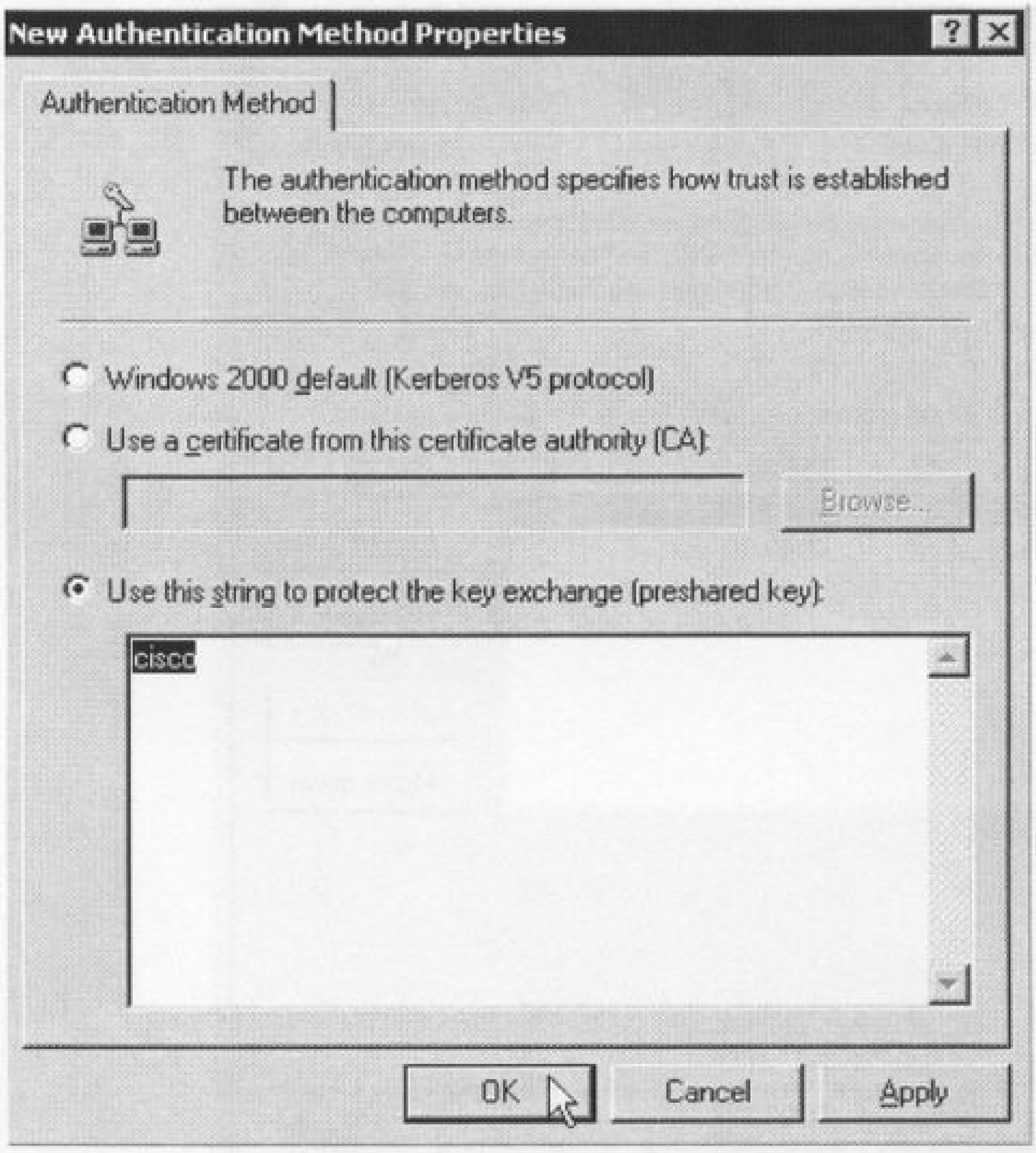

New Filter Action Properties
Security Methods
General
General properties
Name:
3DES-SHA1-IPSec
Description:
OK
Cancel
Apply

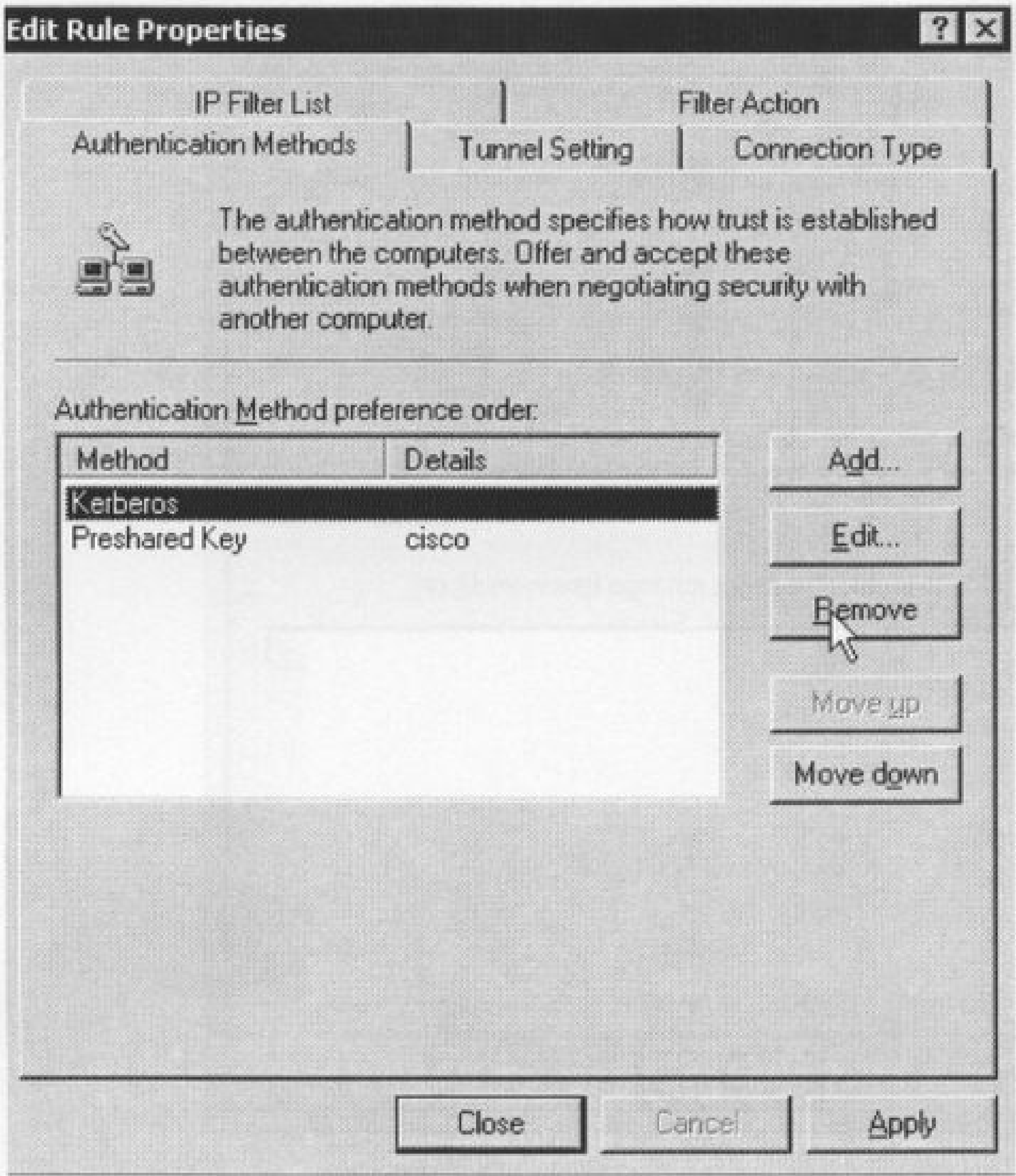

New Filter Action Properties
Security Methods
General
Permit
Block
Negotiate security:
Security Method preference order:
ESP Confidential...
ESP Integrity
Key Lifetimes
3DES
SHA1
0 / 3600
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non IPSec-aware computer
Session key Perfect Forward Secrecy
OK
Cancel
Apply

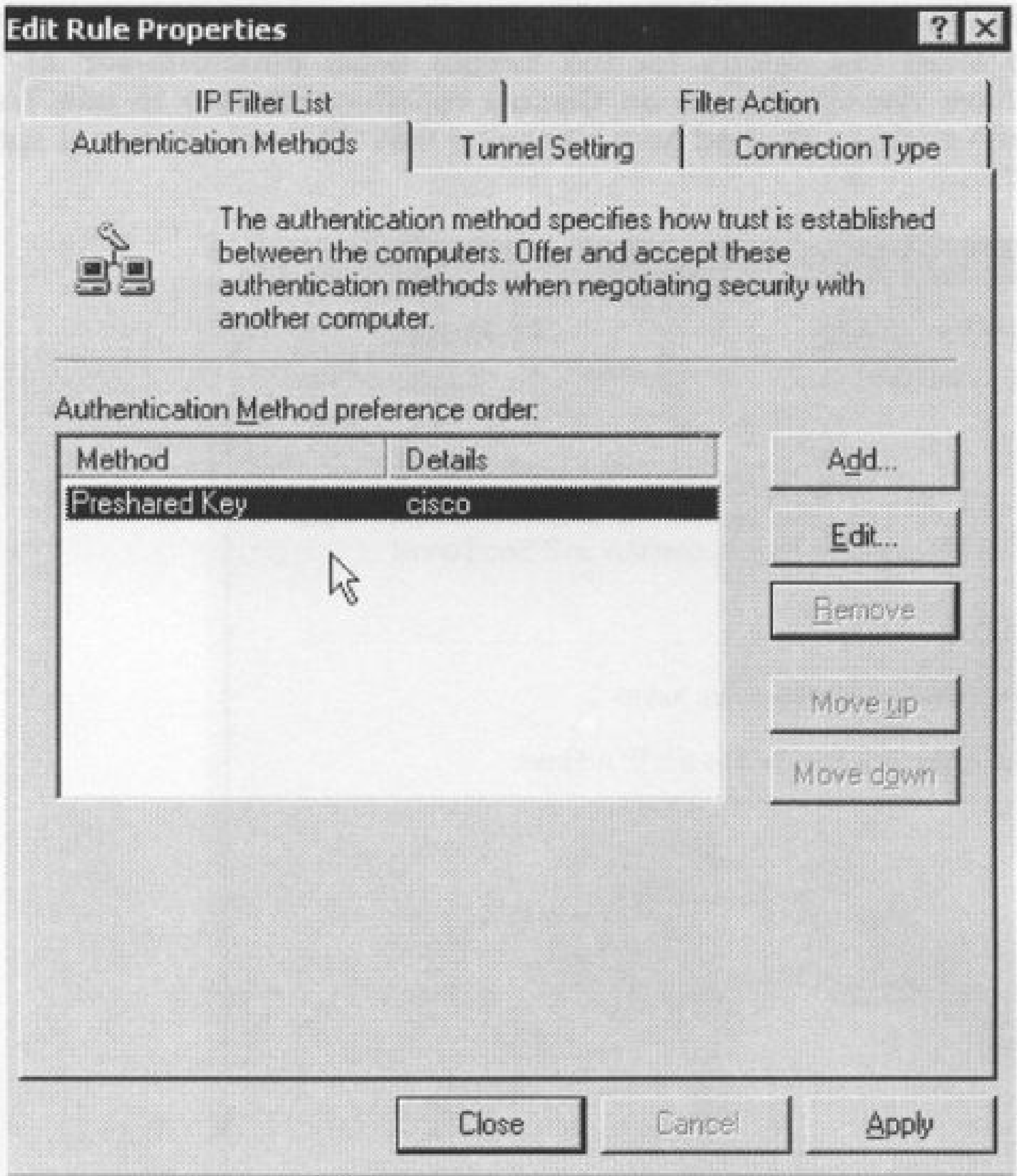

Edit Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.
Filter Actions:
Name
Description
3DES-SHA1-IPSec
Permit
Permit unsecured IP packets to ...
Request Security (Optional)
Accepts unsecured communicat...
Require Security
Accepts unsecured communicat...
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

➔ **Here we need to do away with Kerberos authentication (since we are choosing to use a PreShared key on the IOS router) – and setup the same PreShared key here on the W2k server.**

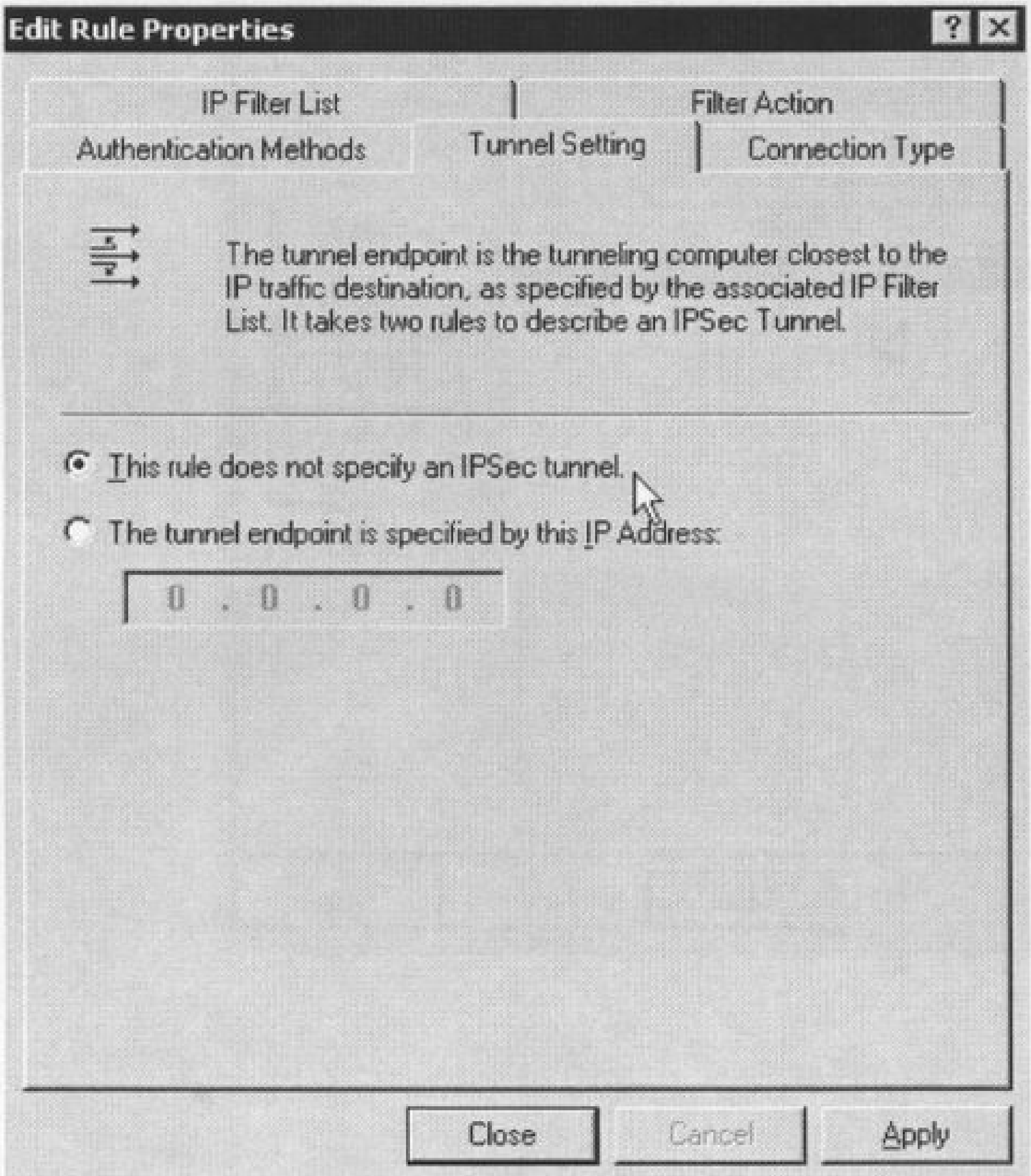


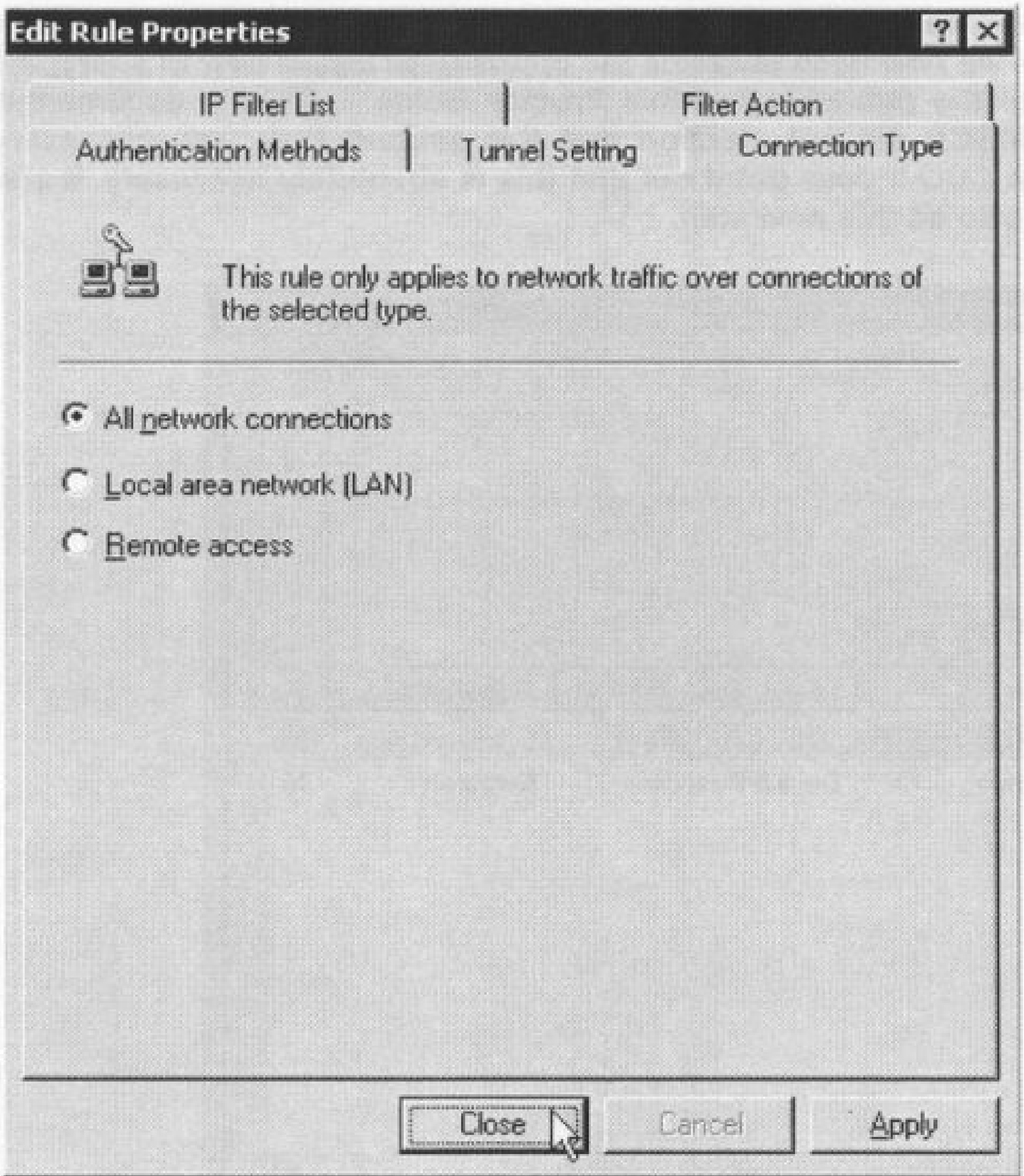

New Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
cisco
OK
Cancel
Apply


Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.
Authentication Method preference order:
Method
Details
Kerberos
Preshared Key
cisco
Add...
Edit...
Remove
Move up
Move down
Close
Cancel
Apply

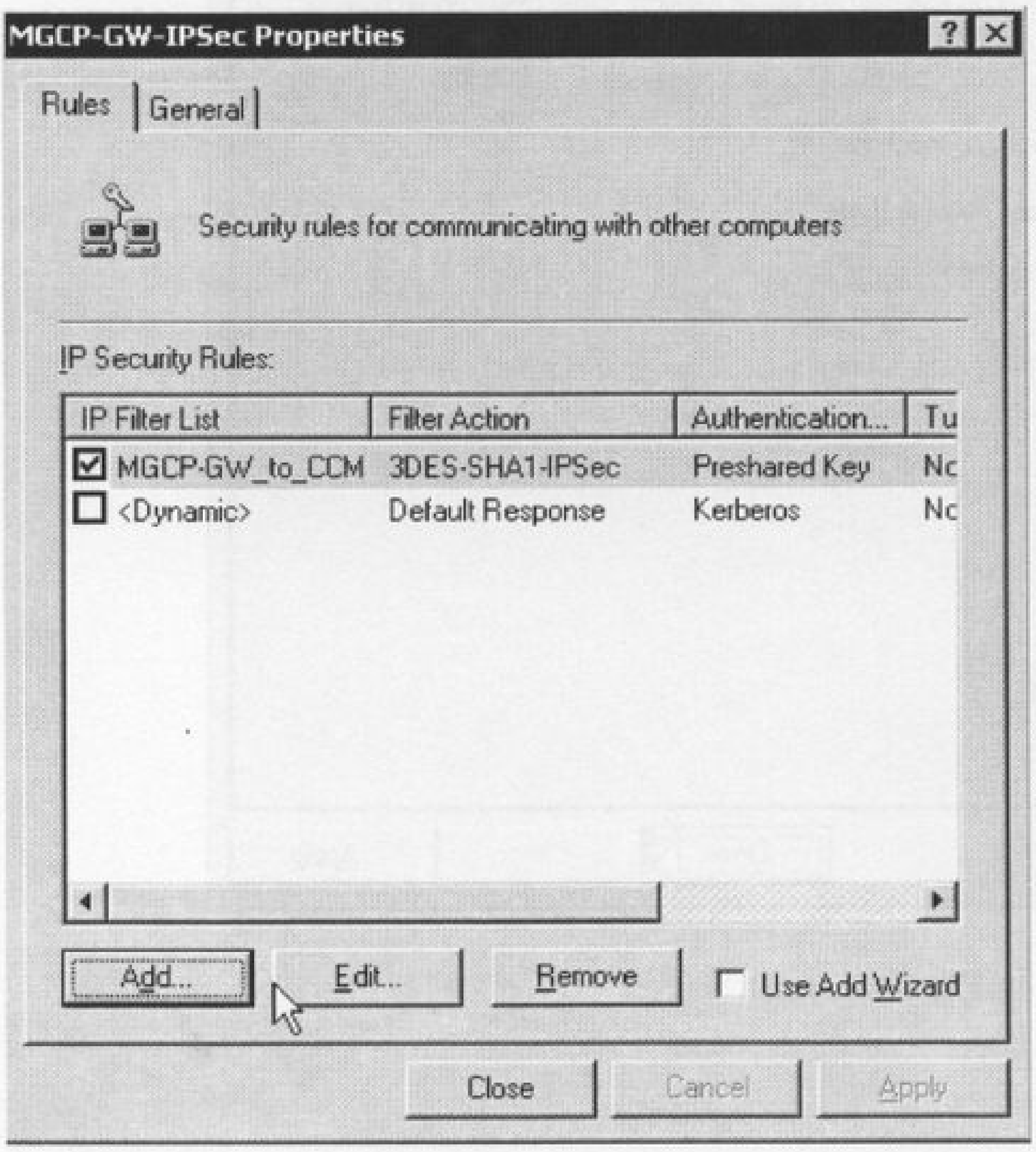

Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.
Authentication Method preference order:
Method
Details
Preshared Key
cisco
Add...
Edit...
Remove
Move up
Move down
Close
Cancel
Apply

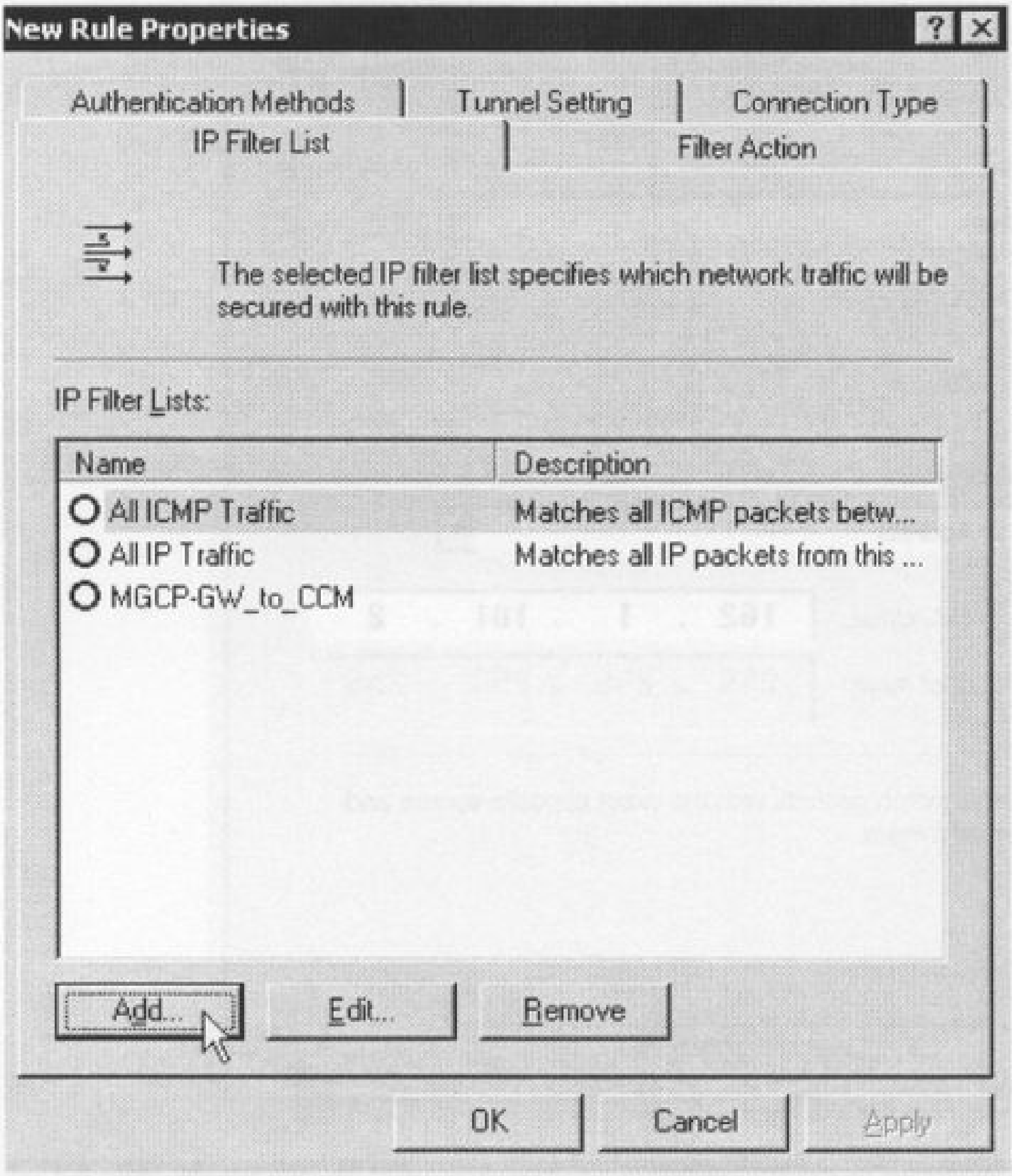
➔ **Here we *could* specify a tunnel endpoint – and on the other end (IOS Rtr) we would also have to leave the default for the 'crypto ipsec transform-set' of Tunnel. Instead, we have chosen (based on Cisco's recommendation) to use Transport method on both ends – specified here by saying that "This rule does not specify an IPSec tunnel".**

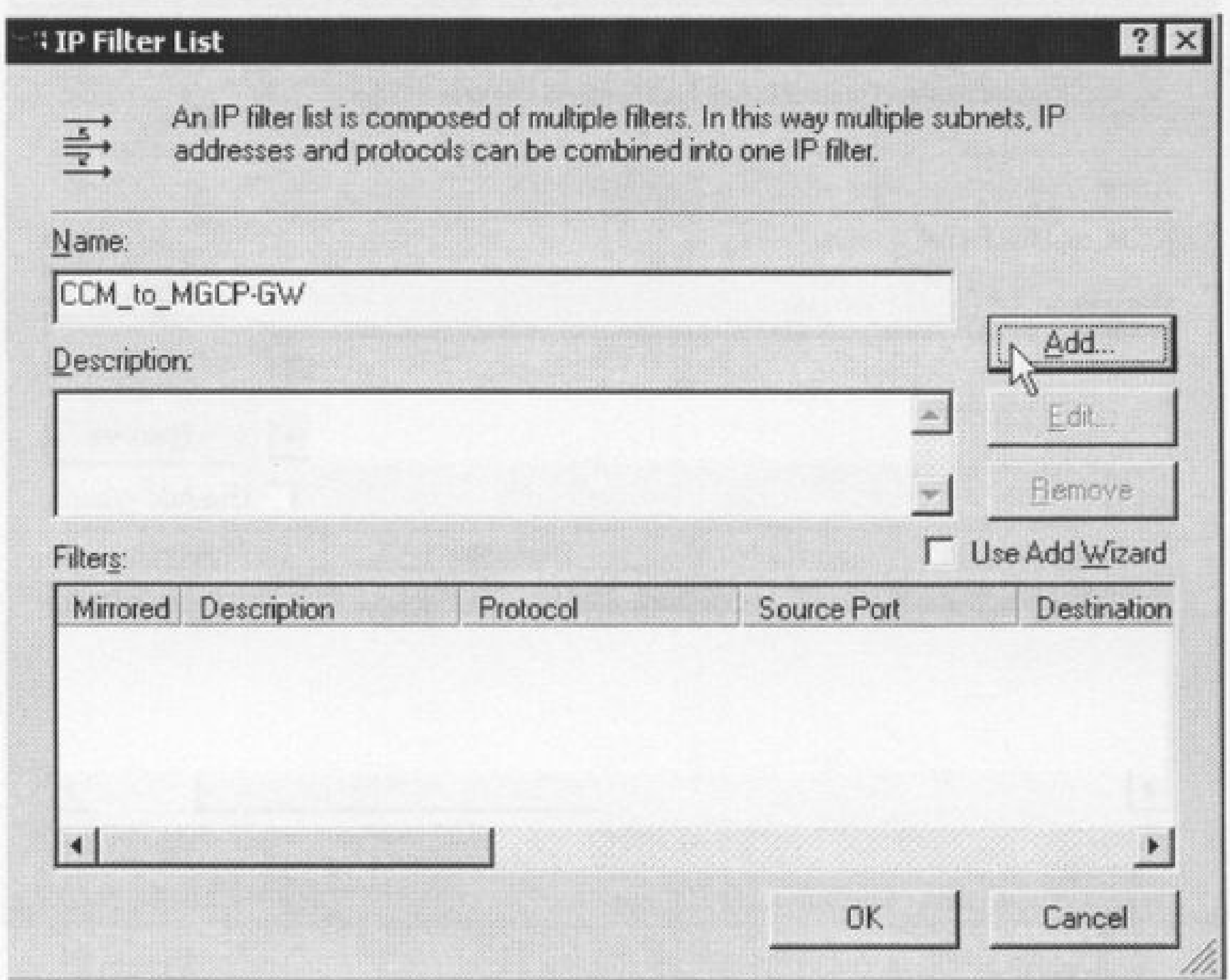


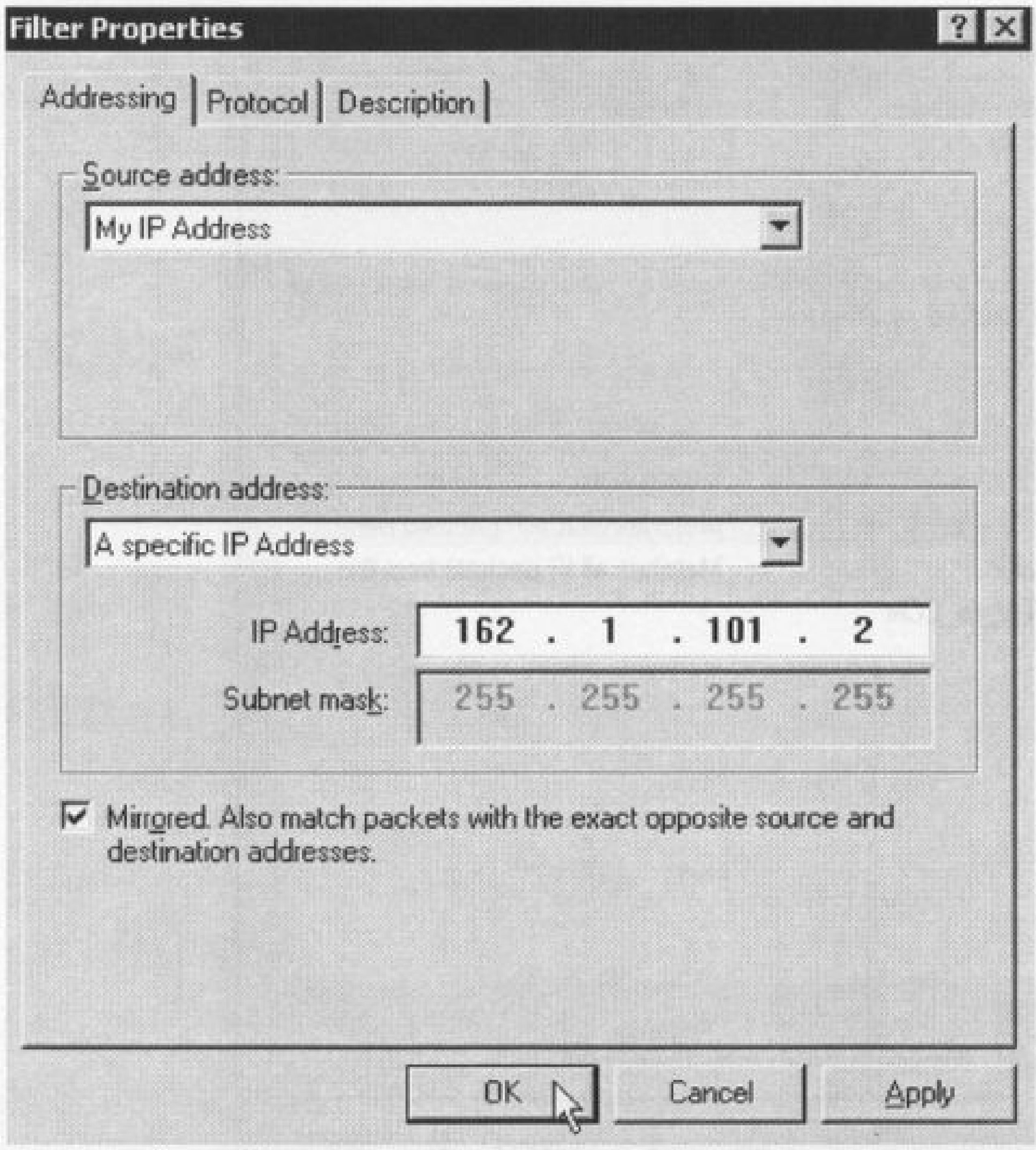

Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
This rule only applies to network traffic over connections of the selected type.
All network connections
Local area network (LAN)
Remote access
Close
Cancel
Apply

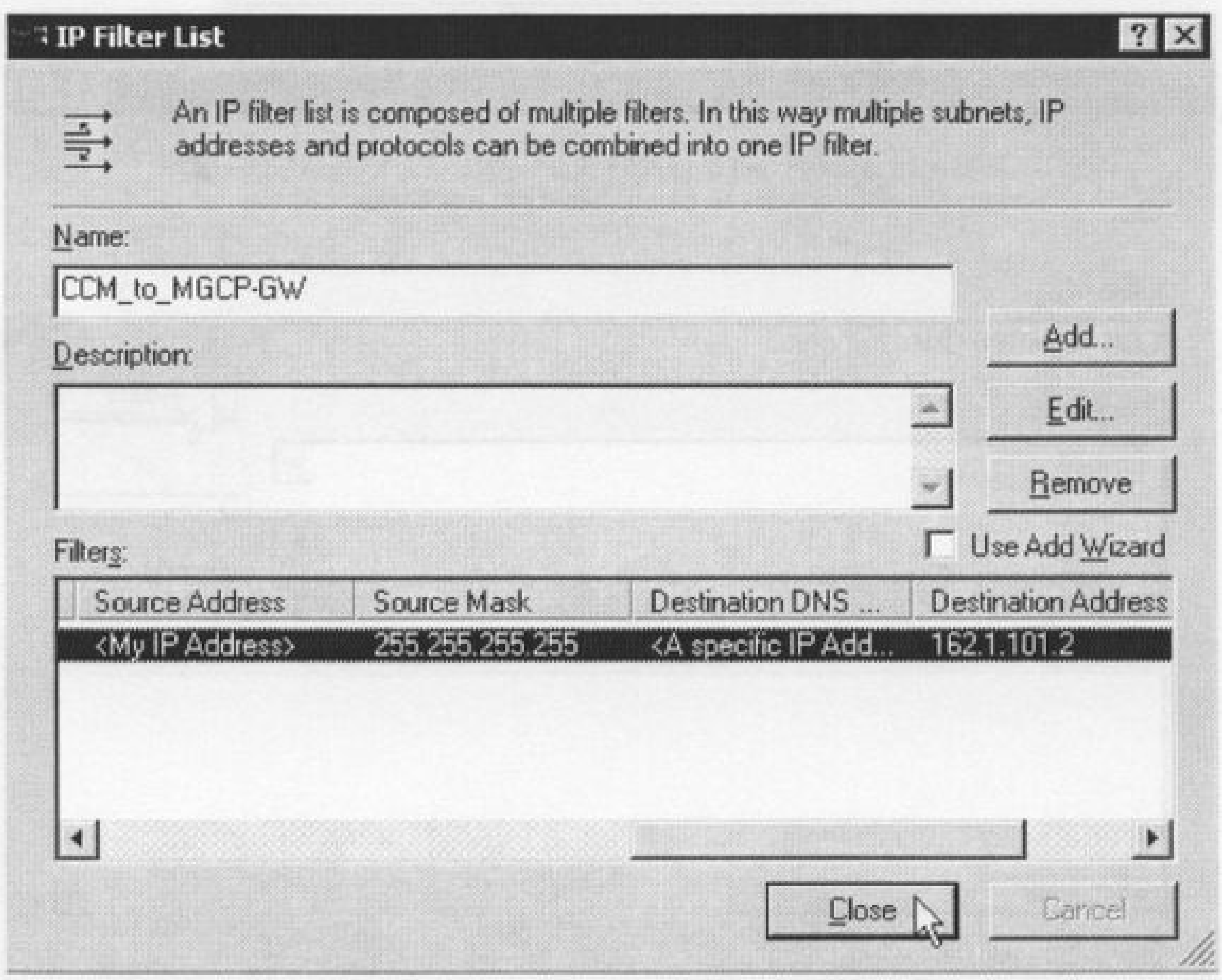
➔ **Now we have created one way of communication – as pointed out before, with MS W2k server – we now need to create the opposite direction flow of encrypted traffic (NOTE: As of the publishing of this Proctor Guide – Cisco's documentation for IPSec with MGCP did not mention that this second Rule was necessary – but elsewhere on CCO it does point out that this is absolutely necessary. It also won't work unless you do this next step. ;)**

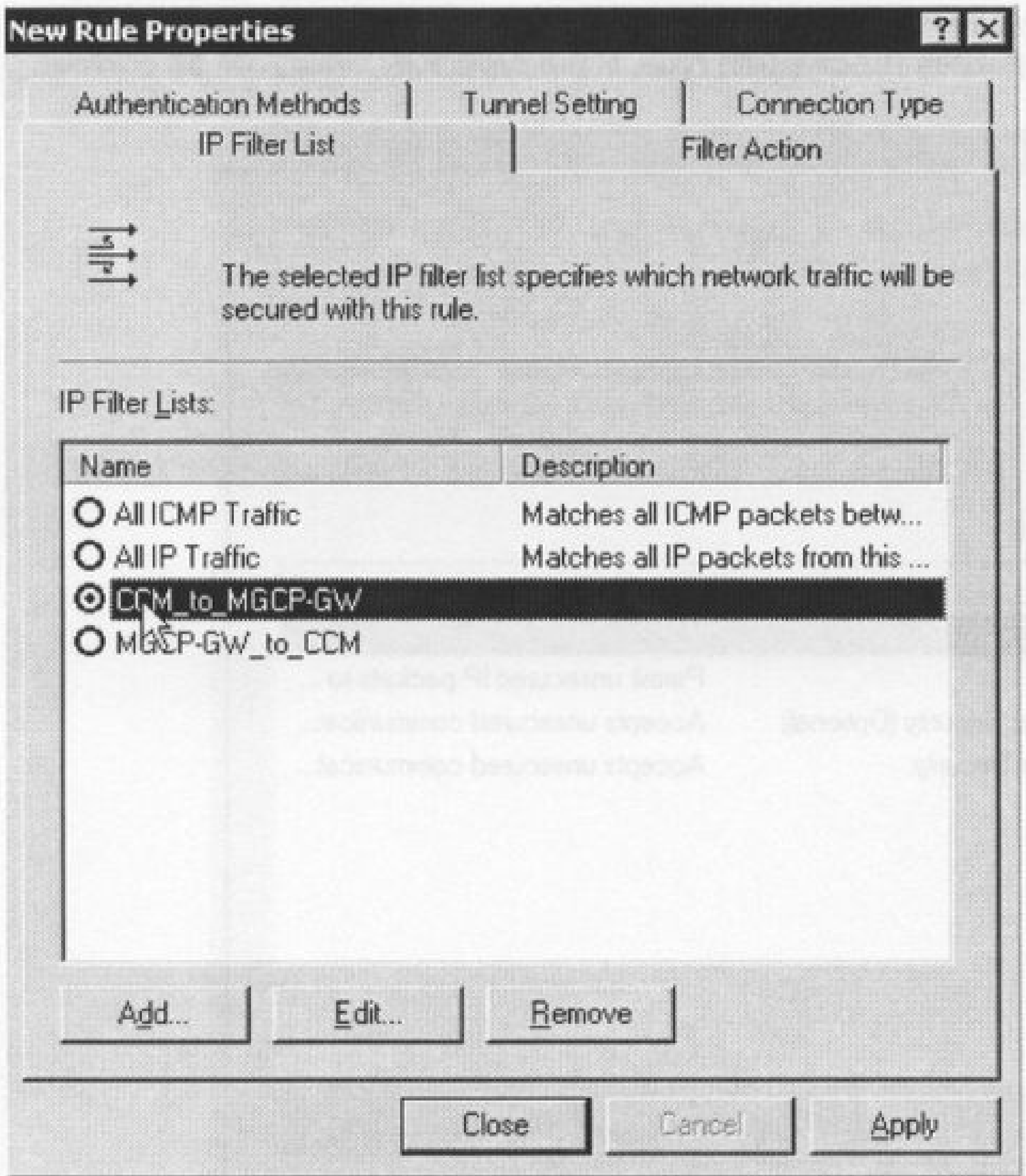



New Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected IP filter list specifies which network traffic will be secured with this rule.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
MGCP-GW_to_CCM
Add...
Edit...
Remove
OK
Cancel
Apply

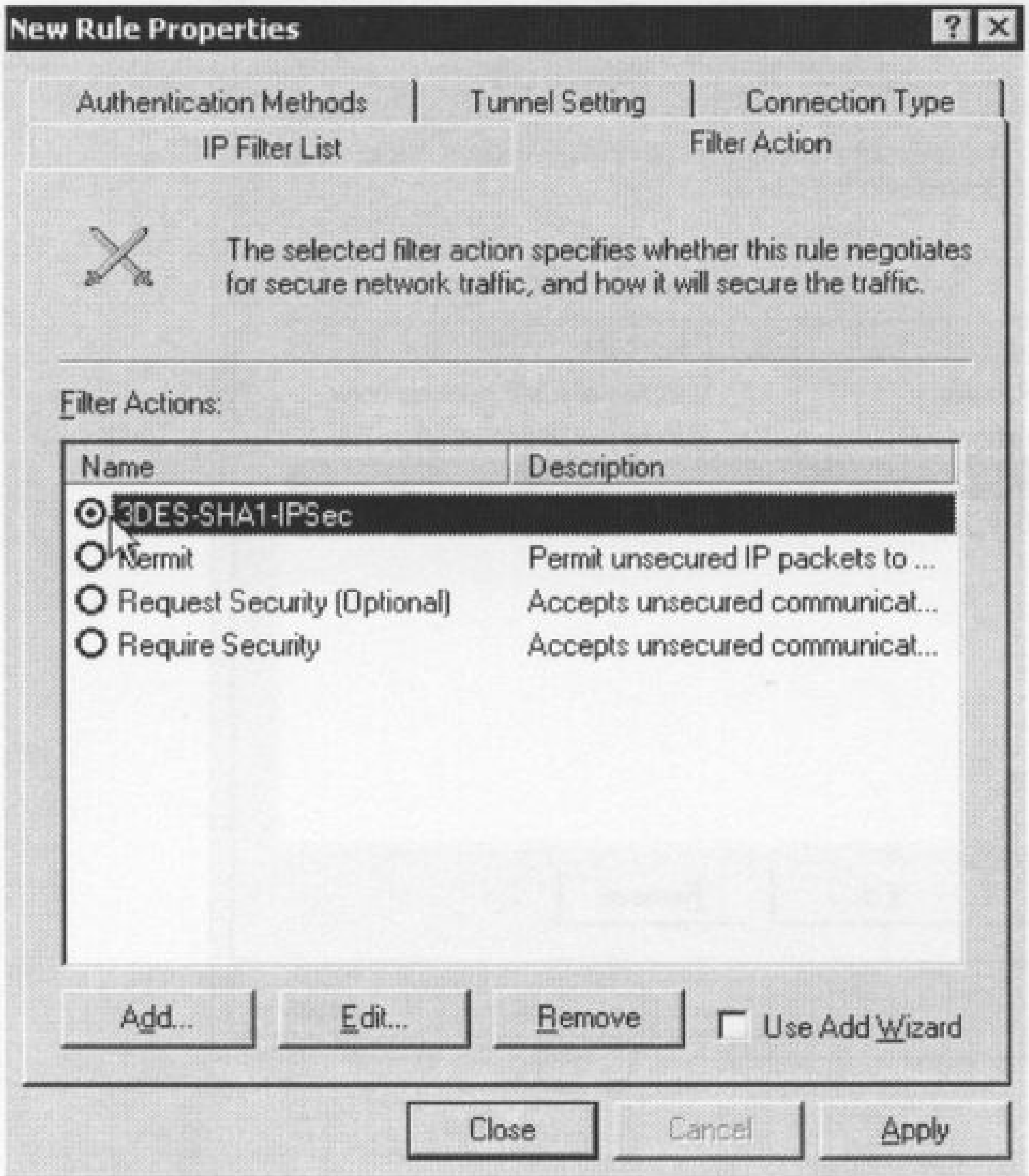

IP Filter List
An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
CCM_to_MGCP-GW
Description:
Add...
Edit...
Remove
Use Add Wizard
Filters:
Mirrored
Description
Protocol
Source Port
Destination
OK
Cancel

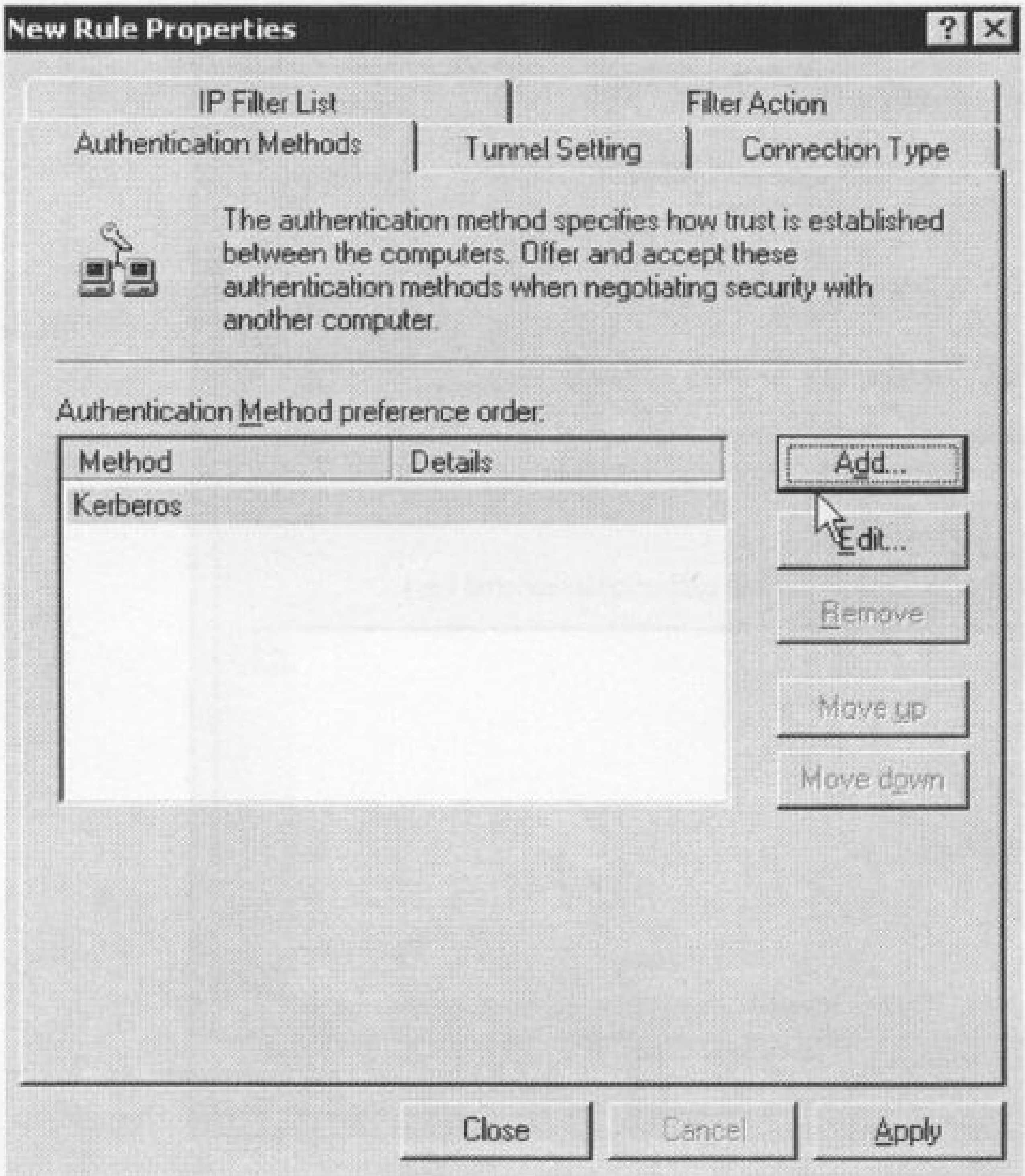

Filter Properties
Addressing
Protocol
Description
Source address:
My IP Address
Destination address:
A specific IP Address
IP Address: 162 . 1 . 101 . 2
Subnet mask: 255 . 255 . 255 . 255
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK
Cancel
Apply

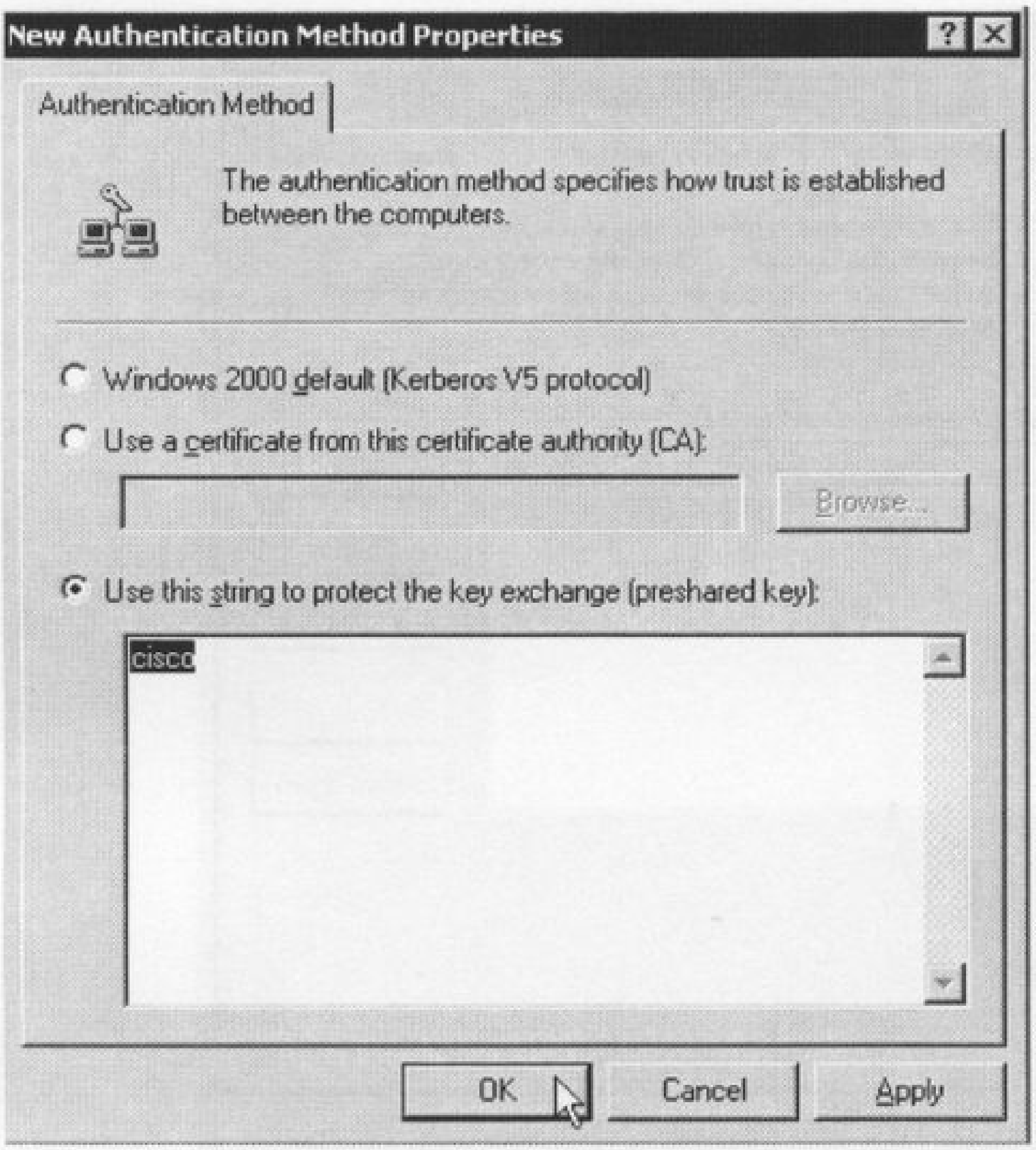

IP Filter List
An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
CCM_to_MGCP-GW
Description:
Add...
Edit...
Remove
Filters:
Use Add Wizard
Source Address
Source Mask
Destination DNS ...
Destination Address
<My IP Address>
255.255.255.255
<A specific IP Add...
162.1.101.2
Close
Cancel

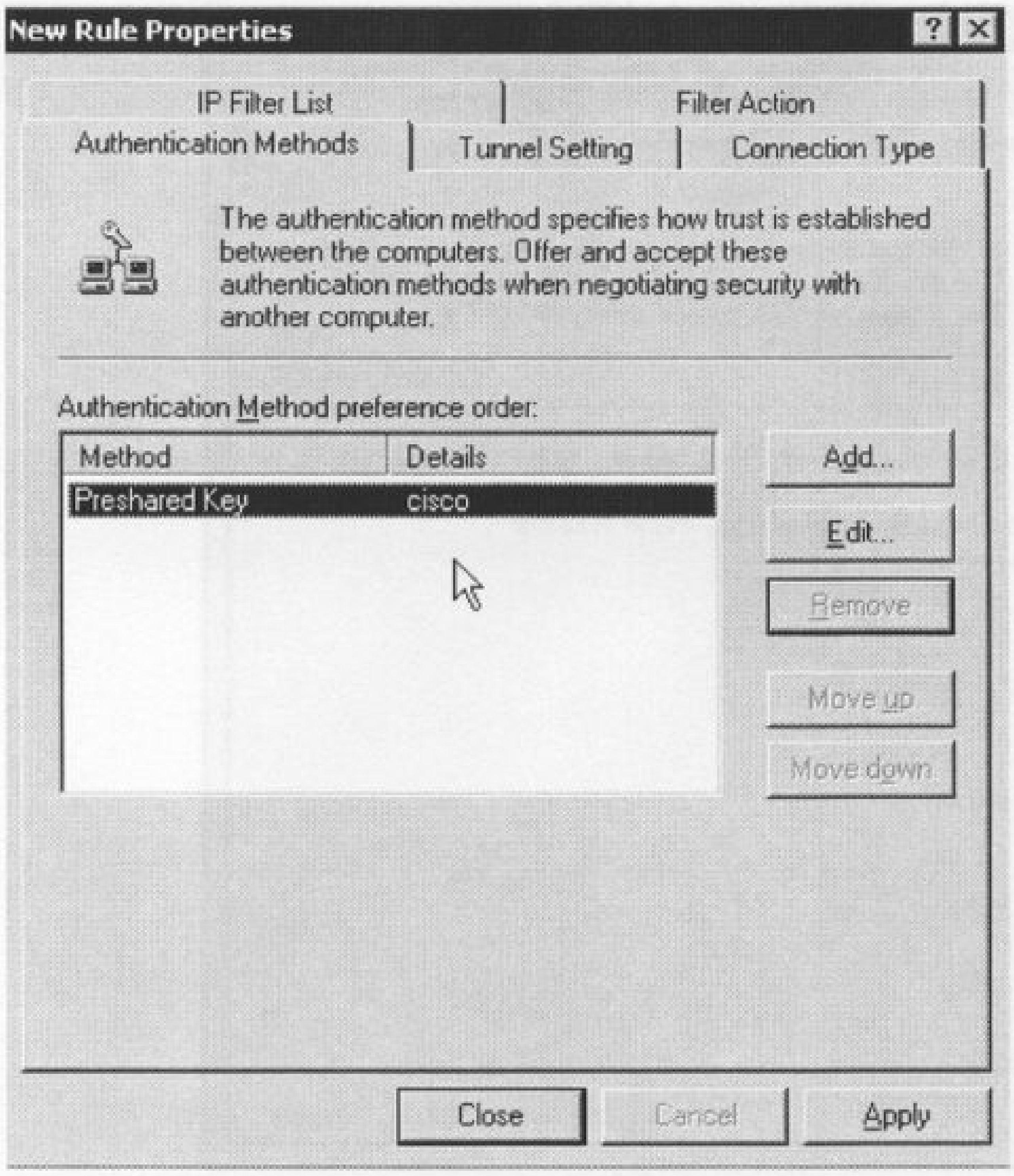

New Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected IP filter list specifies which network traffic will be secured with this rule.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
CCM_to_MGCP-GW
MGCP-GW_to_CCM
Add...
Edit...
Remove
Close
Cancel
Apply

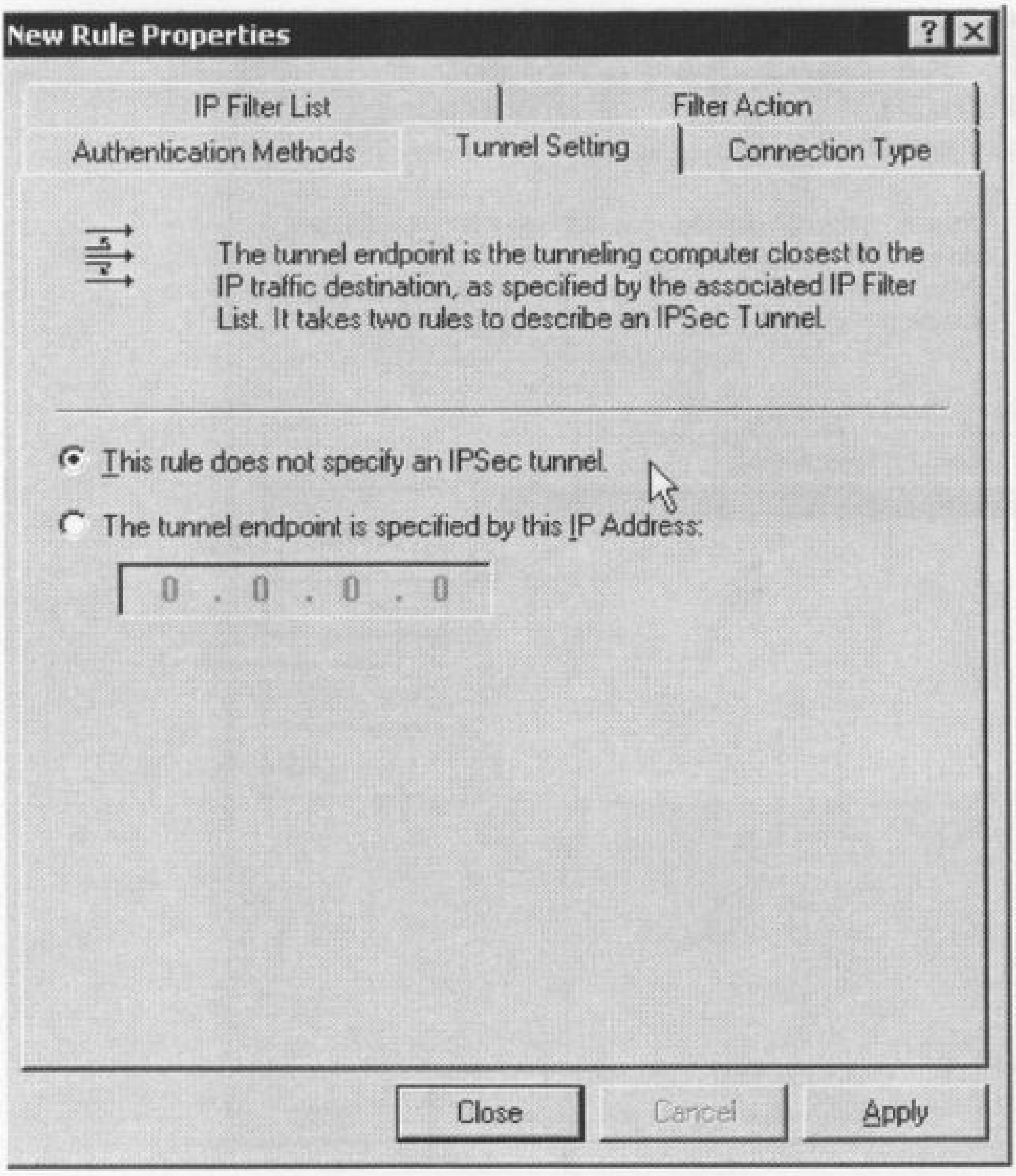
➔ **Here we can use the same Filter that we setup in the previous Rule – since we know its properties (Encryption type, Hash type, Key timer) are all correct.**

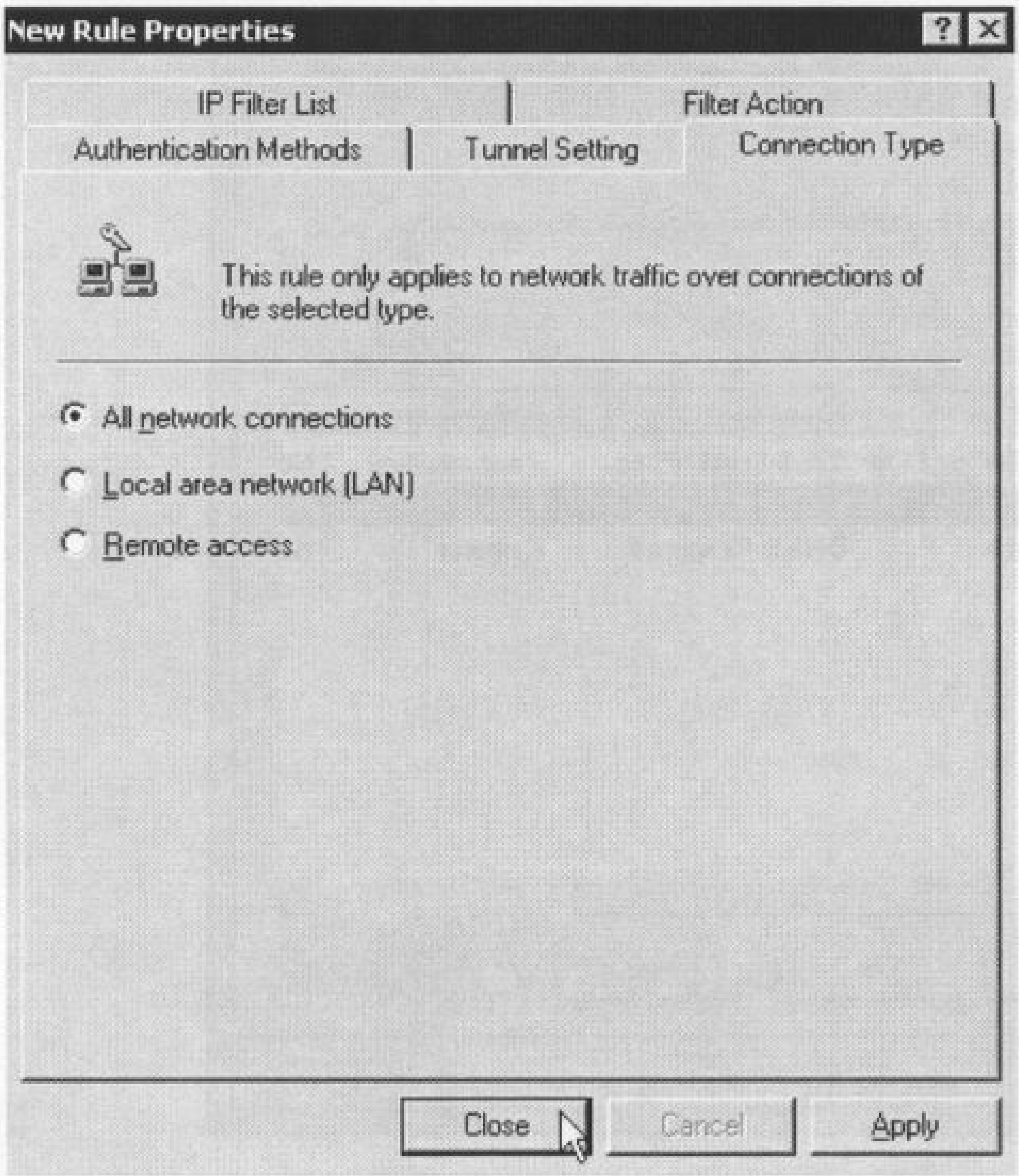


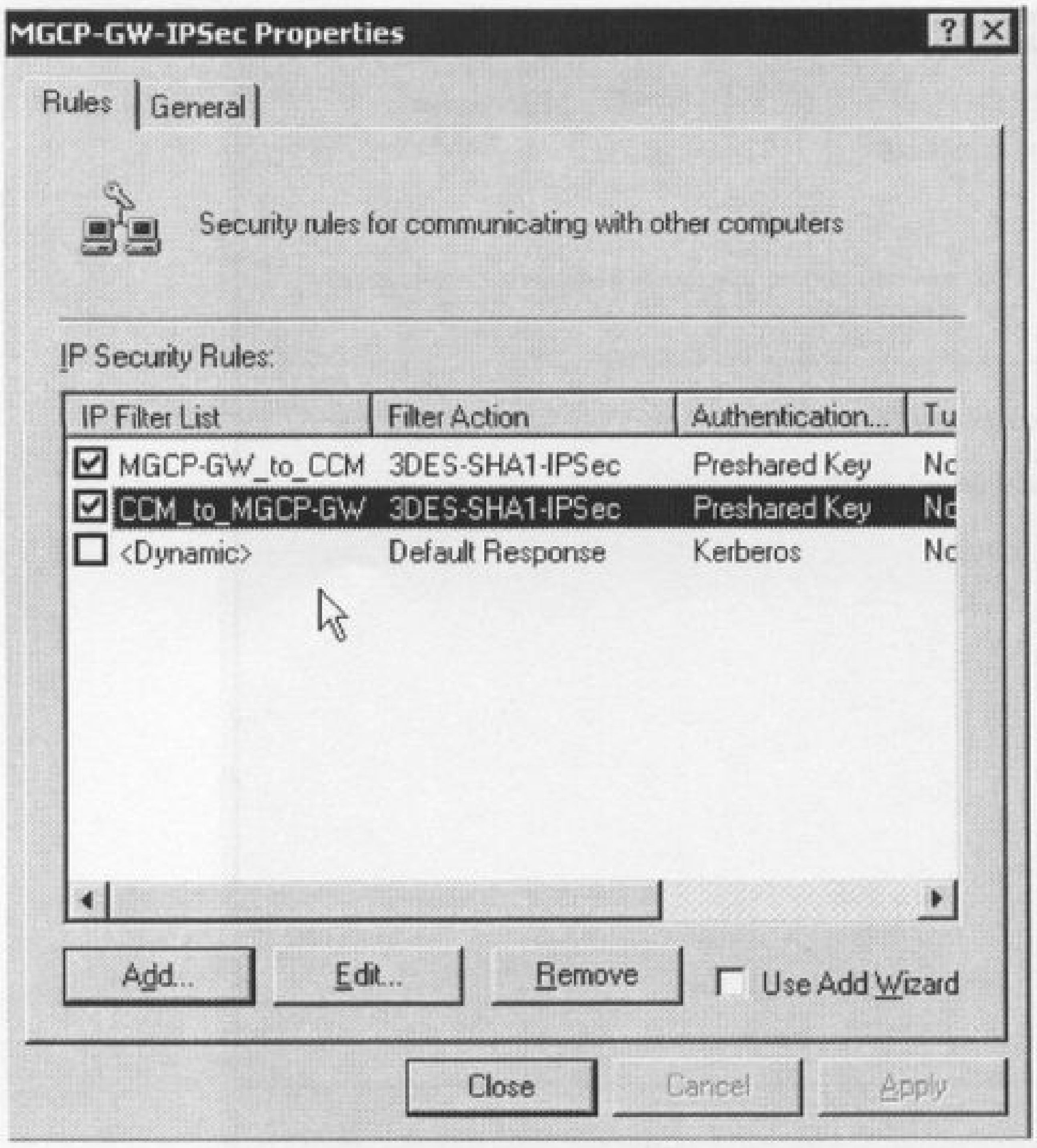

New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.
Authentication Method preference order:
Method
Details
Kerberos
Add...
Edit...
Remove
Move up
Move down
Close
Cancel
Apply


New Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
cisco
OK
Cancel
Apply

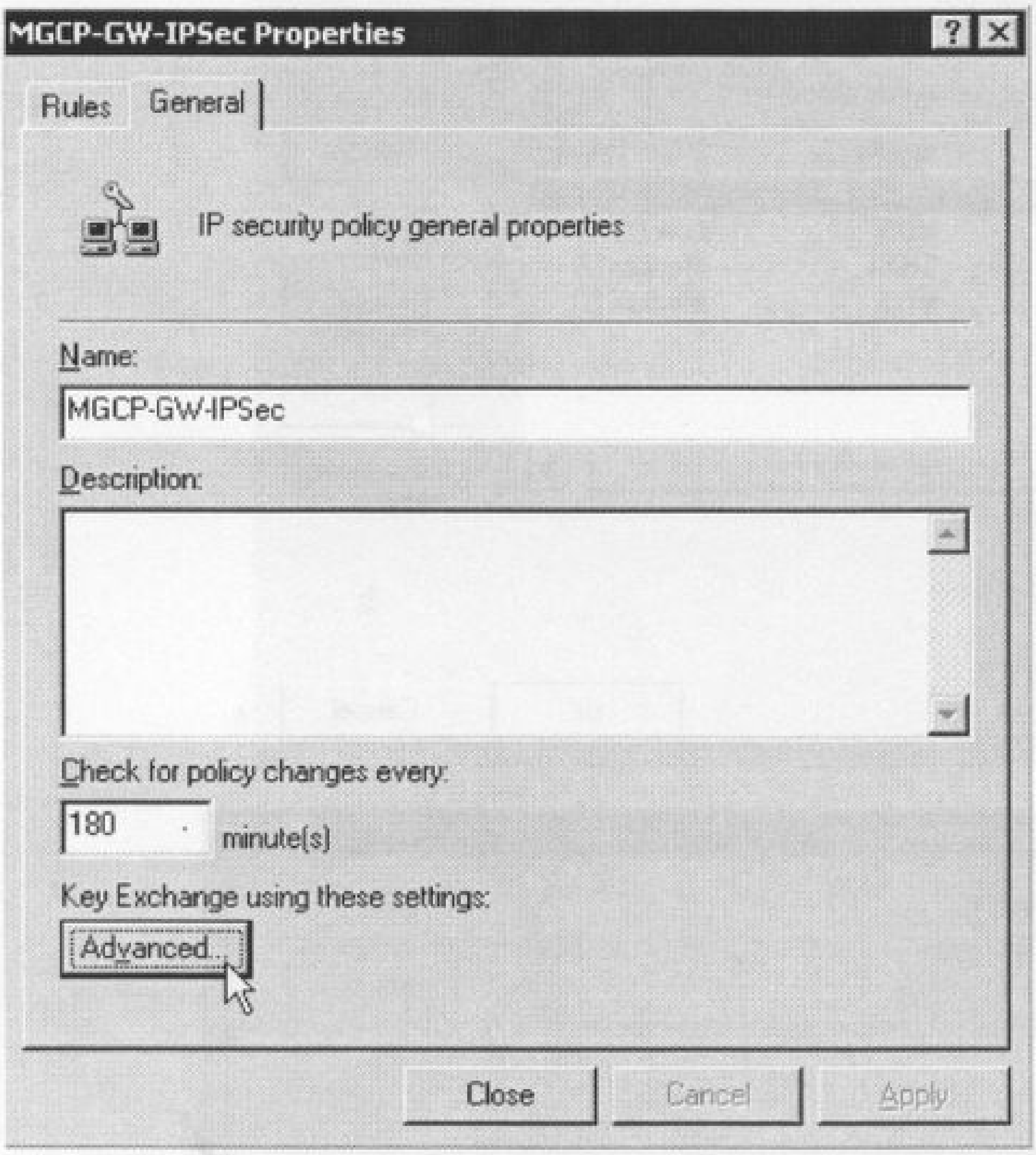

New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.
Authentication Method preference order:
Method
Details
Preshared Key
cisco
Add...
Edit...
Remove
Move up
Move down
Close
Cancel
Apply

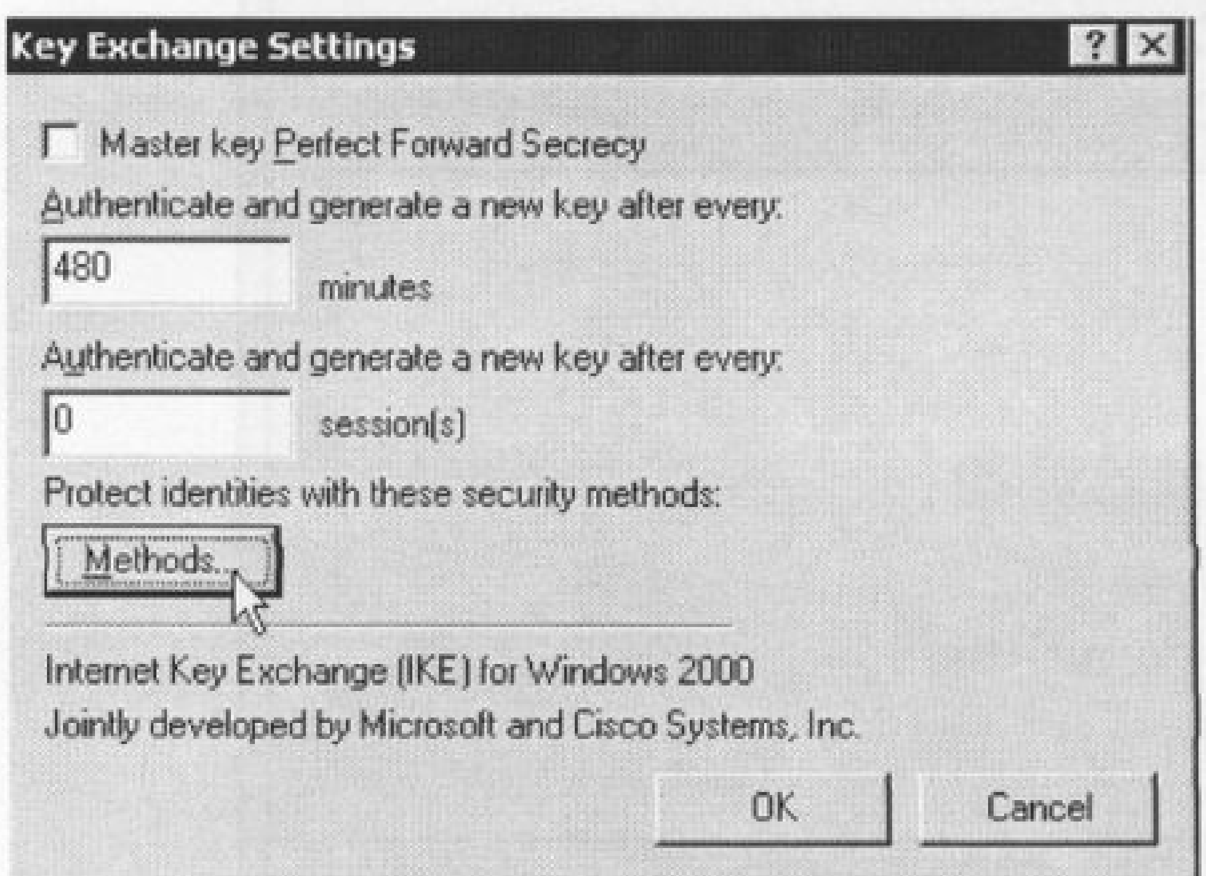

New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.
This rule does not specify an IPSec tunnel.
The tunnel endpoint is specified by this IP Address:
0 . 0 . 0 . 0
Close
Cancel
Apply

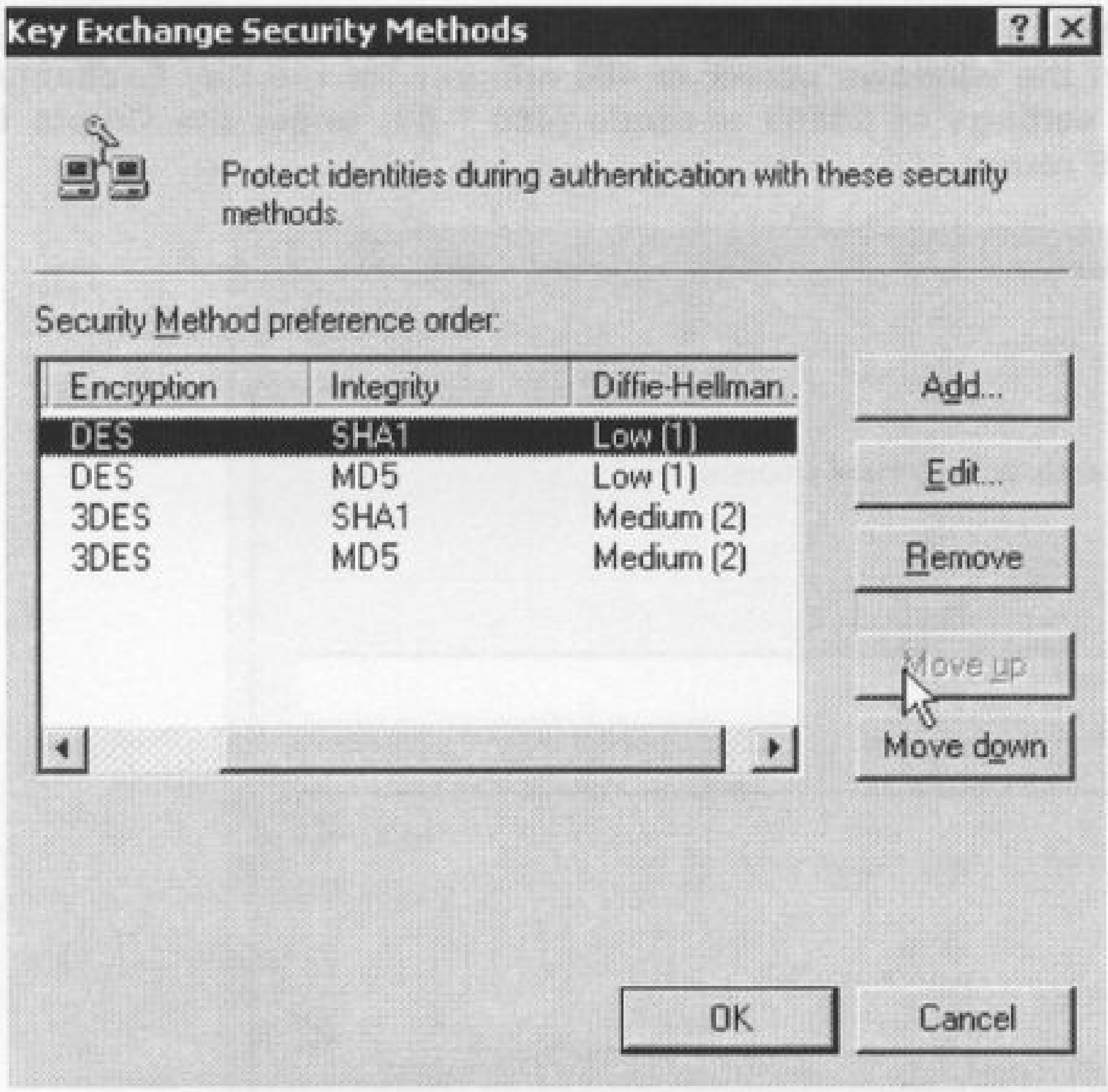

New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
This rule only applies to network traffic over connections of the selected type.
All network connections
Local area network (LAN)
Remote access
Close
Cancel
Apply

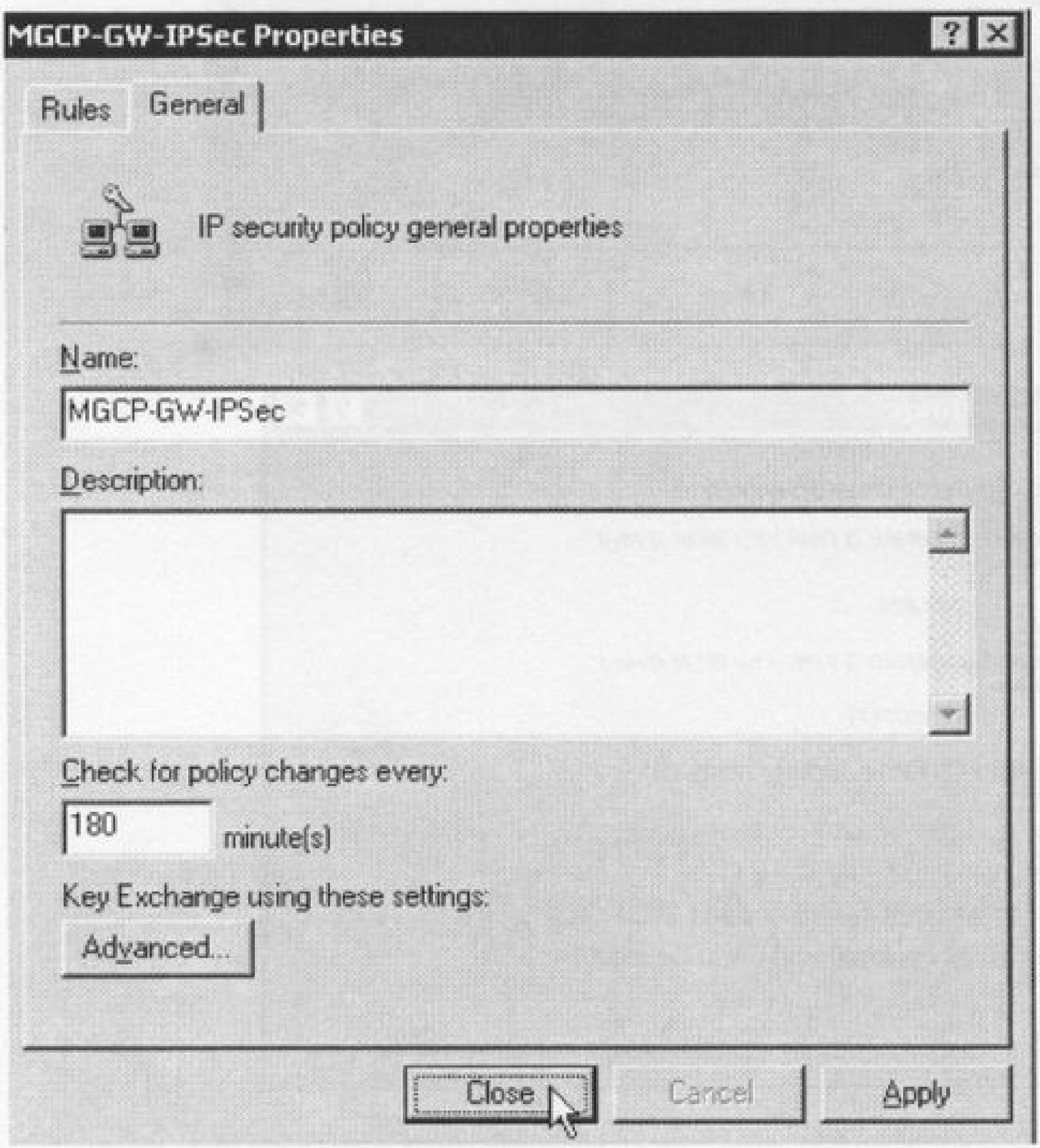

MGCP-GW-IPSec Properties
Rules
General
Security rules for communicating with other computers
IP Security Rules:
IP Filter List
Filter Action
Authentication...
Tu
MGCP-GW_to_CCM
3DES-SHA1-IPSec
Preshared Key
Nc
CCM_to_MGCP-GW
3DES-SHA1-IPSec
Preshared Key
Nc
<Dynamic>
Default Response
Kerberos
Nc
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

➔ **Again – everything needs to match on both sides of the IPSec connection – in this case we will set the windows server to 480 minutes for the Key Exchange which will match the settings of 28800 seconds (480 * 60) under the Crypto ISAKMP Policy in the IOS router.**

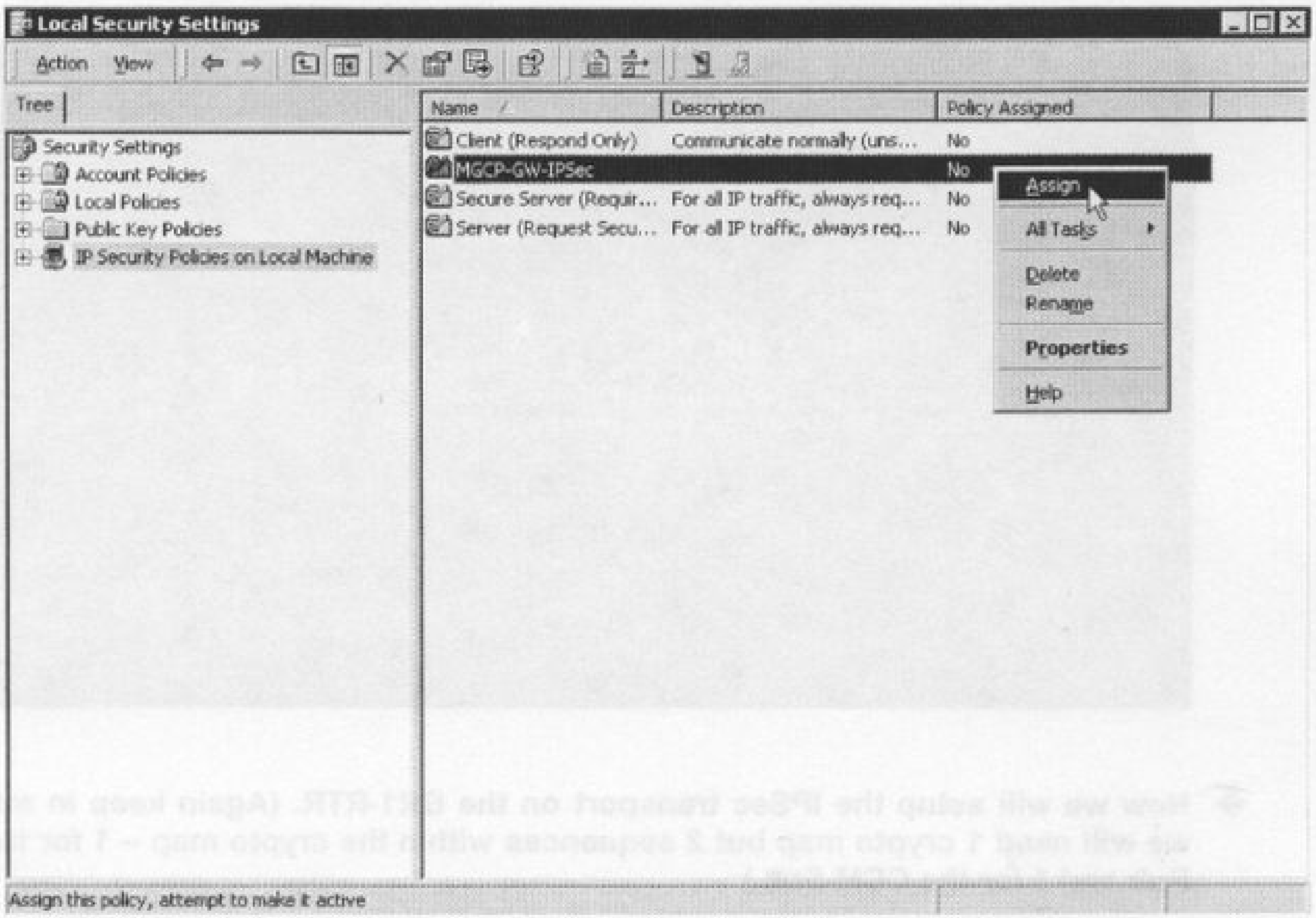


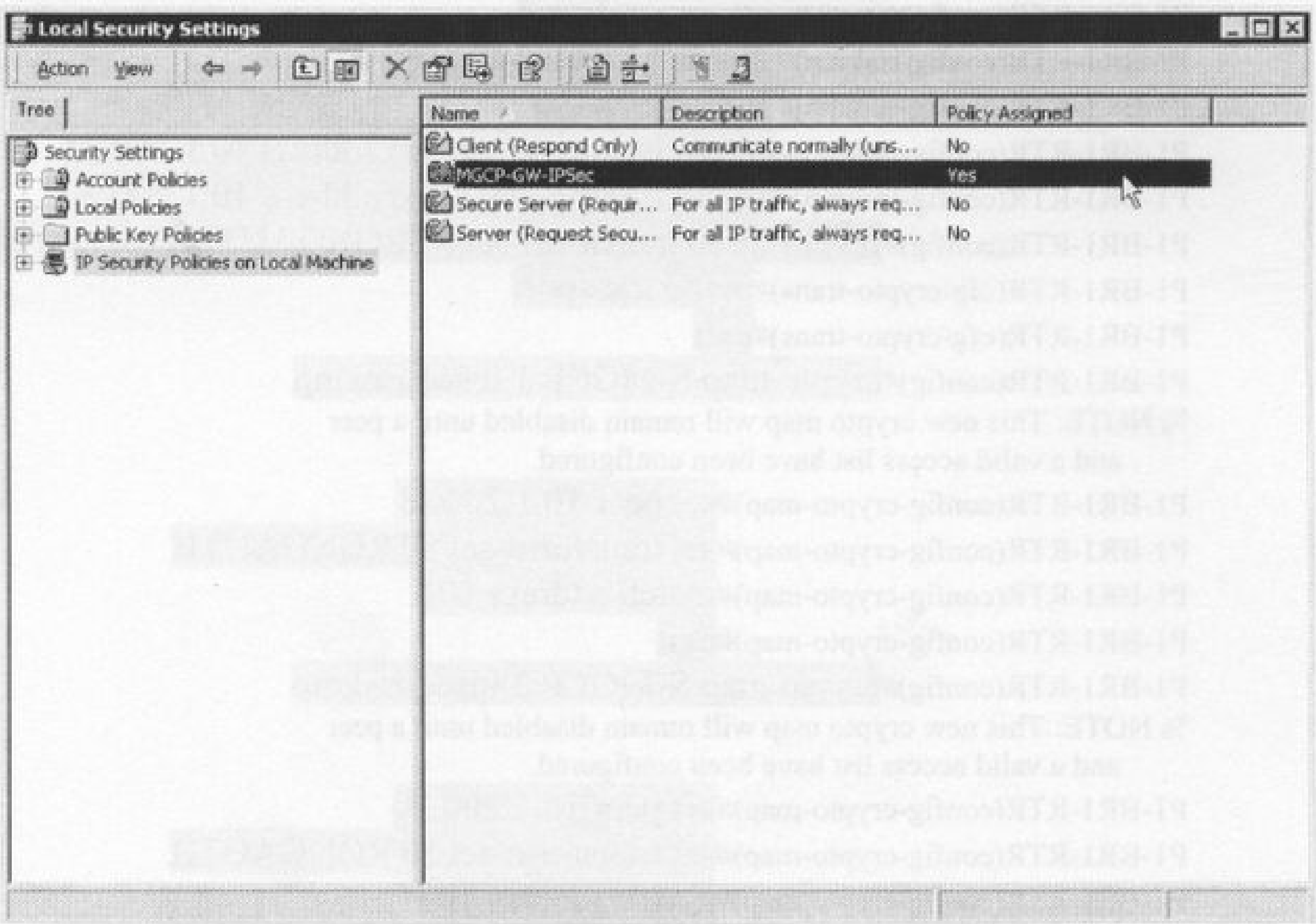



Key Exchange Security Methods
Protect identities during authentication with these security methods.
Security Method preference order:
Encryption
Integrity
Diffie-Hellman ...
DES SHA1 Low (1)
DES MD5 Low (1)
3DES SHA1 Medium (2)
3DES MD5 Medium (2)
Add...
Edit...
Remove
Move up
Move down
OK
Cancel

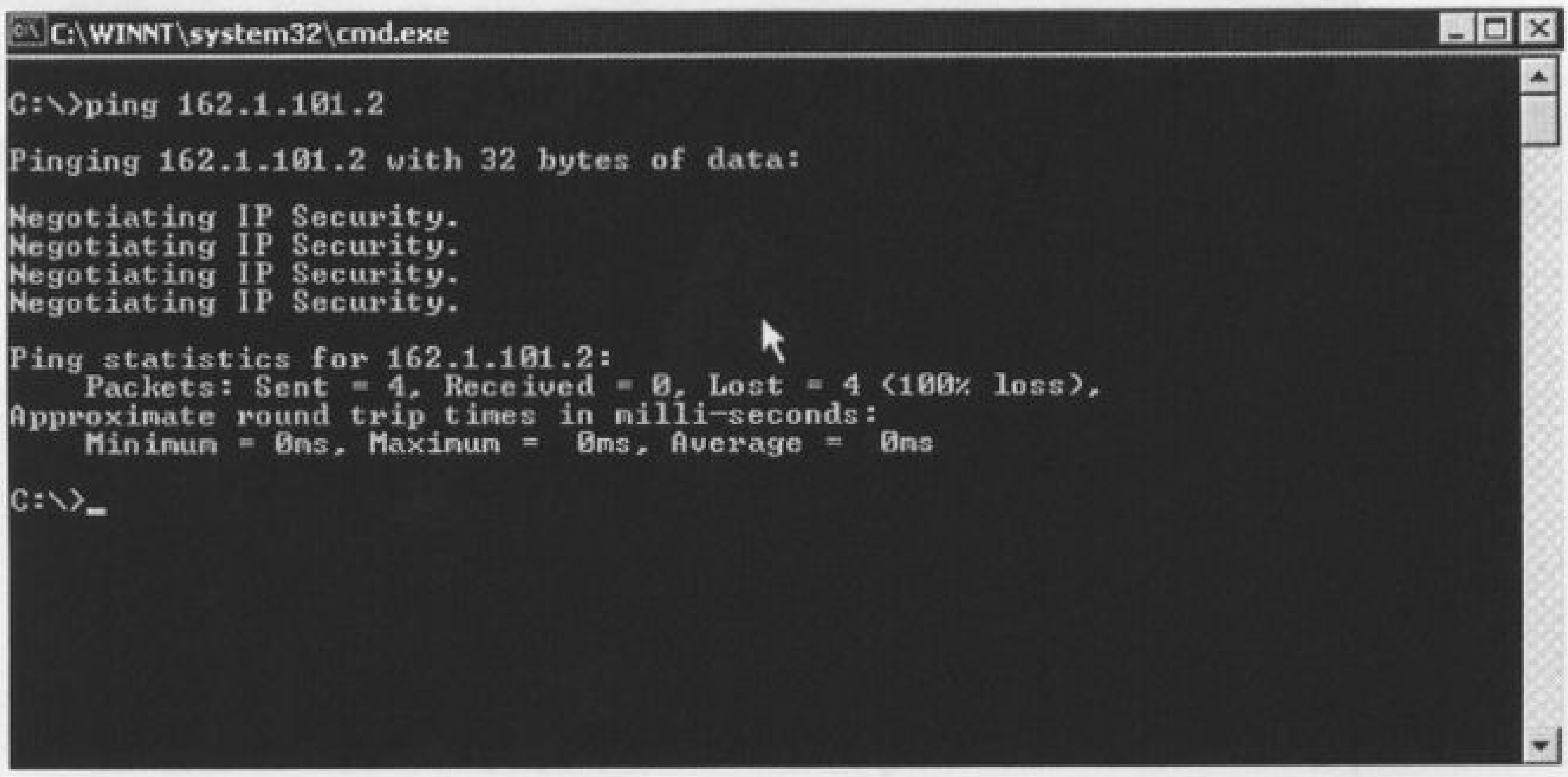

MGCP-GW-IPSec Properties
Rules
General
IP security policy general properties
Name:
MGCP-GW-IPSec
Description:
Check for policy changes every:
180
minute(s)
Key Exchange using these settings:
Advanced...
Close
Cancel
Apply

➔ Finally we will tell the new policy to be "Assigned" and then test with a PING.





➔ **Now we test and notice that it is not working – not yet at least – we must now setup the IOS Router.**



➔ **Now we will setup the IPSec transport on the BR1-RTR. (Again keep in mind that we will need 1 crypto map but 2 sequences within the crypto map – 1 for the CCM-Pub and 1 for the CCM-Sub.)**

```
P1-BR1-RTR(config)#crypto isakmp policy 1
P1-BR1-RTR(config-isakmp)# authentication pre-share
P1-BR1-RTR(config-isakmp)# lifetime 28800
P1-BR1-RTR(config-isakmp)#crypto isakmp key cisco address 10.1.200.21
P1-BR1-RTR(config-isakmp)#crypto isakmp key cisco address 10.1.200.20
P1-BR1-RTR(config)#crypto ipsec transform-set STRONGAUTH esp-3des esp-sha-hmac
P1-BR1-RTR(cfg-crypto-trans)#mode transport
P1-BR1-RTR(cfg-crypto-trans)#exit
P1-BR1-RTR(config)#crypto map S-MGCP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
P1-BR1-RTR(config-crypto-map)#set peer 10.1.200.21
P1-BR1-RTR(config-crypto-map)#set transform-set STRONGAUTH
P1-BR1-RTR(config-crypto-map)#match address 101
P1-BR1-RTR(config-crypto-map)#exit
P1-BR1-RTR(config)#crypto map S-MGCP 2 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
P1-BR1-RTR(config-crypto-map)#set peer 10.1.200.20
P1-BR1-RTR(config-crypto-map)#set transform-set STRONGAUTH
P1-BR1-RTR(config-crypto-map)#match address 102
P1-BR1-RTR(config-crypto-map)#exit
P1-BR1-RTR(config)#access-list 101 permit ip host 162.1.101.2 host 10.1.200.21
P1-BR1-RTR(config)#access-list 102 permit ip host 162.1.101.2 host 10.1.200.20
P1-BR1-RTR(config)#int s0/1/0.1
```

P1-BR1-RTR(config-subif)#crypto map S-MGCP
Mar 21 22:03:16.299: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
P1-BR1-RTR(config)#end
P1-BR1-RTR#ping 10.1.200.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.200.21, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/9/12 ms
P1-BR1-RTR#

P1-BR1-RTR#sh crypto ipsec sa

interface: Serial0/1/0.1
Crypto map tag: S-MGCP, local addr 162.1.101.2

protected vrf: (none)
local ident (addr/mask/prot/port): (**162.1.101.2**/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (**10.1.200.20**/255.255.255.255/0/0) *//(This CCM is not presently online)*
current_peer 10.1.200.20 port 500
PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 4293, #recv errors 0

local crypto endpt.: 162.1.101.2, remote crypto endpt.: **10.1.200.20**
path mtu 1500, ip mtu 1500
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (**162.1.101.2**/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (**10.1.200.21**/255.255.255.255/0/0)
current_peer 10.1.200.21 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 2549, #pkts encrypt: 2549, #pkts digest: 2549
#pkts decaps: 2546, #pkts decrypt: 2546, #pkts verify: 2546
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 162.1.101.2, remote crypto endpt.: **10.1.200.21**
path mtu 1500, ip mtu 1500
current outbound spi: 0xC26DE641(3261982273)

inbound esp sas:
spi: 0x65EAF47C(1709896828)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 3005, flow_id: Onboard VPN:5, crypto map: S-MGCP
sa timing: remaining key lifetime (k/sec): (4437218/1346)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

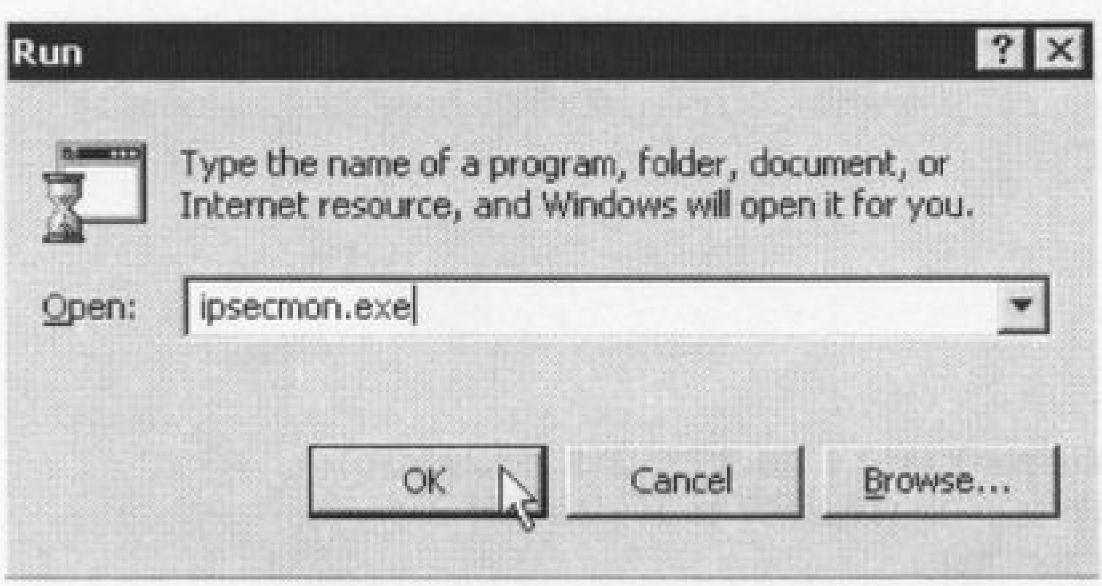
inbound pcp sas:

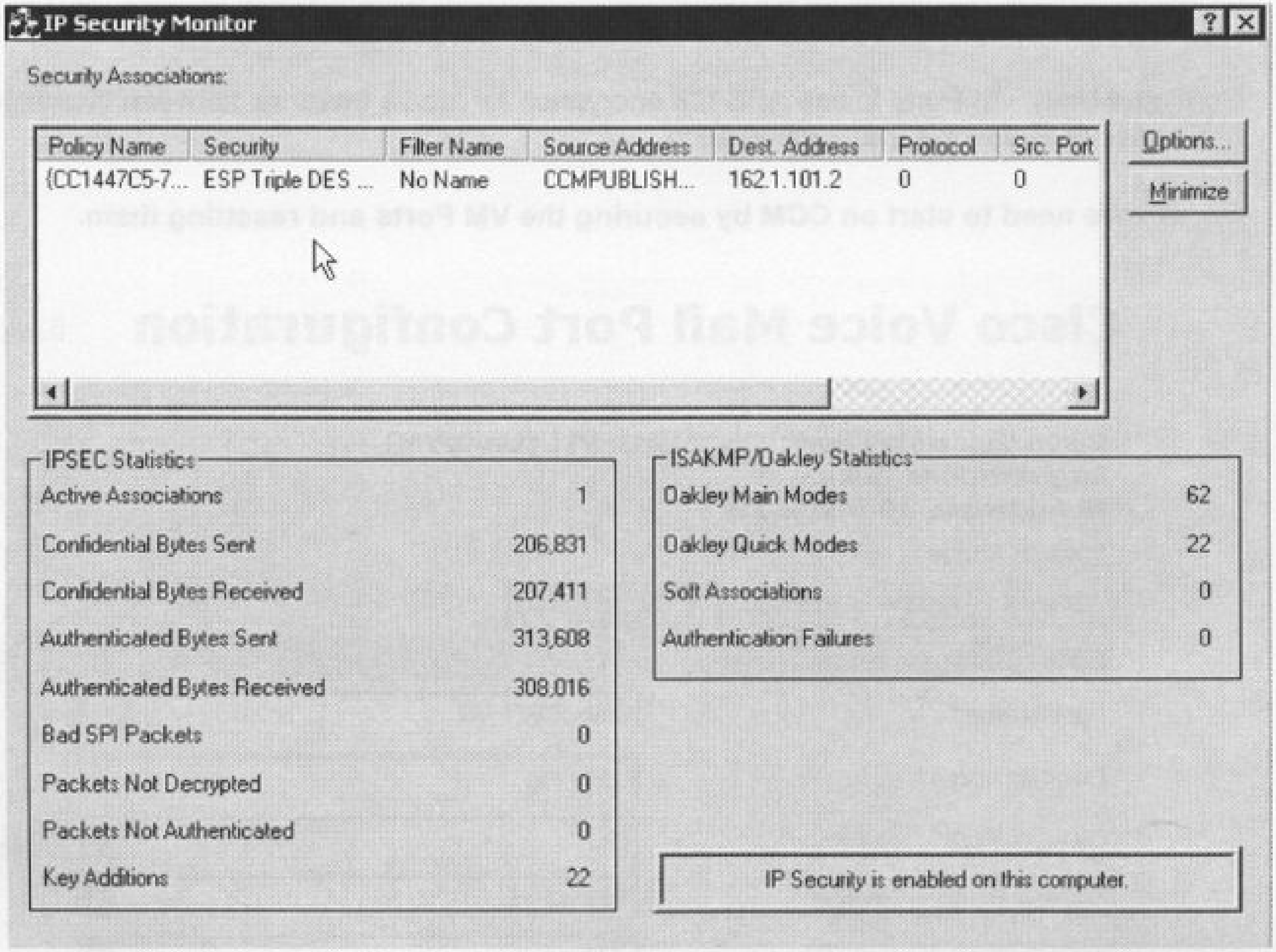
outbound esp sas:
spi: 0xC26DE641(3261982273)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 3006, flow_id: Onboard VPN:6, crypto map: S-MGCP
sa timing: remaining key lifetime (k/sec): (4437229/1346)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

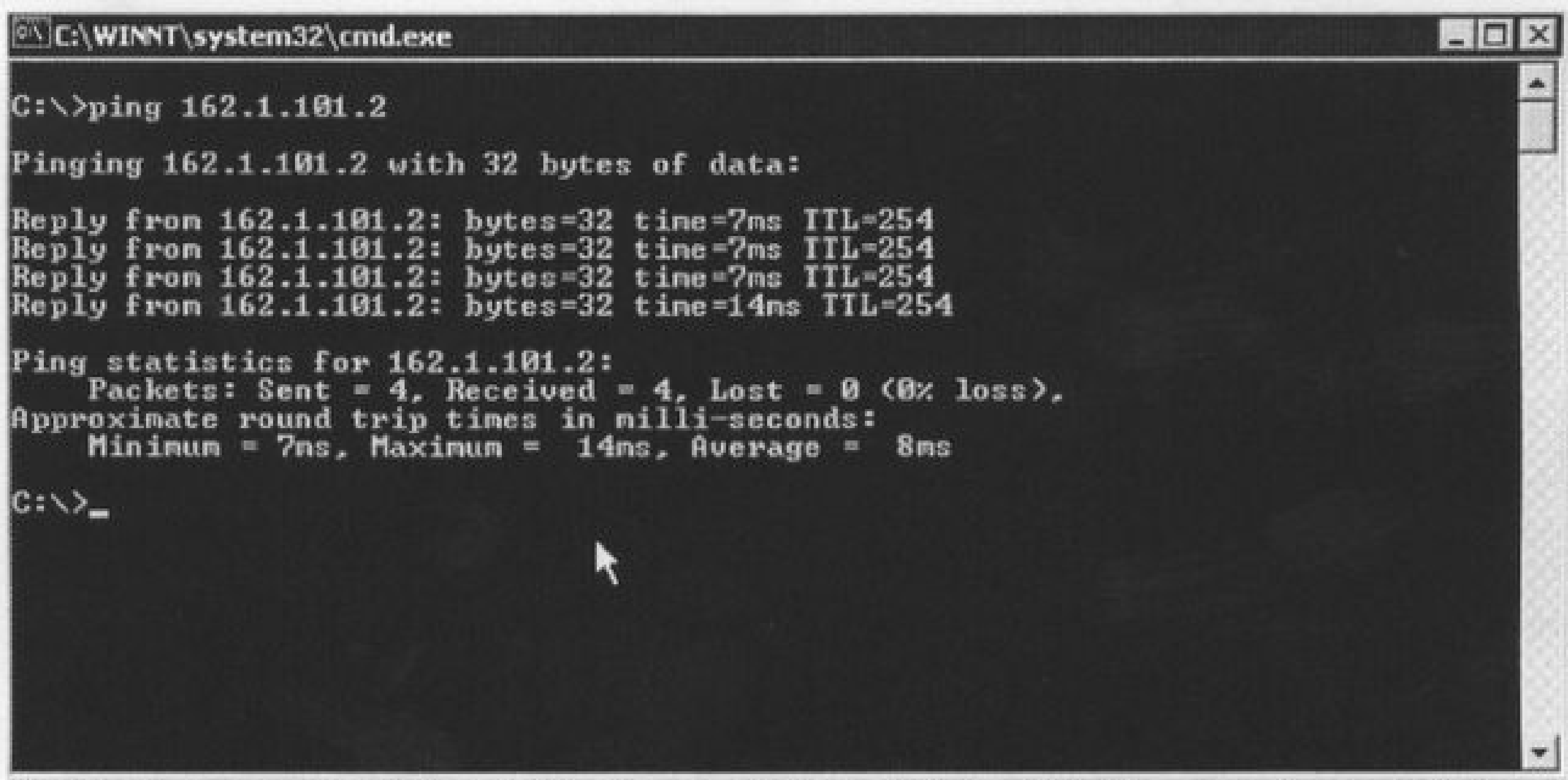
outbound ah sas:

outbound pcp sas:
P1-BR1-RTR#

➔ **Back on the CCM, let's ensure that the tunnel is indeed up.**



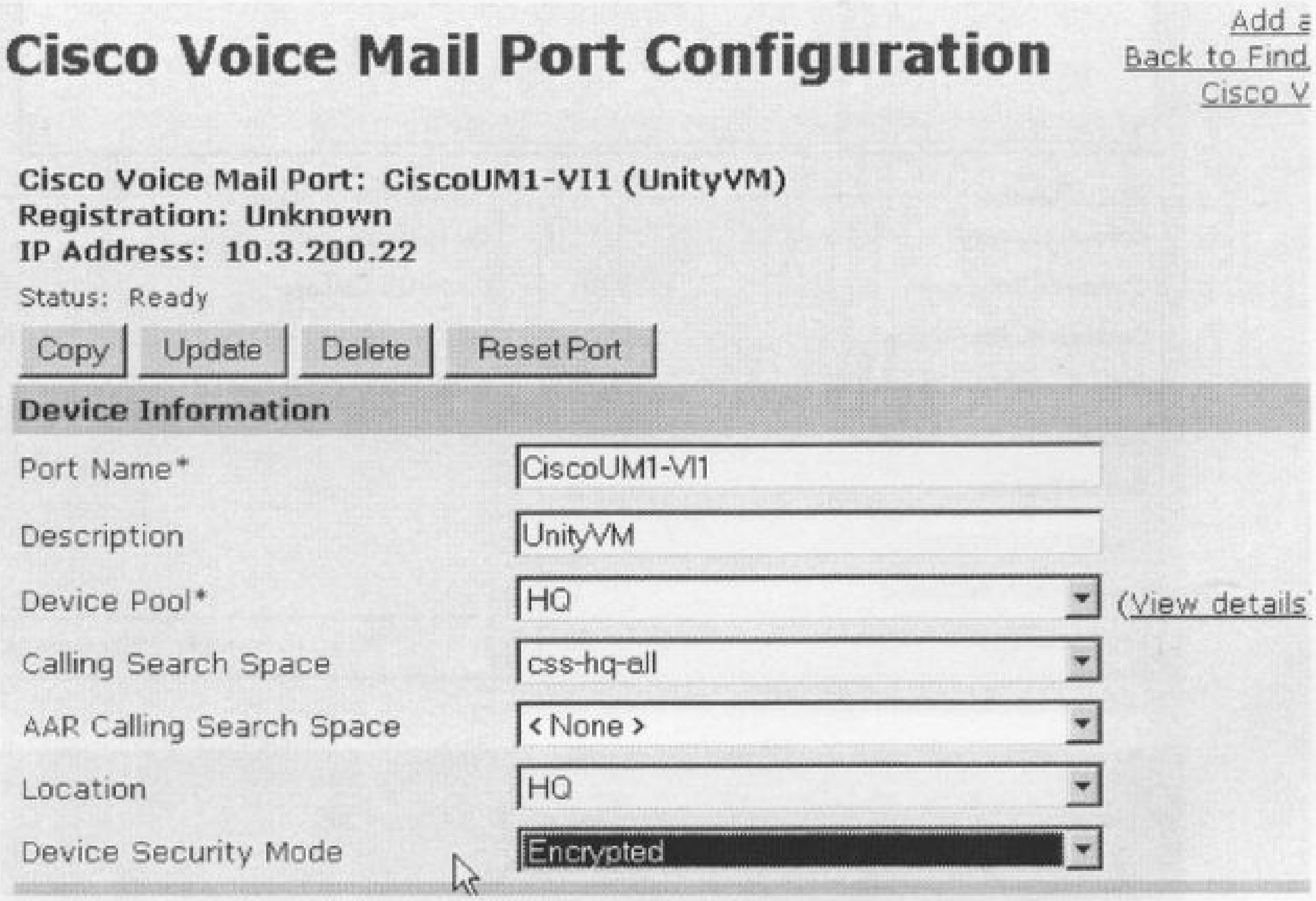

IP Security Monitor
Security Associations:
Policy Name | Security | Filter Name | Source Address | Dest. Address | Protocol | Src. Port
{CC1447C5-7... | ESP Triple DES ... | No Name | CCMPUBLISH... | 162.1.101.2 | 0 | 0
Options...
Minimize
IPSEC Statistics
Active Associations 1
Confidential Bytes Sent 206,831
Confidential Bytes Received 207,411
Authenticated Bytes Sent 313,608
Authenticated Bytes Received 308,016
Bad SPI Packets 0
Packets Not Decrypted 0
Packets Not Authenticated 0
Key Additions 22
ISAKMP/Oakley Statistics
Oakley Main Modes 62
Oakley Quick Modes 22
Soft Associations 0
Authentication Failures 0
IP Security is enabled on this computer.


C:\WINNT\system32\cmd.exe
C:\>ping 162.1.101.2
Pinging 162.1.101.2 with 32 bytes of data:
Reply from 162.1.101.2: bytes=32 time=7ms TTL=254
Reply from 162.1.101.2: bytes=32 time=7ms TTL=254
Reply from 162.1.101.2: bytes=32 time=7ms TTL=254
Reply from 162.1.101.2: bytes=32 time=14ms TTL=254
Ping statistics for 162.1.101.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 7ms, Maximum = 14ms, Average = 8ms
C:\>_

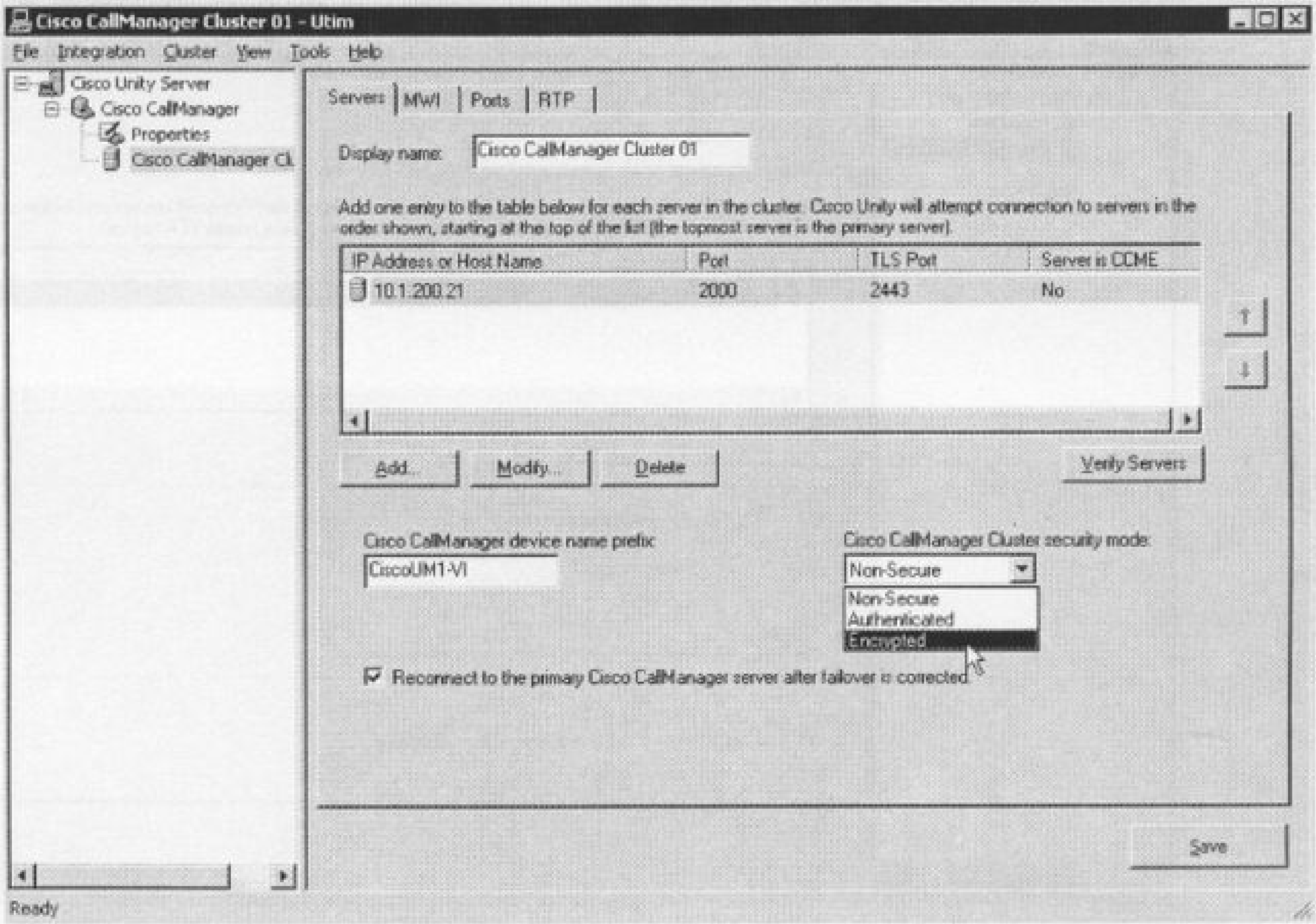
Task 17.6

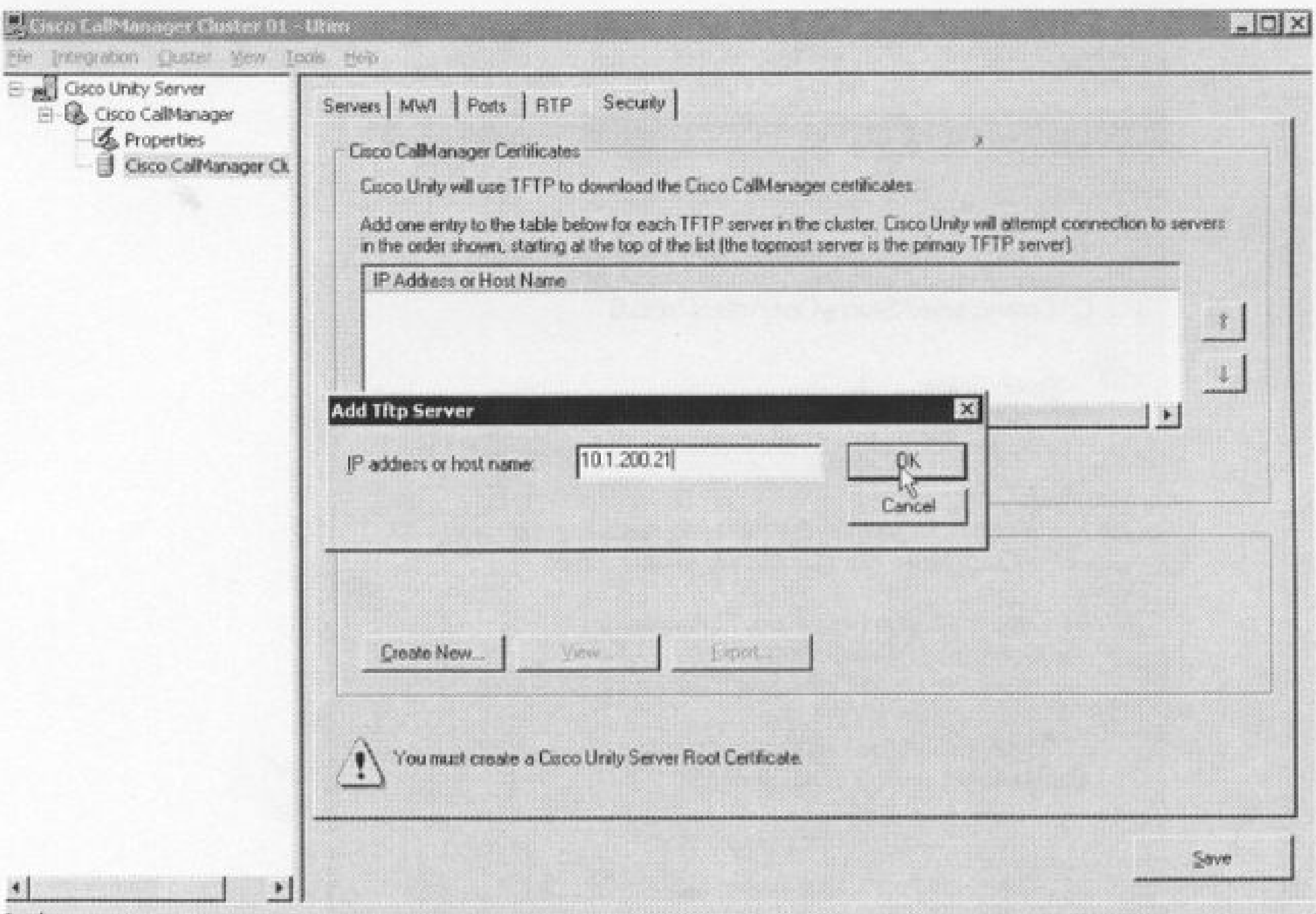
Configure Unity VM Ports to use AES128 encryption for media traversal between themselves and IP Phones or Gateways that support such.

➔ **We need to start on CCM by securing the VM Ports and resetting them.**

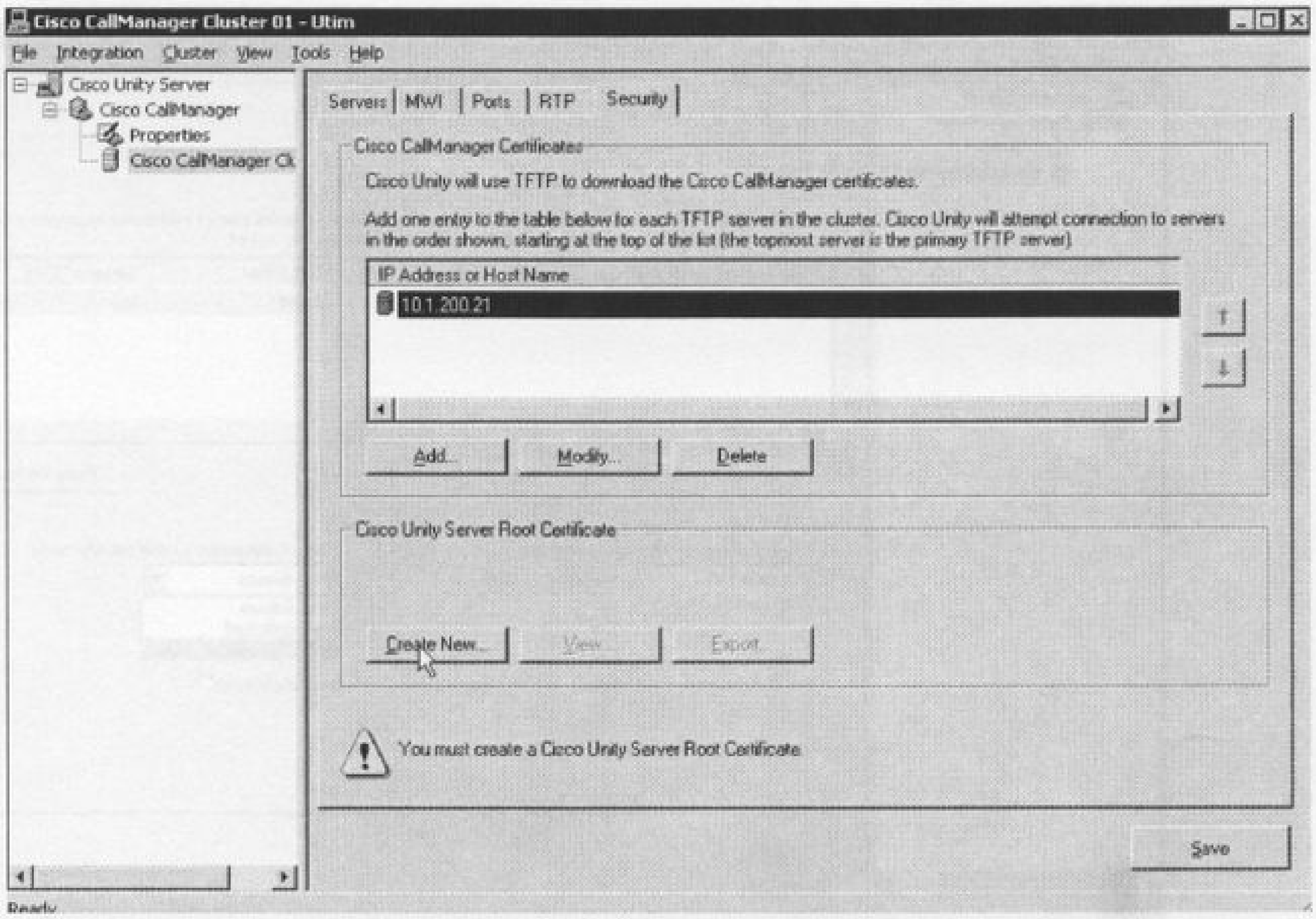


➔ **Next we need to move to the Unity server and re-run the UTIM to secure Unity's side of the ports.**

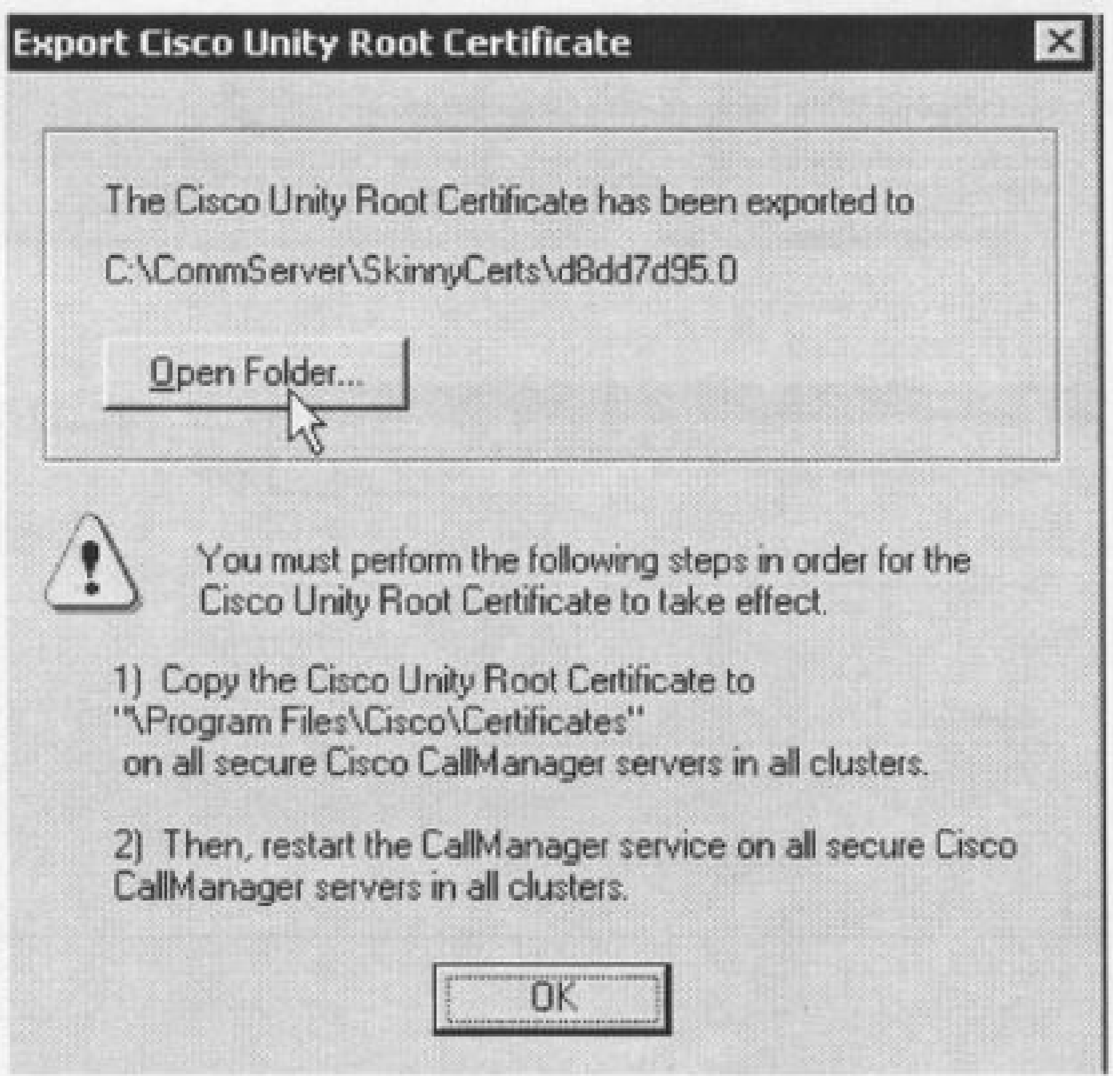




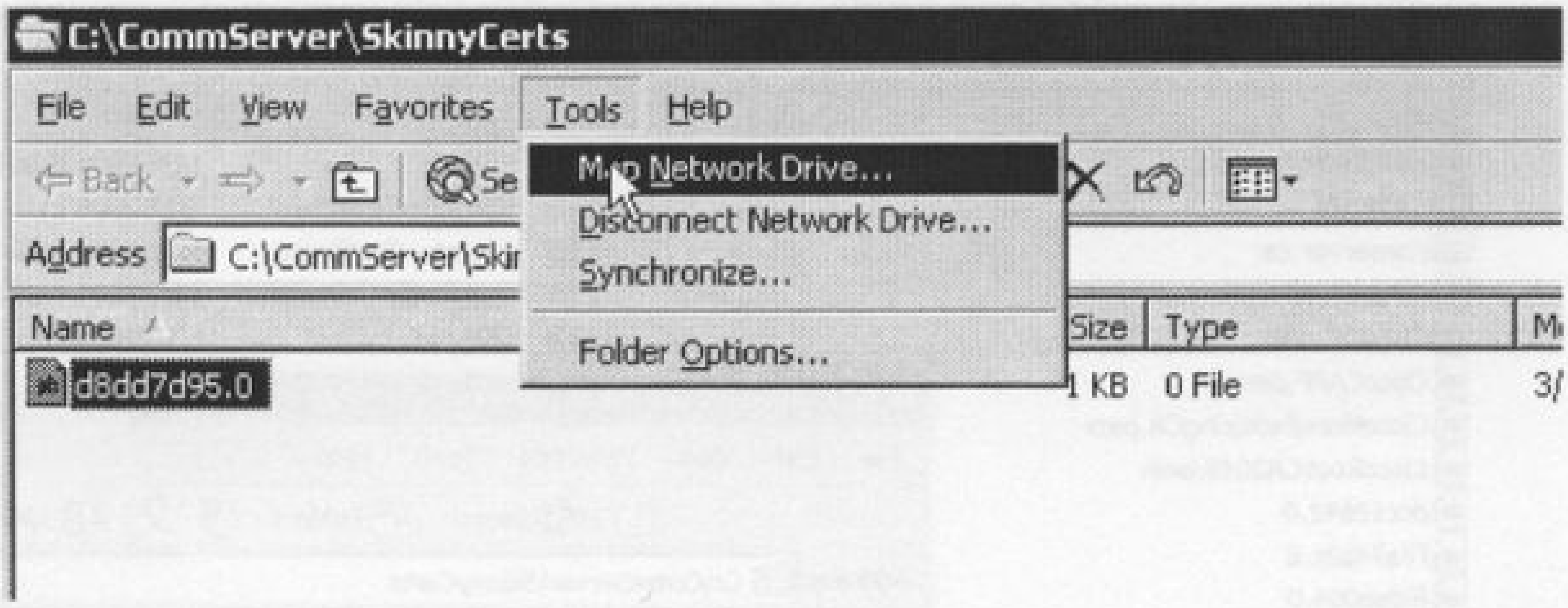
➔ **Notice at the bottom it says we need to create a new Unity Root Certificate and provides a quick method to do so.**

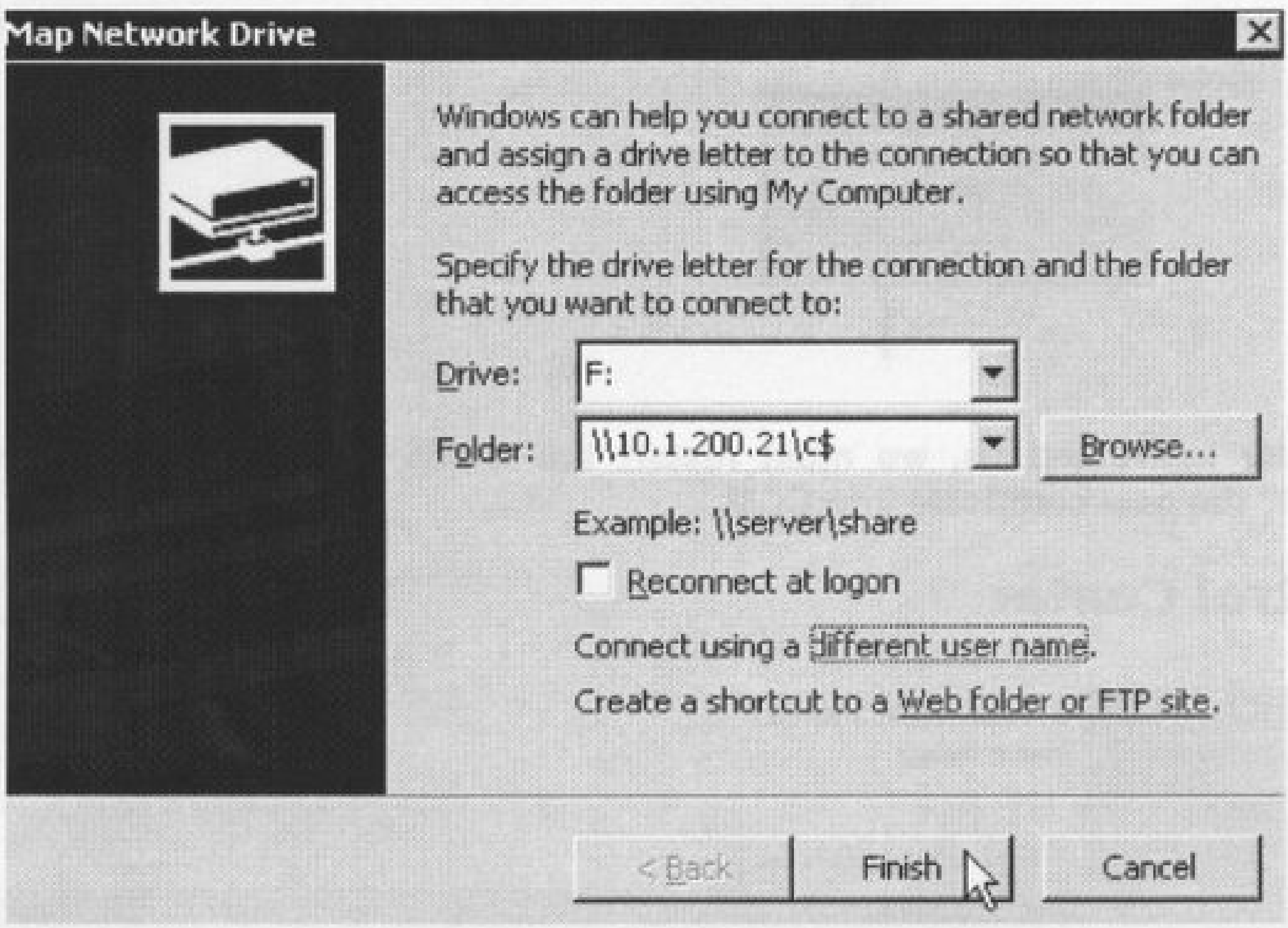


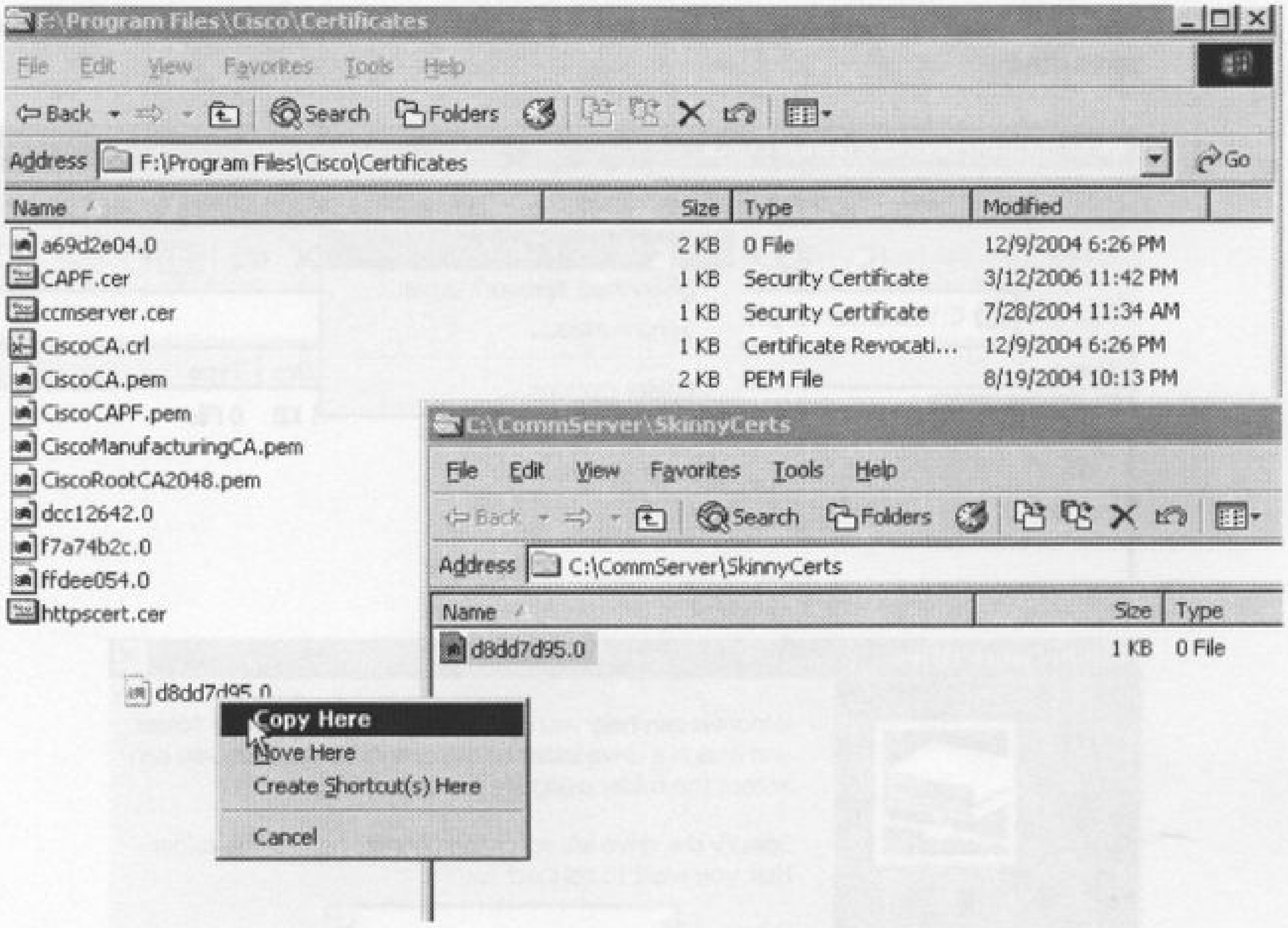
➔ **Once the Certificate is created, we must manually copy the cert file from Unity over to CCM.**



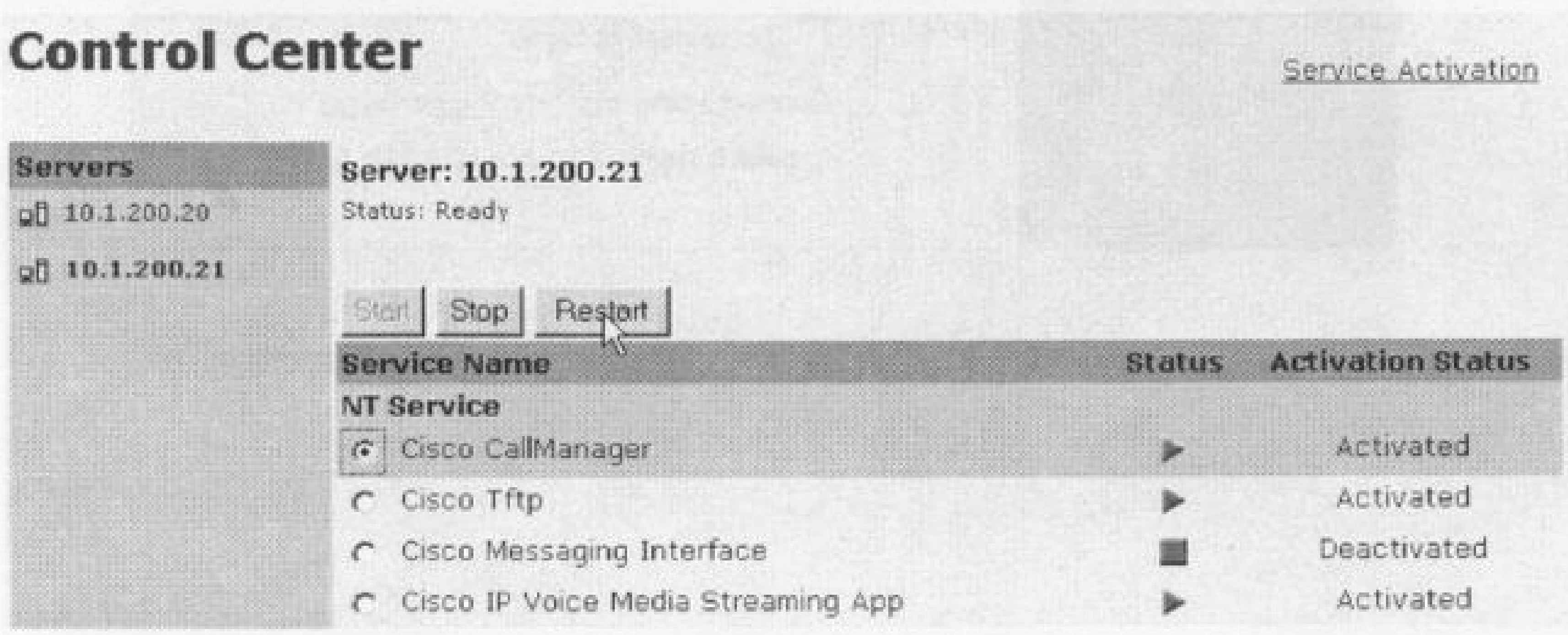
➔ **We will map a network drive over to CCM and copy the file to the directory specified.**



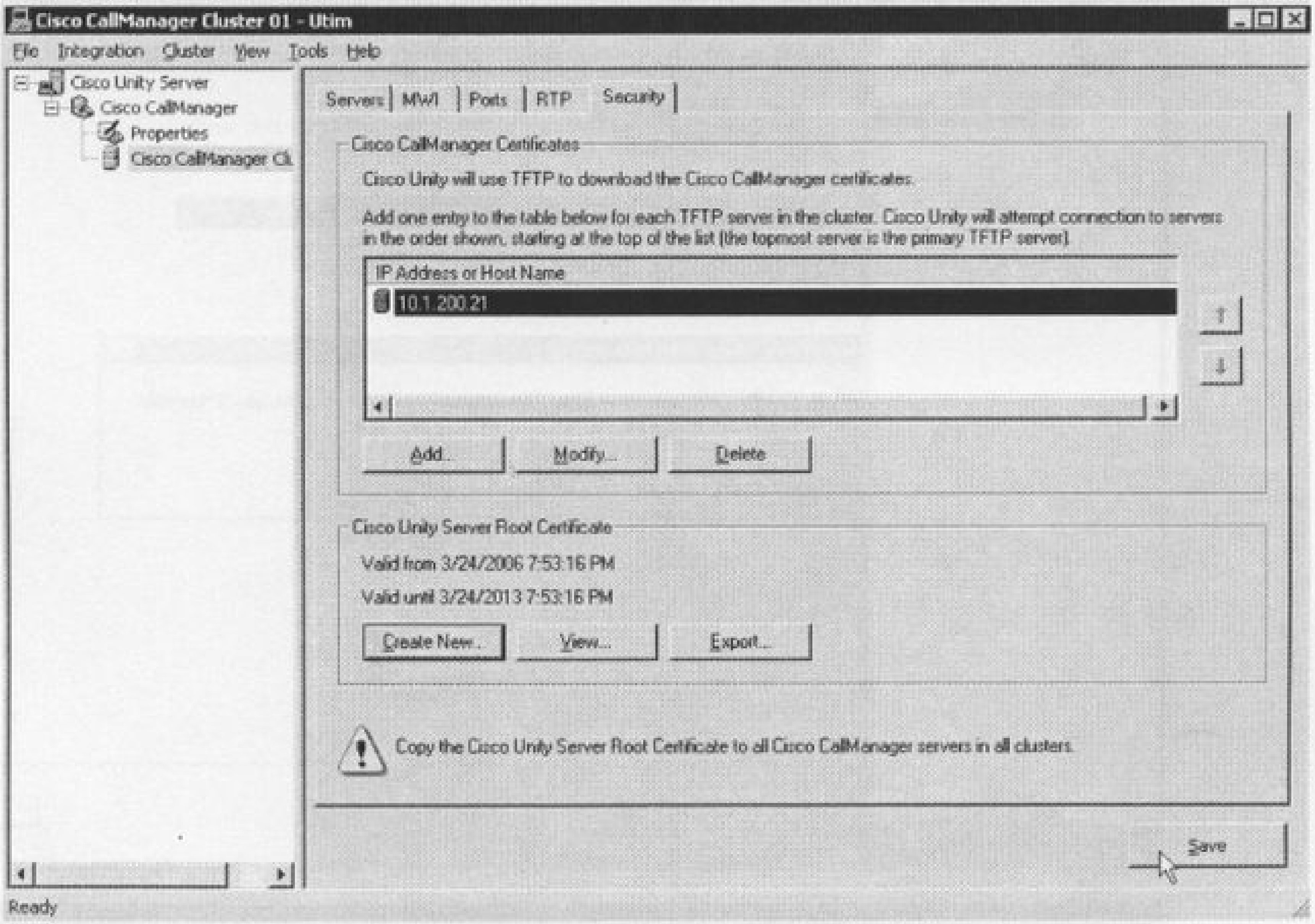




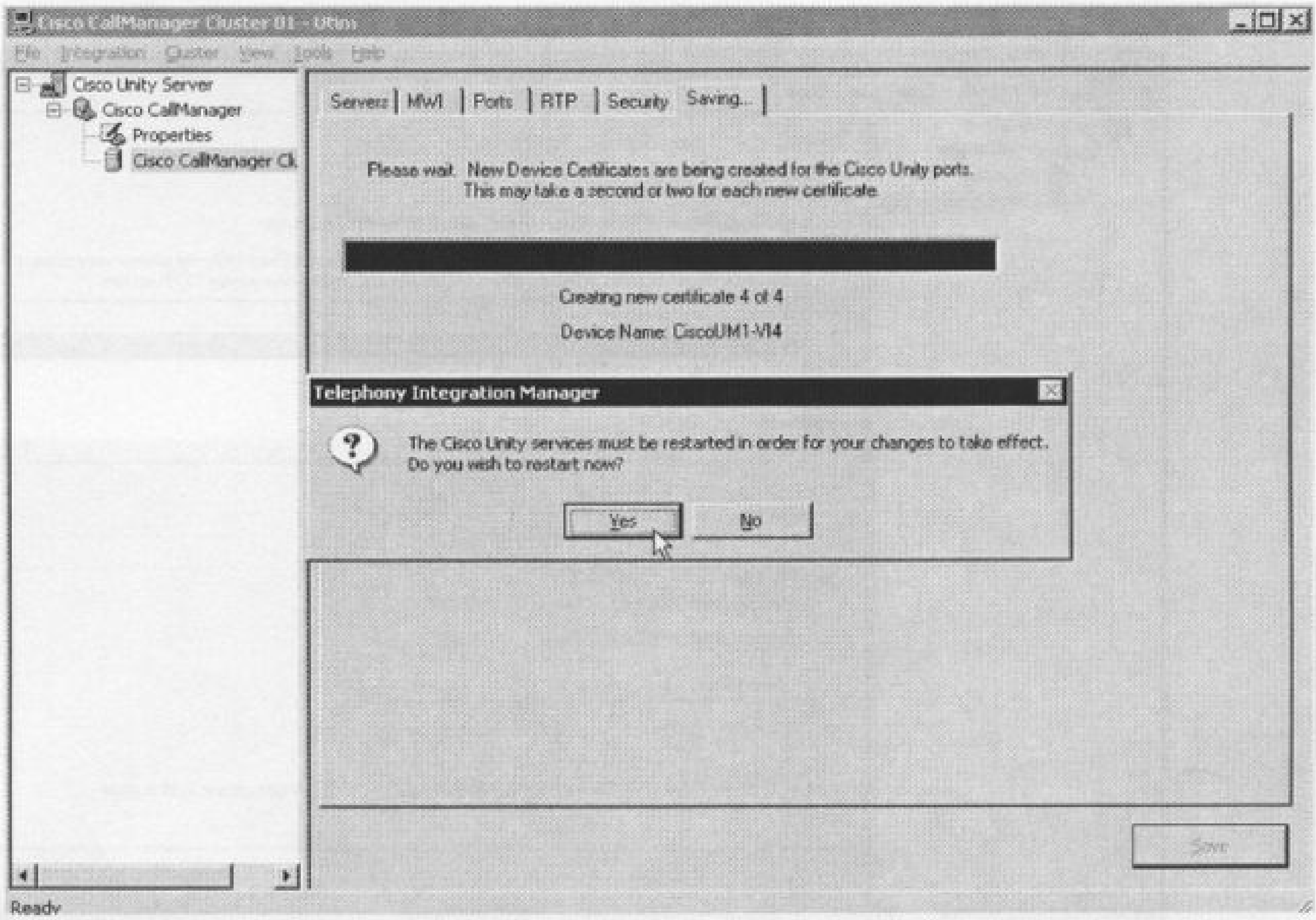
➔ **As Unity instructed us, we must restart the Cisco CCM and TFTP Service to "install" the new certificate into CCM.**

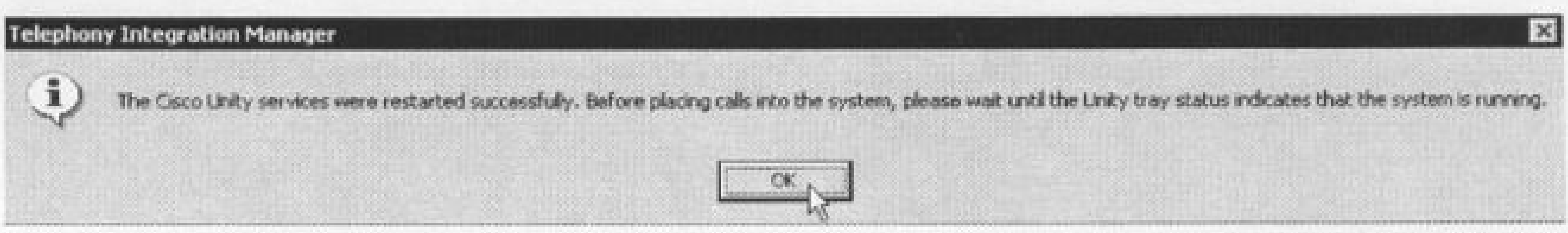


➔ **Now that CCM has our Private Key, we need to download a Public key – ensure that both CCM and TFTP Services on CCM are started before doing this step.**



➔ **Restart the Unity Services.**





➔ **Ensure that Unity is running.**

➔ **And test!**

➔ **If all is well – you will see the small lock icon at the bottom right of your call appearance once you have placed a call from a Secure IP Phone into Unity.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 18: Multiprotocol Challenge A

Estimated Time to Complete: 6 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 18 Multiprotocol Challenge A

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing the previous 13 Labs.

Section 18 Configuration Tasks

Task 18.1

Check all of the Frame Relay connections and connectivity between sites.

➔ **This should be self-explanatory from previous examples - see Task 1.1.**

Task 18.2

Configure voice and data VLANs based on Table 2.

➔ **This should be self-explanatory from previous examples - see Task 1.2.**

Task 18.3

For Headquarter and Branch 1, use Microsoft DHCP server to allocate IP address for the IP phones, VG-248 and 6608. For Branch 2, use IOS DHCP to allocate IP address for the IP phones. For each voice subnet, allocate the IP address from .50 to .69.

➔ **This should be self-explanatory from previous examples – see Task 1.4 and 1.5.**

Task 18.4

Register all phones to Call Manager and assign directory number to devices based on Tables 5, 6 and 7.

➔ **This should be self-explanatory from previous examples – see Task 1.8. It is worth pointing out that all 3 sites register to CCM and BR2 is not a CCME.**

Task 18.5

Assume a Publisher exists (Table 1) and every phone is registered in a CCM Group first to a Subscriber, and then to the Publisher. Configure the keepalive interval between any IP Phone and the Publisher server CallManager to be set to 40 seconds.

➔ **This should be self-explanatory from previous examples – see Task 2.6.**

Task 18.6

Configure PRI for one of the 6608 ports as defined in Table 8. Refer to Table 13 for 6608 port assignment.

➔ **See Task 4.1 to add the 6608 T1 PRI gateway. Top-down signaling is required (i.e. starting at Bchannel 1) therefore the Bchannel Maintenance Status Service Parameter is not required to define the partial PRI.**

Task 18.7

Configure MGCP PRI for the Branch 1 site. Refer to Table 8 for PSTN configuration.

➔ **This should be self-explanatory from previous examples - See Task 4.2.**

Task 18.8

Configure E1 R2 for Branch 2. Use Table 8 for PSTN details. Register to Call Manager as an H323 gateway. H323 packets should be sourced from the voice sub-interface.

➔ **Configure the E1 R2 on the BR2 gateway.**

```
interface FastEthernet0/0.220
 encapsulation dot1Q 220
 ip address 10.2.202.1 255.255.255.0
 h323-gateway voip bind srcaddr 10.2.202.1

controller E1 0/0/0
 ds0-group 0 timeslots 1-3 type r2-digital r2-semi-compelled ani
```

➔ **Add an H323 gateway in Call Manager with Device Name set to the IP Address of the Voice Sub-interface. NOTE: E1 R2 gateways do not have support for MGCP in CCM.**

Task 18.9

Configure CallManager with bandwidth values such that Audio calls within each site are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between any of the sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Region and respective Device Pool.

➔ **This should be self-explanatory from previous examples – see Task 2.1.**

Task 18.10

Use CallManager CAC to limit the number of calls over the WAN between any site to one G729 audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **This should be self-explanatory from previous examples – see Task 2.2.**

Task 18.11

Create a DN of 1005 for Tech Support. Make HQ phone 3 and BR1 Phone 3 ring simultaneously when this DN is called. You may not use a shared line to accomplish this task.

➔ **This should be self-explanatory from previous examples – see Task 2.12.**

Task 18.12

DN 1005 should forward directly to VM anytime outside of normal business hours with no user intervention needed. Check Table 11 for a time schedule.

➔ **This should be self-explanatory from previous examples – see Task 6.7.**

Task 18.13

Configure the route patterns.

➔ **It is a good idea to configure Route Patterns after defining partitions, route lists and route groups. We'll come back to this later on.**

Task 18.14

Configure Call Manager to provide Class of Service such that phone 1 can call everywhere, phone 2 can call 911 and local, other phones can call 911, local and long distance.

➔ **It is a good idea to configure Route Patterns after defining partitions, route lists and route groups. We'll come back to this.**

➔ **Create the following Partitions:**

- **PT-HQ-911-LOC**
- **PT-BR1-911-LOC**
- **PT-BR2-911-LOC**
- **PT-HQ-LD**
- **PT-BR1-LD**
- **PT-BR2-LD**
- **PT-HQ-INT**
- **PT-BR1-INT**
- **PT-BR2-INT**

➔ **Create the following CSS and assign PT accordingly:**

- **CSS-HQ-911-LOC**
- **CSS-BR1-911-LOC**
- **CSS-BR2-911-LOC**
- **CSS-HQ-911-LOC-LD**
- **CSS-BR1-911-LOC-LD**
- **CSS-BR2-911-LOC-LD**
- **CSS-HQ-ALL**
- **CSS-BR1-ALL**
- **CSS-BR2-ALL**

Task 18.15

All calls from HQ and Branch 1 should go through local gateway only.

➔ **See section 18.14.**

Task 18.16

Local calls from Branch 2 will be routed through local gateway first and use 6608 as backup. International calls will be routed through 6608 first and use local gateway as backup. 911 and Long Distance calls will be routed through local gateway only.

➔ **See section 18.14.**

Task 18.17

When someone places a call from Branch 2 to the area code in HQ, calls should be hopped off using the 6608 and use local gateway as backup.

➔ **The following Route Groups should be created.**

Route Group	Gateway	Order
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1
RG-BR2	H323 BR2	1

➔ **The following Route Lists should be created.**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-BR2-HQ	RG-BR2	PREDOT
	RG-HQ	PREDOT + PREFIX 011331
RL-HQ-BR2	RG-HQ	PREDOT
	RG-BR2	PREDOT
RL-BR2	RG-BR2	PREDOT
RL-TOLLBY-2-HQ	RG-HQ	PREDOT
	RG-BR2	PREDOT + PREFIX 1212

➔ **The following Route Patterns should be created.**

Route Pattern	Partition	Route List
911	PT-HQ-911-LOC	RL-HQ
9.911		
911	PT-BR1-911-LOC	RL-BR1
9.911		
911	PT-BR2-911-LOC	RL-BR2
9.911		
9.[2-9]xxxxxx	PT-HQ-911-LOC	RL-HQ
9.[2-9]xxxxxx	PT-BR1-911-LOC	RL-BR1
9.[2-9]xxxxxx	PT-BR2-911-LOC	RL-BR2-HQ
9.1xxxxxxxxxx	PT-HQ-LD	RL-HQ
9.1xxxxxxxxxx	PT-BR1-LD	RL-BR1
9.1xxxxxxxxxx	PT-BR2-LD	RL-BR2
9.011!	PT-HQ-INT	RL-HQ
9.011!#		
9.011!	PT-BR1-INT	RL-BR1
9.011!#		
9.011!	PT-BR2-INT	RL-HQ-BR2
9.011!#		
91212.xxxxxxx	PT-BR2-LD	RL-TOLLBY-2-HQ

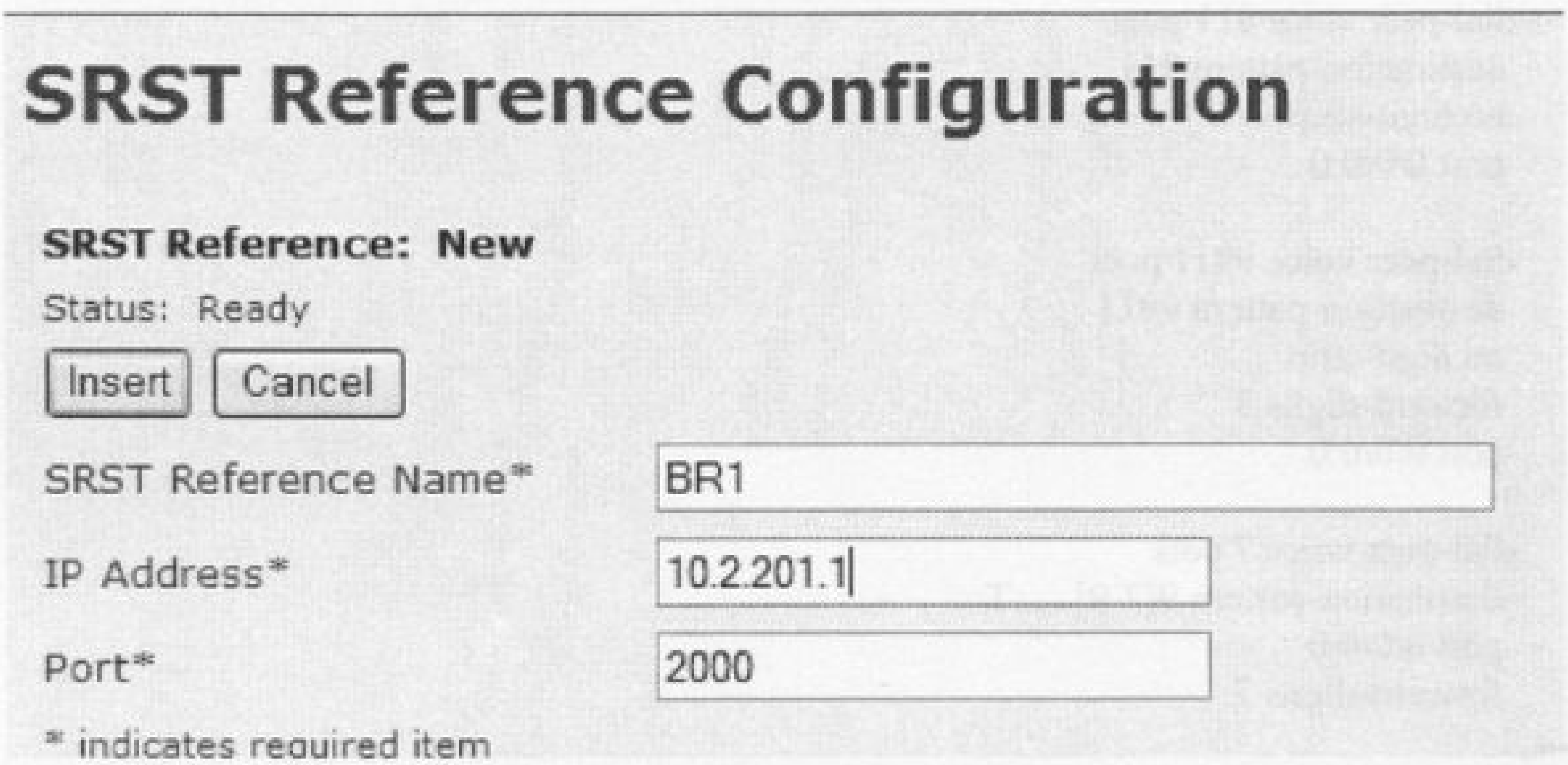
➔ **On the BR2 gateway we need to configure Dial-Peers.**

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
!
dial-peer voice 911 pots
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 destination-pattern 9011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 3000 voip
 destination-pattern 3…
 session target ipv4:10.2.200.21
 voice-class codec 1
 no vad
```

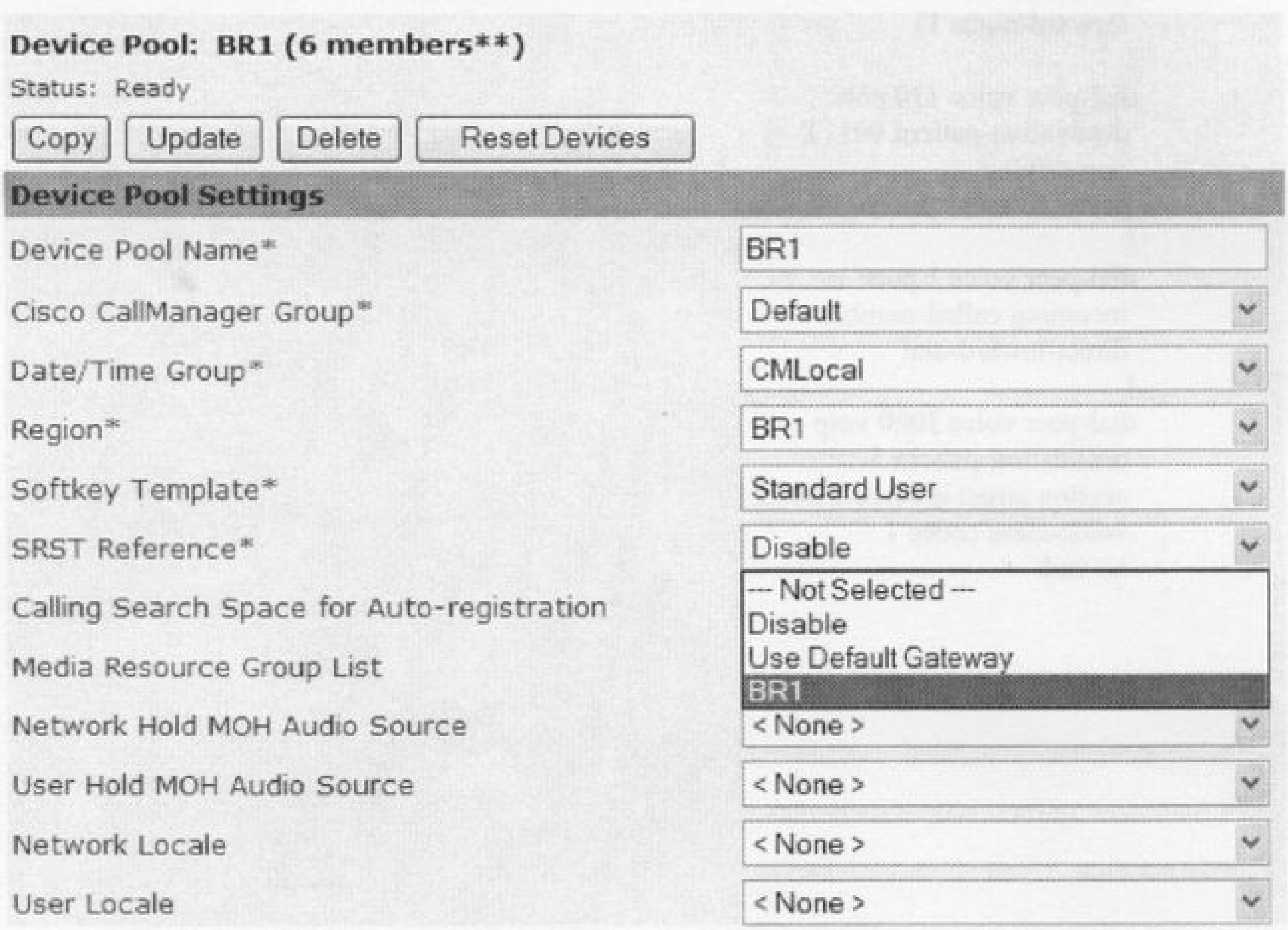

Task 18.18

Configure Survivable Remote Site Telephony for Branch 1. Allow maximum of 5 phones and 10 DNs.

➔ **Create a SRST Reference from the System menu.**



➔ **Assign the SRST Reference to the BR1 Device Pool and reset the BR1 devices.**



```
call-manager-fallback
 ip source-address 10.2.201.1 port 2000
 max-ephones 4
 max-dn 48 10
dialplan-pattern 1 6175222... ext 4
```

P2-BR1-RTR(config)#call application alternate default ← **(This is fine to enter since it will be automatically changed to the new format)**
P2-BR1-RTR(config)#ccm-manager fallback-mgcp

Task 18.19

Configure SRST to provide calling restriction as specified earlier.

```
dial-peer cor custom
 name pt-911-loc
 name pt-ld
 name pt-internl
!
!
dial-peer cor list css-911-loc
 member pt-911-loc
!
dial-peer cor list css-ld
 member pt-911-loc

 member pt-ld
!
dial-peer cor list css-intnl
 member pt-911-loc
 member pt-ld
 member pt-internl
!

dial-peer voice 1 pots
 application mgcpapp
 port 2/0/0:23
!
dial-peer voice 911 pots
 corlist outgoing css-911-loc
 destination-pattern 911
 no digit-strip
 port 2/0/0:23
!
dial-peer voice 9911 pots
 corlist outgoing css-911-loc
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 2/0/0:23
!
dial-peer voice 7 pots
corlist outgoing css-911-loc
 destination-pattern 9[2-9]......
```

```
 port 2/0/0:23
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 port 2/0/0:23
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 9011T
 port 2/0/0:23
 prefix 011
!
call-manager-fallback
 cor incoming css-911-loc 1 2002
 cor incoming css-intnl 2 2001
 cor incoming css-ld 3 2003
```

Task 18.20

Configure SRST such that PSTN caller can reach IP phones directly.

```
P2-BR1-RTR(config)#call-manager-fallback
P2-BR1-RTR(config-cm-fallback)#dialplan-pattern 1 6175222 ext 4

P2-BR1-RTR(config)#dial-peer voice 2 pots
P2-BR1-RTR(config-dial-peer)# incoming called-number .
P2-BR1-RTR(config-dial-peer)# direct-inward-dial
```

Task 18.21

Any inbound unknown numbers should be redirected to 2003.

```
P2-BR1-RTR(config)#call-manager-fallback
P2-BR1-RTR(config-cm-fallback)#default-destination 2003
```

Task 18.22

Configure the BR1 gateway such that users at Branch 1 can dial 4 digits to reach the HQ and Branch 2.

```
dial-peer voice 1001 pots
 destination-pattern 1...
 prefix 1212222
 port 2/0/0:23
!
dial-peer voice 3001 pots
 destination-pattern 3...
 prefix 011331322
 port 2/0/0:23
```


Task 18.23

Configure AAR between the HQ and Branch 2.

➔ **This should be self-explanatory from previous examples – see Task 8.1.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 19: Multiprotocol Challenge B

Estimated Time to Complete: 6 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 19 Multiprotocol Challenge B

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing the first 17 Labs.

Section 19 Configuration Tasks

Task 19.1

Configure each switch port connecting to IP phones and ATA to support both data and voice traffic according to VLAN IDs specified in Table 2.

➔ **HQ Site Catalyst 6500:**

➔ **For IP phones/ATA connected to Cat 6500, configure the following:**

```
>set vlan 120  2/7-8
>set port auxiliaryvlan 2/7-8 220
```

➔ **VG248 does not support trunking so the port connected VG248 needs to be added to the voice vlan only as below:**

```
>set vlan 200 2/48
```

➔ **Branch 1 Cisco 3825 with an Etherswitch module:**

NOTE:

- Do not forget to add voice and data VLANs to the vlan database. Otherwise, the VLANs will not come up.

```
interface FastEthernet1/0
 switchport trunk encapsulation dot1q
 switchport trunk native vlan  120
 switchport mode trunk
 switchport voice vlan 220
 spanning-tree portfast
!
interface FastEthernet1/8
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 120
 switchport mode trunk
 switchport voice vlan 220
 spanning-tree portfast
```


➔ **Branch 2 3550:**

```
interface range FastEthernet0/23 - 24
 switchport access vlan 120
 switchport voice vlan 220
 spanning-tree portfast
```

Task 19.2

In the HQ site, configure MS DHCP server to enable DHCP service for IP phones to get IP addresses and download configurations and phone loads.

➔ **This should be self-explanatory from previous examples – see Task 1.4.**

Task 19.3

In each branch site, configure each router/gateway to provide DHCP service. Configure the lease time to be 8 hours. Exclude the IP address of X.X.X.1 and X.X.X.254.

➔ **On the BR1 gateway:**

```
P5-BR1-RTR(config)#ip dhcp excluded-address 10.5.201.1
P5-BR1-RTR(config)#ip dhcp excluded-address 10.5.201.254
P5-BR1-RTR(config)#ip dhcp pool BR1
P5-BR1-RTR(dhcp-config)#network 10.5.201.0 255.255.255.0
P5-BR1-RTR(dhcp-config)#default-router 10.5.201.1
P5-BR1-RTR(dhcp-config)#option 150 ip 10.5.200.21
P5-BR1-RTR(dhcp-config)#lease 0 8
```

➔ **On the BR2 gateway:**

```
P5-BR2-RTR(config)#ip dhcp excluded-address 10.5.202.1
P5-BR2-RTR(config)#ip dhcp excluded-address 10.5.202.254
P5-BR2-RTR(config)#ip dhcp pool BR2
P5-BR2-RTR(dhcp-config)#network 10.5.202.0 255.255.255.0
P5-BR2-RTR(dhcp-config)#default-router 10.5.202.1
P5-BR2-RTR(dhcp-config)#option 150 ip 10.5.202.1
P5-BR2-RTR(dhcp-config)#lease 0 8
```

Task 15.4

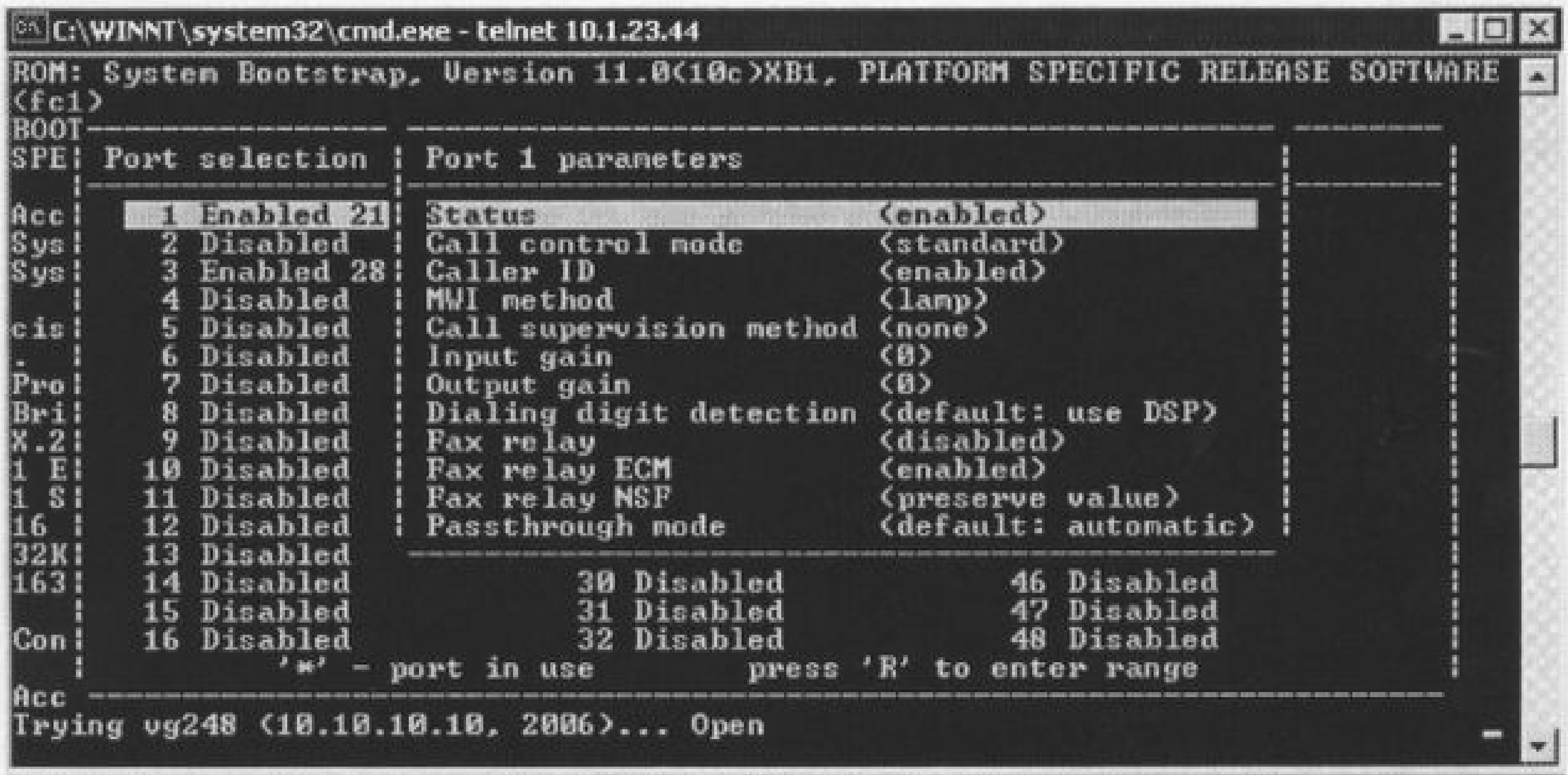
Configure all the phones with 4 digit extensions as shown in Table 5 through 7 (NOTE: Branch 2 router should be configured as CME). Configure all the phones such that each phone displays its own full E.164 number on its LCD display.

➔ **On Call Manager start services from Serviceability, configure IP Address in System-Server and turn on Auto-Registration in Call Manager.**

➔ **Go to Device>Phone and click the Find button to list all phones. Click HQ Ph1 on the phone list and then click Line 1 from left-hand panel to edit the DN for HQ Ph1.**

➔ **Enter 1001 in the Directory Number field. Enter 212222XXXX in the External Phone Number Mask field to display the phone's full E.164 number on its LCD display. Also, enter the name of HQ Ph1 in the Display (Internal Caller ID) field to forward calling name to other phones. Repeat these steps for all other IP phones with a correct DN and external phone number mask.**

➔ **The HQ site has VG248. Once the VG248 ports are registered with CM, follow the same steps as you did for IP phones to configure DN, calling name, and the external phone number mask on the VG248 ports. If the VG248 ports do not auto-register, make sure that the port status is enabled on the VG 248 ports. To enable the port status from the VG248 console interface, go to Main Menu>Configure>Telephony>Port Specific Parameters to open the port selection window. From the port selection window, select the ports and change the port status to "enabled".**



➔ **Branch 2's gateway is CME (Call Manager Express). The IP phones configuration is done on CME as follows, although it is recommended you run the wizard:**

```
telephony-service
 max-ephones 2
 max-dn 2
 ip source-address 10.2.202.1 port 2000
 auto assign 1 to 2
 create cnf-files version-stamp 7960 Mar 02 2004 17:02:20
 dialplan-pattern 1 331322.... extension-length 4
 max-conferences 4
 moh music-on-hold.au
!
!
ephone-dn 1
 number 3001
 description 13313223001
!
!
```

```
ephone-dn 2
 number 3002
description 13313223002
!
!
ephone 1
 mac-address 0007.50A4.D602
 type 7960
 button 1:1
!
!
ephone 2
 mac-address 0030.94C2.8595
 type 7960
 button 1:2
```

Task 19.5

Configure all the phones in Branch 1 and HQ to forward calling name and number. When calling PSTN, each phone should forward full DID DN to PSTN phone and calling names. The PSTN gateway is sending10 digits to all gateways.

➔ **For CCM phones, the External phone number mask and Display (Internal Caller ID) fields have to be properly filled in as discussed in previous Task.**

➔ **For CCME phones configure as follows:**

```
ephone-dn 1
name BR2 Phn1
 number 3001
description 13313223001
!
!
ephone-dn 2
 name BR2 Phn2
 number 3002
description 13313223002
```

NOTE:

- The Calling Party Name is not supported through E1 R2 but will work for VoIP calls.

Task 19.6

Configure the Call Manager and Branch 2 CME to synchronize its clock to the NTP server located on the backbone gatekeeper router (10.x.200.2).

➔ **Follow the below instructions to configure NTP on CM:**

1. Configure **c:\winnt\ntp.conf** file to receive broadcast NTP packets from the router on your local segment. Enter **broadcastclient or server ipaddress** to the top line of the file. The following is sample syntax:

   10.2.200.2
   driftfile %windir%\ntp.drift

2. You must stop the NetworkTimeProtocol service in service manager.
3. At the DOS command line, change the directory to **c:\program files\cisco\xntp**
4. Type the command **ntpdate -b 10.2.200.2**
5. Restart the **NetworkTimeProtocol** service after you see a NTP update message like 29 May 11:30:00 ntpdate[5080]: step time server 10.2.200.2 offset -8.700886 sec
6. Stop and disable the **Windows Time** service.

➔ **On CME:**

```
P2-BR2-RTR#sh ntp stat
Clock is unsynchronized, stratum 16, no reference clock

P2-BR2-RTR(config)# ntp server 10.2.200.2
P2-BR2-RTR(config)# clock timezone EST -5
Sep 16 15:56:47.214: %SYS-6-CLOCKUPDATE: System clock has been updated from 15:56:47
UTC Fri Sep 16 2005 to 10:56:47 EST Fri Sep 16 2005, configured from console by co^Z
P2-BR2-RTR#sh ntp stat
Clock is synchronized, stratum 9, reference is 10.2.200.2
```

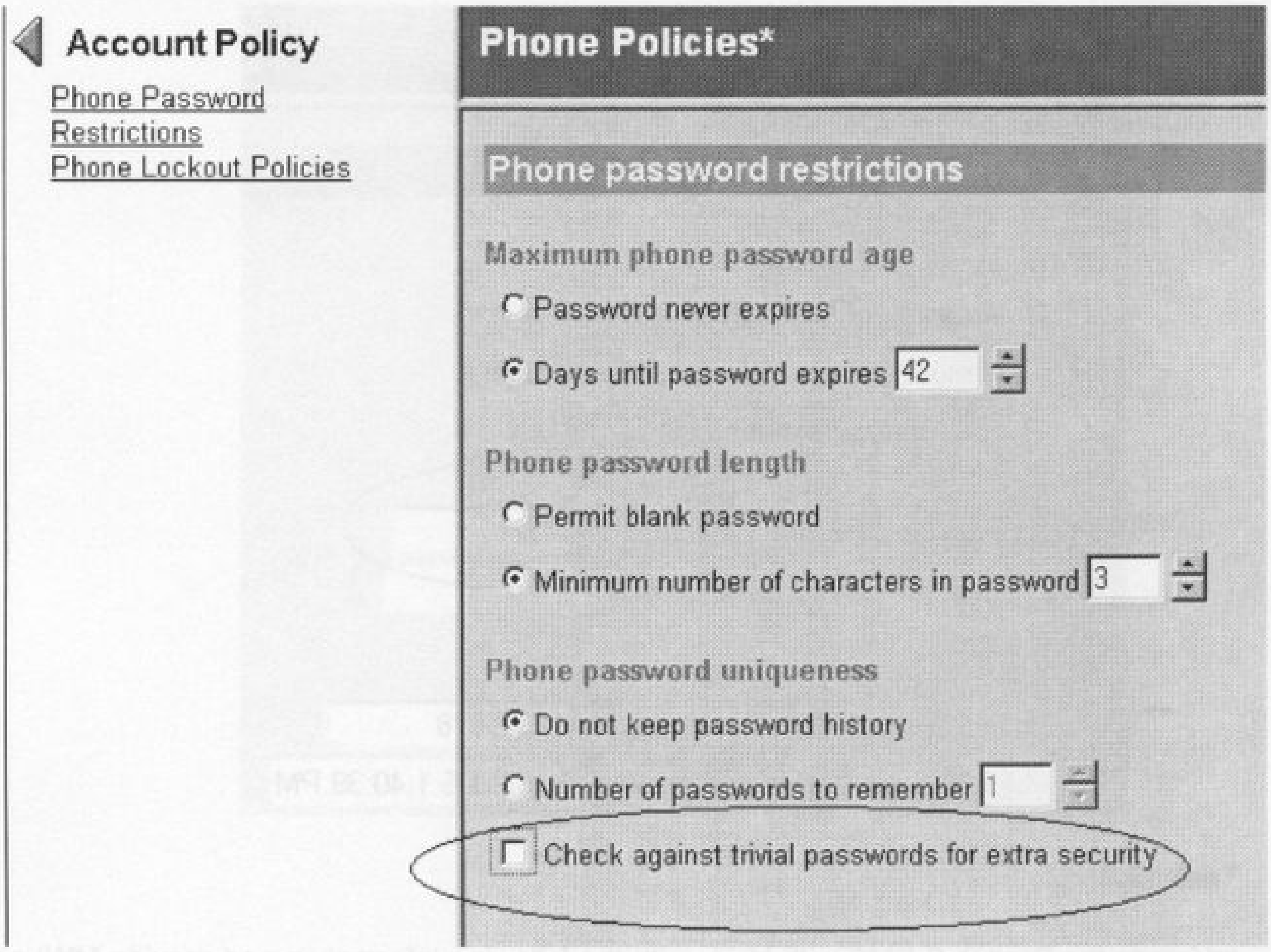
Task 19.7

Setup Unity voice mail boxes for Phone 1 in HQ, and Branch 1. Ensure you can call and reach mailboxes as well as leave messages. Ensure you can light the MWI light.

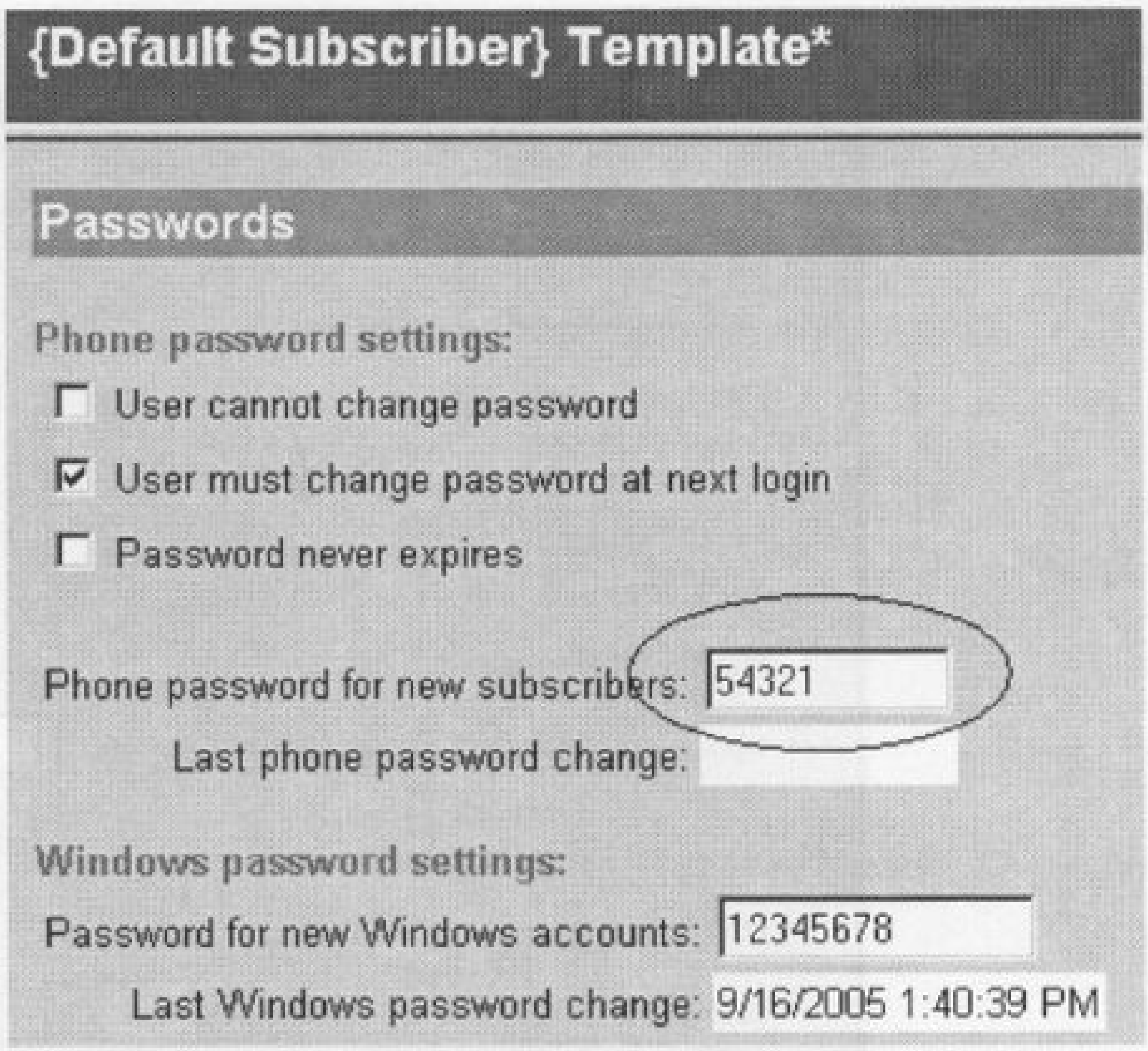
- Pilot Number: 1600
- Unity Port Number: 1601 – 1604
- Set the default password to 54321
- MWI Light – 1998 off
- MWI Light – 1999 on

➔ **You should be comfortable with Unity/CCM Integration – see Task 9.1.**

➔ **To set the Default password go to Subscribers > Account Policy and disable Trivial Passwords.**



➔ **To set the Default password go to Subscribers > Subscriber Template – Passwords and set the Password.**



Task 19.8

Integrate the Branch 2 CME with Unity with the following information and provide MWI and voice mail boxes for Phone 1 and 2 in the Branch 2 CME.

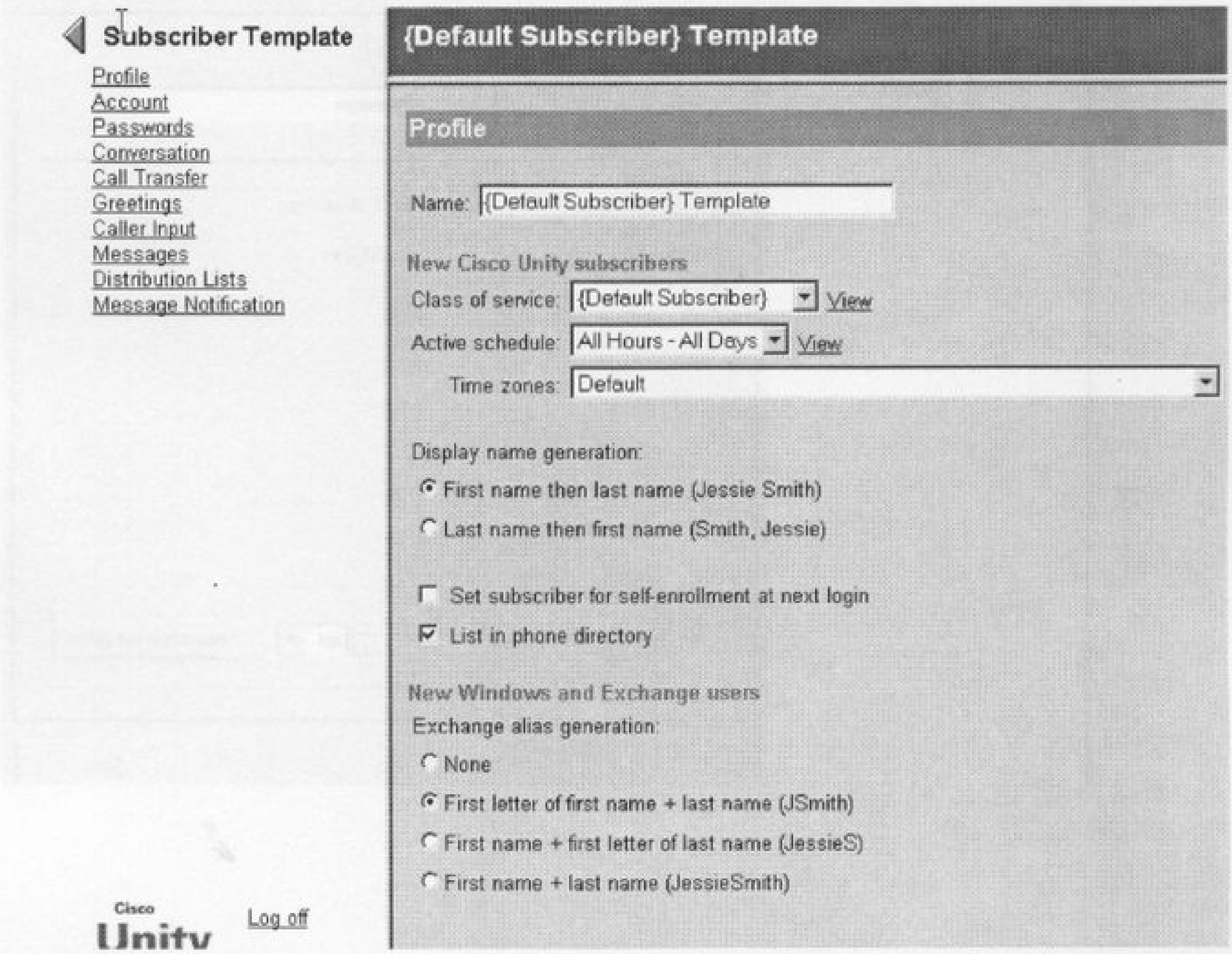
- Pilot Number: 3600
- Unity Port Number: 3600 – 3603
- Set the default password to 54321
- MWI Light – 3998 off
- MWI Light – 3999 on

➔ **You should be comfortable with CCME and Unity Integration – refer to Task 9.2.**

Task 19.9

Configure each mail box such that when a subscriber logs in for the first time, the subscriber is not asked to change the password or to do self-enrollment.

➔ **Uncheck the "Set subscriber for self-enrollment at next login" checkbox in Subscriber Template.**



Task 19.10

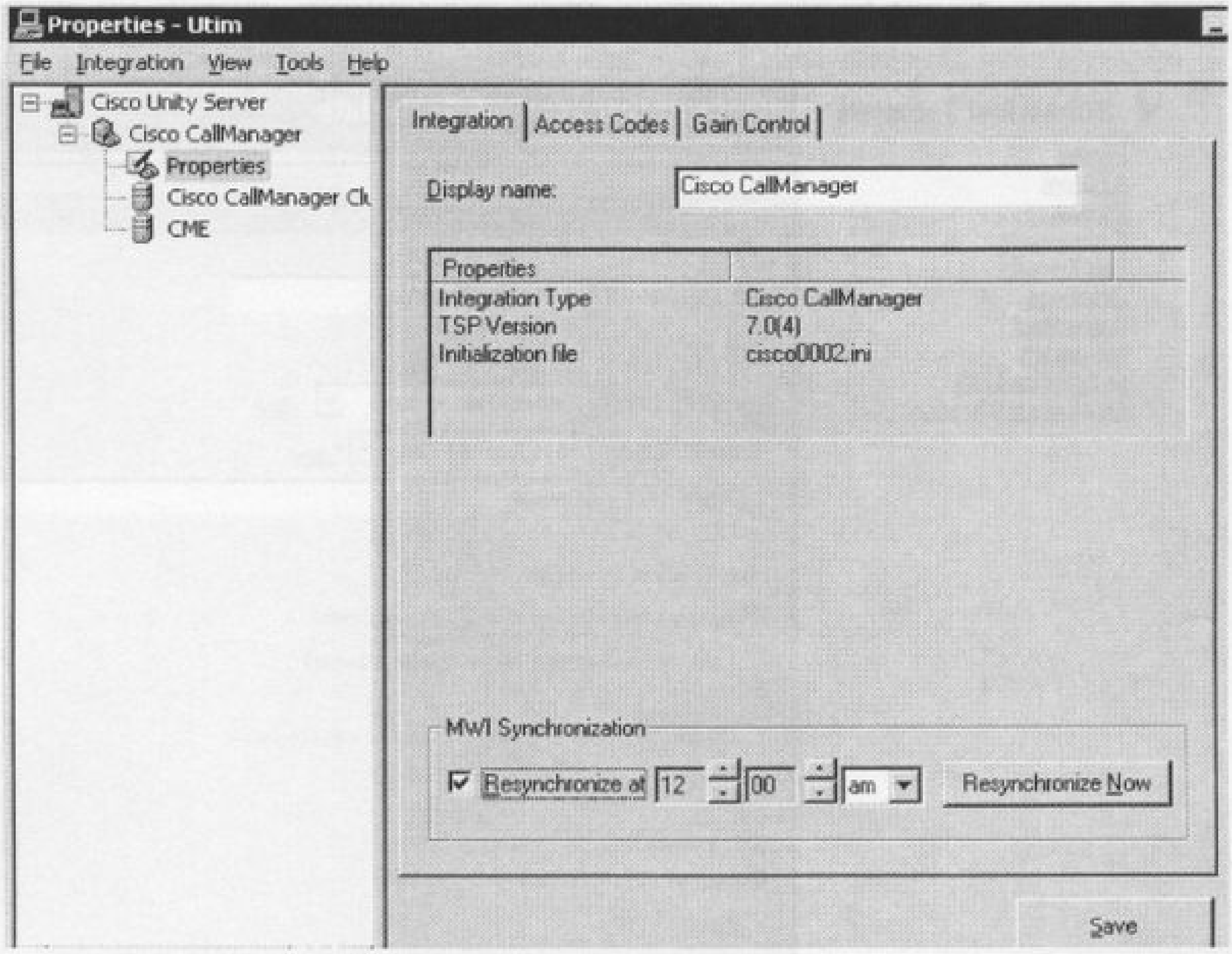
For Unity integration, configure such that only the last Voice Mail port is used to send out a MWI notification.

➔ **This is covered in Task 9.3.**

Task 19.11

Configure Unity such that MWI is synchronized daily at 12:00AM.

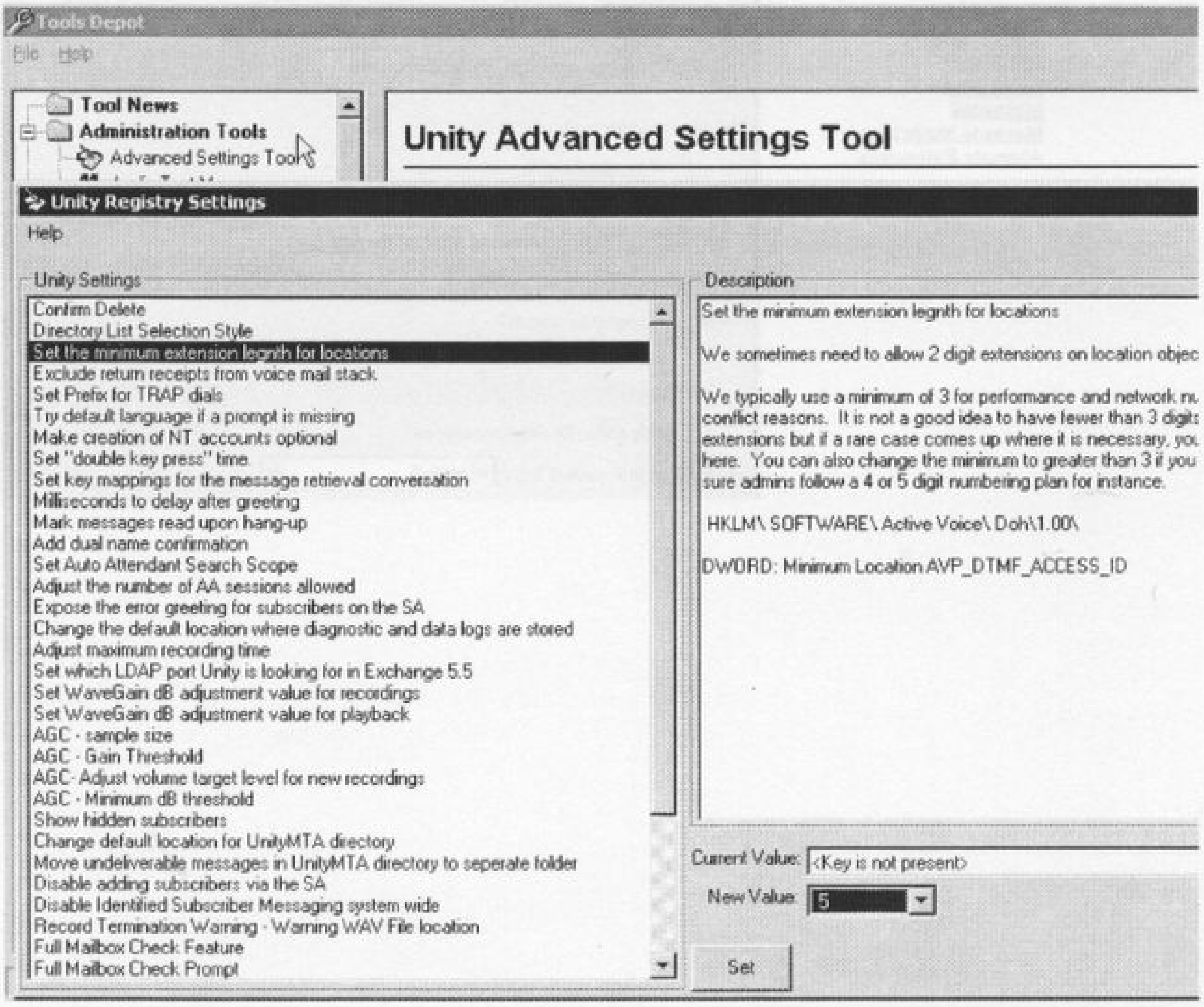
➔ **Open UTIM and enable MWI synchronization.**



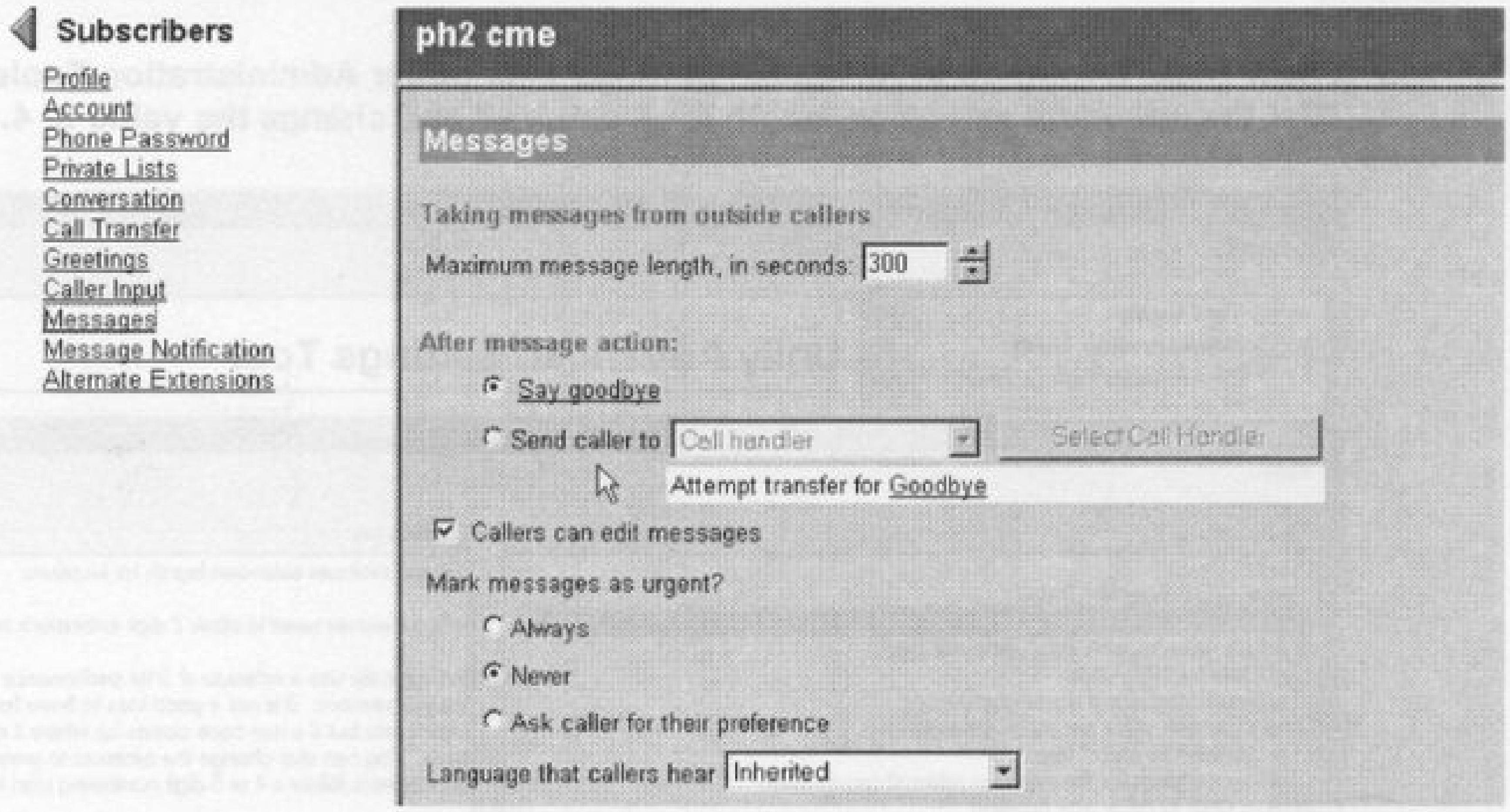
Task 19.12

Set the minimum extension length for locations to be 4 and set the maximum recording time to be 5 minutes.

➔ **From Tools Depot, go to Advanced Settings Tool under Administration Tools. Click "Set the minimum extension length for locations" and change the value to 4.**



➔ **Clarification – the maximum recording time here means message length per mailbox. It is best to do this in the subscriber template before adding subscribers. Change the Maximum message length to 300 seconds.**

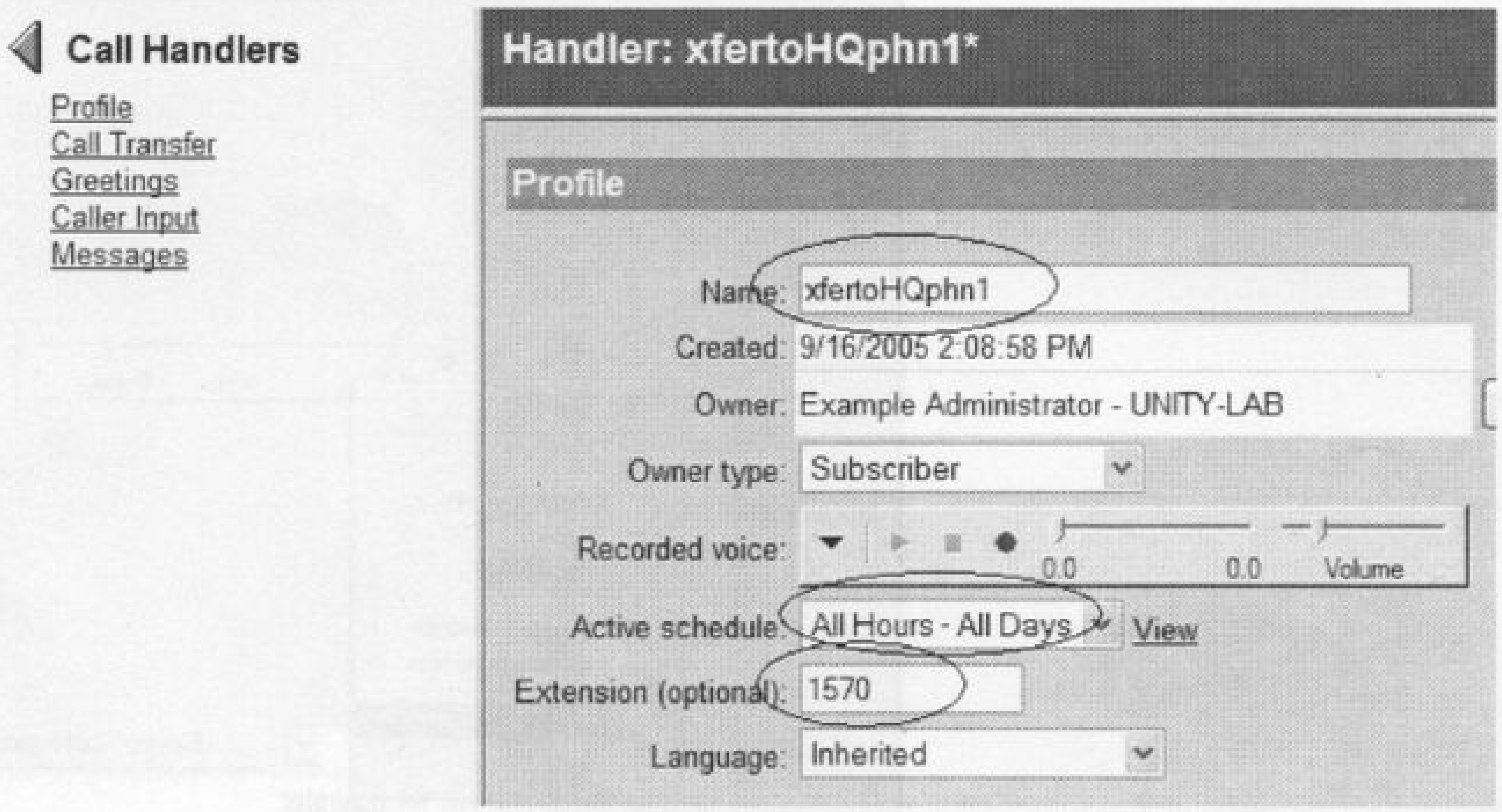


Task 19.13

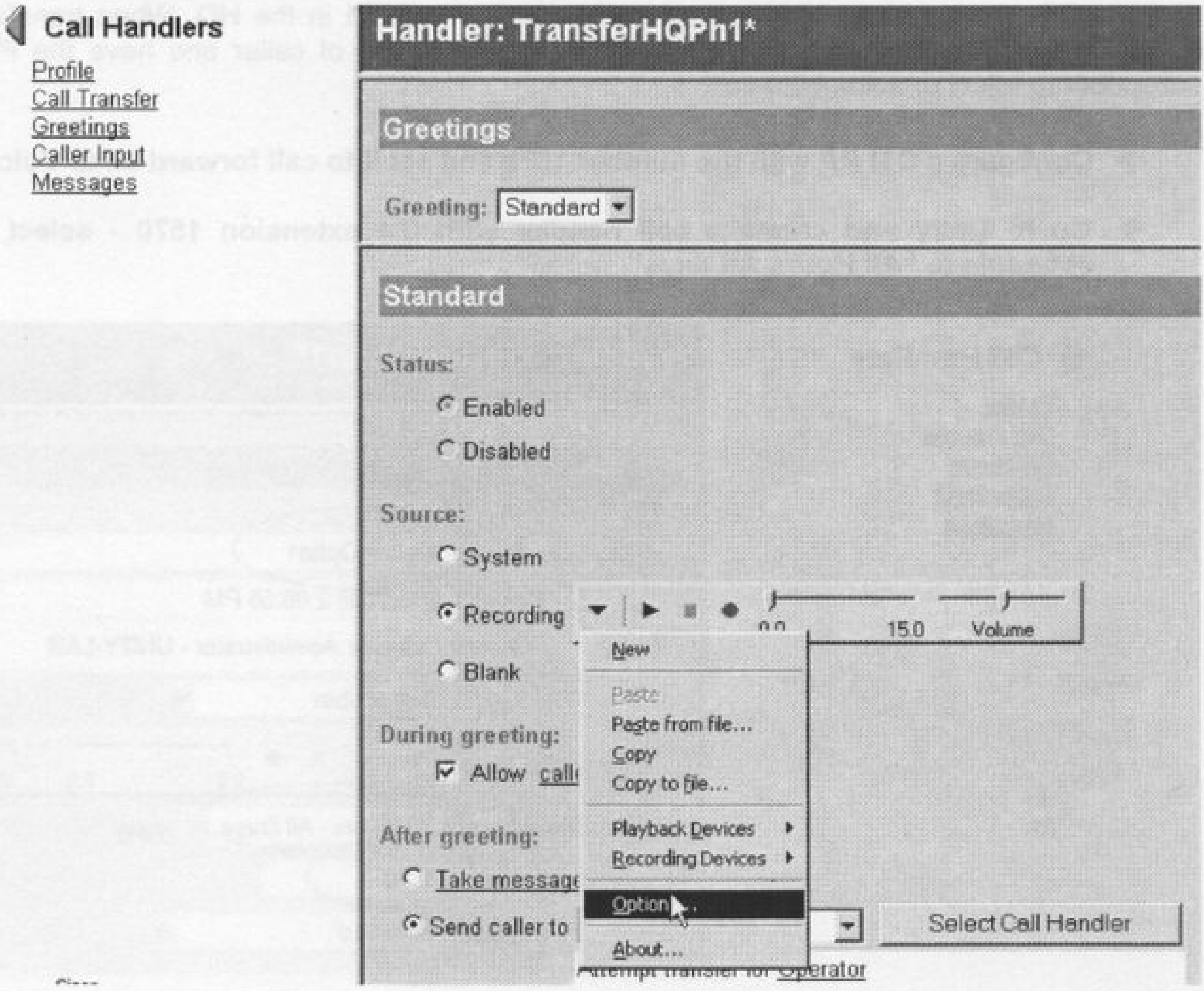
Configure CM and Unity such that when a caller dials 1570, the caller should hear "Welcome to IP Expert" in the greeting, and then be transferred to Phone 1 in the HQ. When transferred to Phone 1, the caller should be asked to announce the name of caller and have the Phone 1 subscriber to reject or accept the call.

➔ **Configure a CTI RP with the number 1570 and set it to call forward all to VoiceMail.**

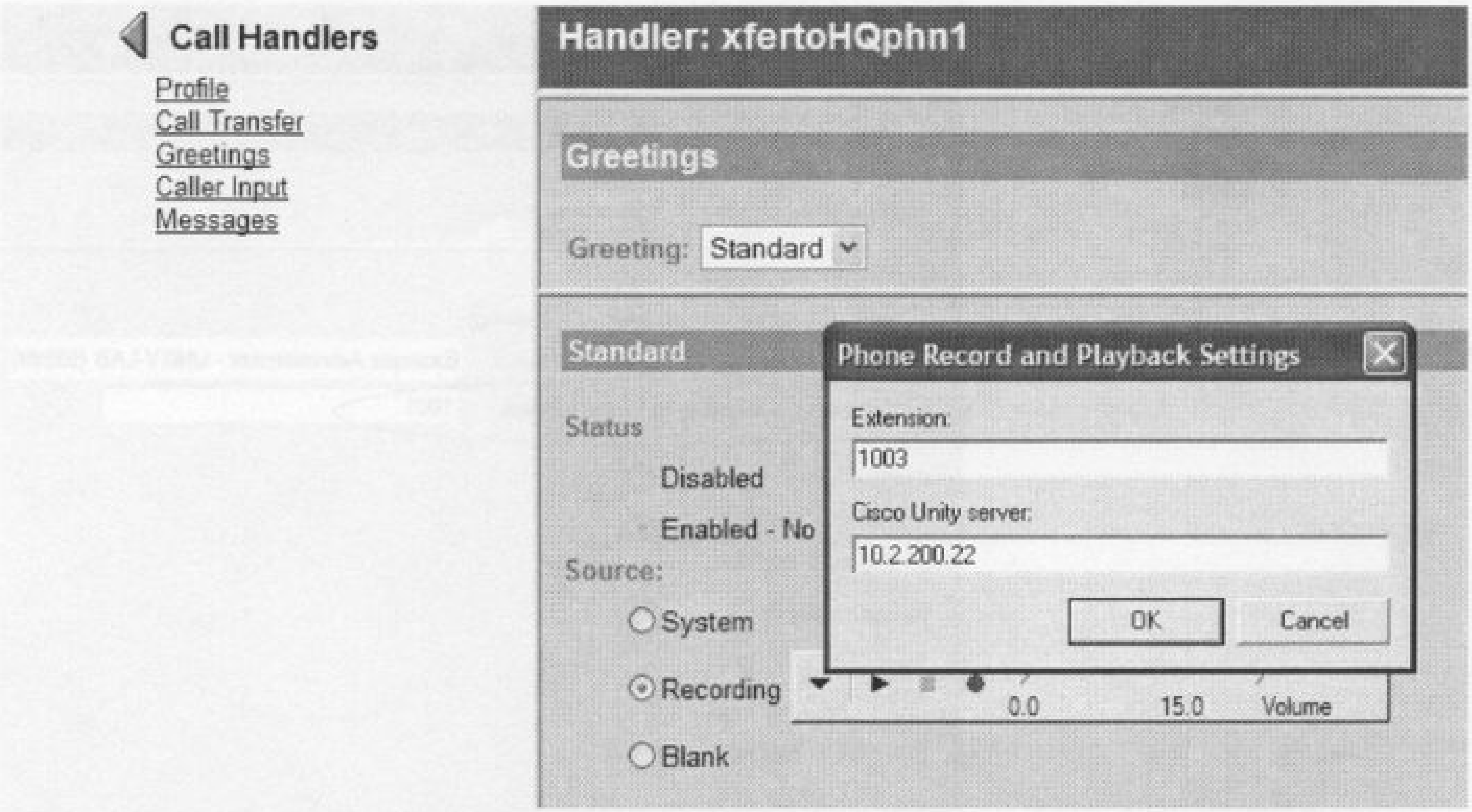
➔ **Go to Unity and create a call handler with the extension 1570 - select Active schedule to "All Hours All days".**



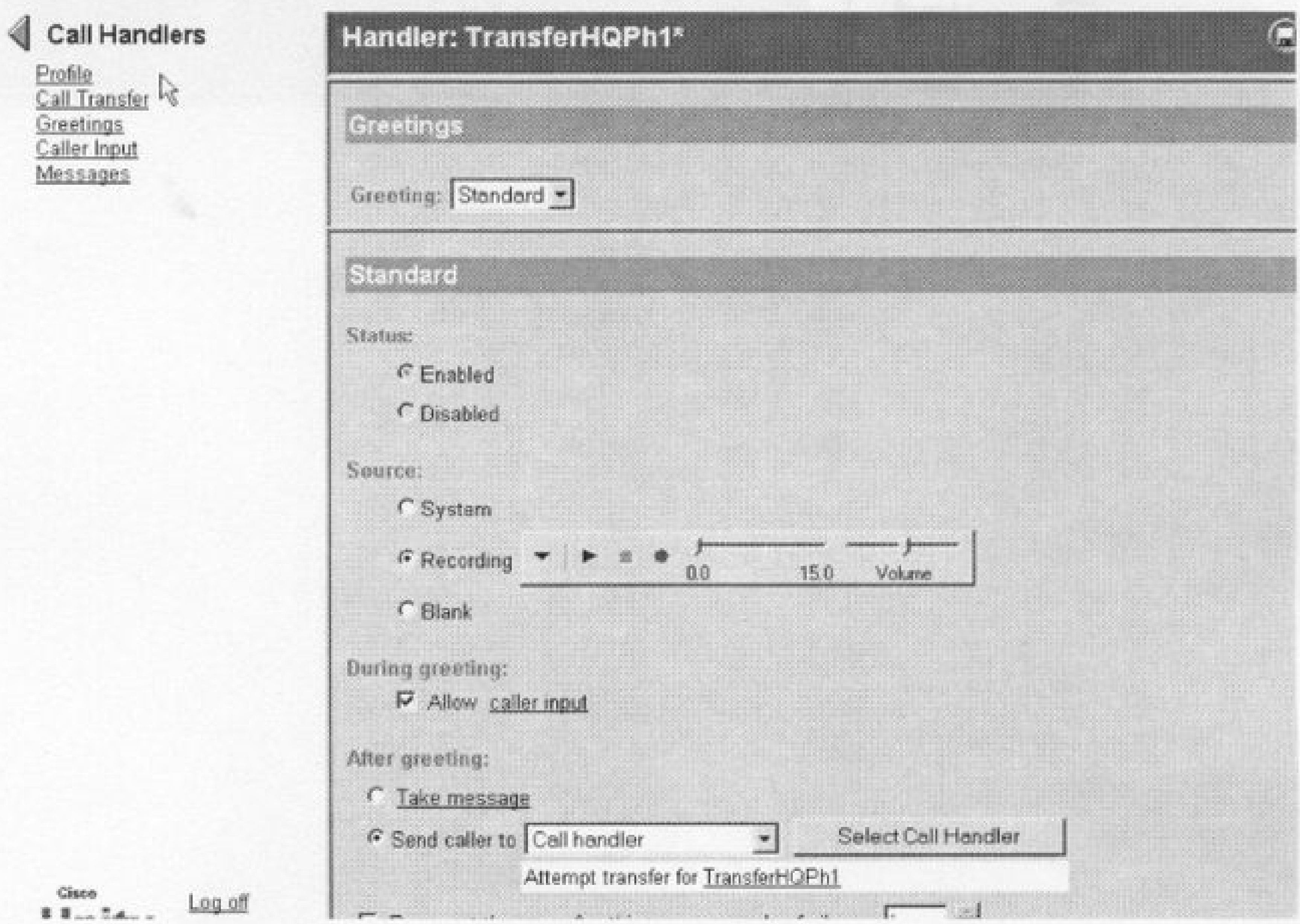
➔ **Go to the Greeting page of the call handler, and record the greeting of "Welcome to IPExpert". Set up a phone to record the greeting as below:**



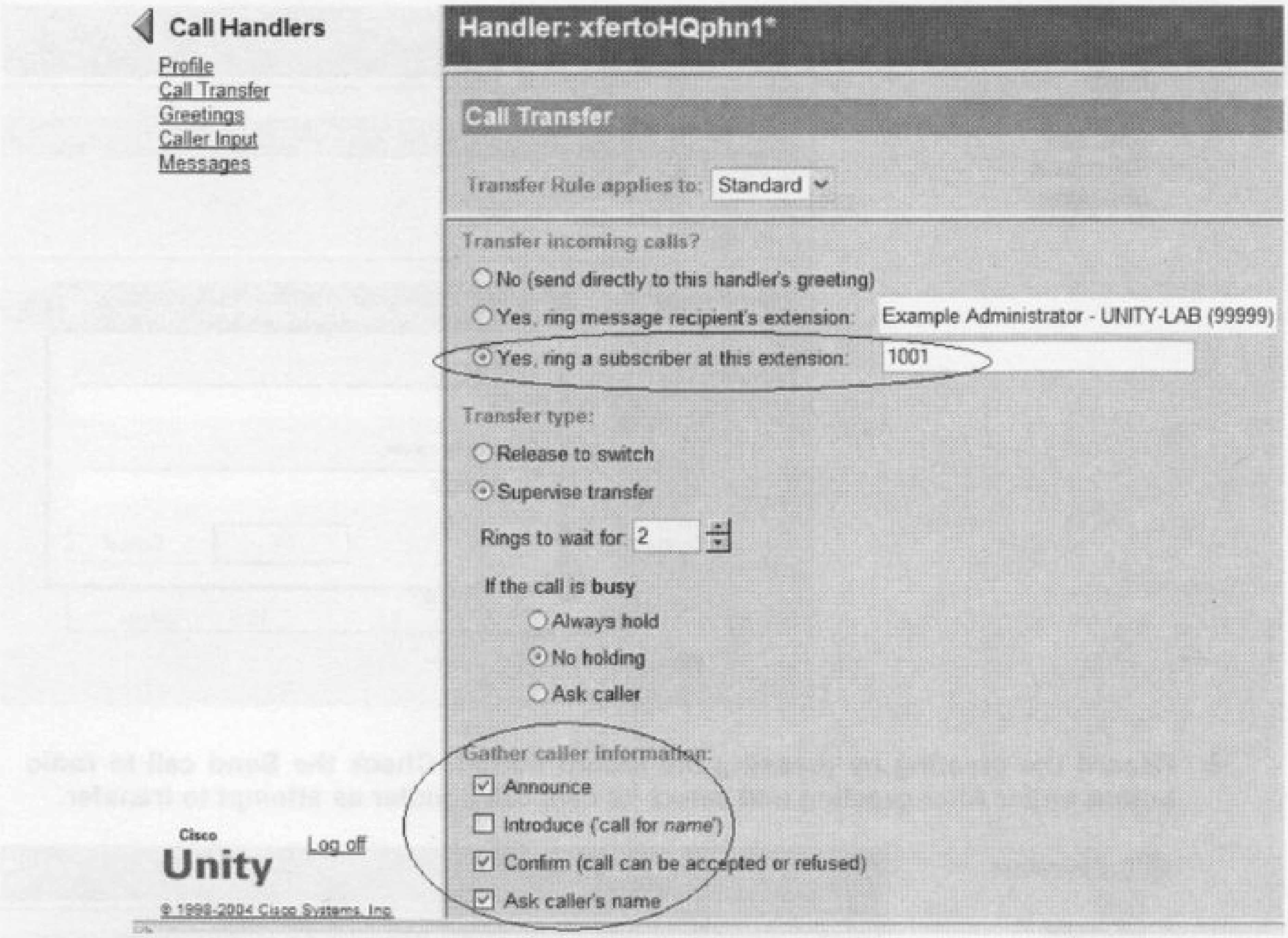
➔ **Enter the extension of an IP phone you want to use to record and the IP address of the Unity server.**



➔ **Record the greeting by pressing the record button. Check the Send call to radio button under After greeting and select its own call handler as attempt to transfer.**

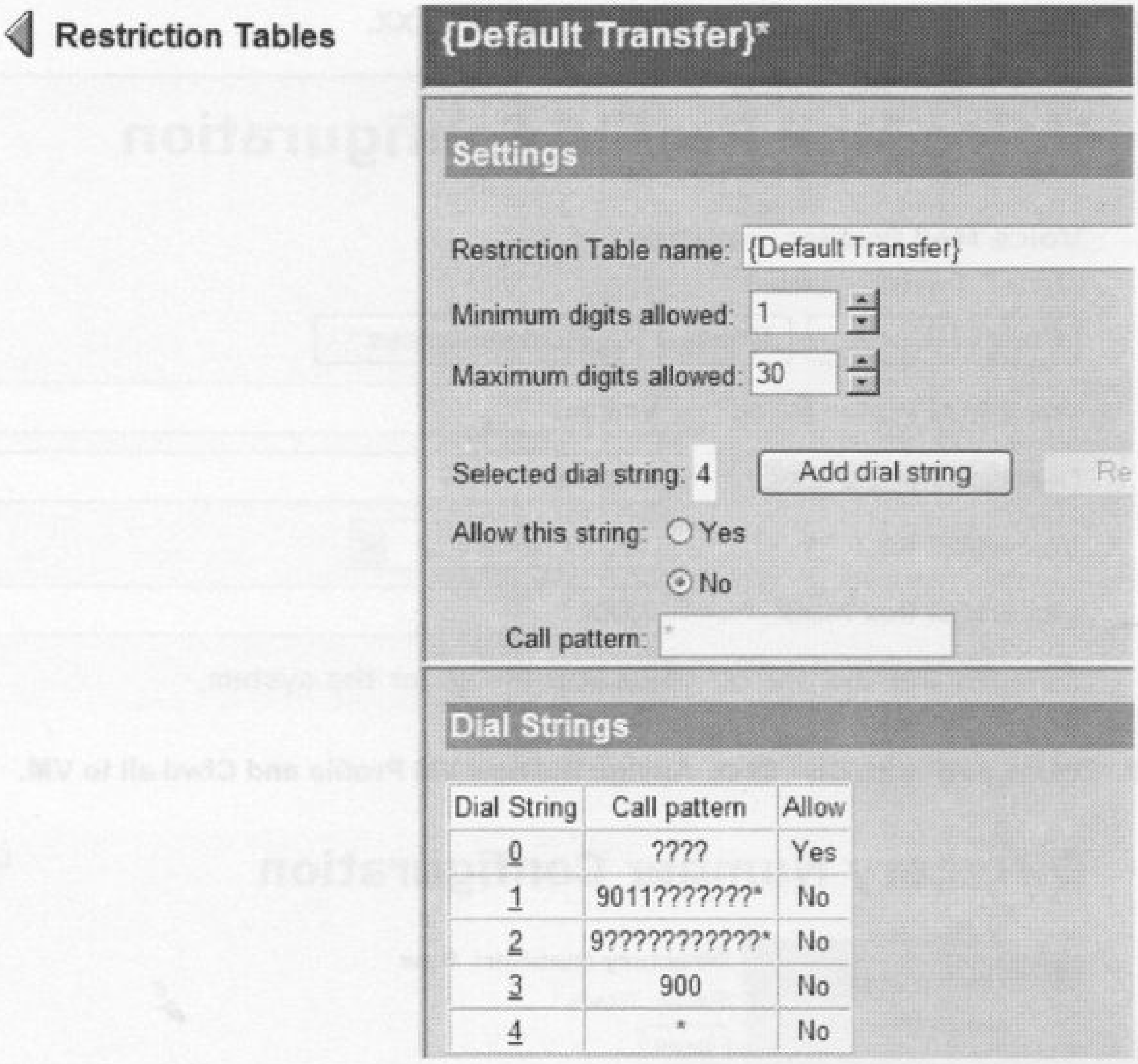


➔ **Go to the call transfer page, and configure the supervised call transfer to 1001 as shown below:**



Task 19.14

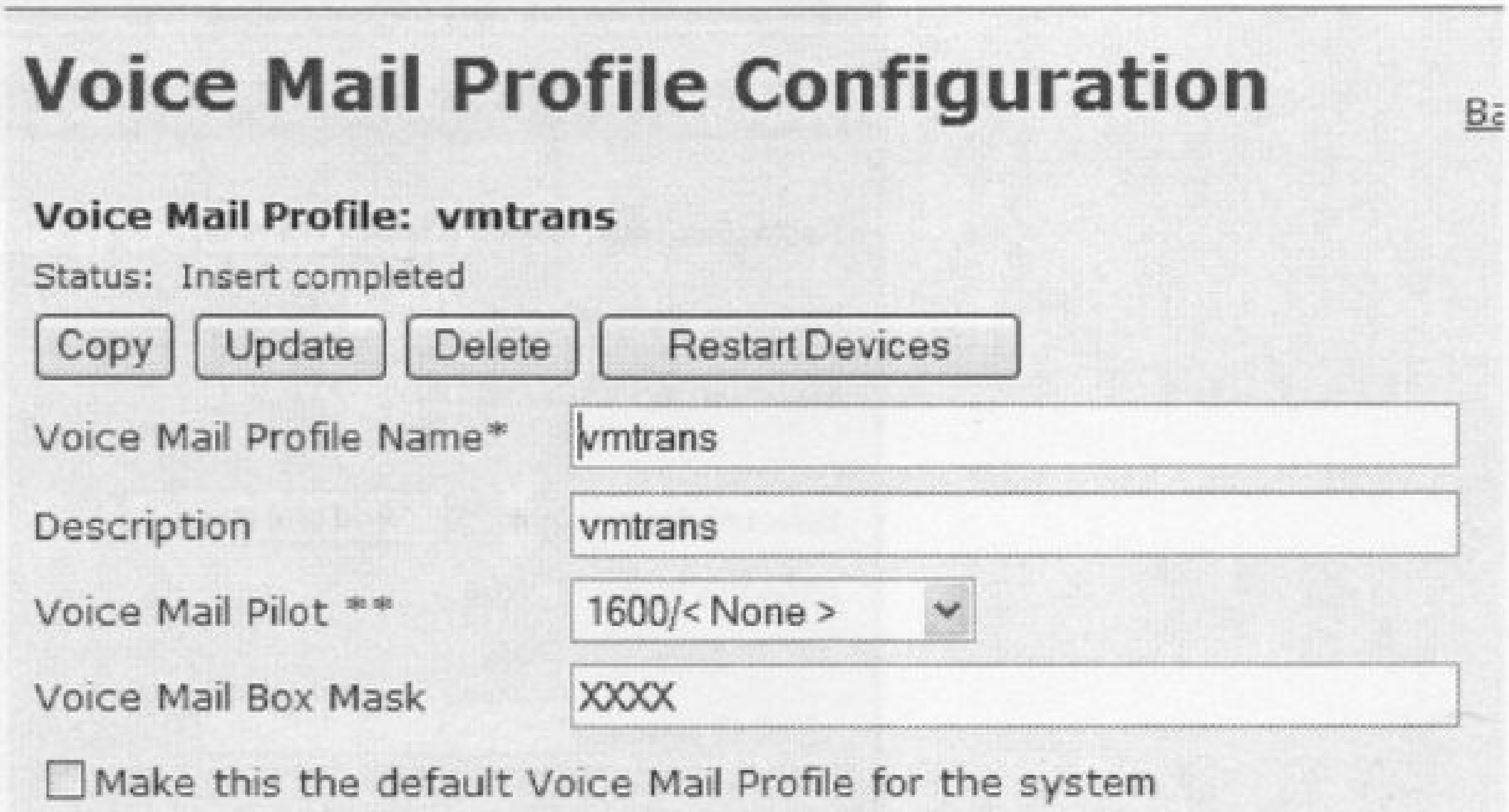
Configure Unity such that call transfers from Unity are allowed only for 4 digit internal numbers. Assume that this is not done by default.



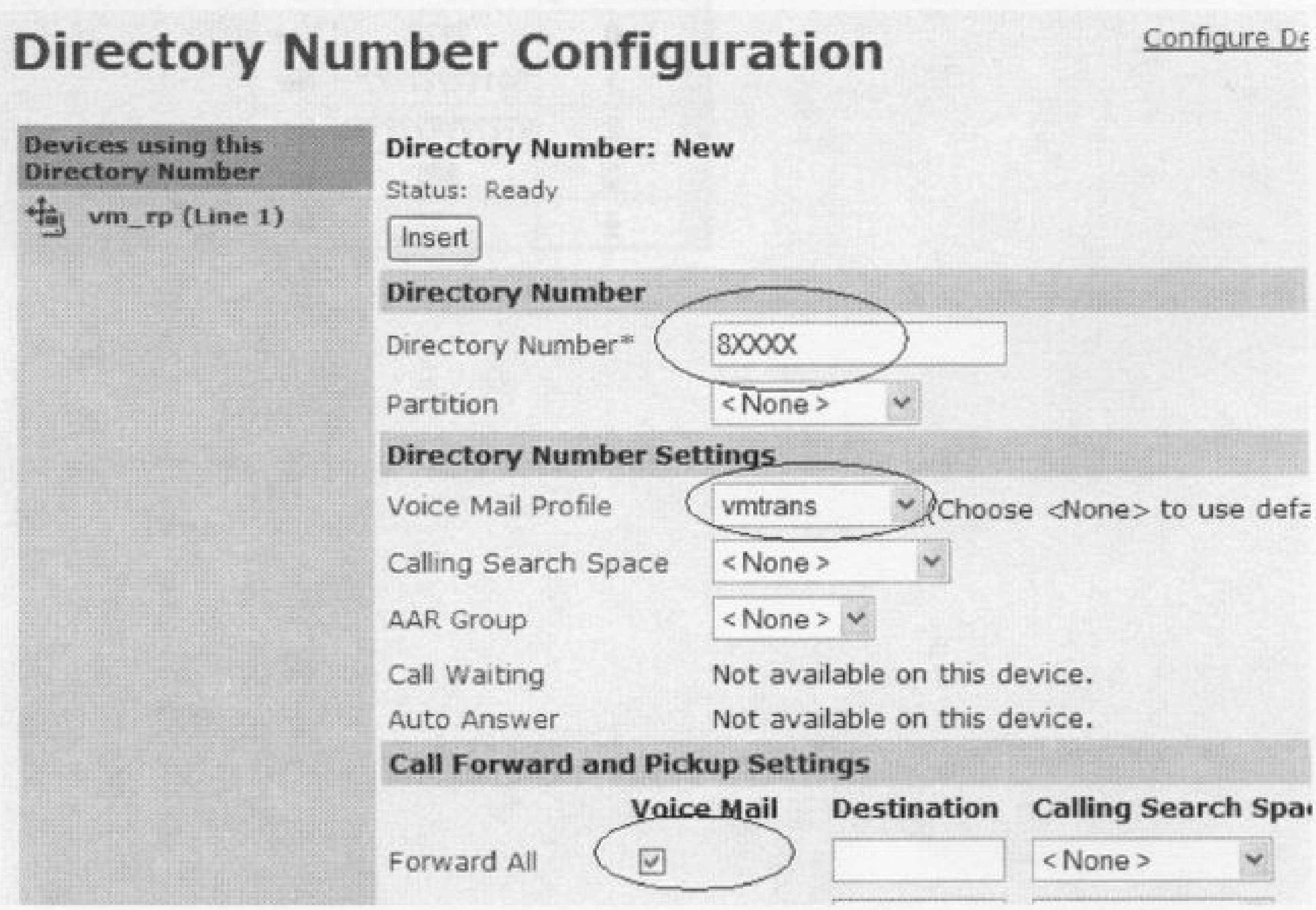
Task 19.15

Configure CM and Unity such that if a caller dials 8 plus 4 digit extension, the call goes directly to the mailbox of the subscriber instead of ringing the phone.

➔ **Create a new VoiceMail Profile with mask of XXXX.**



➔ **Create a RP with DN= 8xxx. Assign the new VM Profile and Cfwd all to VM.**



Task 19.16

Configure Unity so that if a IP Phone caller conferences in Ext 1650, that Unity will record the conversation and forward that recording to the mailbox of the IP Phone that initiated the conference.

➔ **This should be self-explanatory from previous examples – see Task 9.8.**

Task 19.17

➔ **This should be self-explanatory from previous examples – see Task 10.1.**

Task 19.18

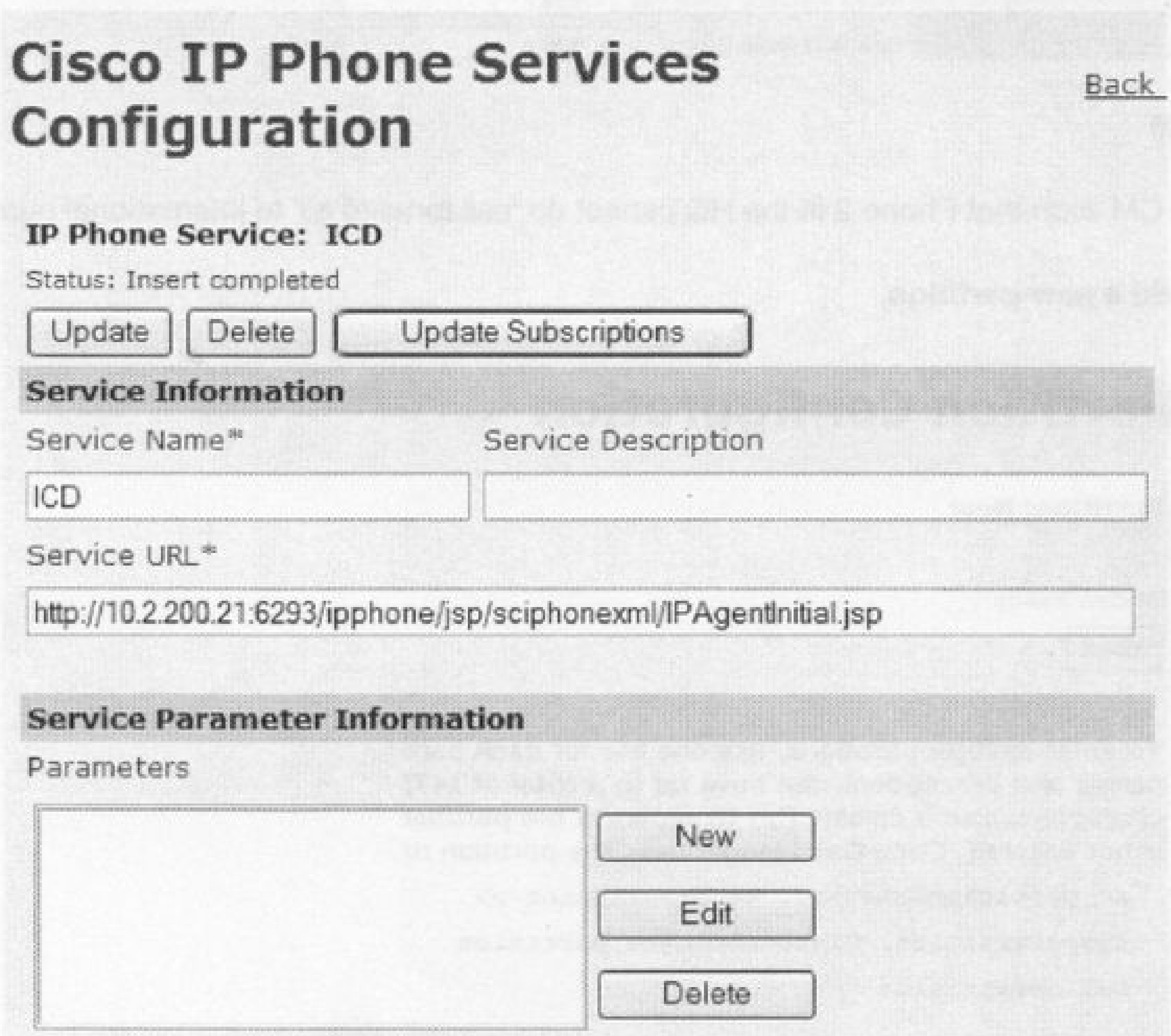
➔ **This should be self-explanatory from previous examples – see Task 10.2.**

Task 19.19

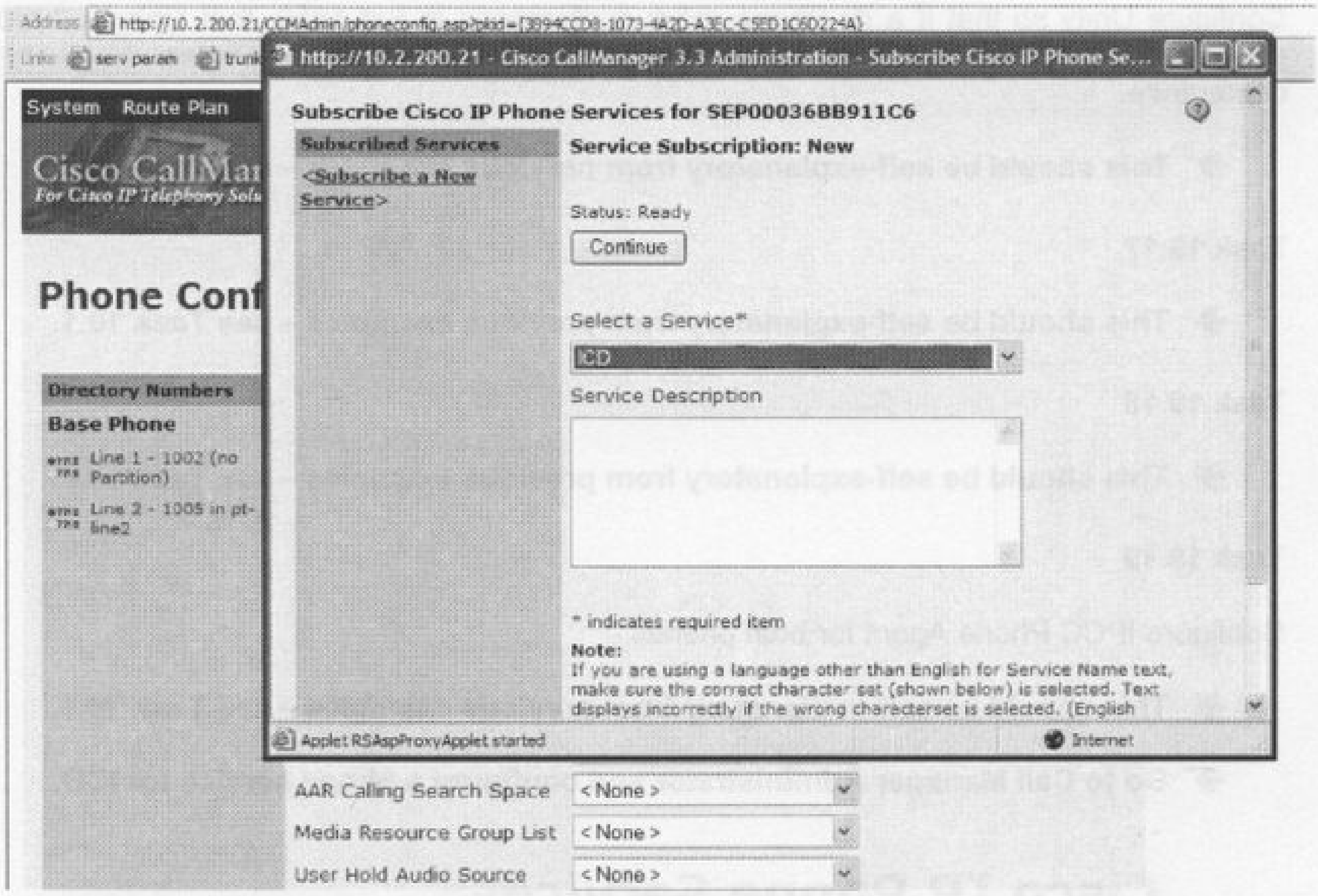
Configure IPCC Phone Agent for both phones.

➔ **This should be self-explanatory from previous examples – see Task 10.3.**

➔ **Go to Call Manager Administrator and configure a phone service for ICD.**



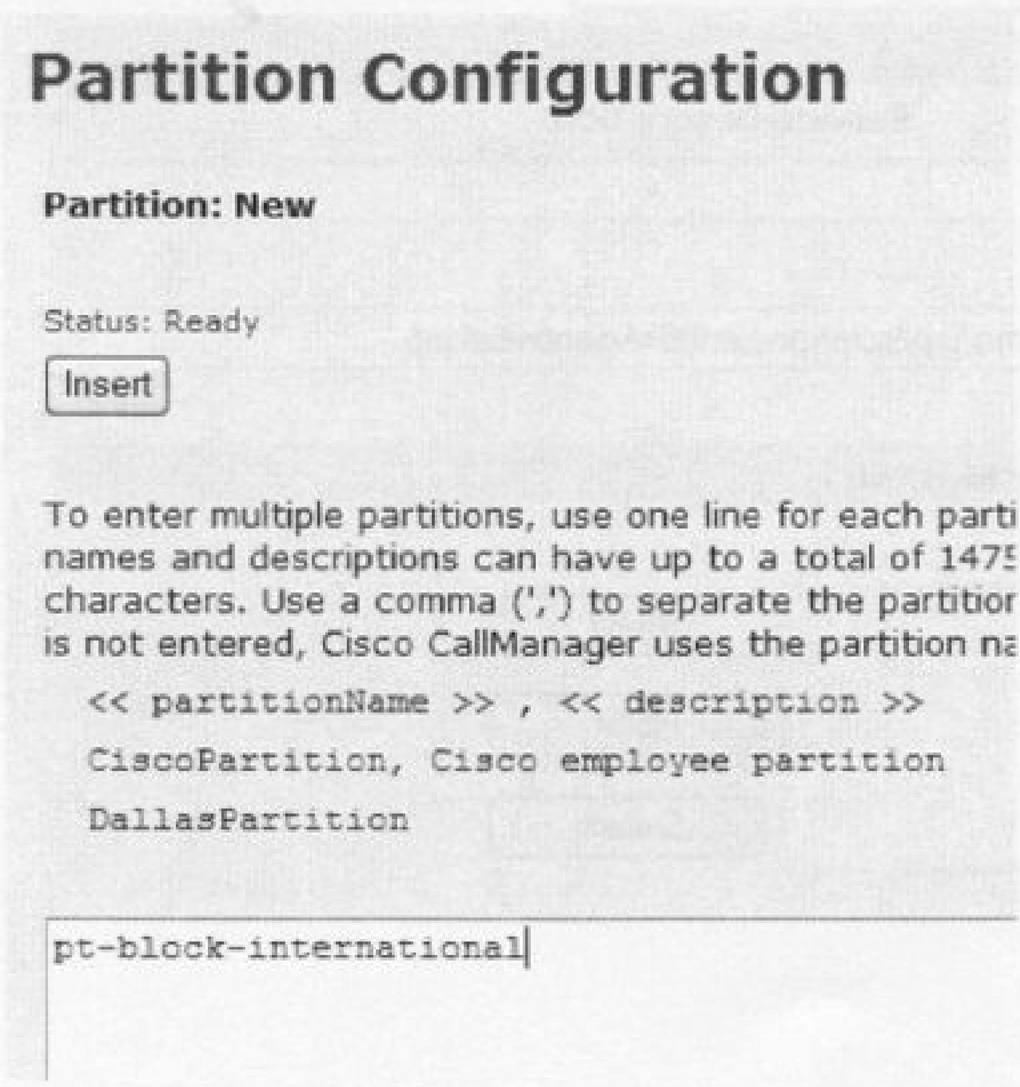
➔ **On the agent phone, subscribe to the ICD service.**



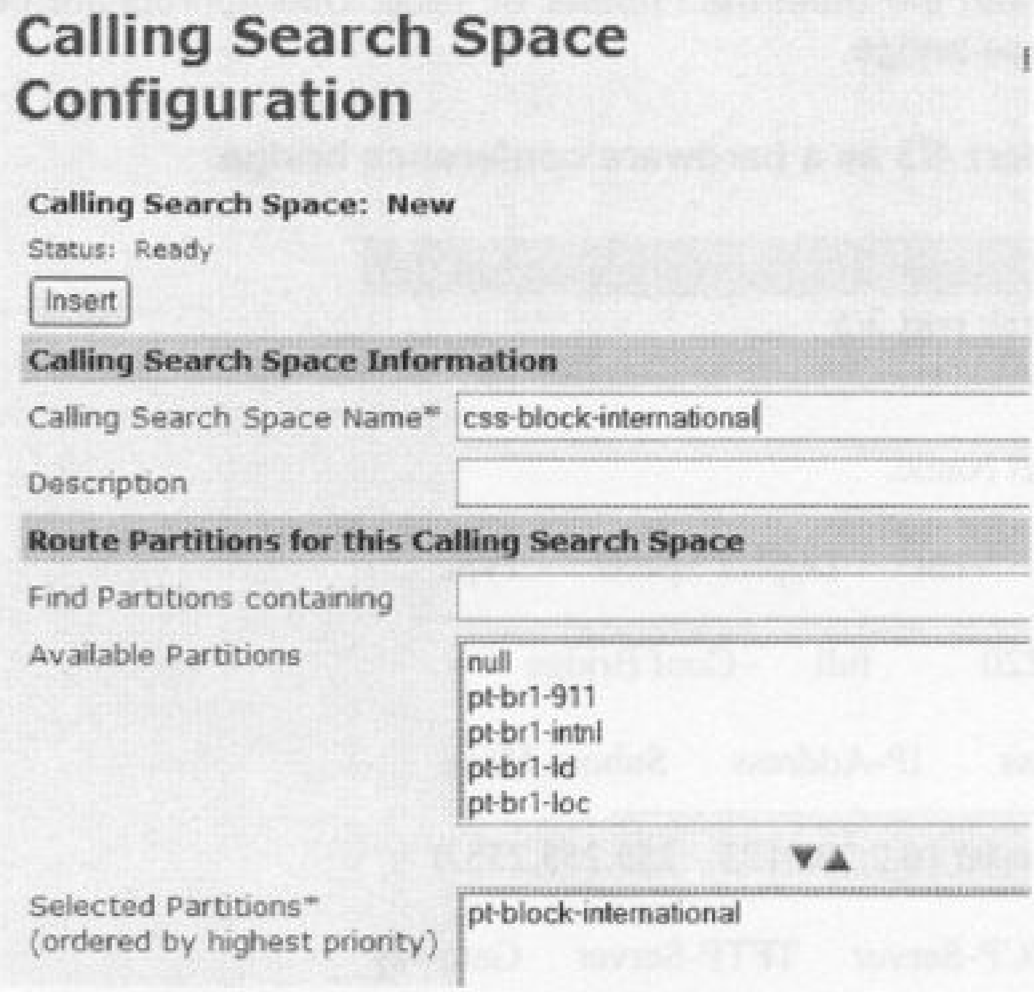
Task 19.20

Configure CM such that Phone 2 in the HQ cannot do 'call forward all' to international numbers.

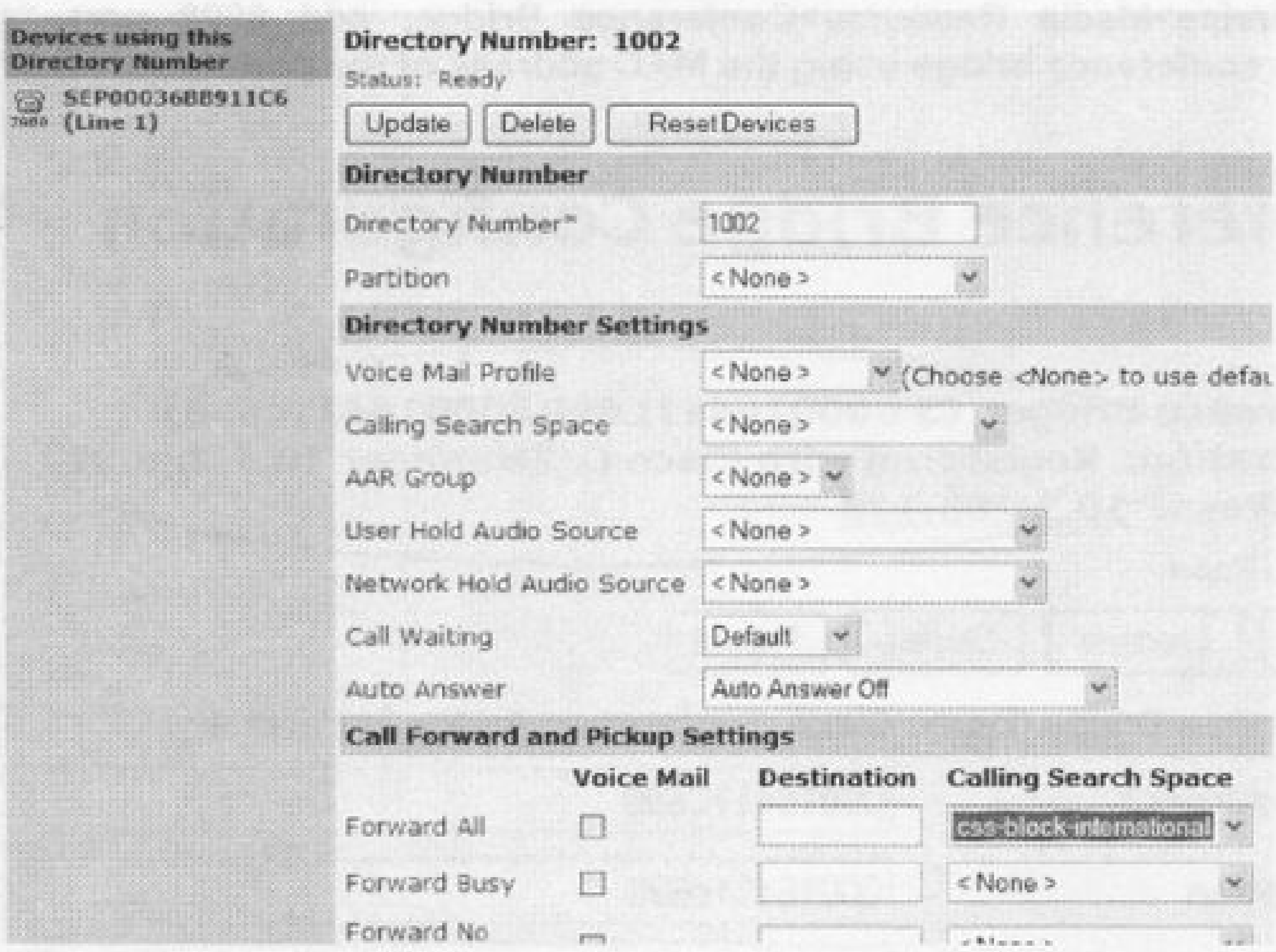
➔ **Add a new partition.**



➔ **Add a new CSS.**



➔ **Assign the CSS to the CFWD ALL CSS on the phone.**



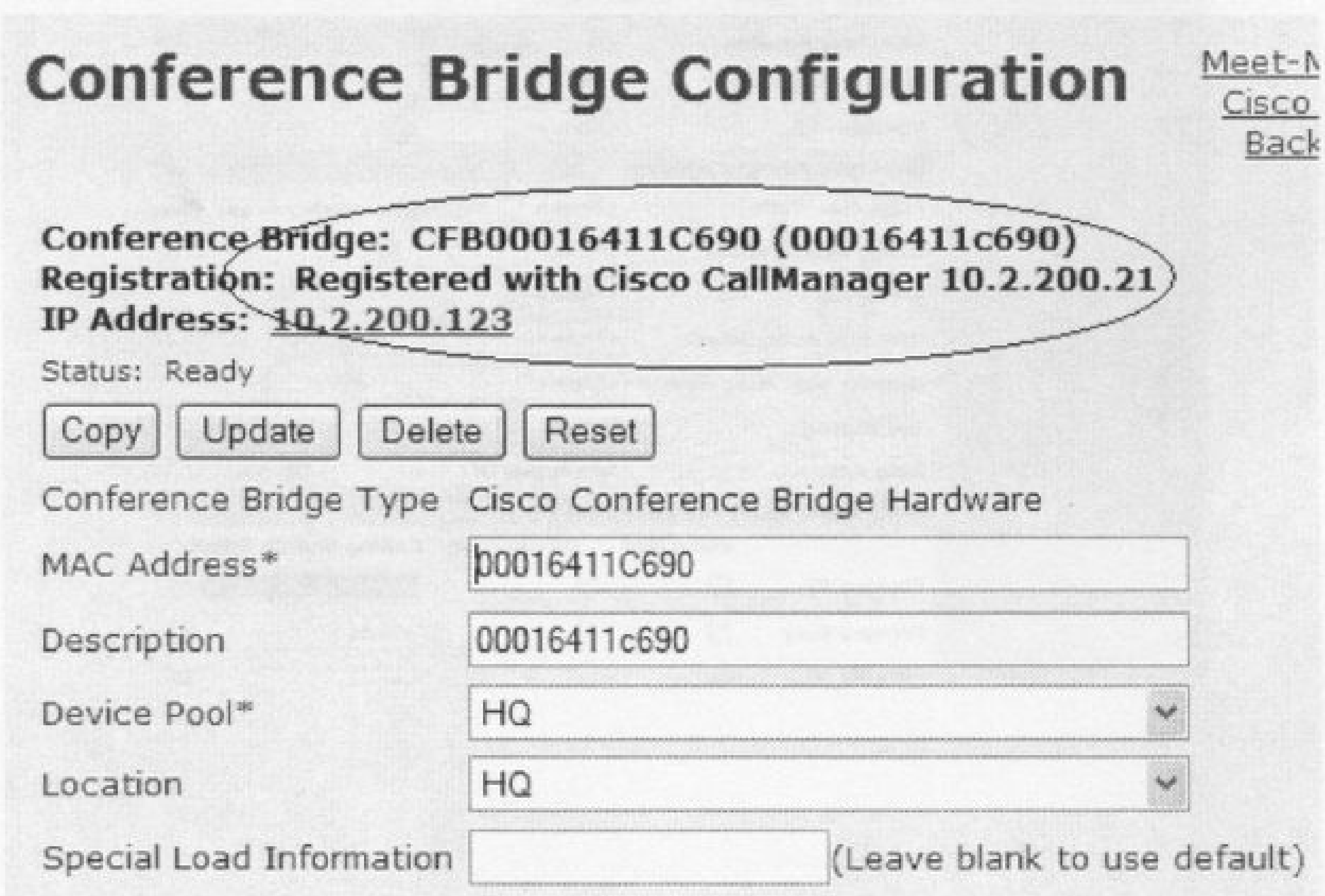
Task 19.21

Configure a meet-me conference with the meet-me number of 1900. Use appropriate 6608 port specified in Table 13 as a conference bridge.

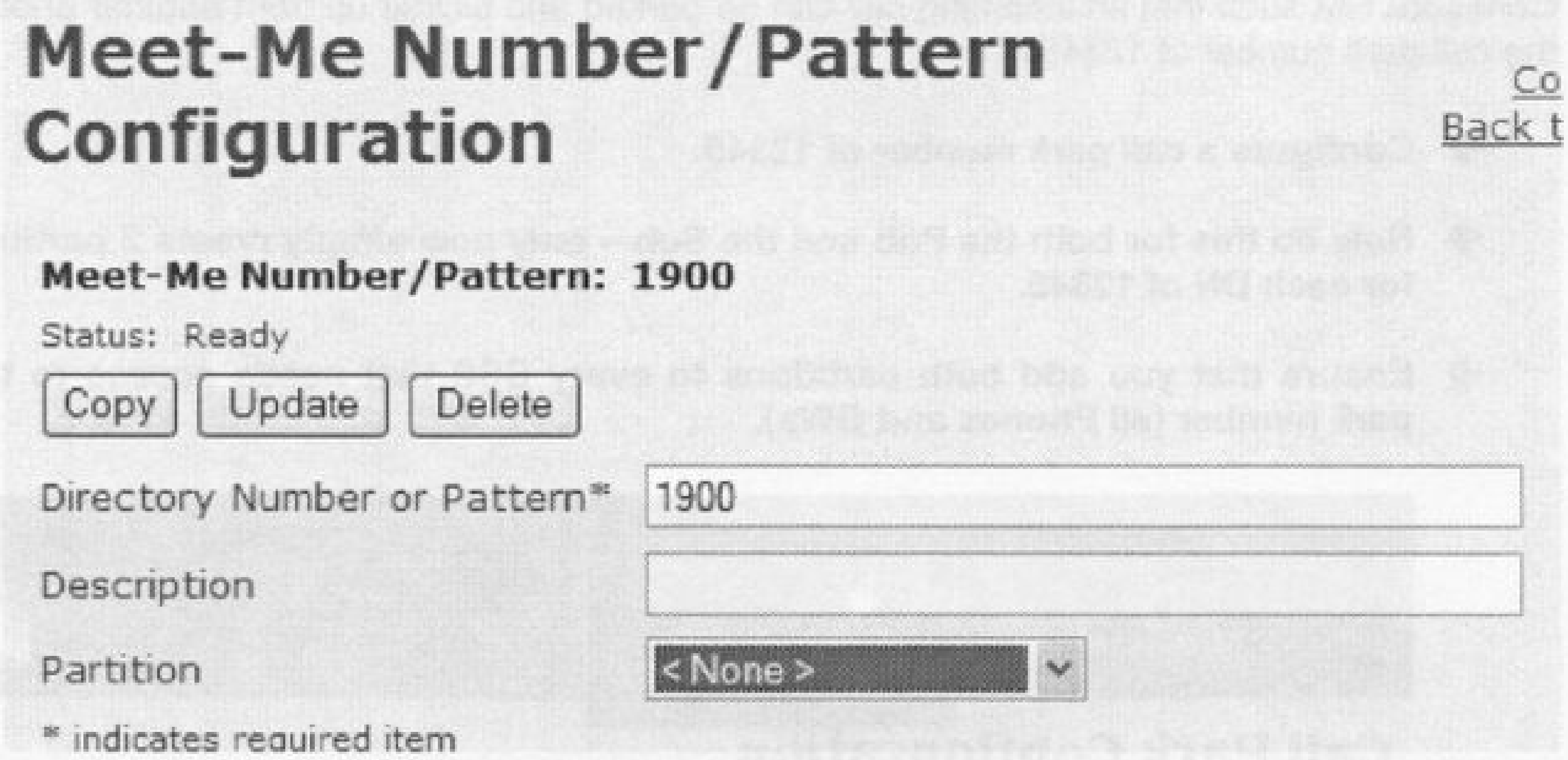
➔ **Configure 6608 module port 4/3 as a hardware conference bridge.**

```
Console>set port voice interface  3/5 dhcp enable vlan 220
PL-VoicePod-6500> (enable) sh port 3/5
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 3/5                       enabled    220        full   - Conf Bridge

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 3/5     enable  00-01-64-11-c6-90 10.2.200.123    255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 3/5     10.2.200.21       10.2.200.21     10.2.200.21     10.2.200.3
```

➔ **From Service>Media Resource>Conference Bridge, add 6608 port 3/5 as a hardware conference bridge using the MAC address of the port.**



➔ **Then configure a MeetMe directory number as shown below.**



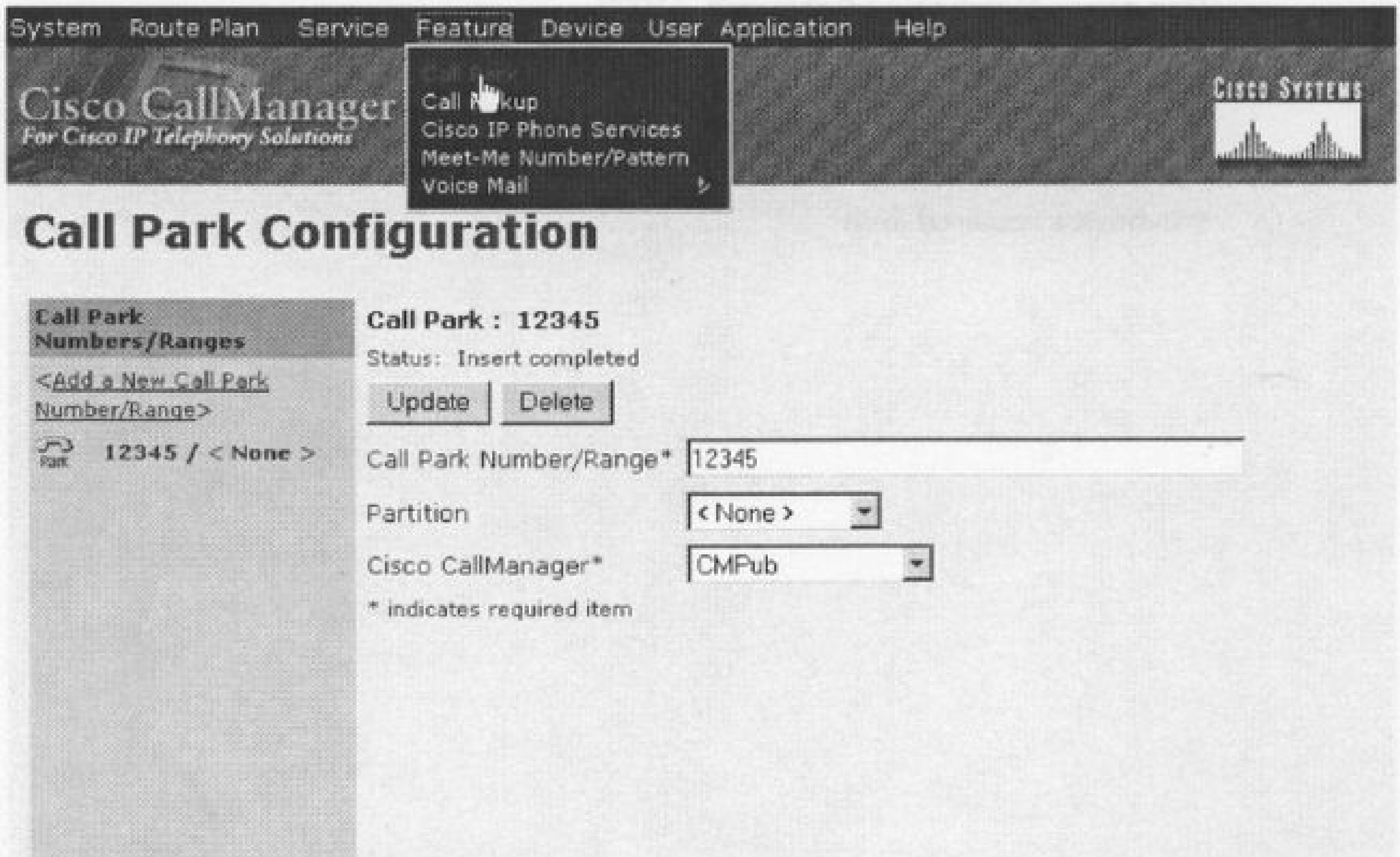
Task 19.22

Configure CM such that an incoming call can be parked and picked up from another phone. Use the call park number of 12345.

➔ **Configure a call park number of 12345.**

➔ **Now do this for both the Pub and the Sub – only now simply create 2 partitions – 1 for each DN of 12345.**

➔ **Ensure that you add both partitions to every CSS that needs access to this call park number (all Phones and GWs).**

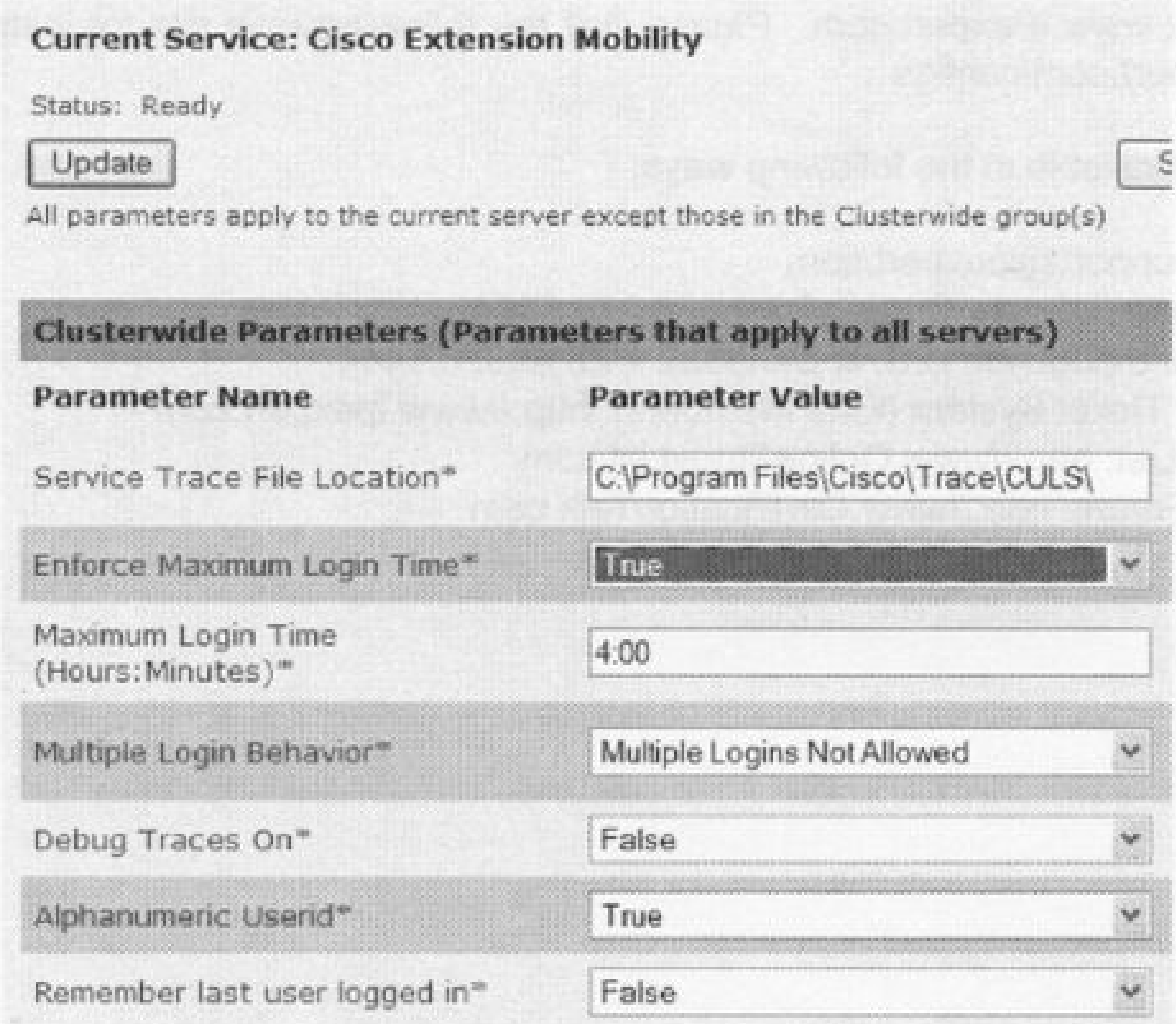


Task 19.23

There is a user in the organization the travels frequently to Branch 1. Configure Extension mobility for this user. The username will be ad, password is abcde. Ensure that his/her number will be the following at each of the sites: 1005 and 2005 for HQ and Branch 1 respectively. Configure EM such that the user be automatically logged out after 4 hours and the user be able to log out any time. Ensure that at each site that when the user dials 911 that the call goes out to the local gateway.

➔ **The steps in Task 11.3 should be followed to achieve this task. Create two Device Profiles with DN-1005 and DN=2005 and assign both Device Profiles to the user 'ad'.**

➔ **Configure EM Service Parameters to auto-logout after 4 hours and allow the user to log out at any time.**



➔ **To allow the user to log out at any time Subscribe the Device Profile to the EM Service.**

Task 19.24

Configure Attendant Console with the pilot number of 1550. Callers should be able to dial 0 as well as 1550 and reach 1003, and 2003. Enable Circular Hunting within the AC huntgroup. Also ensure that if there are up to 20 callers simultaneously calling 1550, and both IP Phones are presently taking calls, that callers will not be dropped but any number greater that 20 callers will be dropped and not sent to VM. Also, a call should not be dropped no matter how long it remains waiting.

➔ **Set up the Attendant Console using the steps in Task 11.1 and 11.3.**

➔ **Create a translation pattern with '0' as a translation pattern and '1550' as a called party transform mask.**

Task 19.25

Configure FAX relay between HQ and Branch 1 with the fax rate of 7200 bps.

➔ **This has been covered in Section 13.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 20: Multiprotocol Challenge C

Estimated Time to Complete: 6 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 20 Multiprotocol Challenge C

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing the first 17 Labs.

Section 20 Configuration Tasks

Task 20.1

Configure the Voice and Data VLANs for all locations detailed in Table 2.

➔ **This should be self-explanatory from previous examples – see Task 1.2.**

Task 20.2

Provide DHCP services for IP phones and gateways for all locations using IOS DHCP service only. Configure the Unity Server as the DNS service; be sure to use this for all name resolution.

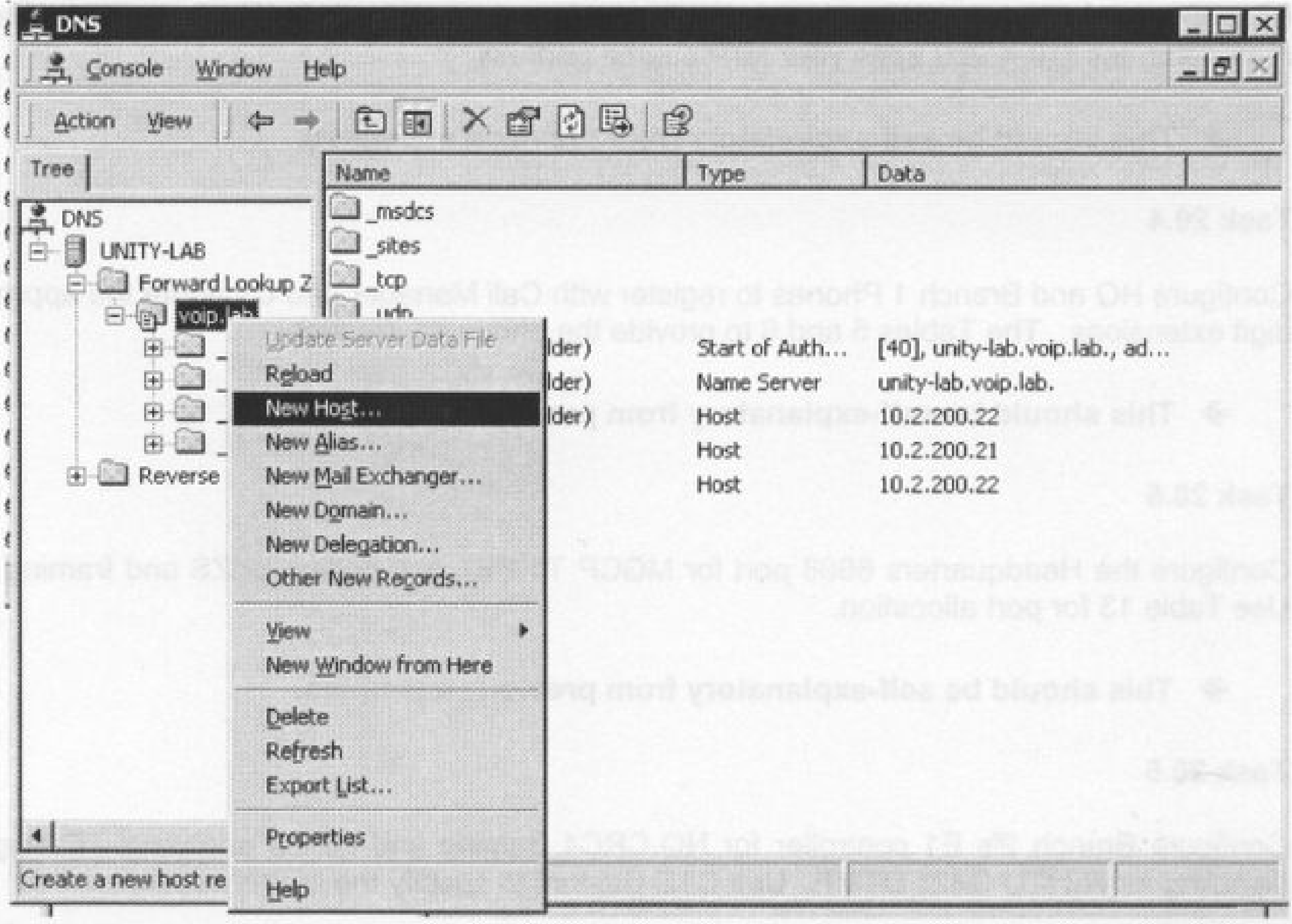
➔ **See Task 1.5 to configure IOS DHCP for HQ-RTR, BR1 and BR2.**

➔ **Log into Unity.**

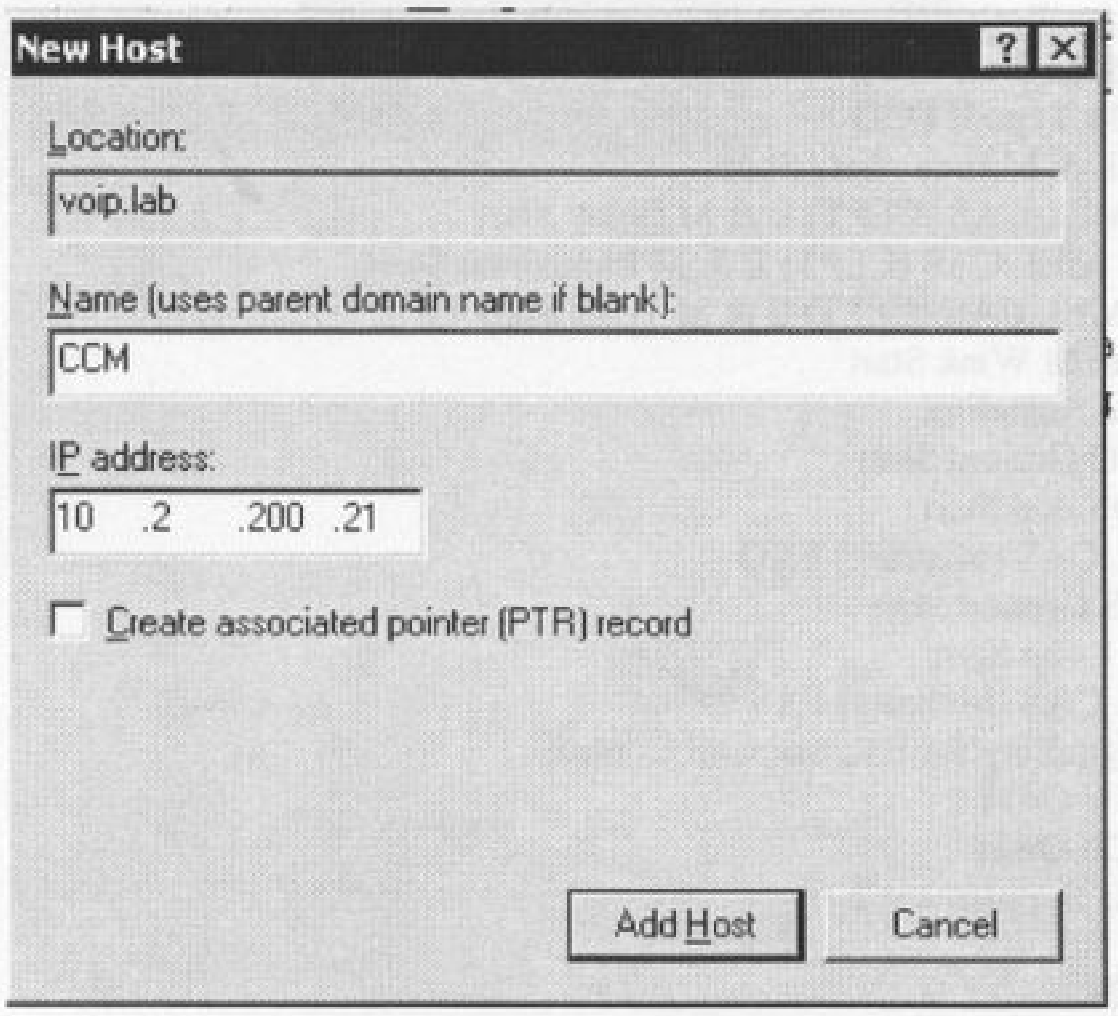
➔ **Confirm the DNS Server are running.**

➔ **Select the DNS Services from Start > Programs > Administrative Tools > DNS.**

➔ **Right-click the server and select New Host.**



➔ **Next add in all the devices into DNS.**



➔ **Add the host. Try pinging hostnames to see if DNS is resolving.**

Task 20.3

Configure time synchronization for Call Manager using the NTP protocol. Configure the backbone router address (10.X.200.2) as your NTP source address.

➔ **This should be self-explanatory from previous examples.**

Task 20.4

Configure HQ and Branch 1 Phones to register with Call Manager and configure the appropriate 4 digit extensions. The Tables 5 and 6 to provide the phone information.

➔ **This should be self-explanatory from previous examples.**

Task 20.5

Configure the Headquarters 6608 port for MGCP T1 PRI, line coding B8ZS and framing is ESF. Use Table 13 for port allocation.

➔ **This should be self-explanatory from previous examples.**

Task 20.6

Configure Branch 2's E1 controller for NO-CRC4 framing and HDB3 encoding. Configure the signaling for R2 ITU Q421 DTMF. Use CAS Custom to specify the country code.

➔ **To find out what ITU Q421 actually is, create the DS0-GROUP and use the ?**

```
P2-BR2-RTR(config-controller)#ds0-group 0 timeslots 1-3 type ?
  e&m-delay-dial       E & M Delay Dial
  e&m-fgd              E & M Type II FGD
  e&m-immediate-start  E & M Immediate Start
  e&m-melcas-delay     MEL CAS (CEPT) E & M Delay Start
  e&m-melcas-immed     MEL CAS (CEPT) E & M Immediate Start
  e&m-melcas-wink      MEL CAS (CEPT) E & M Wink Start
  e&m-wink-start       E & M Wink Start
  ext-sig              External Signaling
  fxo-ground-start     FXO Ground Start
  fxo-loop-start       FXO Loop Start
  fxo-melcas           MEL CAS (Mercury) FXO
  fxs-ground-start     FXS Ground Start
  fxs-loop-start       FXS Loop Start
  fxs-melcas           MEL CAS (Mercury) FXS
  none                 Null Signalling for External Call Control
  r2-analog            R2 ITU Q411
  r2-digital           R2 ITU Q421
  r2-pulse             R2 ITU Supplement 7
```

➔ **R2-Digital is ITU Q421.**

➔ **Configure the country parameter. This loads the default register signals for that country.**

```
P2-BR2-RTR(config-controller)# cas-custom 0
P2-BR2-RTR(config-ctrl-cas)#country ?
  argentina      Argentina
  australia      Australia
  bemilcom       Bemilcom
  bolivia        Bolivia
  brazil         Brazil
  bulgaria       Bulgaria
  china          China
  colombia       Colombia
  costarica      Costa Rica
  croatia        Croatia
  .......
```

Task 20.7

Configure the Branch 1 T1 controller for MGCP PRI. Switch-type NI2 and line coding is B8ZS and framing is ESF.

➔ **This should be self-explanatory from previous examples.**

Task 20.8

Configure the gatekeeper with the following parameters:

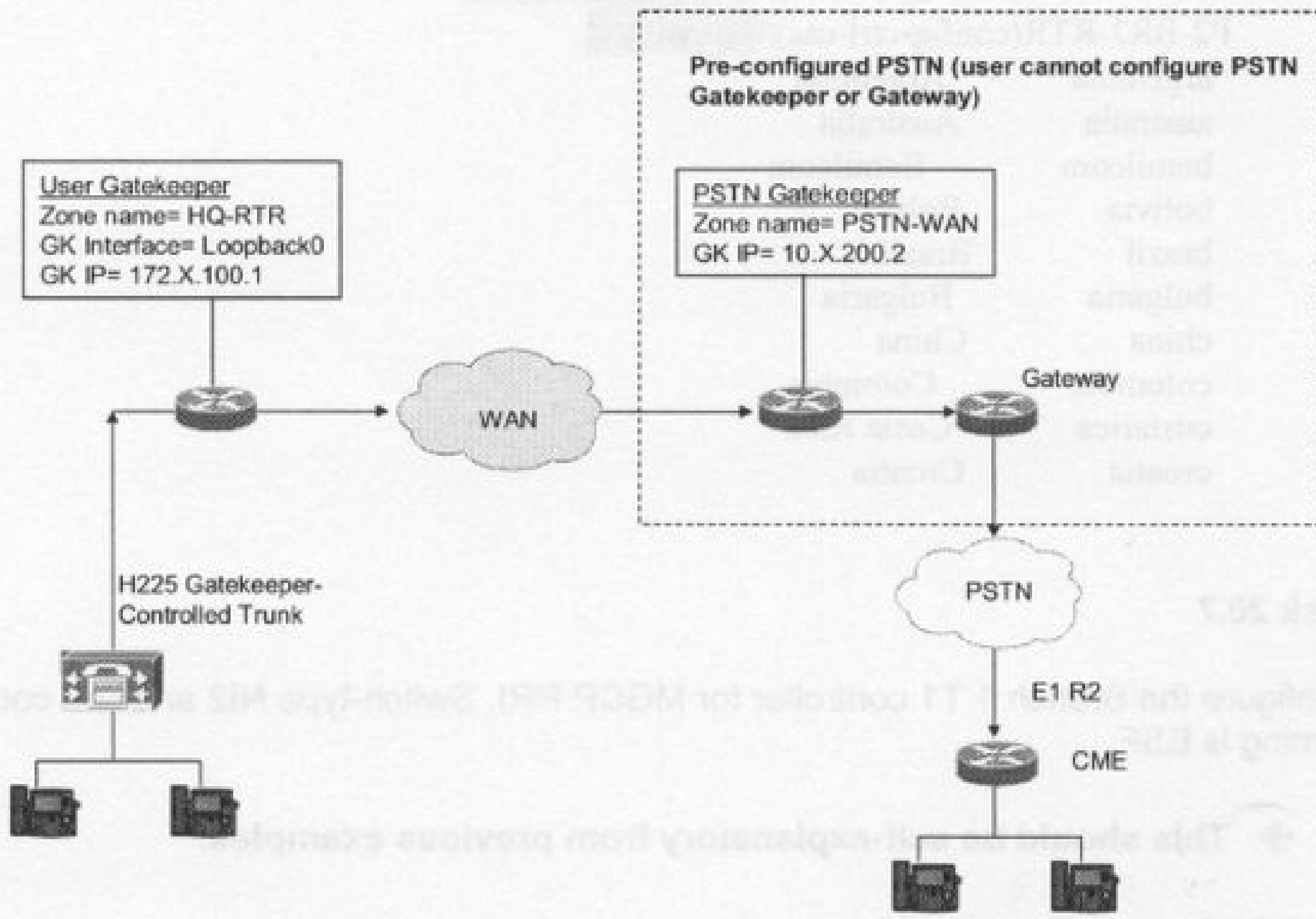
Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

Register Call Manager to the HQ-RTR gatekeeper.

Calls from HQ and BR1 destined for BR2 should be sent out of the gatekeeper. Full E164 number should be sent to gatekeeper including International prefix (see Table 10).

➔ **Be careful to study the exact topology for routing calls to CCME. Most people automatically assume this is an end-to-end VOIP call – not true.**



Call Routing: CM TO CME VIA GK

➔ **As far as you are concerned the call leaves the HQ-RTR gatekeeper and arrives into the CCME via the PSTN – in other words for the call to be successful you are reliant on the E1 R2 working correctly.**

➔ **We are not routing calls TO the CCM therefore we don't need to worry about Tech Prefix.**

➔ **In this scenario you have no control of the PSTN gatekeeper and the PSTN gateway.**

➔ **The first step in configuring the gatekeeper is to define the local zone using the "zone local" command.**

```
zone local gatekeeper-name domain-name [ras-IP-address]
```

➔ **Note that the zone name is case sensitive. A domain name is mandatory even if DNS resolution is not being used. The RAS IP Address is optional but it is recommended that one is defined to avoid gatekeeper registration problems.**

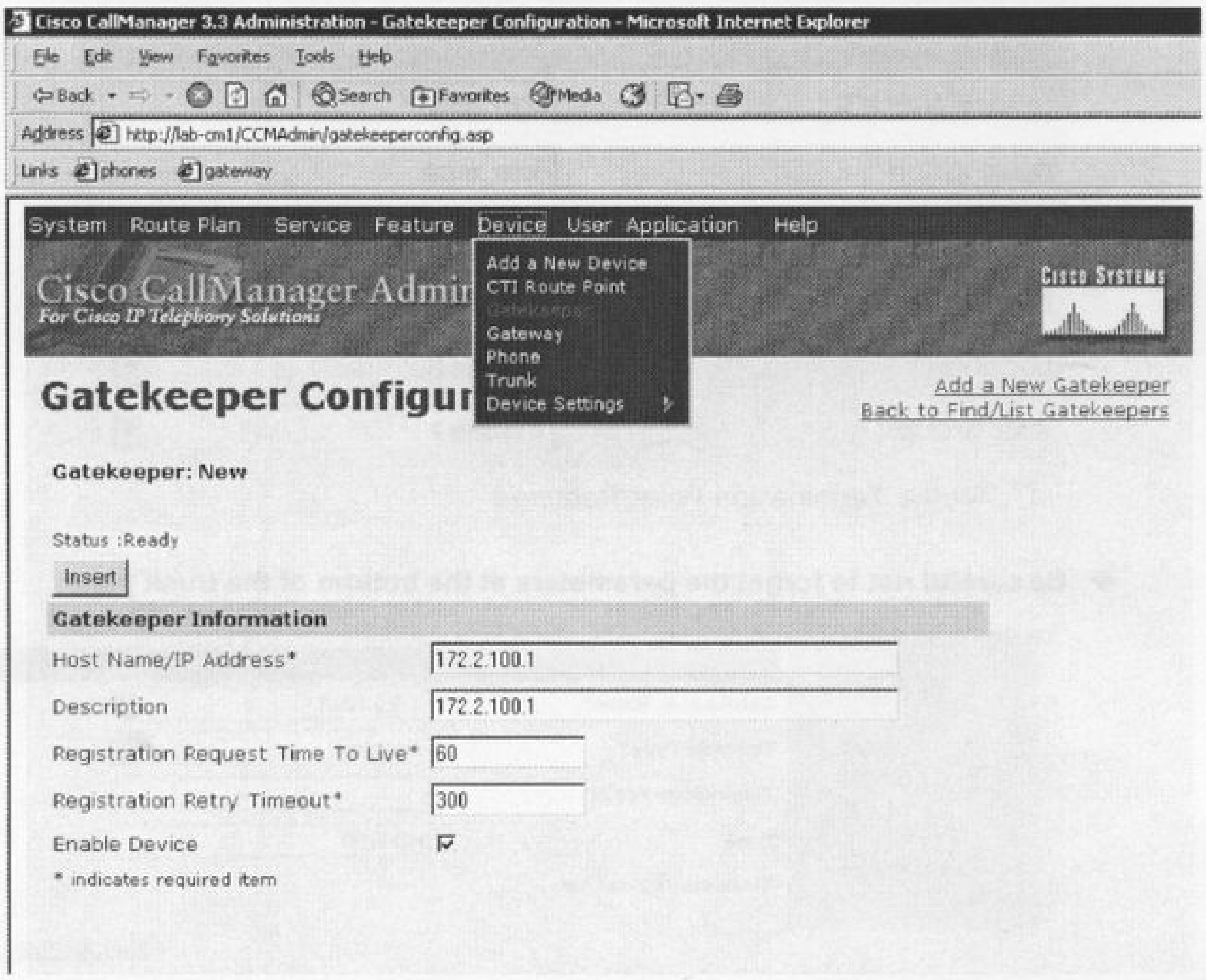
➔ **Remote zones can be defined in using the same command except the keyword "...local..." is replaced with "remote".**

➔ **The zone prefix command is required to route the call to the remote zone.**

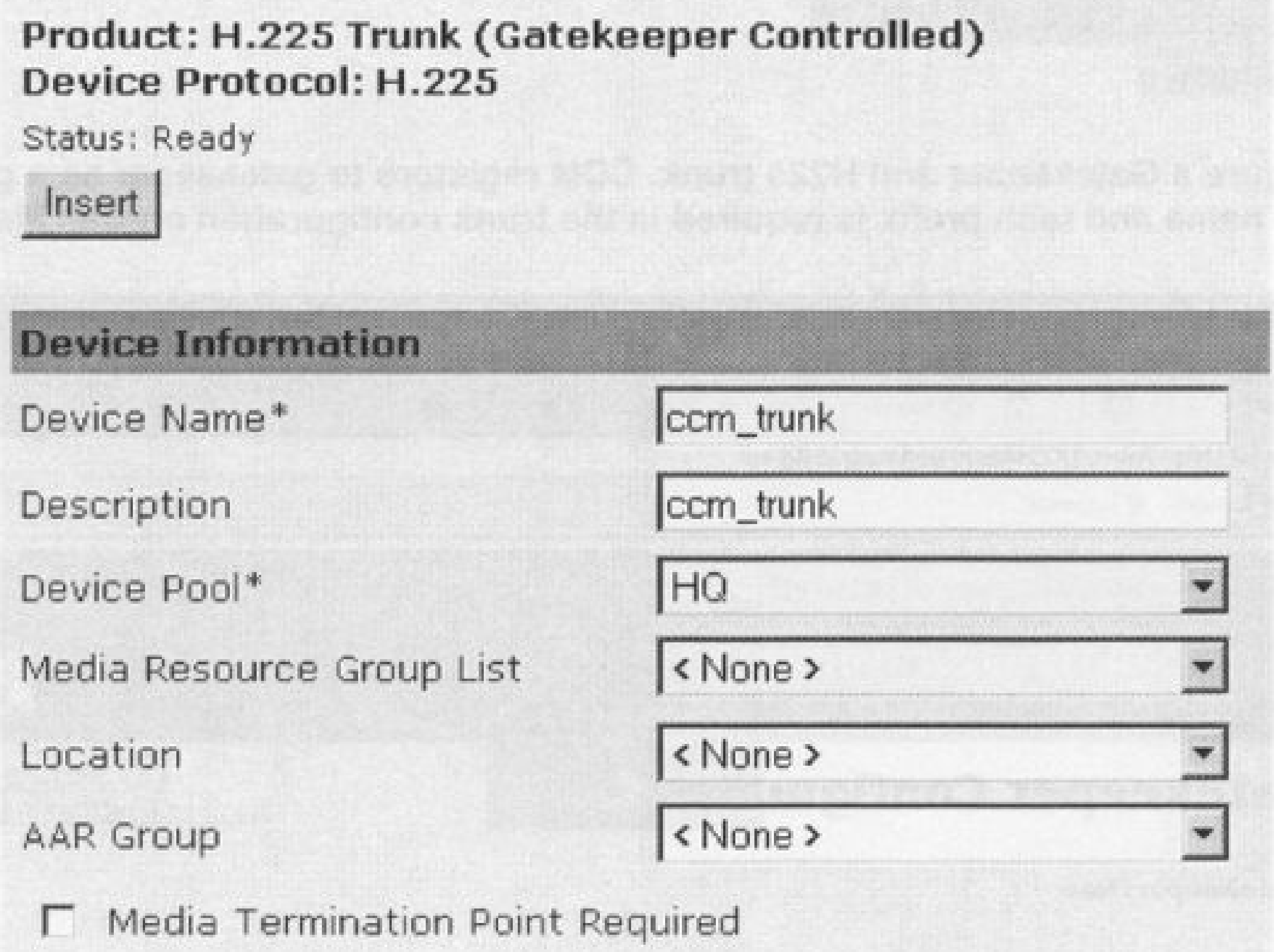
➔ **Tech-Prefix and bandwidth CAC is not required for this task.**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.5.100.1
 zone remote PSTN-WAN ipexpert.com 10.5.200.2 1719
 zone prefix PSTN-WAN 011*
 no shutdown
```

➔ **Configure a Gatekeeper and H225 trunk. CCM registers to gatekeeper as a gateway - zone name and tech prefix is required in the trunk configuration on Call Manager.**



➔ **From Device-Trunk add a H225 Trunk (Gatekeeper Controlled) and give it a unique name. Also don't forget to set Device Pool and Location information. The Location should be the unrestricted location and the Device Pool should contain the relevant region setting.**

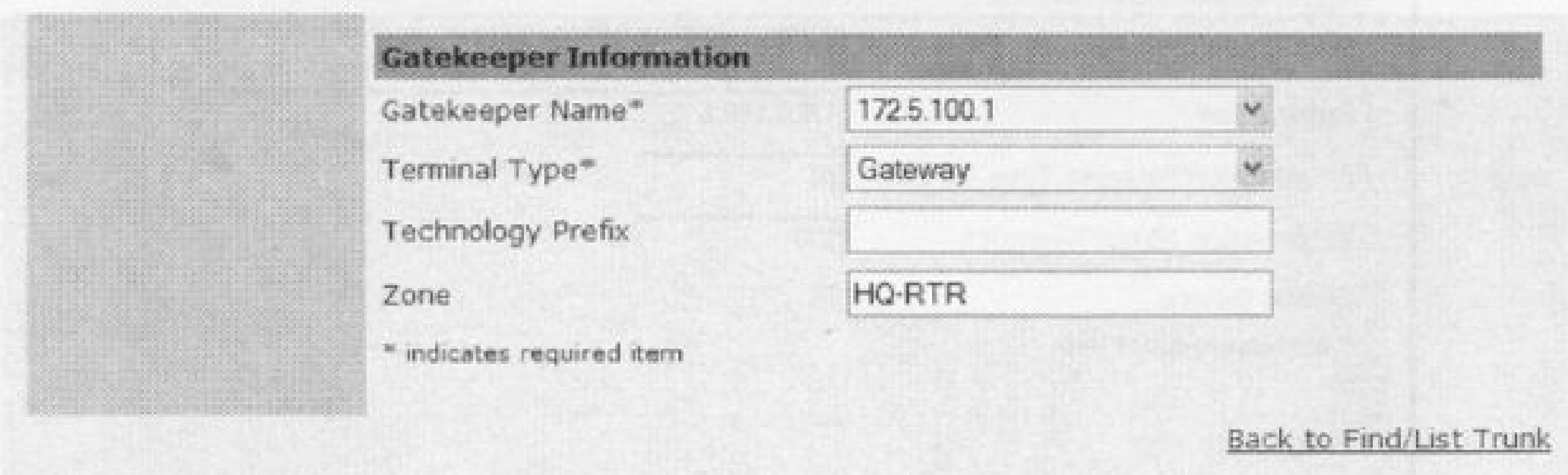

Product: H.225 Trunk (Gatekeeper Controlled)
Device Protocol: H.225
Status: Ready
Insert

Device Information

Device Name*	ccm_trunk
Description	ccm_trunk
Device Pool*	HQ
Media Resource Group List	< None >
Location	< None >
AAR Group	< None >

☐ Media Termination Point Required

➔ **Be careful not to forget the parameters at the bottom of the trunk page.**


Gatekeeper Information

Gatekeeper Name*	172.5.100.1
Terminal Type*	Gateway
Technology Prefix	
Zone	HQ-RTR

* indicates required item

Back to Find/List Trunk

➔ **Verify using the registration status as shown below:**

```
P2-HQ-RTR# sh gatek end
             GATEKEEPER ENDPOINT REGISTRATION
             ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name     Type    Flags
--------------- ----- --------------- ----- ---------     ----    -----
10.2.200.21     54029 10.2.200.21     52991 HQ-RTR        VOIP-GW
   H323-ID: GK-TRUNK_1
   Voice Capacity Max.=  Avail.=  Current.= 0
Total number of active registrations
```

➔ **Put the GK-TRUNK into a Route Group and the Route Group into a Route List. Add a Route Pattern = 3XXX and Prefix 011331322 (Digit Manipulation to be done in the Route List) and make the call.**

➔ **Now it is time to make the call.**

```
P5-HQ-RTR#debug gatekeeper main 10
*Aug 26 00:35:21.143: gk_process: QUEUE_EVENT (minor 0) wakeup
*Aug 26 00:35:21.147: gk_rassrv_arq: arqp=0x44D75E3C, crv=0x1, answerCall=0
*Aug 26 00:35:21.147: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
*Aug 26 00:35:21.147: gk_dns_query: No Name servers
*Aug 26 00:35:21.147: rassrv_get_addrinfo: (0113313253001) Tech-prefix match failed.
*Aug 26 00:35:21.147: rassrv_get_addrinfo: (0113313253001) Matched zone prefix 011 and
remainder 3313253001
*Aug 26 00:35:21.147: rassrv_get_addrinfo: No tech prefix

*Aug 26 00:35:21.147: rassrv_get_addrinfo: Alias not found

*Aug 26 00:35:21.147: rassrv_put_remote_zones_from_zone_list: zone PSTN-WAN
*Aug 26 00:35:21.147: send_lrq: seq_lrq 1, use_be 0, rzone_cnt 1
*Aug 26 00:35:21.147: send_lrq: lrq array index 0, lap 441D96F4
*Aug 26 00:35:21.147: send_lrq: sent lrq - zonecount 1
*Aug 26 00:35:21.151: gk_process: QUEUE_EVENT (minor 0) wakeup
*Aug 26 00:35:21.151: gk_zone_get_proxy_usage: local zone= HQ-RTR, remote zone= PSTN-
WAN, call direction= 1, eptype= 2050 be_entry= 0
*Aug 26 00:35:21.151: gk_zone_get_proxy_usage: returns proxied = 0
*Aug 26 00:35:33.303: gk_process: got a TIMER event

P5-HQ-RTR#sh gatekeeper calls
Total number of active calls = 1.
                    GATEKEEPER CALL INFO
                    ====================
LocalCallID                Age(secs)   BW
7-122                    22        16(Kbps)
 Endpt(s): Alias              E.164Addr
   src EP: gk_trunk_1          1001
        CallSignalAddr  Port  RASSignalAddr   Port
        10.5.200.21     1720  10.5.200.21     1719
 Endpt(s): Alias              E.164Addr
   dst EP:                  0113313253001
        CallSignalAddr  Port  RASSignalAddr   Port
        10.5.200.2      1720  10.5.200.2      1720
```

Task 20.9

Configure the HQ-RTR as an IPIPGW. Calls will be coming into it from CCM via H323 using G711ulaw and then be routed out to the BR2 CME via SIP using G729 (see Table 7 for DNs at CME). Calls will also be coming from CME via H323 using G729 and routed to CCM via SIP using G711ulaw (see Tables 5 and 6 for DNs at CCM). Also ensure when calls are coming from SIP to H323 that RFC 2833 is properly stripped. Ensure that if calls are coming from H323 to SIP, that RFC 2833 is used for the SIP side.

➔ **This should be self-explanatory from previous examples – see Task 4.9.**

Task 20.10

Configure the router in Branch 2 for CallManager Express. Register the devices and configure the DNs described in Table 7.

➔ **This should be self-explanatory from previous examples.**

Task 20.11

Configure a Call Block rule for all CME phones. Block all 900 and 976 calls. Create a user "IPExpert" and allow that user to override the block using Toll Bar Override. Deactivate the user's login after 25 minutes when the phone becomes idle.

```
telephony-service
load 7910 P00403020214
load 7960-7940 P00306000300
max-ephones 10
max-dn 15
ip source-address 10.2.200.21 port 2000
max-conferences 8
after-hours block pattern 1 91900 7-24
after-hours block pattern 2 91976 7-24
login timeout 25

P2-BR2-RTR(config)#ephone 1
P2-BR2-RTR(config-ephone)#pin 12345
P2-BR2-RTR(config)#ephone 2
P2-BR2-RTR(config-ephone)#pin 12345


P2-BR2-RTR(config-telephony)#reset all
```

Task 20.12

Create a Call Pickup group for both IP phones using 55 for the group number.

```
ephone-dn 1
number 3001
pickup-group 55

ephone-dn 2
number 3002
pickup-group 55
```

➔ **The phone user presses the PickUp soft key and then dials the ephone-dn of the ringing telephone. This method can also be used to pick up a call that is on hold on another ephone-dn.**

➔ **The phone user presses the GPickUp soft key and then dials the group number of the ringing telephone. The user needs only to press the GPickUp soft key.**

➔ **A ephone-dn that does not belong to any pickup group can still pick up a ringing call by dialing the ephone-dn on which the call is ringing or the pickup group number of that ephone-dn.**

Task 20.13

Configure both CME IP Phones with night service. Define the night service period of Mon-Through Friday 5:01pm to 7:59am and all weekend. Allow phone 1 to enter a code of *123 to manually disable it.

```
telephony-service
night-service code *123
night-service day Sun 08:00 07:59
night-service day Mon 17:01 07:59
night-service day Tue 17:01 07:59
night-service day Wed 17:01 07:59
night-service day Thu 17:01 07:59
night-service day Fri 17:01 07:59
night-service day Sat 08:00 07:59
!
!
ephone-dn 1
number 3001
night-service bell
!
ephone-dn 2
number 3002
night-service bell
```

Task 20.14

Configure Voice Mail Integration for Call Manager. The information is provided below.

- Pilot Number: 1600
- Unity Port Number: 1601 – 1604
- Set the default password to 54321
- MWI Light – 1998 off
- MWI Light – 1999 on

➔ **This task should be self-explanatory and is covered in section 9.**

Task 20.15

Configure the BR2 router to support the CUE module using information from **Table 16**. Setup the basic information needed to work the CUE module including what is needed to access the web-based GUI to manipulate user's extensions and mailboxes.

Integrate CME into Unity Express using the same information as follows:

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

Finally setup mailboxes for all 3 phones at BR2

➔ **This task should be self-explanatory – see Task 15.1.**

Task 20.16

Configure all IP Phones with Unity or Unity Express Voicemail (depending on site). Use names that are descriptive to the site (e.g. HQ Phone1).

➔ **You may want to use the Bulk Import Wizard.**

Task 20.17

Configure Unity so that if a IP Phone caller conferences in Ext 1650, that Unity will record the conversation and forward that recording to the mailbox of the IP Phone that initiated the conference.

➔ **This task should be self-explanatory – see Task 9.8.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 21: Multiprotocol Challenge D

Estimated Time to Complete: <u>6 hours</u>

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 21 Multiprotocol Challenge D

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing the first 17 Labs.

Section 21 Configuration Tasks

Task 21.1

Check all of the Frame Relay connections and connectivity between sites.

- ➔ **This should be self-explanatory from previous examples.**

Task 21.2

Check all basic OSPF has been set up correctly – If not assign all interfaces to area 0 and verify the routing.

- ➔ **This should be self-explanatory from previous examples.**

Task 21.3

Configure both voice and data VLANs based on Table 2.

- ➔ **This should be self-explanatory from previous examples.**

Task 21.4

For Headquarter and Branch 1, use Microsoft DHCP server to allocate IP address for the IP phones, VG-248 and 6608. For Branch 2, use IOS DHCP to allocate IP address for the IP phones.

- ➔ **This should be self-explanatory from previous examples.**

Task 21.5

Configure Call Manager to allow ALL devices to register manually. Assign directory number to devices based on Tables 5, 6 and 7.

- ➔ **NOTE: No CCME in this lab.**

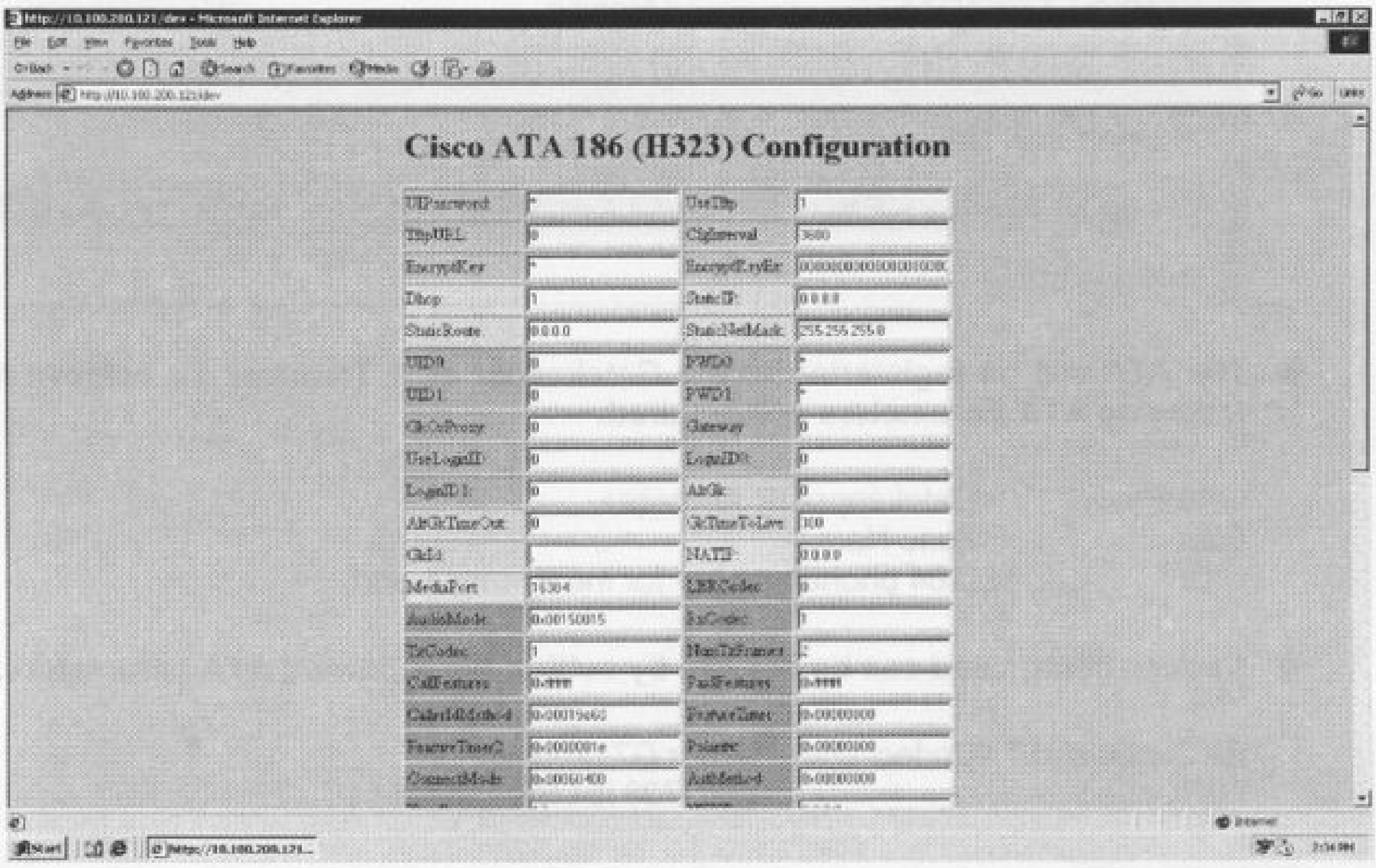
Task 21.6

Configure ATA-186 with H323 firmware image and allocate appropriate DN. Configure such that line 1 can use G711 and G729.

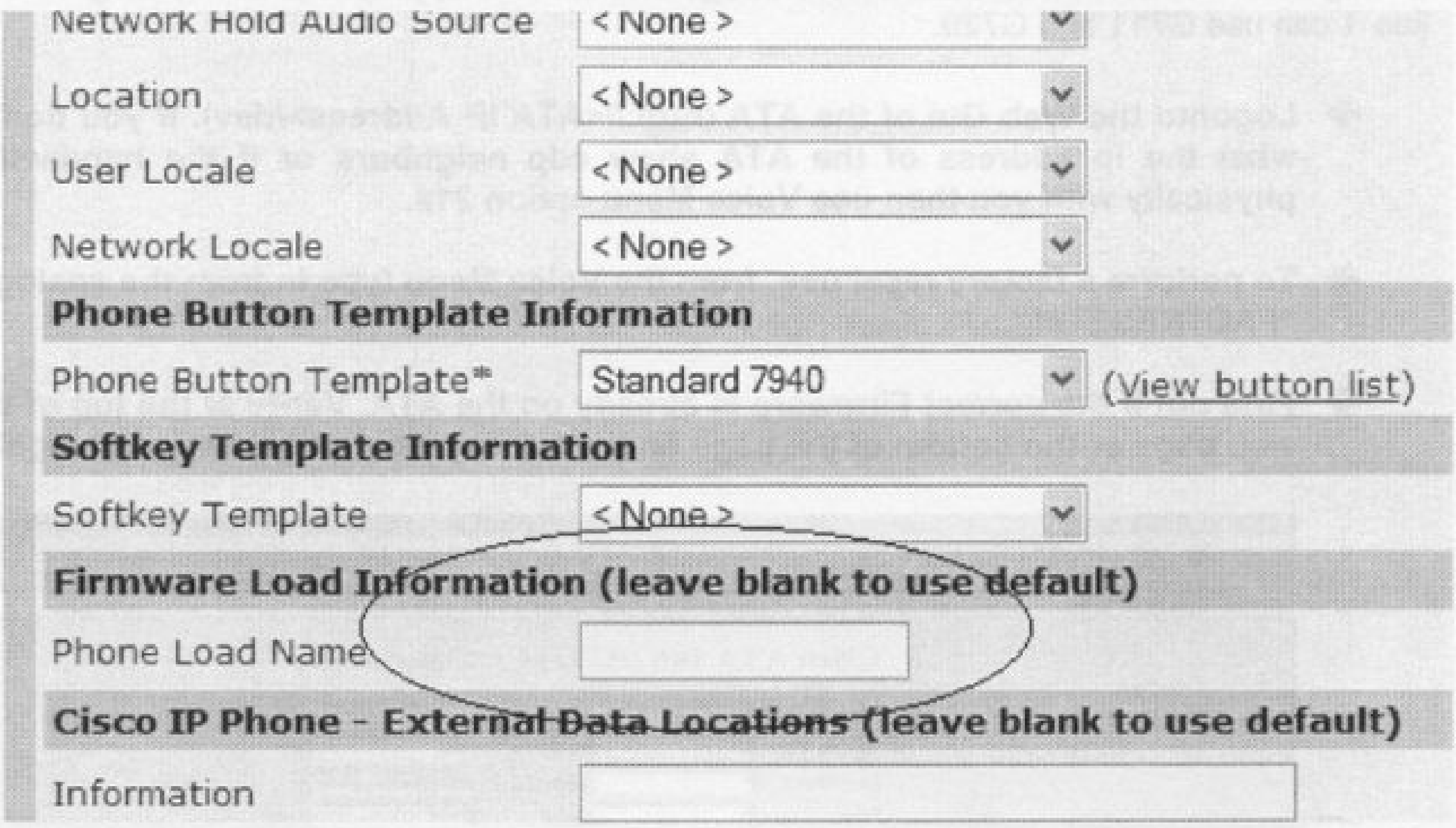
➔ **Logonto the Web Gui of the ATA (http://<ATA IP Address>/dev). If you don't know what the ip address of the ATA show cdp neighbors or if the handset/ATA is physically with you then use Voice Menu option 21#.**

➔ **To perform a factory reset use, from the Voice Menu type in from the analog phone "FACTRESET#*".**

➔ **Find out if the correct Firmware is already on the ATA. Verify at the top of the ATA web page or the bottom of the page on the left hand side or show cdp neighbors.**



➔ **If the SCCP firmware image is on the ATA then register to CCM and then update the load to the H323 firmware image changing the Device setting shown below.**



➔ **The ATA will be registering to the Gatekeeper as a Terminal. To achieve this, the following ATA Parameters are required.**

GKorProxy:	<Gatekeeper IP Address>
GkId	<Zone Name>
UID0	E.164 phone number for the **Phone 1** port.

➔ **Codecs being used can be defined by setting the following ATA parameters.**

RXCodec and TXCodec:	2 (for G711ulaw)
LBRCodec:	3 (G729 is LBR codec)

➔ **If the ATA needs to insert a Tech-Prefix (required when there is no Default-Technology set on the GK and the ATA needs to call the CCM) set the following parameters in the ATA:**

AutMethod	=0x0….4 (PWD field is inserted on outgoing calls)
PWD0	1#

NOTE:

- If you have Gatekeeper security (no zone subnet …) then remember to add the IP Address of the ATA into the allowed subnets. If you are only allowed to define hosts in the zone subnet commands then you will have to define a static IP on the ATA.
- The Audiomode parameter in the ATA config will override the RX/TX Codec and LBRCodec. Only G711ulaw will be supported so unless you only want to support G711ulaw leave the Audiomode parameter alone.

Task 21.7

Configure PRI for the allocated 6608 port as follows. Refer to Table 13 for 6608 port assignment.

- Linecode – B8ZS
- Framing – ESF
- PRI Protocol - PRI NI2
- Protocol Side - User
- Channel Selection - Top Down

➔ **This should be self-explanatory from previous examples.**

Task 21.8

Configure MGCP PRI for Branch 1.

- Linecode – B8ZS
- Framing – ESF
- PRI Protocol - PRI NI2
- Protocol Side - User
- Channel Selection - Top Down
- Use the first 3 channels only.

➔ **This should be self-explanatory from previous examples.**

Task 21.9

Configure E1 R2 for Branch 2. Use Table 8 for PSTN details. Register to Call Manager as an H323 gateway. H323 packets should be sourced from the voice sub-interface.

➔ **This should be self-explanatory from previous examples.**

Task 21.10

Configure the HQ router as a gatekeeper to perform call routing from Call Manager to ATA-186. Use the zone name – HQ-RTR. Register ATA to the gatekeeper.

➔ **The ATA settings are covered in Task 21.6.**

➔ **Registration of the CCM to the Gk should be self-explanatory - include the Tech-Prefix at the bottom of the Trunk page. For the ATA to call CCM use the Default-Technology since this is the easiest method to route calls to CCM.**

➔ **The gatekeeper config is shown below.**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.5.100.1
 gw-type-prefix 1# default-technology
 no shutdown
```

➔ **Let's check registration status on the gatekeeper:**

```
P2-HQ-RTR#sh gatek end
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name       Type    Flags
--------------- ----- --------------- ----- ---------       ----    -----
10.2.200.21     51243 10.2.200.21     51242 HQ-RTR          VOIP-GW
    H323-ID: ccm_trunk_1
    Voice Capacity Max.=  Avail.=  Current.= 0
10.2.200.51     1720  10.2.200.51     1719  HQ-RTR          TERM
    E164-ID: 1002
Total number of active registrations = 2
```

➔ **Calling TO the ATA is easy since the ATA registers its E164 (1002) shown above. ATA registers as a Terminal and CCM as a gateway.**

➔ **For calling TO the CCM from the ATA we will rely on Default-Tech prefix.**

➔ **Let's check where we are and aren't using the proxy:**

```
P2-HQ-RTR#sh gatekeeper zone status
                  GATEKEEPER ZONES
                  ================
GK name      Domain Name   RAS Address     PORT  FLAGS
-------      -----------   -----------     ----- -----

HQ-RTR       ipexpert.net  172.2.100.1     1719  LS
  BANDWIDTH INFORMATION (kbps) :
    Maximum total bandwidth : unlimited
    Current total bandwidth : 0
    Maximum interzone bandwidth : unlimited
    Current interzone bandwidth : 0
    Maximum session bandwidth : unlimited
  SUBNET ATTRIBUTES :
    subnet 10.2.200.51/255.255.255.255 : (Enabled)
    subnet 10.2.200.21/255.255.255.255 : (Enabled)
    All Other Subnets : (Disabled)
  PROXY USAGE CONFIGURATION :
    Inbound Calls from all other zones :
      to terminals in local zone HQ-RTR : use proxy
      to gateways in local zone HQ-RTR  : do not use proxy
      to MCUs in local zone HQ-RTR  : do not use proxy
    Outbound Calls to all other zones :
      from terminals in local zone HQ-RTR : use proxy
      from gateways in local zone HQ-RTR  : do not use proxy
      from MCUs in local zone HQ-RTR  : do not use proxy

PSTN-WAN     ipexpert.net  10.2.200.2      1719  RS
```

➔ **As you can see calls to/from the ATA will use the proxy. Since we do not have the proxy configured (or the ability to configure a MCM Proxy in IOS 12.4 code) then we should disable the proxy to calls to/from Terminals.**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.5.100.1
 gw-type-prefix 1# default-technology
 no use-proxy HQ-RTR default inbound-to terminal
 no use-proxy HQ-RTR default outbound-from terminal
 no shutdown
```

Task 21.11

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 21.12

Configure CallManager to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **This should be self-explanatory from previous examples – See Task 2.2.**

Task 21.13

Configure the dial plan as follows:

911	Emergency
9.911	Emergency
9.[2-9]XXXXXX	Local
9.1XXXXXXXXXX	Long Distance
9.011!	International
9.011!#	International

➔ **Best to leave the dial plan until the end of this dial plan part of the section.**

Task 21.14

Configure Call Manager to provide Class of Service such that phone 1 can call everywhere, phone 2 can call 911 and local, other phones can call 911, local and long distance.

➔ **See Task 21.18**

Task 21.15

4 digit dialing should be preserved to reach the ATA from all other sites. Calls will be sent to the gatekeeper for call routing.

➔ **See Task 21.18**

Task 21.16

For Branch 1, local calls should be sent to the local gateway and then use 6608 as backup. All other calls should be sent to local gateway only. For HQ, all calls should be sent to local gateway only.

➔ **See Task 21.18**

Task 21.17

Local calls from Branch 2 will be routed through local gateway first and use 6608 as backup. International calls will be routed through 6608 first and use local gateway as backup. 911 and Long Distance calls will be routed through local gateway only.

➔ **See Task 21.18**

Task 21.18

When someone places the calls from Branch 2 to the area code in HQ, calls should be hopped off using the 6608 and use local gateway as backup.

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1
RG-BR2	H323 BR2	1
RG-GK	GK-TRUNK	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-BR2-HQ	RG-BR2 RG-HQ	PREDOT PREDOT + PREFIX 011331
RL-HQ-BR2	RG-HQ RG-BR2	PREDOT PREDOT
RL-BR2	RG-BR2	PREDOT
RL-TOLLBY-2-HQ	RG-HQ RG-BR2	PREDOT PREDOT + PREFIX 1212
RL-GK	RG-GK	

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911-LOC	RL-HQ
911 9.911	PT-BR1-911-LOC	RL-BR1
911 9.911	PT-BR2-911-LOC	RL-BR2
9.[2-9]xxxxxx	PT-HQ-911-LOC	RL-HQ
9.[2-9]xxxxxx	PT-BR1-911-LOC	RL-BR1
9.[2-9]xxxxxx	PT-BR2-911-LOC	RL-BR2-HQ
9.1xxxxxxxxxx	PT-HQ-LD	RL-HQ
9.1xxxxxxxxxx	PT-BR1-LD	RL-BR1
9.1xxxxxxxxxx	PT-BR2-LD	RL-BR2
9.011! 9.011!#	PT-HQ-INT	RL-HQ
9.011! 9.011!#	PT-BR1-INT	RL-BR1
9.011! 9.011!#	PT-BR2-INT	RL-HQ-BR2
91212.xxxxxxx	PT-BR2-LD	RL-TOLLBY-2-HQ
1002	<None>	RL-GK

➔ **On the BR2 gateway we need to configure Dial-Peers.**

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
!
dial-peer voice 911 pots
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 destination-pattern 9011T
 port 0/0/0:0
```

```
prefix 011
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 3000 voip
 destination-pattern 3…
 session target ipv4:10.2.200.21
 voice-class codec 1
 no vad
```

Task 21.19

Based on Table 13, configure one of the 6608 ports as a transcoder.

➔ **This should be self-explanatory from previous examples.**

Task 21.20

Based on Table 13, configure one of the 6608 ports as a conference bridge.

➔ **This should be self-explanatory from previous examples.**

Task 21.21

Configure media resources using NM-HDV on Branch 1 gateway. Configure two transcoder and two conference bridge sessions.

➔ **In Section 7 we covered setting up the DSPFARM for NM-HDV2 modules which is what Proctor Labs is equipped with. It is worth covering setting up the media resource for the NM-HDV module, shown below. Setup in CCMADMIN is the same as procedure as defined in Section 7.**

```
voice-card 1
 dsp services dspfarm
!
sccp local FastEthernet0/0
sccp
sccp ccm 10.2.200.21 priority 1
!
dspfarm transcoder maximum sessions 2
dspfarm confbridge maximum sessions 2
dspfarm
```

Task 21.22

Configure the MoH server to support both G.711 and G.729 region.

➔ **You could use transcoder if MOH were sent to devices via Unicast streams.**

➔ **Multicast MOH thru the Transcoder will not work though so change the IP Voice Media Stream App to allow the MOH server to natively support G729 and G711. Use the CTRL key to select multiple codecs. Restart the IP Media Stream App Service once this has been completed.**

Clusterwide Parameters (Parameters that apply to all servers)		
Parameter Name	**Parameter Value**	**Suggested Value**
Supported MOH Codecs*	711 mulaw 711 alaw 729 Annex A	711 mulaw

Task 21.23

Configure the MoH server and the network to support multicast music on hold. HQ should receive unicast MoH, Branch 1 should get multicast MoH and PSTN caller should get tone on hold.

➔ **Check out Section 7 for MOH setup.**

➔ **Place the MOH server in a MOH-MRG.**

➔ **The HQ MRG should have the Enable Multicast checkbox disabled. Even though the Audio Source and MOH Server have Multicast enabled, because the HQ MRG does not will result in Unicast MOH to the HQ Devices.**

➔ **The BR1 MRG should have Multicast enabled and BR1 devices will receive Multicast MOH if the source and server have been set up correctly.**

➔ **We want the PSTN to receive Tone-on-Hold. That means the gateway should not have access to the MOH Server via the MRGL. That means we must assign the gateways a MRGL which contains the CFB but not the MOH server.**

NOTE:

- MRGL can be assigned to the Device or Device Pool. If a media resource is not in an MRG then it belongs to null MRG which in turn belongs to the null MRGL.\
- When a media resource is required the Device MRGL is searched first, then the Device Pool MRGL and finally the null MRGL.
- All Devices will get there MRGL from the Device Pool with the exception of the gateways which have MRGL assigned at the Device level.

Task 21.24

Branch 1 should receive music stream from the IOS gateway – not from CCM.

➔ **Let's put the MOH server into a Device Pool which contains a region which uses G711 to all other Regions.**

➔ **On the MOH Server set Max-Hops to 1.**

Device Information	
Host Server	10.2.200.21
Music On Hold Server Name*	MOH_10.2.200.21
Description	MOH_10.2.200.21
Device Pool*	HQ
Location	HQ
Maximum Half Duplex Streams*	250
Maximum Multicast Connections*	30
Fixed Audio Source Device	
Run Flag*	Yes
Multicast Audio Source Information	
☑ Enable Multicast Audio Sources on this MOH Server	
Base Multicast IP Address	239.1.1.1
Base Multicast Port Number	16384 (Even numbers only)
Increment Multicast on	○ Port Number ◉ IP Address

Selected Multicast Audio Sources		
No.	**Audio Source Name**	**Max Hops**
1	SampleAudioSource	1

➔ **On the BR1 gateway:**

```
P2-BR1-RTR(config)#call-manager-fallback
P2-BR1-RTR(config-cm-fallback)#moh music-on-hold.wav
P2-BR1-RTR(config-cm-fallback)#multicast moh 239.1.1.1 port 16384
```

➔ **Because no "route" has been defined in the multicast moh command, multicast moh will be output to the interface which has been assign the "ip source-address" in SRST (which in this case is fine since we are using the voice subinterface).**

Task 21.25

Configure media resource redundancy for the HQ so it will use 6608 as Conference Bridge and BR1 Conference Bridge as backup.

➔ **Create an HQ MRG – place the 6608 CFB into this MRG.**

➔ **Create a BR1-MRG – place the IOS CFB into this MRG.**

➔ **In the HQ-MRGL assign HQ-MRG higher up in the list than BR1-MRG. Also assign MOH-MRG.**

➔ **BR1-MGRL should have BR1-MRG and MOH-MRG.**

➔ **PSTN-MRGL should not have MOH-MRG.**

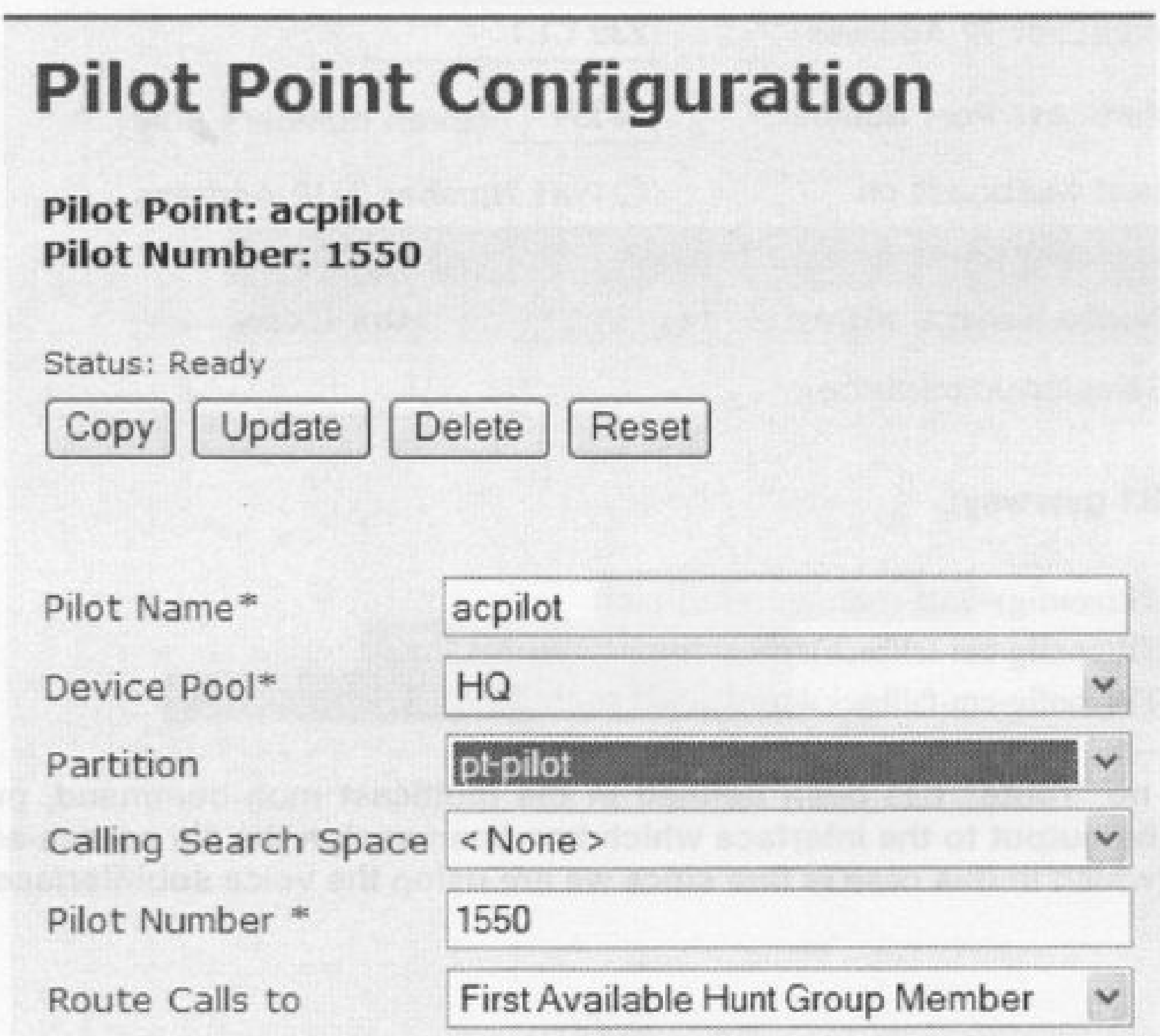
Task 21.26

Configure the Attendant Console as follows:

- Pilot Point Number: 1550
- Members: 1001, 2001 and 2002
- Users cannot call 1550 directly. They need to dial 0 instead to reach these members. Calls should be distributed in a circular fashion.

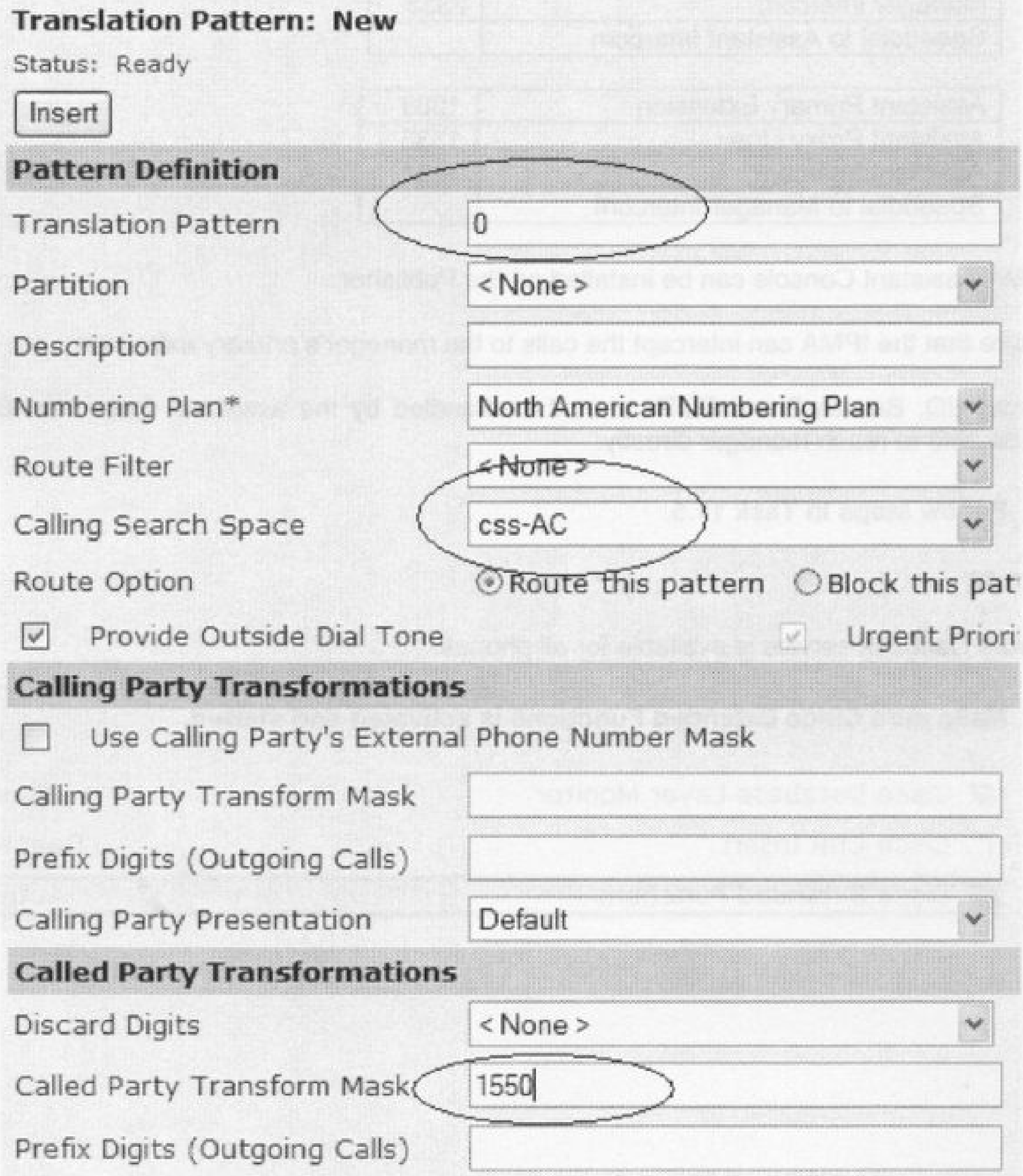
➔ **Set up the Attendant Console as shown in Section 11.**

➔ **Place Pilot in Partition that no device can see.**



➔ **Create a CSS which has visibility of the partition created in previous step.**

➔ **Create a Translation Pattern with DN = 0 and Called Party Mask = 1550 and CSS which can see the Pilot Partition.**



Task 21.27

Configure the IPMA for Call Manager as follows:

Manager Primary Extension	2003
Manager Intercom	2333
Speeddial to Assistant Intercom	

Assistant Primary Extension	1003
Assistant Proxy Line	1333
Assistant Intercom	1334
Speeddial to Manager Intercom	

The IPMA Assistant Console can be installed on the Publisher.

Make sure that the IPMA can intercept the calls to the manager's primary extension.

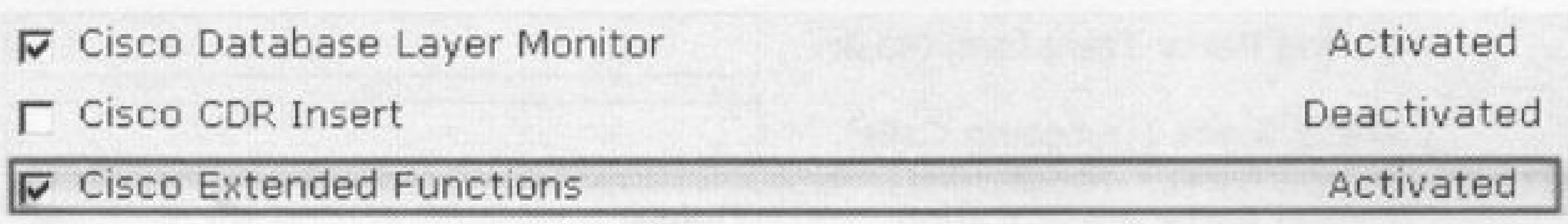
Calls from HQ, Branch 2 and PSTN should be handled by the assistant. Calls from Branch 1 should be able to reach manager directly.

➔ **Follow steps in Task 11.5.**

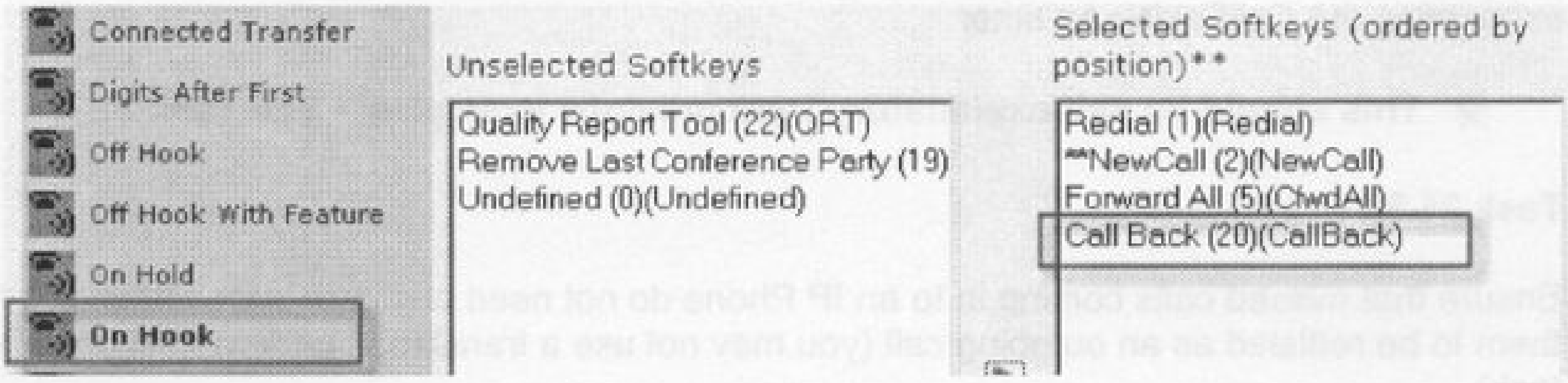
Task 21.28

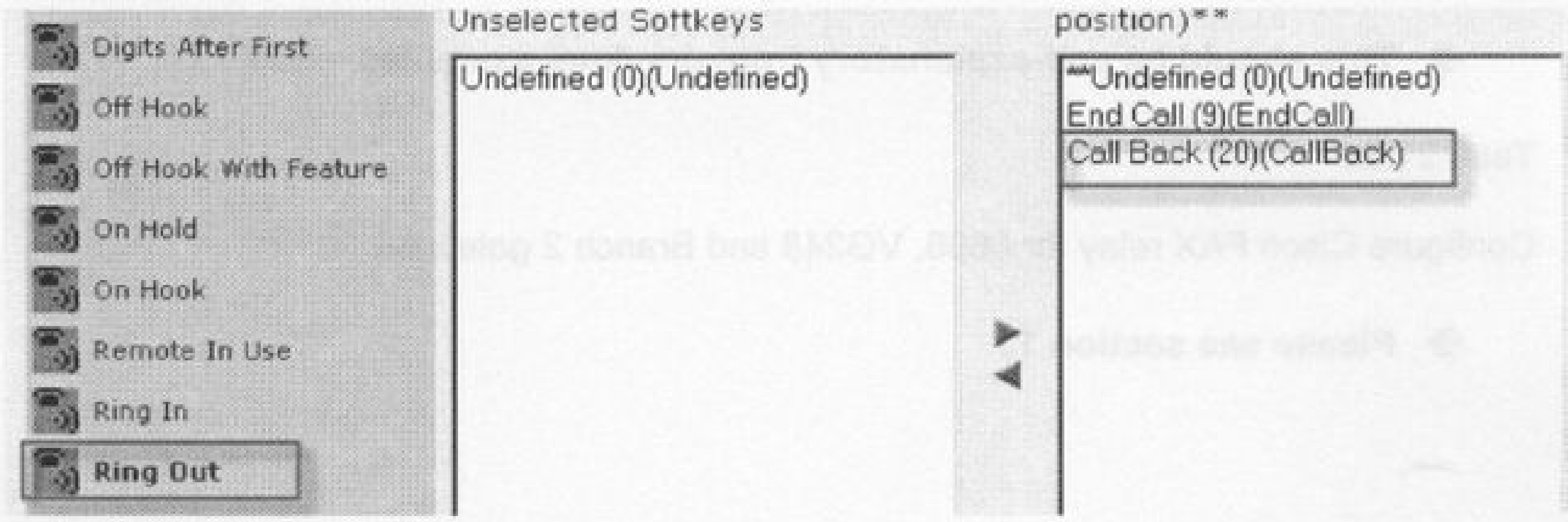
Make sure CallBack service is available for all phones.

➔ **Make sure Cisco Extended Functions is activated and started.**

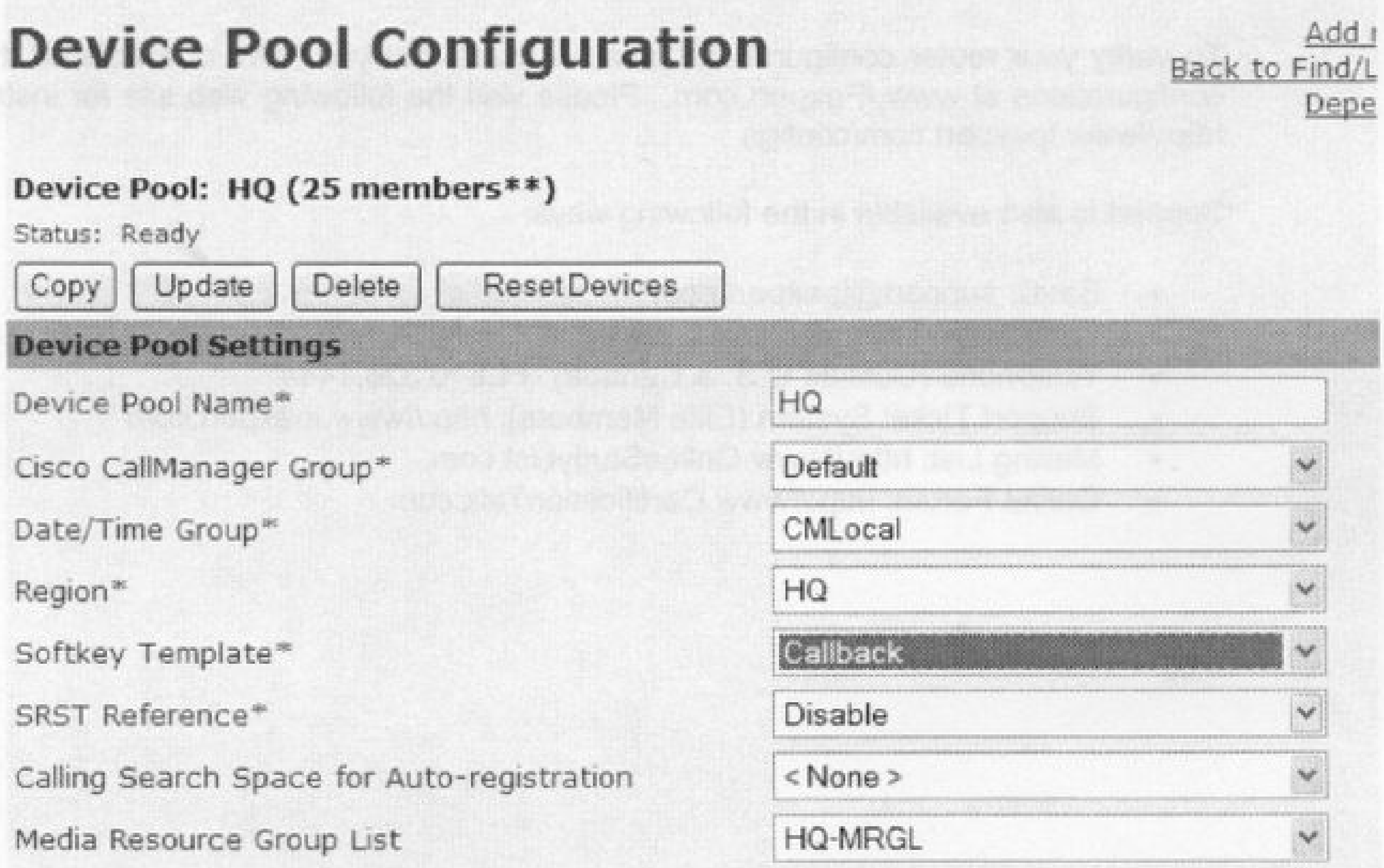


➔ **Copy an existing softkey template and then create a new one. Add the CallBack softkey to On Hook and Ring out call state.**





➔ **Assign the new Softkey Template to the Device Pools.**



Task 21.29

If a call rings into HQ Phone 3, that user must have the option of sending that call to VM without exhausting the CallFwdNoAn timer.

➔ **This should be self-explanatory from previous examples – See Task 11.7.**

Task 21.30

Ensure that missed calls coming in to an IP Phone do not need any user intervention in order for them to be redialed as an outgoing call (you may not use a translation pattern to accomplish this task).

➔ **This should be self-explanatory from previous examples – See Task 11.9.**

Task 21.31

Configure Cisco FAX relay for 6608, VG248 and Branch 2 gateway.

➔ **Please see section 13.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 22: Multiprotocol Challenge E

Estimated Time to Complete: 8 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 22 Multiprotocol Challenge E

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing the first 17 Labs.

Section 22 Configuration Tasks

Task 22.1

Check and configure OSPF as a routing protocol in the network so that all the router interfaces including loopback interfaces are reachable from anywhere in the network.

➔ **This should be self-explanatory from previous examples.**

Task 22.2

Configure each switch port connecting to IP phones and ATA to support both data and voice traffic according to VLAN IDs specified in Table 2.

➔ **This should be self-explanatory from previous examples.**

Task 22.3

In the HQ site, configure MS DHCP server to enable DHCP service for IP phones to get IP addresses and download configurations and phone loads.

➔ **This should be self-explanatory from previous examples.**

Task 22.4

In each branch site, configure each router/gateway to provide DHCP service. Configure the lease time to be 8 hours. Exclude the IP address of X.X.X.1 and X.X.X.254.

➔ **This should be self-explanatory from previous examples.**

Task 22.5

Configure all the phones in HQ and Branch 1 with 4 digit extensions as shown in Tables 5 and 6. Configure all the phones such that each phone displays its own full E.164 number on its LCD display.

➔ **This should be self-explanatory from previous examples.**

Task 22.6

Configure the Branch 2 router as a CME and register all the phones based on Table 7. When calling PSTN, each phone should forward full DID DN and calling name to the PSTN phone.

➔ **This should be self-explanatory from previous examples.**

Task 22.7

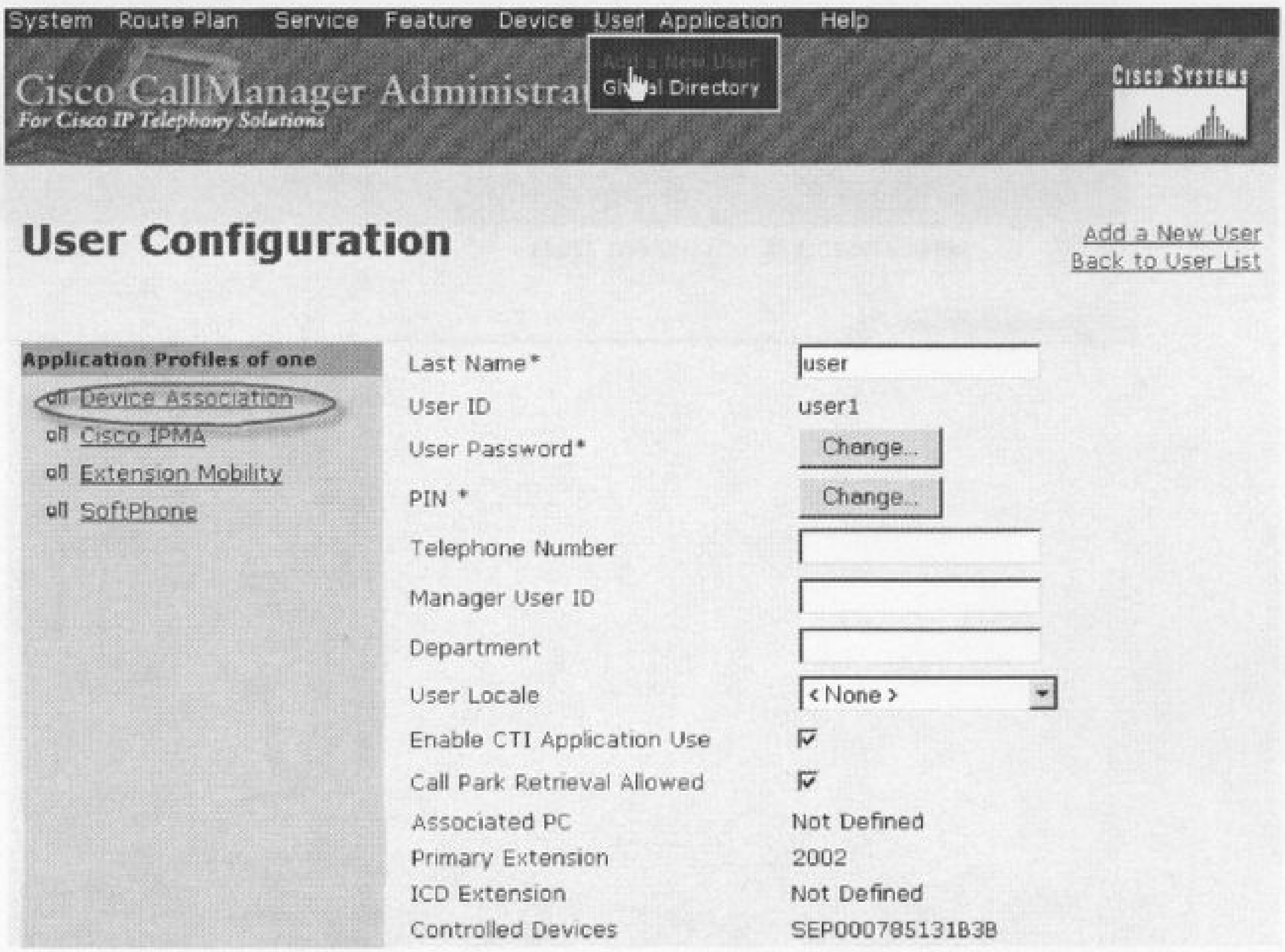
Configure Call Manager to be synchronized to the NTP server which is the backbone PSTN gateway with the IP address of 10.X.200.2. Use the correct time zone (EST) for the server.

➔ **This should be self-explanatory from previous examples.**

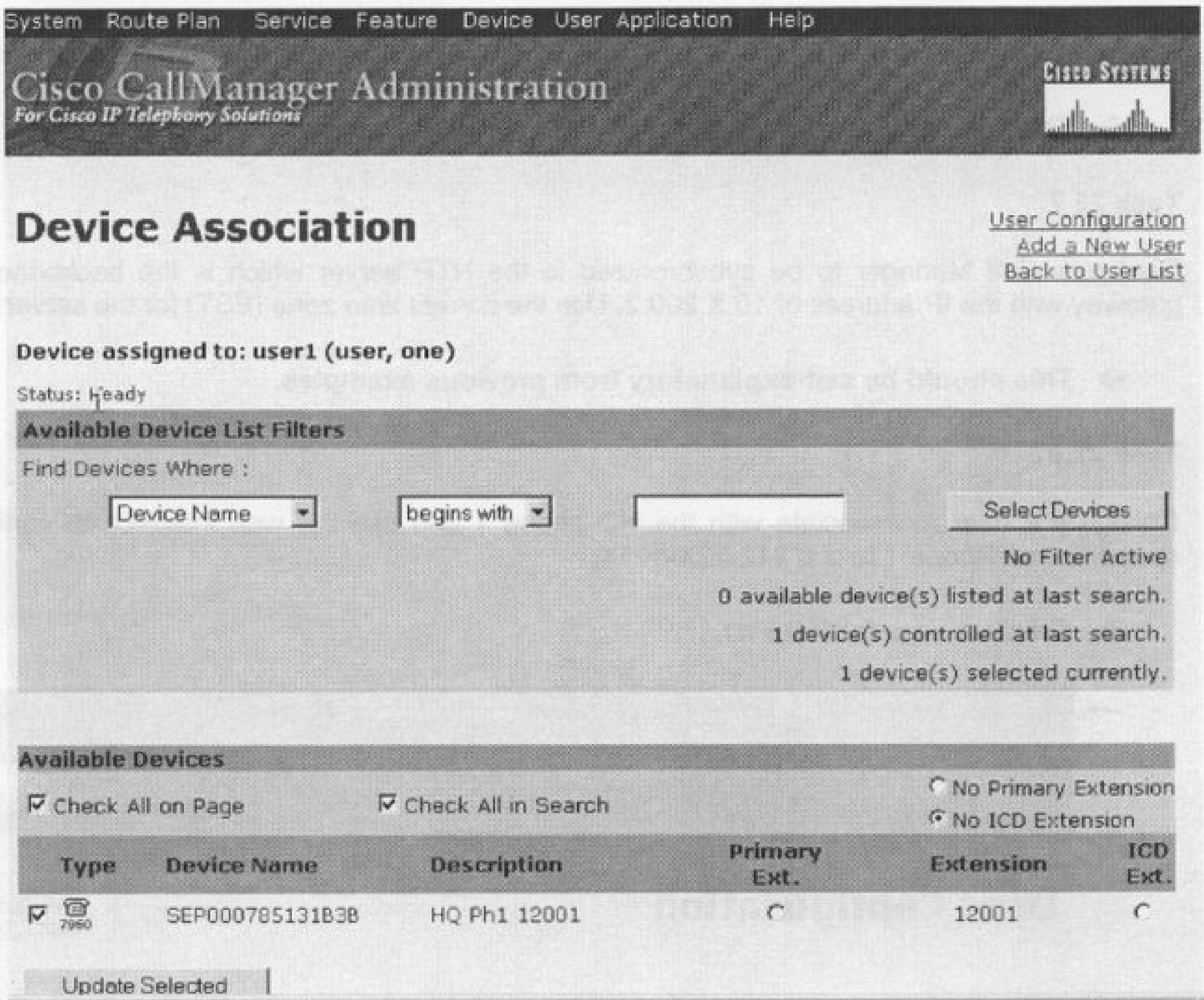
Task 22.8

Configure a user to associate with the HQ phone 1 and use the web interface to configure a speed dial on Phone 1 to dial 212-22X-1111.

➔ **Create a user for HQ Ph1.**

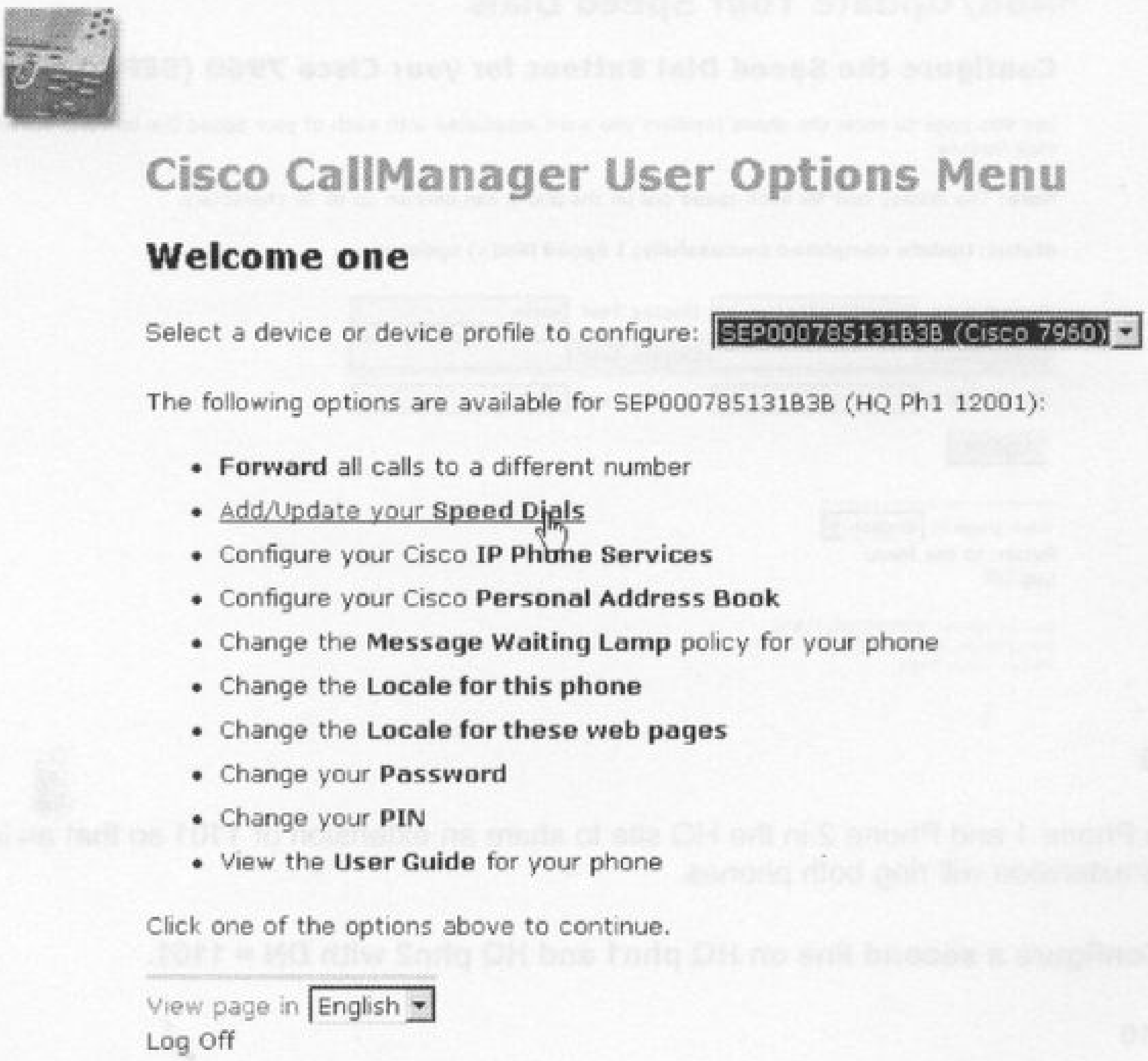


➔ **Associate HQ Ph1 to this user.**

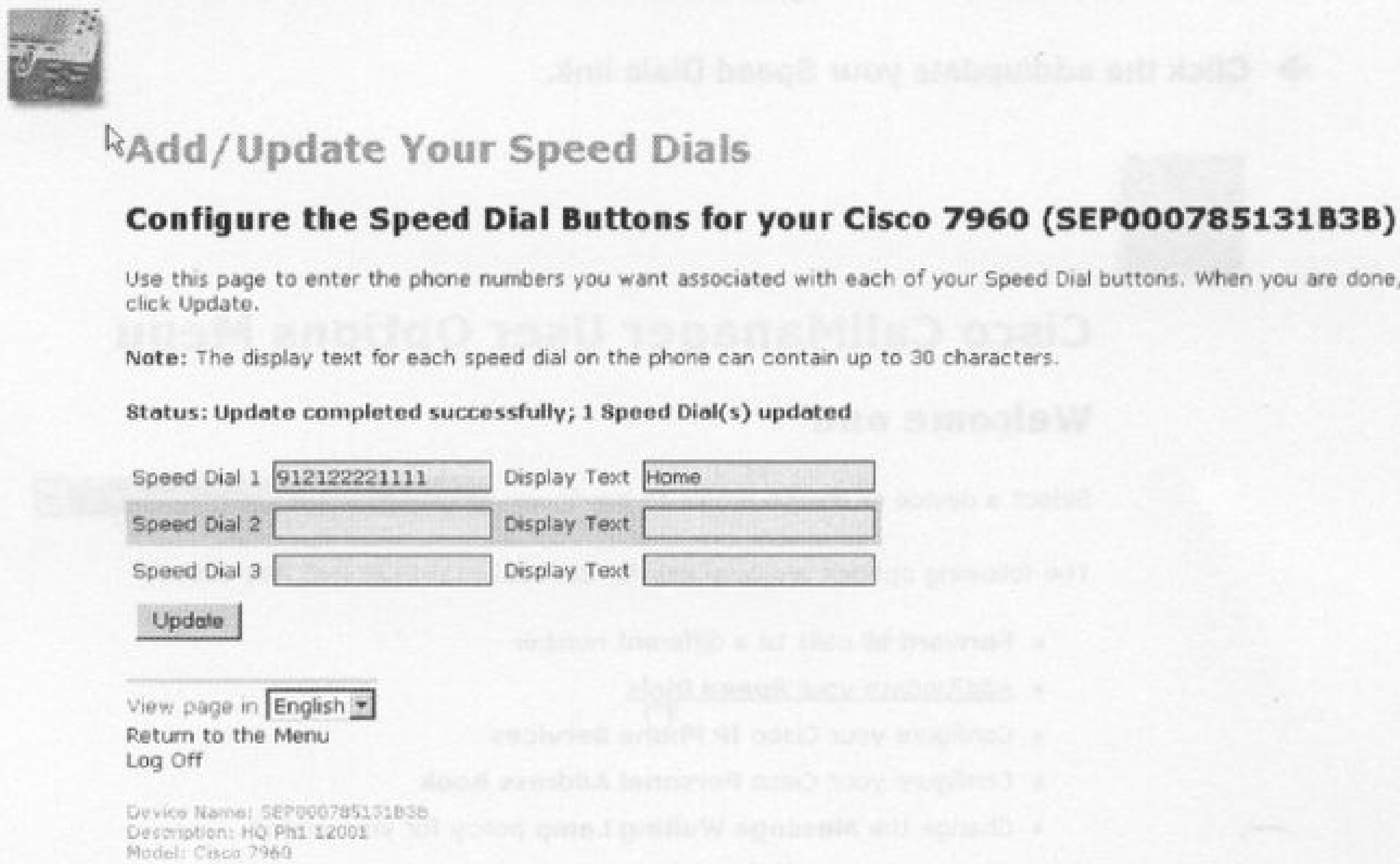


➔ **Browse to http://10.2.200.21/CCMUser and log in as a phone user with the user id of user1 and the password you used.**

➔ **Click the add/update your Speed Dials link.**



➔ **Configure Speed Dial 1 to 912122221111.**



Task 22.9

Configure Phone 1 and Phone 2 in the HQ site to share an extension of 1101 so that an incoming call to this extension will ring both phones.

➔ **Configure a second line on HQ phn1 and HQ phn2 with DN = 1101.**

Task 22.10

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **Configure the gateway based on Task 4.1 – you will need to configure bottom-up channel selection. Don't forget to change the CCM Service Parameter Bchannel maintenance and mark the checkbox "Enable Status Poll".**

Task 22.11

Configure BR1 as an MGCP gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed.

➔ **Ascending is the same as Top-Down signaling.**

Task 22.12

Ensure that the correct transport for DTMF digits is used for the BR1 gateway.

➔ **This should be self-explanatory from previous examples.**

Task 22.13

Configure BR2 as a Gateway based on the information in Table 8.

➔ **Configure the E1 R2.**

Task 22.14

Configure gatekeeper on HQ-RTR with the following information:

Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

Register Call Manager to the HQ-RTR gatekeeper.

➔ **There are no restrictions so use Tech-Prefix if you want - it doesn't make a difference since we are not routing calls TO CCM via the Gatekeeper (see Task 22.29 further ahead and you will see that for calls from CME to CCM you have a choice - it is quicker and easier to add the CME as a gateway in CCM).**

Task 22.15

Register phones to CME based on Table 7. Configure a second line of 3005 on Phone 1. If the first line whose DN is 3001 is busy, the call should roll to the second line.

➔ **We suggest you run the wizard for the first two phones and DNs (auto-assign ephone-dn 1 and 2 to ephone 1 and 2). After the initial setup, increase max-dn and add the shared line manually.**

```
telephony-service
 max-ephones 3
 max-dn 4
 ip source-address 10.2.202.1 port 2000
 auto assign 1 to 2
 create cnf-files version-stamp 7960 Mar 02 2004 17:02:20
 dialplan-pattern 1 331322... extension-length 4
 max-conferences 4
!
!
```

```
ephone-dn 1
 number 3001
 call-forward busy 3005
 description 3313223001
!
!
ephone-dn 2
 number 3002
 description 3313223002
!
!
ephone-dn 3
 number 3005
!
!
ephone 1
 mac-address 0007.50A4.D602
 type 7960
 button 1:1 2:3
!
```

Task 22.16

Configure the CME phone LCD to display "Welcome to IPExpert".

➔ **This should be self-explanatory from previous examples.**

Task 22.17

Configure CME such that outbound calls to 1 900 XXX-XXXX from Phone 1 and 2 are blocked.

➔ **Define the after-hours block pattern and use the 7-24 keyword.**

```
P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)# after-hours block pattern 1 91900....... 7-24
```

Task 22.18

Configure CME such that outbound calls from Phone 2 do not forward caller ID. All other phones from CME should forward caller IDs.

```
ephone-dn 2
 number 3002
 description 3313223002
caller-id block
```

Task 22.19

Configure the inter-digit timeout to be 3 seconds on CME.

```
P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)# timeout interdigit 3
```

Task 22.20

Create a circular hunt group for Support with a DN of 3210 at BR2 between phones 1 and 3, and ensure that those phones can login-to and out-of the hunt group in order to receive calls. Allow the call to ring at around 3 times before searching for the next member.

- ➔ **This should be self-explanatory from previous examples – See Task 14.8.**

Task 22.21

Create an incoming AutoAttendant at the DN of 3000. Also Create a Basic ACD using the support team hunt group you just created (The necessary TCL scripts are already loaded in BR2 router's flash memory). Have the AA script automatically hand-off the callers into the support ACD hunt group when a user presses 2. Allow no more than 20 callers in the Q at any one point. Play a prompt for the user every 30 seconds to let them know that all agents are busy. Allow the users to dial-by-extension by pressing 4. Ensure that the Q is collecting statistics and view them as part of your troubleshooting.

- ➔ **This should be self-explanatory from previous examples – See Task 14.10.**

Task 22.22

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 10 calls at the minimum bandwidth supported by a Cisco VTA camera in H263 mode and between each site with values such that Video calls be allowed to use 2 call at the minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

- ➔ **This should be self-explanatory from previous examples – See Task 2.1.**
- ➔ **Only change the Video bandwidths to 256kbps for any site but HQ – change HQ to 1280kbps.**

Task 22.23

In Branch 2, use G729 codec when placing calls to any of the other sites.

- ➔ **Inside the VoIP dial-peer don't use voice-class codec. G729 is the default codec so no configuration is required.**
- ➔ **This Dial-peer will be used for CME calls TO CCM.**

Task 22.24

Use CallManager's only CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to 3 audio call and 2 video call using the minimum bandwidth allowable by a VTA camera in H263 mode.

→ **This should be self-explanatory from previous examples – See Task 2.2.**

→ **Only change the bandwidth values to 72kbps and 256kbps respectively.**

Task 22.25

Allow only four concurrent G.711 calls through the HQ site gatekeeper from anywhere.

```
P2-HQ-RTR(config)#gatekeeper
P2-HQ-RTR(config-gk)#bandwidth remote 512
```

Task 22.26

Configure Calling Restriction.

→ **This should be self-explanatory from previous examples.**

Task 22.27

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

→ **See Section 22.32 for configuration.**

Task 22.28

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

→ **See Section 22.32 for configuration.**

Task 22.29

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed out of the local gatekeeper with the appropriate local gateway acting as backup. Users must be able to dial the BR2 site using extension (4 digit) dialing. **NOTE**: The gatekeeper is expecting the full E164 number, i.e. international prefix '011' plus 10 digits.

→ **See Section 22.32 for configuration.**

Task 22.30

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway. You must 4 different types of methods to manipulate the digits sent to the PSTN (e.g. one method is by using the 'forward-digits' command inside the POTS dial-peer).

➔ **See Section 22.32 for configuration.**

Task 22.31

Calls originating from BR2 to Call Manager (both HQ and BR1) should use VoIP and PSTN as backup. If you decide to register the CME to the gatekeeper use your local HQ-RTR gatekeeper as opposed to the PSTN-WAN gatekeeper. 4-digit dialing must be preserved.

➔ **You have a choice to use GK or add a gateway in CCM - choose the latter. Add the gateway in CCM – remember in Task 22.22 G729 must be used to so leave the codec in the outgoing VoIP dial-peers in CME and in CCM create a new Device Pool called CME and this should contain a Region which uses G729 to all other Regions.**

➔ **See Section 22.32 for configuration.**

Task 22.32

Enable DID for PSTN users dialing into the CM/CME (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits.

➔ **When implementing a dial plan it is a good idea to look at all the tasks together rather than treat each question as a separate question.**

➔ **Digit Manipulation should be done in the Route List.**

➔ **The following Route Groups should be created:**

Gateway	Route Group	Order
GK TRUNK	RG-GK	1
HQ-6608	RG-HQ	1
IOS-MGCP	RG-BR1	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1-LOC	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-BR1-HQ-LOC	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617
RL-HQ-BR1-LD-INT	RG-HQ	PREDOT
	RG-BR1	PREDOT
RL-BR1-HQ-LD-INT	RG-BR1	PREDOT
	RG-HQ	PREDOT
RL-TOLLBY-2-BR1	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617
RL-TOLLBY-2-HQ	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-GK-HQ	RG-GK	PREFIX 01133132X
	RG-HQ	PREFIX 01133132X
RL-GK-BR1	RG-GK	PREFIX 01133132X
	RG-BR1	PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911	PT-HQ-911	RL-HQ
9.911		
911	PT-BR1-911	RL-BR1
9.911		
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ-BR1-LOC
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ-LOC
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ-BR1-LD-INT
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1-HQ-LD-INT
91212.xxxxxxx	PT-BR1-LD	RL-BR1-TOLLBY
91617.xxxxxxx	PT-HQ-LD	RL-HQ-TOLLBY
9.011!	PT-HQ-INT	RL-HQ-BR1-LD-INT
9.011!#		
9.011!	PT-BR1-INT	RL-BR1-HQ-LD-INT
9.011!#		
3xxx	PT-HQ-911	RL-GK-HQ
3xxx	PT-BR1-911	RL-GK-BR1

➔ **For CCME use the following dial-peers:**

```
dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 corlist outgoing css-911
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 9011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1000 voip
 destination-pattern 1...
 session target ipv4:10.2.200.21
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1001 voip
 preference 1
 destination-pattern 1...
 session target ipv4:10.2.200.20
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1002 pots
 preference 2
 destination-pattern 1...
 no digit-strip
 port 0/0/0:0
 prefix 1212222
!
dial-peer voice 2000 voip
 destination-pattern 2...
 session target ipv4:10.2.200.21
 dtmf-relay h245-alphanumeric
!
```

```
dial-peer voice 2001 voip
 preference 1
 destination-pattern 2...
 session target ipv4:10.2.200.20
 dtmf-relay h245-alphanumeric
!
dial-peer voice 2002 pots
 preference 2
 destination-pattern 2...
 no digit-strip
 port 0/0/0:0
 prefix 1617522
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
```

➔ **We are sending calls directly from CCME to CCM in this particular case. We must therefore add the CCME as an Non-GK Controlled ICT Trunk (previously a H323 GW for CME 3.0 and before) in CCM otherwise CCM will ignore Call attempts from CCME (since it is an unregistered gateway). We must bind H323 to an interface first (otherwise it will default to the closest interface) - in this example the Loopback.**

```
P2-BR2-RTR(config)#int loopback 0
P2-BR2-RTR(config-if)#h323-gateway voip bind srcaddr 172.2.102.1
```

➔ **Add the Non-GK Controlled ICT Trunk in CCMAdmin.**

➔ **Configure settings on trunk page. Ensure you use the IP Address of the interface you specified as the source Address for H323. CAC is not specified in the question therefore use the default location.**

➔ **Place the trunk in a Device Pool which contains a Region that uses G729 to all other Regions.**

➔ **For inbound Call Routing set Significant Digits to 4 and assign CSS if required.**

➔ **We are not using the ICT Trunk for outbound call routing therefore use any settings. Update and Reset and check the registration status. The trunk has successfully been added you will see the IP Address appear – Note the Registration status remains Unknown.**

Task 22.33

Configure in Call Manager such that if there is not enough bandwidth to make calls to and from Branch 1, use PSTN to complete the calls.

➔ **This should be self-explanatory from previous examples.**

Task 22.34

Setup SRST on the Branch 1 gateway such that when the Call Manager or WAN is down, subscribers can still make calls to PSTN. Calls from PSTN should still work. Configure the SRST gateway such that subscribers can still dial 4 digit extensions to reach other sites.

➔ **This should be self-explanatory from previous examples.**

Task 22.35

Configure the appropriate 6608 port as a conference bridge. Configure a conference bridge on the Branch 1 router: Allow 4 Sessions. Use Table 13 for port allocation.

➔ **This should be self-explanatory from previous examples.**

Task 22.36

Configure MoH server on the Call Manager such that multicast MoH is provided to phones in Branch 1.

➔ **This should be self-explanatory from previous examples.**

Task 22.37

Configure MoH on the Branch 2 CME such that PSTN phones calling into BR2 phones should get music when calls from or to CME are placed on hold.

➔ **This should be self-explanatory from previous examples.**

Task 22.38

In the HQ site Cat 6500, mark the DSCP PHB label as AF31 for SCCP traffic between IP phones and CM.

```
set qos enable
set port qos 2/7-8 vlan-based
set port qos 2/42 vlan-based
set qos acl ip POD-12-PHONES dscp 26 tcp any any range 2000 2002
set qos acl ip POD-12-PHONES dscp 26 tcp any range 2000 2002 any


commit qos acl POD-12-PHONES
set qos acl map POD-12-PHONES 220
```

Task 22.39

In the Branch 2 Cat 3550, mark the DSCP PHB label as EF for RTP traffic from the port connected to IP phones.

```
mls qos

ip access-list extended VOICE
 permit udp any any range 16384 32767

class-map match-all VOICE
 match access-group name VOICE

policy-map LAN-EDGE-IN
 class VOICE
  set ip dscp 46

int range fa0/1 – 4
 service-policy input LAN-EDGE-IN
```

Task 22.40

Map CoS 3 to AF31 and CoS 5 to EF on 3550 in the Branch 2 site. Configure the appropriate priority queuing for the CoS 5 traffic on the port fa0/4 in the Branch 2.

Correction: Configure Priority Queueing on Phone ports.

➔ **Let's take a look at what transmit queue frames with COS=5 is placed into.**

```
Switch#sh mls qos interface queueing

FastEthernet0/23
Egress expedite queue: ena
wrr bandwidth weights:
qid-weights
 1 - 25
 2 - 25
 3 - 25
 4 - 25   when expedite queue is disabled
Cos-queue map:
cos-qid
 0 - 1
 1 - 1
 2 - 2
 3 - 2
 4 - 3
 5 - 3
 6 - 4
 7 - 4
```

➔ **Now change the default behavior to move Cos 5 to use the PQ.**

```
mls qos

mls qos map cos-dscp 0 8 16 26 34 46 48 56

interface range fa0/23 - 24
 mls qos trust cos
  switchport voice vlan 220
  switchport access vlan 120
  switchport priority extend cos 0
  priority-queue out
I  wrr-queue cos-map 4 5
```

➔ **Now verify:**

```
Switch#sh mls qos interface queueing

FastEthernet0/23
Egress expedite queue: ena
wrr bandwidth weights:
qid-weights
 1 - 25
 2 - 25
 3 - 25
 4 - 25    when expedite queue is disabled
Cos-queue map:
cos-qid
 0 - 1
 1 - 1
 2 - 2
 3 - 2
 4 - 3
 5 - 4
 6 - 4
 7 - 4
```

Task 22.41

The link speed between HQ and Branch 2 is 256 Kbps. Employ the well-known technique to minimize serialization delay. There is no need to do this on the link between HQ and Branch 1 since its link speed is 1544kbps.

➔ **We will need to define the Frame Relay parameters for CIR, MINCIR, BC and BE and Frame-Relay Fragment. Using page 130 of the QoS SRND (Aug 2002) the commands for the link with PVC speed of 768kbps is as follows:**

```
P2-HQ-RTR(config)# map-class frame-relay FRTS
P2-HQ-RTR(config-map-class)#frame-relay cir 252832
P2-HQ-RTR(config-map-class)#frame-relay mincir 252832
P2-HQ-RTR(config-map-class)#frame-relay bc 2530
P2-HQ-RTR(config-map-class)#frame-relay be 0
P2-HQ-RTR(config-map-class)# frame-relay fragment 320
```

```
P2-HQ-RTR(config-map-class)# interface Serial0/1/0:0
P2-HQ-RTR(config-if)# bandwidth 256
P2-HQ-RTR(config-if)#frame-relay traffic-shaping
P2-HQ-RTR(config-if)#interface Serial0/1/0:0.2
P2-HQ-RTR(config-subif)# frame-relay interface-dlci 202
P2-HQ-RTR(config-fr-dlci)# class FRTS
```

➔ **The value of frame-relay fragment will vary depending on the PVC speed - see QoS SRND (Aug 2002) page 130.**

➔ **On the BR2 Router.**

➔ **We again will need to define the usual Frame Relay parameters:**

```
P2-BR2-RTR(config)#map-class frame-relay FRTS
P2-BR2-RTR(config-map-class)#frame-relay cir 252832
P2-BR2-RTR(config-map-class)#frame-relay mincir 252832
P2-BR2-RTR(config-map-class)#frame-relay bc 2530
P2-BR2-RTR(config-map-class)#frame-relay be 0
P2-BR2-RTR(config-map-class)# frame-relay fragment 320
```

➔ **Enable frame-relay traffic shaping on the physical and assign map-class to the DLCI.**

```
P2-BR2-RTR(config-subif)#interface Serial0/1/0
P2-BR2-RTR(config-if)#frame-relay traffic-shaping
P2-BR2-RTR(config-if)#interface Serial0/1/0.1 point-to-point
P2-BR2-RTR(config-if)# bandwidth 256
P2-BR2-RTR(config-subif)# frame-relay interface-dlci 102
P2-BR2-RTR(config-fr-dlci)# class FRTS
```

Task 22.42

From HQ Site to Branch 2, reserve 50% of the bandwidth for voice RTP traffic on a priority queue and reserve 5% minimum guaranteed bandwidth for voice control traffic.

➔ **On the HQ-RTR router configure class-maps and policy maps shown below.**

```
class-map match-any RTP
 match ip dscp ef
class-map match-any SIG
 match ip dscp af31
!
!
policy-map LLQ
 class RTP
  priority percent 50
 class SIG
  bandwidth percent 5
 class class-default
  fair-queue
```

```
P2-HQ-RTR(config)#map-class frame-relay FRTS
P2-HQ-RTR(config-map-class)#service-policy output LLQ
```

```
P2-HQ-RTR#sh policy-map interface Serial0/1/0:0.2
 Serial0/1/0:0.2: DLCI 202 -

  Service-policy output: LLQ

    Class-map: RTP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp ef
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 72
        Bandwidth 50 (%)
        Bandwidth 128 (kbps) Burst 6300 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: SIG (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Output Queue: Conversation 73
        Bandwidth 5 (%)
```

```
        Bandwidth 12 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      1 packets, 84 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 64
        (total queued/total drops/no-buffer drops) 0/0/0
```

Task 22.43

From Branch 2 to HQ Site, reserve 128 kbps for voice RTP traffic on a priority queue and reserve minimum guaranteed bandwidth of 12kbps for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queueing.

➔ **On BR2:**

```
class-map match-any RTP
 match ip dscp ef
class-map match-any SIG
 match ip dscp af31
!
!
policy-map LLQ
 class RTP
  priority 128
 class SIG
  bandwidth 12
 class class-default
  fair-queue
```

```
P2-BR2-RTR(config)#map-class frame-relay FRTS
P2-BR2-RTR(config-map-class)#service-policy output LLQ
```

Task 22.44

From the HQ site to the Branch 1 site, reserve 50% of bandwidth for voice RTP traffic on a high priority queue and 5 % of bandwidth for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queueing.

➔ **On BR1:**

```
class-map match-any RTP
 match ip dscp ef
class-map match-any SIG
 match ip dscp af31
!
!
policy-map LLQ
 class RTP
  priority percent 50
 class SIG
  bandwidth percent 5
 class class-default
  fair-queue


interface Serial0/1/0.2 point-to-point
 ip address 162.2.102.1 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf mtu-ignore
 frame-relay interface-dlci 202
service-policy output LLQ
```

Task 22.45

Create a custom application with the HQ CM such that when a caller from PSTN places a call to 1202, the application should ask the caller to enter a 4 digit PIN. If the entered PIN matches "1234", route the call to Phone 2 in the HQ site.

➔ **Set up the JTAPI Subsystem as defined in Task 10.1 using the following information (NOTE: There is no need to setup the ICD subsystem):**

CTI Route Point: 1202
CTI Ports: 1203 – 1206

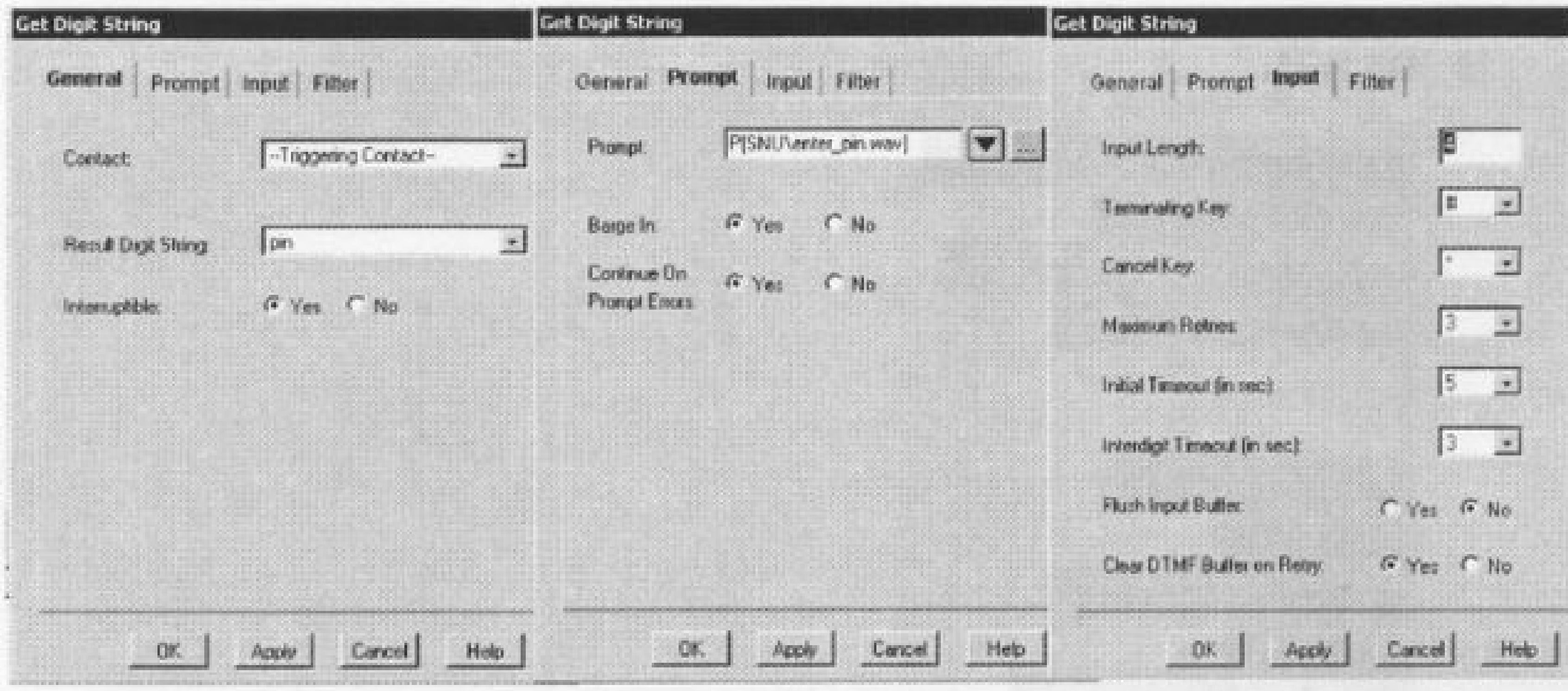
CRA Admin User: crsadmin
CRA Admin password: cisco

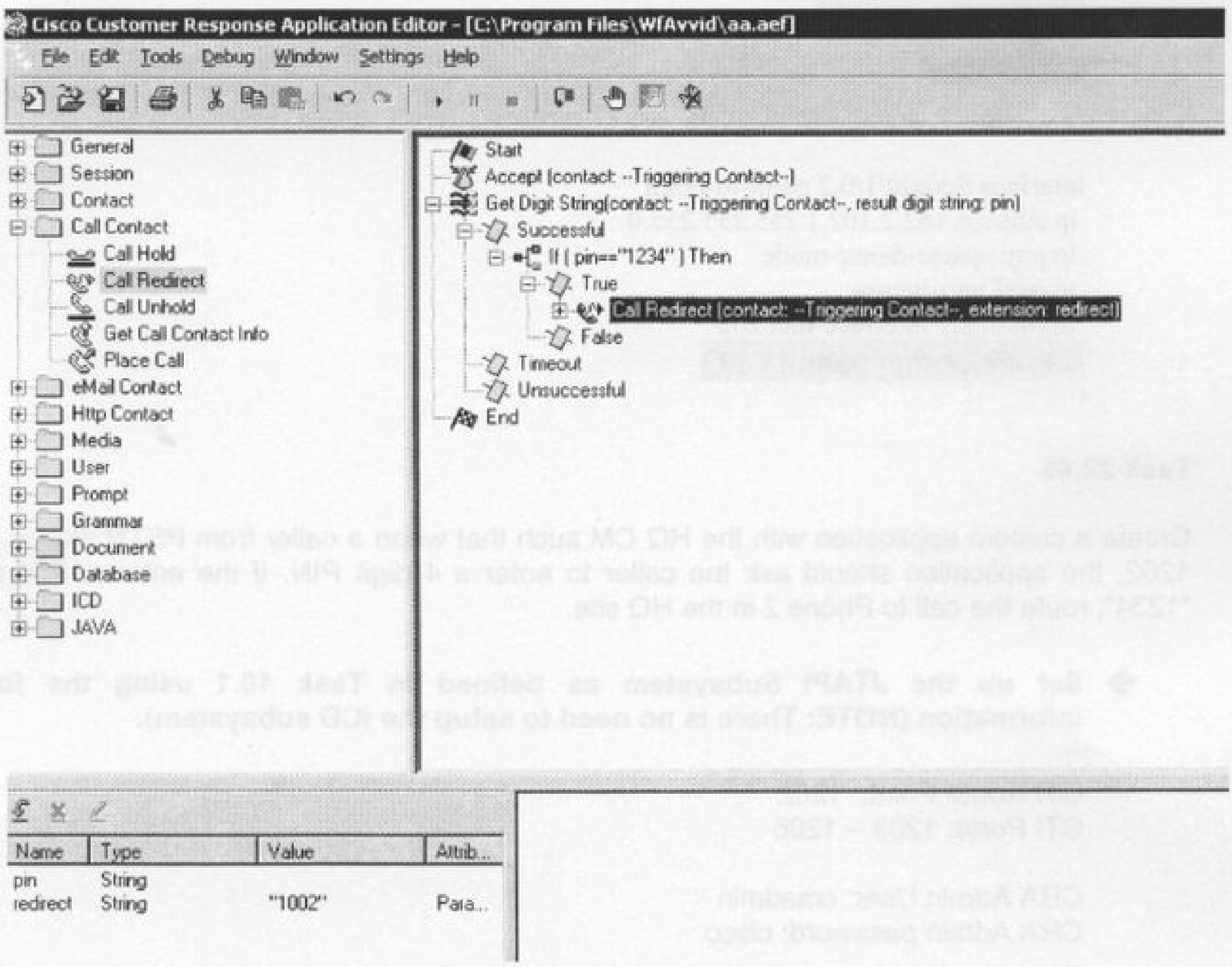
JTAPI user ID: jtapi
JTAPI user password: cisco

➔ **Create a script that meets the requirement using a CRA Script Editor from Programs>Cisco CRA Administrator>Cisco CRA Editor.**

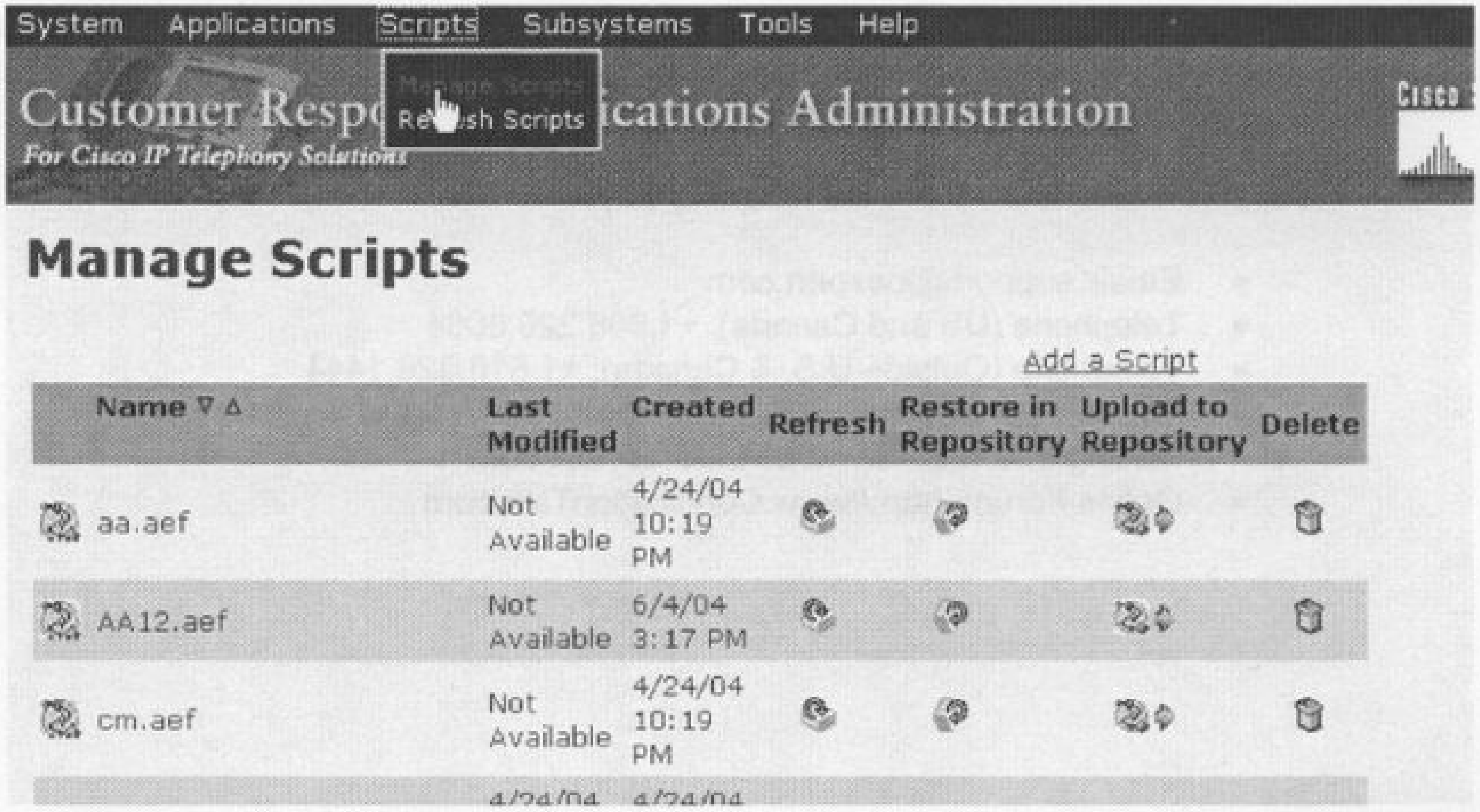
➔ **Need to create two variables. One is an empty string variable, PIN to collect the entered digit and the other is a string variable contains HQ Ph2 DN.**

➔ **Use the "get digit string" step with configuration below.**

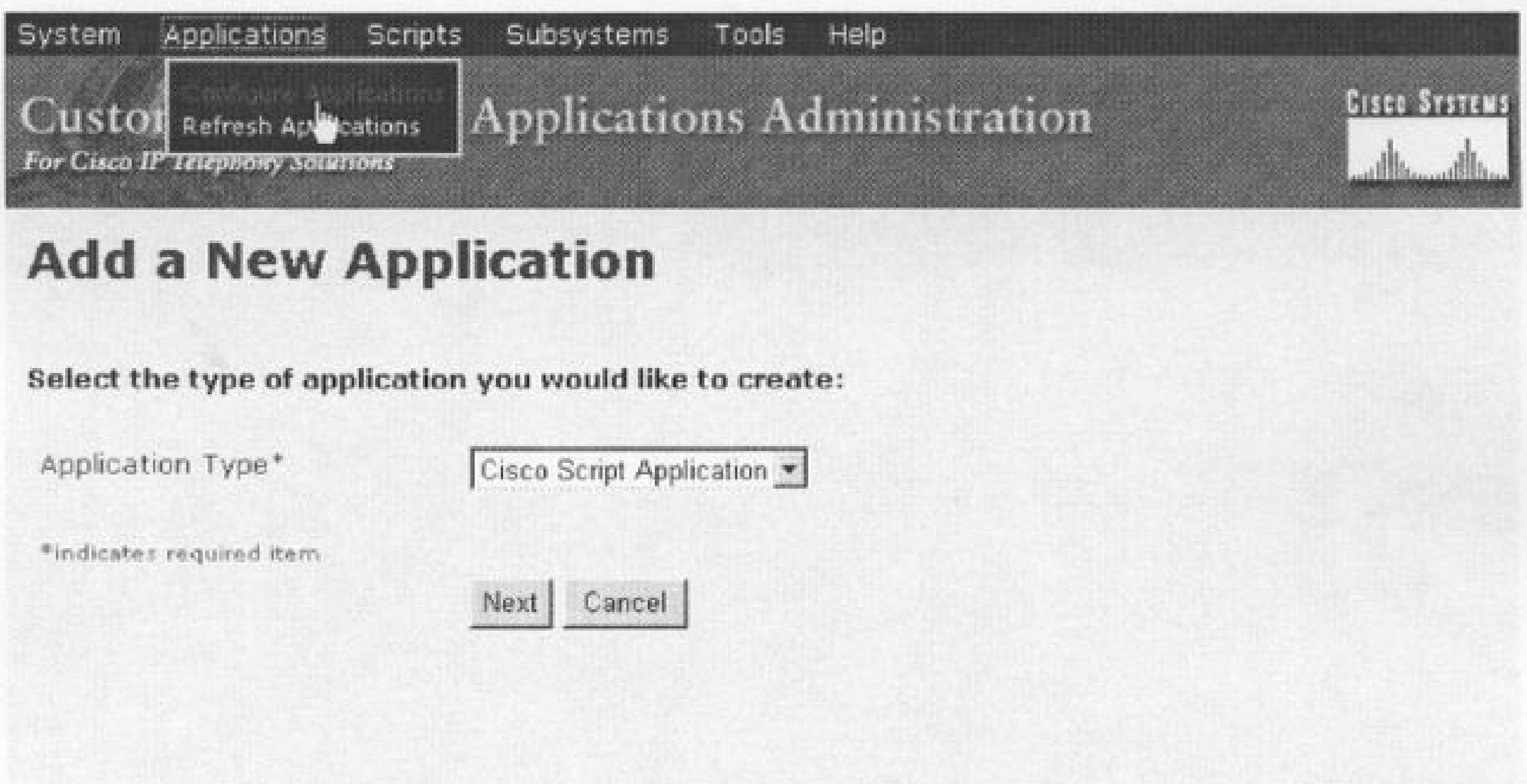




➔ **Add this script to the CRA repository.**



➔ **Add an application called "PIN" for this script. Enter 4 for the Maximum number of sessions.**



➔ **Go back to Subsystems>JATPI and add a JTAPI trigger for this application. Enter 12204 as a CTI RP directory number and select "PIN" as a application.**

Task 22.46

Configure FAX pass through between the HQ VG248 FAX and Branch 1 FAX phones.

➔ **Fax options are covered in Section 13.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 23: Multiprotocol Challenge F

Estimated Time to Complete: 6 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 23 Multiprotocol Challenge F

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing the first 17 Labs.

Section 23 Configuration Tasks

Task 23.1

Check and configure basic OSPF – If not configured assign all interfaces to area 0 using the IP Network addresses found in Table 1. Configure Loopback interfaces on each router from Table 9.

- ➔ **This should be self-explanatory from previous examples.**

Task 23.2

Configure the Voice and Data VLANs for all locations detailed in Table 2.

- ➔ **This should be self-explanatory from previous examples.**

Task 23.3

Provide DHCP services for IP phones and gateways at the Headquarters location using the Call Manager Microsoft DHCP service. For Branch 1 and 2, use the local routers for IOS DHCP service. Configure the lease time to be 168 hours at each site.

- ➔ **This should be self-explanatory from previous examples.**

Task 23.4

Register HQ and BR1 Phones to Call Manager and configure with the appropriate 4 digit extensions. Tables 5 and 6 provide the phone information.

- ➔ **This should be self-explanatory from previous examples.**

Task 23.5

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

- ➔ **This should be self-explanatory from previous examples.**

Task 23.6

Configure BR1 as an MGCP gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed.

➔ **This should be self-explanatory from previous examples.**

Task 23.7

Ensure that the correct transport for DTMF digits is used for the BR1 gateway.

➔ **This should be self-explanatory from previous examples.**

Task 23.8

Configure BR2 as an H323 gateway based on the information in Table 8.

➔ **This should be self-explanatory from previous examples.**

Task 23.9

Configure the HQ-RTR as an IPIPGW. Calls will be coming into it from CCM via H323 using G711ulaw and then be routed out to the BR2 CME via SIP using G729 (see **Table 7** for DNs at CME). Calls will also be coming from CME via H323 using G729 and routed to CCM via SIP using G711ulaw (see **Table 5** and **6** for DNs at CCM). Also ensure when calls are coming from SIP to H323 that RFC 2833 is properly stripped. Ensure that if calls are coming from H323 to SIP, that RFC 2833 is used for the SIP side.

➔ **This should be self-explanatory from previous examples – See Task 4.9.**

Task 23.10

Configure gatekeeper on HQ-RTR with the following information:

Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

Register CallManager to the HQ-RTR gatekeeper.

➔ **There are no restrictions so use Tech-Prefix if you want - it doesn't make a difference since we are not routing calls TO CCM via the Gatekeeper (see Task 23.20 further ahead and you will see that for calls from CME to CCM you have a choice – it is quicker and easier to add the CME as a ICT trunk in CCM).**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.1.100.1
 zone remote PSTN-WAN ipexpert.com 10.1.200.2 1719
zone prefix PSTN-WAN 011*
no shutdown
```

Task 23.11

Configure the router in Branch 2 for CallManager Express. Register the devices and configure the DNs described in Table 7. Enable the ability to add directory numbers through the web interface.

➔ **Run the telephony-service wizard.**

➔ **To enable the Web Interface:**

➔ **From global configuration mode, enable HTTP service (enabled by default).**

```
Router#ip http server
```

➔ **Configure HTTP root directory to be router flash.**

```
Router#ip http path flash:
```

➔ **Enter telephony service configuration mode.**

```
Router#telephony-service
```

➔ **Specify CCME(ITS) GUI administrator name and password.**

```
Router(telephony)#web admin system name admin password ipexpert
```

Where admin is name of administrator account and ipexpert is the administrator password.

➔ **Enable ability to add extension number using GUI tool.**

```
Router(telephony)#dn-webedit
```

➔ **Enable ability to change time setting on phone using GUI tool.**

```
Router(telephony)#time-webedit
```

Task 23.12

Create an incoming AutoAttendant at the DN of 3000. Also Create a Basic ACD using the support team hunt group you just created (The necessary TCL scripts are already loaded in BR2 router's flash memory). Have the AA script automatically hand-off the callers into the support ACD hunt group when a user presses 2. Allow no more than 20 callers in the Q at any one point. Play a prompt for the user every 30 seconds to let them know that all agents are busy. Allow the users to dial-by-extension by pressing 4. Ensure that the Q is collecting statistics and view them as part of your troubleshooting.

➔ **This should be self-explanatory from previous examples – see Task 14.10.**

Task 23.13

Configure the gatekeeper to allow only Four G.729 calls to the remote zone.

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.2.100.1
 zone remote PSTN-WAN ipexpert.com 10.2.200.2 1719
 zone prefix PSTN-WAN 011*
 bandwidth remote 64
 no shutdown
```

Task 23.14

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 23.15

Configure Call Restrictions.

➔ **Create the following partitions:**

- PT-HQ-911
- PT-HQ-LOCAL
- PT-HQ-TOLLBYPASS
- PT-HQ-LD
- PT-HQ-INTERNATIONAL
- PT-BR1-911
- PT-BR1-LOCAL
- PT-BR1-TOLLBYPASS
- PT-BR1-LD
- PT-BR1-INTERNATIONAL

➔ **Create the following CSS putting relevant partitions into each CSS.**

- CSS-HQ-RESTRICTED
- CSS-HQ-LOC-LD
- CSS-HQ-INTERNATIONAL
- CSS-BR1-RESTRICTED
- CSS-BR1-LOC-LD
- CSS-BR1-INTERNATIONAL

Task 23.16

Configure the Phones with Class of Restrictions (COR).

For differing types of PSTN Calls refer to Route/Destination patterns defined in the Table in Workbook.

To verify your dial plan use the PSTN Phone DNs as defined in Table 10. Ensure the PSTN phone is placed into the correct Voice VLAN as defined in Table 11

For full E164 numbering plan for each site please refer to Table 12.

➔ **Assign CSS to Devices.**

Task 23.17

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

➔ **See Task 23.22.**

Task 23.18

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

➔ **See Task 23.22.**

Task 23.19

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed first out of the local Gatekeeper and then through the HQ-IPIPGW as a backup. Users must be able to dial the BR2 site using extension (4 digit) dialing. (**Test both** call routing methods, one at a time, before moving on to the next question). **NOTE**: The gatekeeper is expecting the full E164 number, i.e. international prefix '011' plus 10 digits.

➔ **See Task 23.22.**

Task 23.20

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway. You must 4 different types of methods to manipulate the digits sent to the PSTN (e.g. one method is by using the 'forward-digits' command inside the POTS dial-peer).

➔ **Num-exp, Translation rules, forward-digits, no digit-strip, prefix can be used. See Task 23.22.**

Task 23.21

Calls originating from BR2 to Call Manager (both HQ and BR1) should use VoIP and PSTN as backup. If you decide to register the CME to the gatekeeper use your local HQ-RTR gatekeeper as opposed to the PSTN-WAN gatekeeper. 4-digit dialing must be preserved.

➔ **See Task 23.22.**

Task 23.22

Enable DID for PSTN users dialing into the Call Manager (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits.

➔ **When implementing a dial plan it is a good idea to look at all the tasks together rather than treat each question as a separate question.**

➔ **Digit Manipulation should be done in the Route List.**

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-GK	GK TRUNK	1
RG-IPIPGW-ICT	H323 (non-GK controlled) InterClusterTrunk	1
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1-LOC	RG-HQ RG-BR1	PREDOT PREDOT + PREFIX 1212
RL-BR1-HQ-LOC	RG-BR1 RG-HQ	PREDOT PREDOT + PREFIX 1617
RL-HQ-BR1-LD-INT	RG-HQ RG-BR1	PREDOT PREDOT
RL-BR1-HQ-LD-INT	RG-BR1 RG-HQ	PREDOT PREDOT
RL-TOLLBY-2-BR1	RG-BR1 RG-HQ	PREDOT PREDOT + PREFIX 1617
RL-TOLLBY-2-HQ	RG-HQ RG-BR1	PREDOT PREDOT + PREFIX 1212
RL-GK-ICT	RG-GK RG-IPIPGW-ICT	PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ-BR1-LOC
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ-LOC
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ-BR1-LD-INT
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1-HQ-LD-INT
91212.xxxxxxx	PT-BR1-TOLLBYPASS	RL-BR1-TOLLBY
91617.xxxxxxx	PT-HQ-TOLLBYPASS	RL-HQ-TOLLBY
9.011! 9.011!#	PT-HQ-INTERNATIONAL	RL-HQ-BR1-LD-INT
9.011! 9.011!#	PT-BR1-INTERNATIONAL	RL-BR1-HQ-LD-INT
3xxx	(Null PT)	RL-GK-ICT

➔ **For CCME use the following dial-peers.**

```
translation-rule 1
 Rule 0 91 1

dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 corlist outgoing css-911
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 translate-outgoing called 1
 port 0/0/0:0

dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 9011T
 port 0/0/0:0
 prefix 011
```

```
!
dial-peer voice 1000 voip
 destination-pattern 1...
 session target ipv4:10.2.200.21
 dtmf-relay h245-alphanumeric

dial-peer voice 1001 pots
 preference 1
 destination-pattern 1...
 no digit-strip
 port 0/0/0:0
 prefix 1212222
!
dial-peer voice 2000 voip
 destination-pattern 916175222...
 session target ipv4:10.2.200.21
 dtmf-relay h245-alphanumeric
!
dial-peer voice 2001 pots
 preference 1
 destination-pattern 916175222...
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
num-exp 2... 916175222...
```

➔ **We are sending calls directly from CCME to CCM in this particular case. We must therefore add the CCME as a Non-GK Controlled Trunk in CCM otherwise CCM will ignore Call attempts from CCME (since it is an unregistered gateway). We must bind H323 to an interface first – in this example the Loopback.**

```
P2-BR2-RTR(config)#int loopback 0
P2-BR2-RTR(config-if)#h323-gateway voip bind srcaddr 172.2.102.1
```

➔ **Add the ICT in CCMAdmin.**

➔ **Configure settings on trunk page. Ensure you use the IP Address of the interface you specified as the source Address for H323. CAC is not specified in the question therefore use the default location.**

➔ **Place the gateway in a Device Pool which contains a Region that uses G729 to all other Regions.**

➔ **For inbound Call Routing set Significant Digits to 4 and assign CSS if required.**

➔ **We are not using the ICT for outbound call routing therefore use any settings. Update and Reset and check the registration status. When a trunk has successfully been added you will see the IP Address appear - Note the Registration status remains Unknown.**

Task 23.23

All users with a class of service that includes access to PSTN numbers should be given access to Toll Free Services. Block access to all 1-900 and 1-976 numbers.

➔ **Click Route Plan --> Route Pattern**
Under the Route Pattern, enter 9.1900XXXXXXX
Under the Gateway, select the normal gateway you use
Under Route Option, select Block this pattern.
Then Insert the route pattern.
You can block 976 numbers as well by doing
Under the Route Pattern, enter 9.976xxxx
Under the Gateway, select the normal gateway you use
Under Route Option, select Block this pattern.
Then Insert the route pattern.

Task 23.24

Create a DN of 1005 for Tech Support. Make HQ phone 3 and BR1 Phone 3 ring when this DN is called. You may not use a shared line to accomplish this task. The call should alternate back and forth between these 2 phones equally.

➔ **This should be self-explanatory from previous examples – See Task 2.12.**

➔ **Only instead of using the Distribution Algorithm of "Broadcast" – choose "Circular".**

Task 23.25

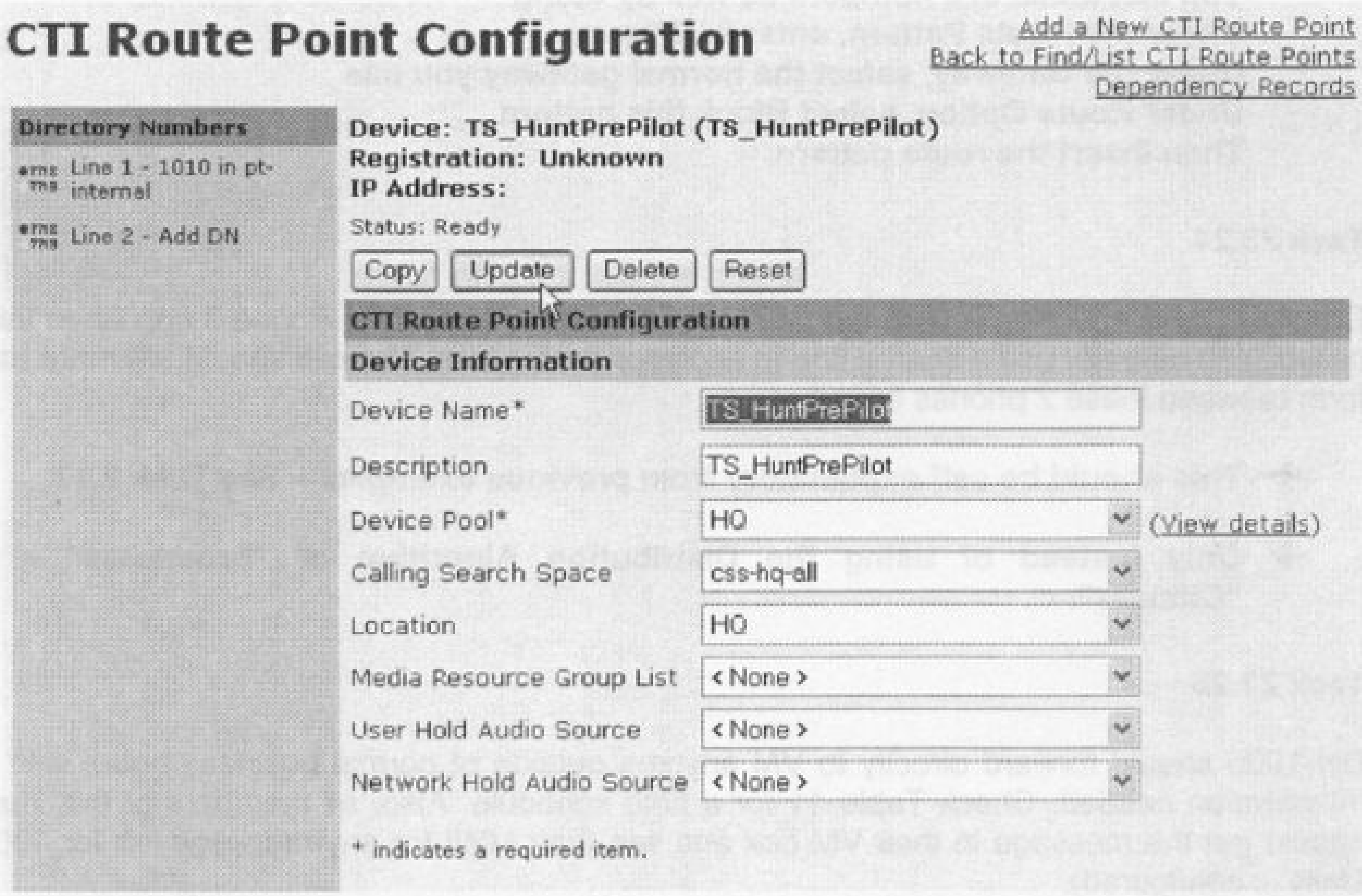
DN 1005 should forward directly to VM anytime outside of normal business hours with no user intervention needed. Check Table 11 for a time schedule. Also, all members of this HuntGroup should get the message in their VM box and see their MWI for any message left for 1005 (once Unity is configured).

➔ **This should be self-explanatory from previous examples – See Task 6.7.**

Task 23.26

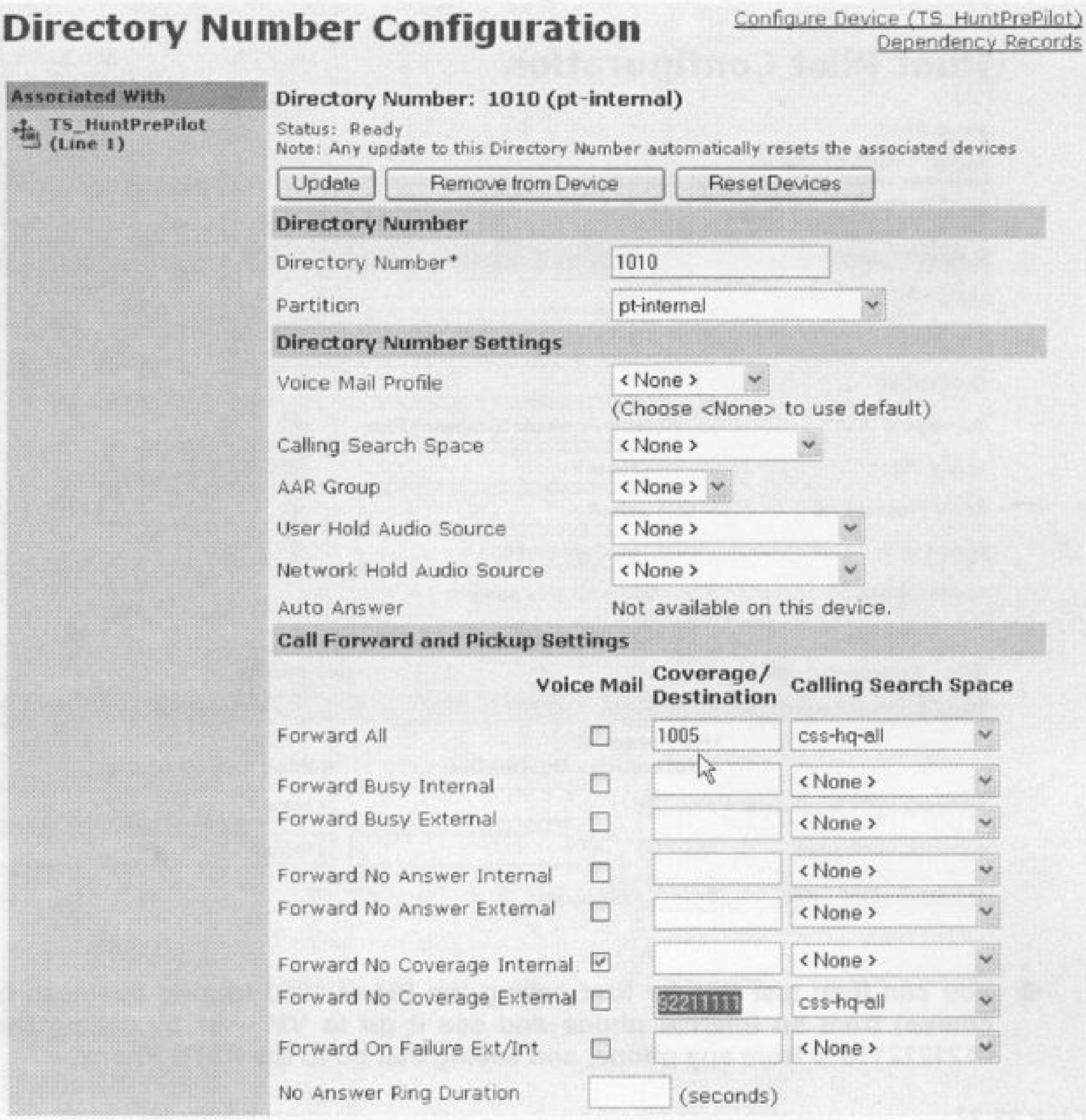
Create a new DN of 1010. When this DN is called, all calls should be directed to the DN of 1005. The call should ring this DN for approximately 2 rings. If for any reason this DN does not answer, the call should then be forwarded to VM if the call originated from an internal number, however if the call originated from an external number, the call should then be forwarded to the PSTN phone at '221-1111'.

➔ **We need to create a CTI Route Point with the DN of 1010 in the PT-Internal or Null PT if you choose to use it.**

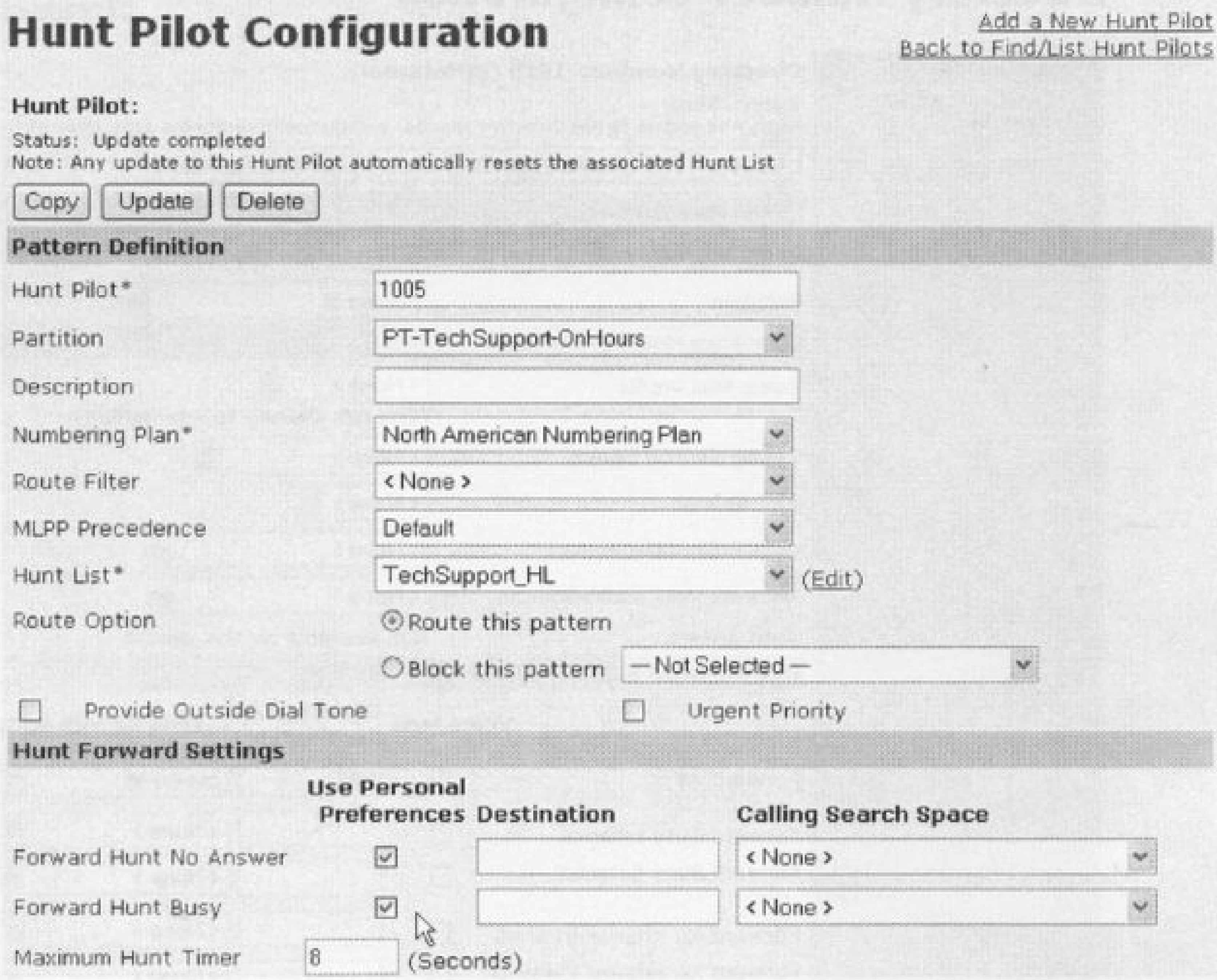


➔ **We will then configure this CTI RP DN with the setting to 'Forward All' to the DN of 1005 (our Hunt Pilot).**

➔ **Then configure the 'Forward No Coverage Internal' with the VM checkbox and the 'Forward No Coverage External' to '912211111' with a CSS allowing the call to go out the HQ gateway with Local privileges.**



➔ **Now we need to go back to our Hunt Pilot and configure it to only try the Hunt Group for 2 rings (which is approximately 8 seconds – 4 seconds per ring roughly) and then also tell the 'Forward Hunt No Answer' and 'Forward Hunt Busy' to 'Use Personal Preferences' which causes the Pilot number to revert back to the Call Coverage settings of whomever forwarded the call to it in the first place – which in this case is of course the CTI Route Point. This is what will enable the 'Forward No Coverage Internal/External' settings in the CTI RP DN page to take effect.**



➔ **You can then test this by first calling the DN of 1010 (during business hours of course) from an internal phone and see it go to VM – or by calling the DN of 912122211010 from any phone, and seeing that go to the PSTN Phone.**

Task 23.27

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 23.28

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 23.29

Configure conference bridge on BR1 router. Use a maximum of 1 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 23.30

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 23.31

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should load share the IOS resources and 6608 resources.

➔ **Create a MRG called HQ-MRG. Put HQ media resources - 6608 conference bridge, 6608 transcoder and MOH Server – into the MRG.**

➔ **Create a MRG called IOS-MRG. Put IOS media resources into this MRG.**

➔ **Create a third MRG called BR1-MRG. Put ALL media resources into this group.**

➔ **Create a MRGL called HQ-MRGL and put HQ-MRG and IOS-MRG into this MRGL - HQ-MRG should be listed above IOS-MRG.**

➔ **Create a MRGL called BR1-MRGL. Put BR1-MRG into this MRGL.**

Task 23.32

Configure a Music on Hold server on the Publisher Call Manager. Add another music source which can be found on the C: drive of your Call Manager. Ensure that the default (Sample) audio source is used when a User presses the 'Hold' button on his/her phone. For all other events that require music to be played use the newly added music source. You may not configure music sources on line, device or device pool to accomplish this task.

➔ **See Task 7.6. Configure music sources in CCM Service Parameters.**

Task 23.33

Configure the Call Manager such that HQ phones will receive music using the G711 codec and BR1 phones will receive music using the G729 codec. You must use the transcoder to achieve this task.

➔ **Transcoding MOH will only work for Unicast so in the next task change the IP Media Streaming Application. The idea is to verify the transcoder is working - use the following command on the Cat 6K.**

```
sh port voice active transcode
```


Task 23.34

Ensure that the HQ and BR1 phones receive multicast music on hold.

➔ **This should be self-explanatory from previous examples.**

Task 23.35

Configure music on hold on the BR2 CME.

➔ **This should be self-explanatory from previous examples.**

Task 23.36

Create a meet-me conference with DN=1900.

➔ **This should be self-explanatory from previous examples.**

Task 23.37

Configure the CoS-to-DSCP Mappings for the Catalyst 6500 and the Catalyst 3550 switches. The recommended settings are DSCP of AF31 for VoIP control plane and DSCP of EF for VoIP bearer plane.

➔ **On the Cat 6K:**

```
set qos enable
set port qos 2/7-8 vlan-based
set qos acl ip ACL-IPPhones trust-cos any
commit qos all
set qos acl ACL_IPPhones 220
```

Move Cos 3 to queue 2

```
set qos map 2q2t tx 2 1 cos 3
```

COS to DSCP and IPPREC to DSCP map

```
set qos cos-dscp-map 0 8 1 26 34 46 48 56
set qos ipprec-dscp-map 0 8 1 26 34 46 48 56
```

➔ **For VG248 port:**

```
set port qos 2/48 port-based
set qos acl ip VG248 trust-dscp any
commit qos acl VG248
set qos acl map VG248 2/48
```


➔ **For WAN link:**

```
set port qos 2/21 port-based
set qos acl ip WAN trust-dscp any
commit qos acl WAN
set qos acl map WAN 2/21
```

➔ **On 3550:**

➔ **For IP phone:**

```
interface range FastEthernet0/23 - 24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 120
 switchport mode trunk
 switchport voice vlan 220
 spanning-tree portfast
 switchport priority extend cos 0
 mls qos trust cos
```

COS to DSCP or IPPREC to DSCP map

```
mls qos map cos-dscp 0 8 16 26 34 46 48 56
mls qos map ip-prec-dscp 0 8 16 26 34 46 48 56
```

Priority Queue

```
interface range FastEthernet0/23 - 24
Priority-queue out
wrr-queue cosc-map 4 5
```

Uplink

```
Int fastethernet 0/1
Mls qos trust dscp
Priority queue out
Wrr-queue cosc-map 4 5
```

Task 23.38

Configure video traffic so it is mapped from the DSCP value AF41 to the 802.1Q CoS value 4. Apply this policy only to the data/video VLAN FE sub-interface in Branch 2.

➔ **On BR2 router:**

```
ip cef
!
policy-map REMOTE-LAN-EDGE
class VIDEO
set cos 4
!
interface FastEthernet0/1
description CAT3500 REMOTE-BRANCH ACCESS-SWITCH
no ip address
load-interval 30
speed auto
duplex auto
!
interface FastEthernet0/1.102
description data vlan 102
encapsulation dot1Q 102
ip address 192.1.102.1 255.255.255.0
service-policy output REMOTE-LAN-EDGE
```

Task 23.39

Configure FRTS between HQ and BR2 such that the traffic shaper only engages when Voice traffic is present on the link. For this task you may assume that the FR port speed is 768kbps and that the CIR provided by the carrier is 384. A proper LFI mechanism should be engaged at all times and should be relevant to the CIR not the Port speed.

➔ **See next task 23.40.**

Task 23.40

Configure LLQ between Headquarters and Branch 1 location. From Headquarters to Branch 1 configure 32kbps control traffic and 256kbps bearer traffic. From Branch 1 to Headquarters configure 6% control traffic and 40% bearer traffic. You may assume the speed of the PVC from HQ to BR1 is 1544Kbps.

➔ **On HQ-RTR:**

```
policy-map LLQ-HQ
 class RTP
  priority 256
 class SIG
  bandwidth 32
 class class-default
  fair-queue
```



```
policy-map FR-VATS
 class class-default
  service-policy output LLQ-HQ
  shape average 729600 3648 0
  shape adaptive 364800
  shape fr-voice-adapt deactivation 30
!
interface Serial0/1/0:0
 frame-relay fragmentation voice-adaptive deactivation 30
!
interface Serial0/1/0:0.2
 bandwidth 768
 frame-relay interface-dlci 202
  class FRTS-FRF12
!
map-class frame-relay FRTS-FRF12
 service-policy output FR-VATS
 frame-relay fragment 480
```

➔ **On BR2:**

```
policy-map LLQ-BR2
 class RTP
  priority percent 40
 class SIG
  bandwidth percent 6
 class class-default
  fair-queue

policy-map FR-VATS
 class class-default
  service-policy output LLQ-BR1
  shape average 729600 3648 0
  shape adaptive 364800
  shape fr-voice-adapt deactivation 30
!
interface Serial0/1/0
 frame-relay fragmentation voice-adaptive deactivation 30
!
interface Serial0/1/0.1
 bandwidth 768
 frame-relay interface-dlci 102
  class FRTS-FRF12
!
map-class frame-relay FRTS-FRF12
 service-policy output FR-VATS
 frame-relay fragment 480
```


Task 23.41

Configure Voice Mail Integration for Call Manager. The information is provided below.

- Pilot Number: 1600
- Unity Port Number: 1601 – 1604
- Set the default password to 54321
- MWI Light – 1998 off
- MWI Light – 1999 on

➔ **This should be self-explanatory from previous examples – see Task 9.1.**

Task 23.42

Subscribers have recently migrated from Octel Voicemail system to Unity and expect Unity to have the same Message Retrieval Menus. Configure Unity such that when users retrieve messages the prompts will be transparent.

➔ **Go into Unity admin page, click on subscriber template.**

➔ **Click on Conversation.**

➔ **Conversation style: (choose) Optional Conversation 1.**

Task 23.43

Configure a subscriber mailbox for phone 2 at the HQ and BR1 locations. Record the subscriber's greeting to say "I am not in the office right now. If you need to reach me press 3 to be transferred to my cell phone". Have callers transferred from Voicemail to the External Numbers listed below.

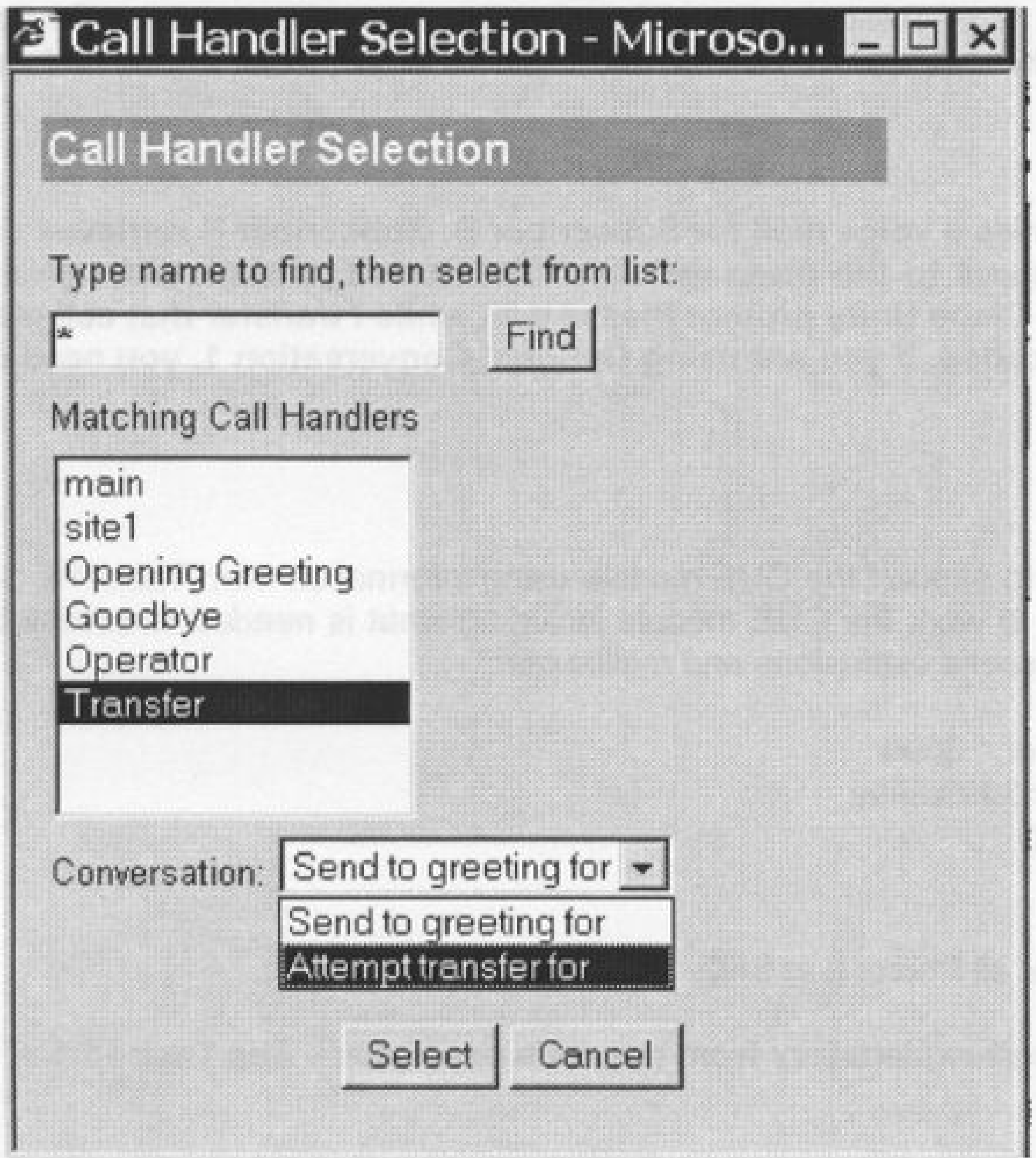
- HQ phone 2 transfers to 212-22X-1111
- BR1 phone 2 transfers to 617-52X-2222

➔ **Create a call handler - "Transfer". The purpose of this new call handler is to act as a transfer agent to the external phone.**

➔ **From the Call Transfer section under the Call Handlers heading, select Yes, Ring a subscriber at this extension - "912122221111".**

➔ **Now go to the subscriber (created in an earlier exercise) . From the Subscriber heading, select Caller Input and select the number you want callers to press in order to transfer to an external phone - "3".**

➔ **Select "Send caller to" using the pull down menu, choose the new Call handler. Click the find button to select your newly created call handler "Transfer".**



➔ **Under the Conversation menu of this screen select Attempt transfer for and save.**

➔ **Change your voicemail greeting to "I am not in the office right now. If you need to reach me press 3 to be transferred to my cell phone".**

Task 23.44

Enable the Live Reply feature in Unity. Allow the subscriber to call back another subscriber immediately after listening to the voice message, through the Telephone User Interface (TUI). Use the first line for phone 1 at Headquarters and Branch 2 locations.

➔ **Set the Default Class of Service.**

➔ **Go to Subscriber > Class of Service > Messages. Check Live Reply: Subscriber can reply to messages from other subscriber by calling them. Click Save. All subscribers created from this template are configured to allow Live Reply.**

➔ **Configure the calling subscriber.**

➔ **It is necessary to configure the calling subscriber's Call Transfer settings for Live Reply to be fully functional. Go to the calling subscriber's settings by clicking Subscriber > Call Transfer. By default, No (send directly to subscriber's greeting) is checked. It is necessary to check the Yes, ring subscriber's extension: option.**

➔ **Configure the called subscriber.**

➔ **If you have customized Class of Service settings, make sure that the Live Reply Class of Service is enabled for the subscriber you want to use Live Reply. To do this, go to the subscriber's profile and check the Class of service.**

➔ **Test Live Reply.**

➔ **Subscriber A leaves a voice mail for Subscriber B. Subscriber B retrieves the voice message and listens to the message. After the message is played , press 4-4 in succession. The Cisco Unity prompt Please wait while I transfer that call plays, and Subscriber A is called. If you are using Optional Conversation 1, you need to press 8-8 instead.**

Task 23.45

Configure the BR2 router to support the CUE module using information from Table 16. Setup the basic information needed to work the CUE module including what is needed to access the web-based GUI to manipulate user's extensions and mailboxes.

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

Finally setup mailboxes for all Phone 2 at BR2.

➔ **This should be self-explanatory from previous examples – See Task 15.1.**

Task 23.46

Ensure that if a call is forwarded from any one of the 3 phones for reasons of No-Answer or Busy that the call goes to the appropriate mailbox.

➔ **This should be self-explanatory from previous examples – See Task 15.2.**

Task 23.47

Ensure that when users listen to their voicemail messages, that they hear the ANI announced of the phone who left them the message.

➔ **This should be self-explanatory from previous examples – See Task 15.3.**

Task 23.48

Network CUE with Unity. Allow messages to be seamlessly forwarded back and forth.

➔ **This should be self-explanatory from previous examples – See Task 16.5.**

Task 23.49

Configure the Personal Address Book and Fast Dial IP Phone Services on Call Manager. Have all phones at this Branch 1 subscribe to this service. Use the Cisco CallManager Lightweight Directory Access Protocol (LDAP). Enter three IP Phones user information from the Headquarters site into the address book. Use names that are descriptive to the site (Example: HQ Phone1 / 212-22X-1001).

➔ **See Task 11.5.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 24: Multiprotocol Challenge G

Estimated Time to Complete: 7 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 24 Multiprotocol Challenge G

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 24 Configuration Tasks

Task 24.1

Check the configuration of basic Frame Relay connections.

- ➔ **This should be self-explanatory from previous examples.**

Task 24.2

Check the configuration of basic OSPF – all interfaces should be assigned to area 0. Verify the connectivity between sites.

- ➔ **This should be self-explanatory from previous examples.**

Task 24.3

Configure both voice and data VLANs based on Table 2.

- ➔ **This should be self-explanatory from previous examples.**

Task 24.4

For Headquarter and Branch 1, use Microsoft DHCP server to allocate IP address for the IP phones, VG-248 and 6608. For Branch 2, use IOS DHCP to allocate IP address for the IP phones.

- ➔ **This should be self-explanatory from previous examples.**

Task 24.5

Configure CallManager to allow devices to register manually. Assign directory number to devices based on Tables 5, 6 and 7.

- ➔ **This should be self-explanatory from previous examples - Note there is no CCME in this Lab.**

Task 24.6

Ensure that Security based services are started – that tokens exist, and that all media and signaling traffic between HQ Phone 3 and BR1 Phone 3 are secured with 128bit AES encryption.

➔ **This should be self-explanatory from previous examples – See Task 17.1 – 2.**

Task 24.7

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **This should be self-explanatory from previous examples.**

Task 24.8

Configure BR1 as an MGCP gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed.

➔ **This should be self-explanatory from previous examples.**

Task 24.9

Ensure that the correct transport for DTMF digits is used for the BR1 gateway.

➔ **This should be self-explanatory from previous examples.**

Task 24.10

Ensure that RTP traffic between the any capable IP Phone and the BR1 MGCP gateway is encrypted with AES128.

➔ **This should be self-explanatory from previous examples – See Task 17.4.**

Task 24.11

Ensure that all MGCP signaling between CallManager and BR1 gateway is encrypted with 3DES 168bit encryption using a SHA hashing algorithm.

➔ **This should be self-explanatory from previous examples – See Task 17.5.**

Task 24.12

Configure BR2 as an H323 gateway based on the information in Table 8. Register the gateway to Call Manager using the voice subinterface.

➔ **This should be self-explanatory from previous examples.**

Task 24.13

Configure gatekeeper on HQ-RTR with the following information:

Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

Register Call Manager to the HQ-RTR gatekeeper.

➔ **The gatekeeper will be used to route calls between HQ/BR1 and BR2 when the WAN is down. The configuration of the gatekeeper is given below:**

```
gatekeeper
zone local HQ-RTR ipexpert.net 172.2.100.1
zone remote PSTN-WAN ipexpert.net 10.2.200.2 1719
zone prefix PSTN-WAN 011*
no shutdown
```

Task 24.14

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 24.15

Use Locations CAC to limit the number of calls over the WAN between the HQ and BR1/BR2 to one audio call. Limit video to one call per site using the minimum bandwidth allowable by a VTA camera in H263 mode.

➔ **Create 3 locations – HQ (0Kbps), BR1 (24Kbps) and BR2 (24Kbps) for audio and BR1 (128Kbps) and BR2 (128Kbps) for video.**

Task 24.16

Ensure that when a user presses the 'Services' or 'Directories' button the error message is not displayed.

➔ **This should be self-explanatory from previous examples.**

Task 24.17

Configure the Calling Restriction.

➔ **Create the following Partitions:**

- PT-HQ-911-LOC
- PT-BR1-911-LOC
- PT-BR2-911-LOC
- PT-HQ-LD
- PT-BR1-LD
- PT-BR2-LD
- PT-HQ-INT
- PT-BR1-INT
- PT-BR2-INT

➔ **Create the following CSS and assign PT accordingly:**

- CSS-HQ-911-LOC
- CSS-BR1-911-LOC
- CSS-BR2-911-LOC
- CSS-HQ-911-LOC-LD
- CSS-BR1-911-LOC-LD
- CSS-BR2-911-LOC-LD
- CSS-HQ-ALL
- CSS-BR1-ALL
- CSS-BR2-ALL

Task 24.18

Configure CallManager to provide Class of Service such that phone 1 can call everywhere, phone 2 can call 911 and local, other phones (if applicable) can call 911, local and long distance. Configure device and line CSS to achieve this configuration. You cannot restrict any calls from the device CSS level.

➔ **Apply CSS to device. The restriction that "You cannot restrict any calls from the device CSS level" is reference to the best practice method of designing Calling Restriction (see CCM SRND Calling Restriction). In the lab we deem the best practice method as NOT being the most efficient way of implementing Calling Restriction!**

Task 24.19

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

➔ **See Task 24.23.**

Task 24.20

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

➔ **See Task 24.23.**

Task 24.21

Calls originating from both the HQ and BR1 sites destined for the BR2 PSTN numbers should be routed out of the local gatekeeper with the appropriate local gateway acting as backup. Users must be able to dial the BR2 site using extension (4 digit) dialing. **NOTE**: The gatekeeper is expecting the full E164 number, i.e. international prefix '011' plus 10 digits.

Correction: This is referring to PSTN number dialing so ignore the sentence about dialing BR2 with 4 digit dialing – BR2 is a CCM site so this is already enabled.

➔ **See Task 24.23.**

Task 24.22

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway.

➔ **See Task 24.23.**

Task 24.23

Enable DID for PSTN users dialing into the Call Manager (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits.

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1
RG-BR2	H323 BR2	1
RG-GK	Gatekeeper-Trunk	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-BR2	RG-BR2	PREDOT
RL-HQ-BR1-LOC	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212222
RL-BR1-HQ-LOC	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617522
RL-HQ-BR1-LD-INT	RG-HQ	PREDOT
	RG-BR1	PREDOT
RL-BR1-HQ-LD-INT	RG-BR1	PREDOT
	RG-HQ	PREDOT
RL-TOLLBY-2-HQ	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-TOLLBY-2-BR1	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617
RL-GK-HQ	RG-GK	PREDOT
	RG-HQ	PREDOT
RL-GK-BR1	RG-GK	PREDOT
	RG-BR1	PREDOT

➔ **The following Route Patterns should be created.**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911-LOC	RL-HQ
911 9.911	PT-BR1-911-LOC	RL-BR1
911 9.911	PT-BR2-911-LOC	RL-BR2
9.[2-9]xxxxxx	PT-HQ-911-LOC	RL-HQ-BR1-LOC
9.[2-9]xxxxxx	PT-BR1-911-LOC	RL-BR1-HQ-LOC
9.[2-9]xxxxxx	PT-BR2-911-LOC	RL-BR2
9.1xxxxxxxxxx	PT-HQ-LD	RL-HQ-BR1-LD-INT
9.1xxxxxxxxxx	PT-BR1-LD	RL-BR1-HQ-LD-INT
9.1xxxxxxxxxx	PT-BR2-LD	RL-BR2
9.011! 9.011!#	PT-HQ-INT	RL-HQ-BR1-LD-INT
9.011! 9.011!#	PT-BR1-INT	RL-BR1-HQ-LD-INT
9.011! 9.011!#	PT-BR2-INT	RL-BR2
91212.xxxxxxx	PT-BR1-LD	RL-TOLLBY-2-HQ
91617.xxxxxxx	PT-HQ-LD	RL-TOLLBY-2-BR1
0113313223xxx	PT-HQ-INT	RL-GK-HQ
0113313223xxx	PT-BR1-INT	RL-GK-BR1

➔ **On the BR2 gateway we need to configure Dial-Peers:**

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
voice class h323 1
 h225 timeout tcp establish 3
!
dial-peer voice 911 pots
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
```

```
!
dial-peer voice 110 pots
 destination-pattern 9011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 3000 voip
 destination-pattern 3…
 session target ipv4:10.2.200.21
 voice-class h323 1
 voice-class codec 1
 no vad
!
dial-peer voice 3001 voip
 preference 1
 destination-pattern 3…
 session target ipv4:10.2.200.20
 voice-class h323 1
 voice-class codec 1
 no vad
```

Task 24.24

There are multiple tenants and overlapping extension scenario in the HQ and Branch 1 sites. Create a line with DN=1010 and assign to both HQ phone 3 and BR1 phone 3. Ensure that when HQ users dial 1010 HQ phone 3 will ring and when BR1 users ring 1010 BR1 phone 3 will ring. Also ensure that calls coming in from the PSTN destined for the overlapping DN will ring the local phone, for example calls coming in from the 6608 for 1010 will ring HQ phone 3.

➔ **Create two partitions:**

- PT-HQ-OVERLAP
- PT-BR1-OVERLAP

➔ **Create a LINE with DN-1010 on HQphn3 in partition PT-HQ-OVERLAP and BR1Phn3 in partition PT-BR1-OVERLAP.**

➔ **Add the PT-HQ-OVERLAP partition in all the HQ CSS. Add the PT-BR1-OVERLAP partition to all the BR1 CSS.**

➔ **Assign the 6608 HQ gateway the CSS-HQ-ALL so that the gateway ONLY has visibility of the HQ partitions. Assign the IOS MGCP BR1 gateway CSS-BR1-ALL.**

Task 24.25

Configure Survivable Remote Site Telephony for Branch 1. Allow maximum of 5 phones and 10 DNs. Ensure that if BR1 gateway does go into fallback mode, that it has already created its own certificate, forwarded that certificate to CallManager and that CallManager in turn has installed that certificate into the IP Phones at BR1, so that signaling and media continue to be encrypted during SRST.

➔ **This should be self-explanatory from previous examples – See Task 17.3.**

Task 24.26

When "Message" button is pressed, users should be able to hear the general greeting from Unity.

```
call-manager-fallback
 voicemail 1600
```

Task 24.27

Configure SRST to provide calling restriction as specified in question #7.

➔ **This should be self-explanatory from previous examples.**

Task 24.28

Configure Branch 1 gateway such that users at Branch 1 can dial 4 digits to reach the other sites.

➔ **This should be self-explanatory from previous examples.**

Task 24.29

Configure hunt group in SRST. Incoming calls will be routed to 2002 and then 2003.

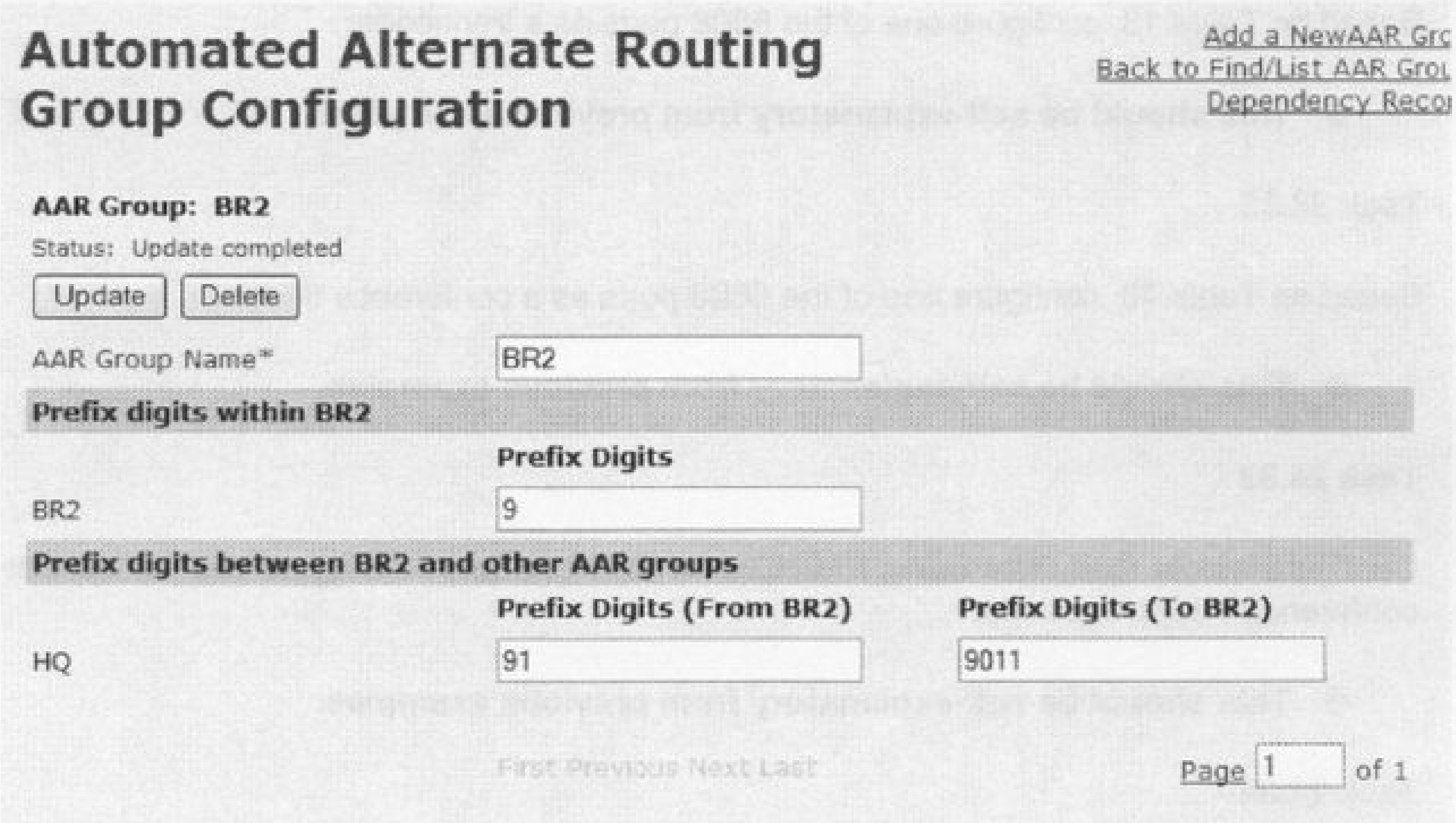
```
P2-BR1-RTR(config)#call-manager-fallback
P2-BR1-RTR(config-cm-fallback)#default-destination 2002
P2-BR1-RTR(config-cm-fallback)#alias 1 2002 to 2003
```

Task 24.30

Configure AAR between the HQ and Branch 2. Calls should only use the local gateway at each site (and not the gatekeeper).

➔ **Enable AAR system wide.**

➔ **Create two AAR Groups – HQ and BR2.**



➔ **Create two new partitions:**

- o PT-HQ-AAR
- o PT-BR2-AAR.

➔ **Create two new CSS:**

- o CSS-HQ-AAR which only has visibility of PT-HQ-AAR
- o CSS-BR2-AAR which only has visibility of PT-BR2-AAR

- o Assign CSS-HQ-AAR to AAR CSS for HQ Phones
- o Assign CSS-BR2-AAR to AAR CSS for BR2 phones.

- o Assign Location HQ to HQ devices.
- o Assign Location BR2 to BR2 devices.

- o Assign HQ AAR Group to HQ phones. Also assign 10 digit External Number Mask.
- o Assign BR2-AAR Group to BR2 phones. Also assign 10 digit External Number Mask.

➔ **Create two new Route Patterns:**

- o 9011331322xxxx in PT-HQ-AAR pointing to RL-HQ
- o 912122221xxx in PT-BR2-AAR pointing to RL-BR2

➔ **Restart the CCM Service.**

Task 24.31

Based on Table 13, configure one of the 6608 ports as a transcoder.

➔ **This should be self-explanatory from previous examples.**

Task 24.32

Based on Table 13, configure one of the 6608 ports as a conference bridge.

➔ **This should be self-explanatory from previous examples.**

Task 24.33

Configure media resources using NM-HDV on BR1 gateway. Configure two transcoder and two conference bridge sessions.

➔ **This should be self-explanatory from previous examples.**

Task 24.34

Configure the MoH server to support both G.711 and G.729 codecs.

➔ **This should be self-explanatory from previous examples.**

Task 24.35

Configure the MoH server and the network to support multicast music on hold. HQ should receive unicast MoH, Branch 1 and 2 should receive multicast MoH and PSTN should receive tone on hold.

➔ **Create 2 MRGs – "unicast-MOH-MRG" and "multicast-MOH-MRG". Place the MOH into each MRG and tick the multicast option for multicast-MOG-MRG.**

➔ **Create a third MRG called media-MRG and place all CFBs and XCODERs into this MRG.**

➔ **Create 2 MRGL – multicast-MRGL and unicast MRGL. Assign unicast-MOH-MRG to unicast MRGL and multicast-MOH-MRG to multicast-MRGL. Assign media-MRG into both MRGL.**

➔ **Create a third MRGL called media-MRGL and add the media-MRG.**

➔ **Assign unicast-MRGL to HQ Device Pool. Assign multicast-MRGL to BR1 and BR2 Device Pools. Assign media-MRGL to the PSTN gateways.**

Task 24.36

Configure Voice Mail Integration for Call Manager. The information is provided below.

- Pilot Number: 1600
- Unity Port Number: 1601 – 1604
- Set the default password to 54321
- MWI Light – 1998 off
- MWI Light – 1999 on

➔ **This should be self-explanatory from previous examples in section 9.**

Task 24.37

Configure Unity VM Ports to use AES128 encryption for media traversal between themselves and IP Phones or Gateways that support such.

➔ **This should be self-explanatory from previous examples – See Task 17.6.**

Task 24.38

Create 4 subscribers shown below in Unity using the Bulk ExchangeTool.

➔ **This should be self-explanatory from previous examples.**

Task 24.39

HQ needs Auto Attendant feature. Configure Unity to provide such functionality. Use 1570 as the extension for the call handler. User should hear a greeting saying "Press 1 for directory handler, 2 for HQ phone 1". When caller press 1, send the call to directory handler. When caller press 2, send the call to phone 1 at HQ. Any other entry should take the caller back to the original greeting.

➔ **This should be self-explanatory from previous examples.**

Task 24.40

Configure Unity so that MWI will be resynchronized at 3:00am every day.

➔ **This should be self-explanatory from previous examples.**

Task 24.41

Configure Extension Mobility as follows:

- Username: ptw
- Password: gjmpt

- HQ Device Profile: 1666
- Branch 2 Device Profile: 3666

Correction: Each user can only dial 911 and local.

Task 24.42

Configure Phone 3 at HQ and Phone 2 at Branch 2 to support Extension Mobility. User's calling restriction should be preserved. Long distance call should be routed through 6608. All other calls should be routed through local gateway only.

Correction: Configure Phone 3 at HQ and Phone 2 at Branch 2 to support Extension Mobility. User's calling restriction should be preserved. Call routing shall be inherited from the device the user is logged in.

➔ **The basic setup of Extension Mobility has been covered in Section 11. The only deviation is apply Calling Restriction and appropriate Call Routing.**

➔ **Create two new Partitions – PT-HQ-EM and PT-BR2-EM.**

➔ **Create two new CSS – CSS-HQ-EM which has visibility of PT-HQ-EM and CSS-BR2-EM which has visibility of PT-BR2-EM.**

➔ **Create the following Route Patterns should be created.**

Route Pattern	Partition	Route List
9.1xxxxxxxxxx	PT-HQ-EM	BLOCK CALL
9.1xxxxxxxxxx	PT-BR2-EM	BLOCK CALL
9.011! 9.011!#	PT-HQ-EM	BLOCK CALL
9.011! 9.011!#	PT-BR2-EM	BLOCK CALL
91212.xxxxxxx	PT-BR1-EM	BLOCK CALL
91617.xxxxxxx	PT-HQ-EM	BLOCK CALL
0113313223xxx	PT-HQ-EM	BLOCK CALL
0113313223xxx	PT-BR1-EM	BLOCK CALL

➔ **The main point here is that the Device and Line CSS is concatenated so we can use the Device CSS for routing 911 and Local calls but we must also add a CSS to the Line to preserve Calling Restriction.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 25: Multiprotocol Challenge H

Estimated Time to Complete: 6 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 25 Multiprotocol Challenge H

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 25 Configuration Tasks

Task 25.1

Ensure that the link between the HQ/BR1/BR2 routers and appropriate switches are configured as DOT1Q trunks. Give the voice sub-interface the appropriate ip address from Table 1. Check connectivity between all sites and to Call Manager/Unity.

➔ **This should be self-explanatory from previous examples.**

Task 25.2

Configure Voice and Data VLAN for all IP Phones including ATA and VG248. VLAN IDs are defined in Table 2. Use Table 3 for HQ site 6500 port assignment. For BR1 and BR2 port allocation you are required to find out port allocation by your own methods.

➔ **This should be self-explanatory from previous examples.**

Task 25.3

Configure all phone ports such that they bypass the spanning-tree listening and learning states.

➔ **This should be self-explanatory from previous examples.**

Task 25.4

Set the clock on the BR2 router to the correct time.

```
P2-BR2-RTR#clock set ?
  hh:mm:ss  Current Time
```

Task 25.5

For Headquarter and Branch 1, use Microsoft DHCP server to allocate IP address for all Devices. For Branch 2, use IOS DHCP to allocate IP address for the IP phones. For each voice subnet, allocate the IP address from .50 to .69.

➔ **This should be self-explanatory from previous examples.**

Task 25.6

Configure CallManager to register devices. Assign directory number to devices based on **Tables 5** and **6**. Also Configure CallManager such that HQ Phones 1 and 2 and BR1 Phones 1 and 2, will encrypt their signaling and media streams using AES128 with any device that will allow such to occur. Configure CCM to install a 1028 bit LSC on each phone. Configure the phones so that when a LSC is to be installed on the phone – that **no** user interaction is required on the IP Phone.

➔ **This should be self-explanatory from previous examples – See Task 17.2 for Security setup.**

Task 25.7

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **This should be self-explanatory from previous examples.**

Task 25.8

Configure BR1 as an MGCP gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed. Ensure that RTP packets as well as signaling packets on this GW are encrypted so that a sniffer would not be able to decode the traffic.

➔ **This should be self-explanatory from previous examples – See Task 17.4 – 5 for security setup.**

Task 25.9

Ensure that the correct transport for DTMF digits is used for the BR1 gateway.

➔ **This should be self-explanatory from previous examples.**

Task 25.10

Configure BR2 as an H323 gateway based on the information in Table 8.

➔ **This should be self-explanatory from previous examples.**

Task 25.11

Configure the E1 R2 such that calls to the PSTN are set up 3 seconds quicker (where possible) than the default. You may assume the maximum length digit string is 11 digits.

➔ **This should be self-explanatory from previous examples.**

Task 25.12

Configure gatekeeper on HQ-RTR with the following information:

Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

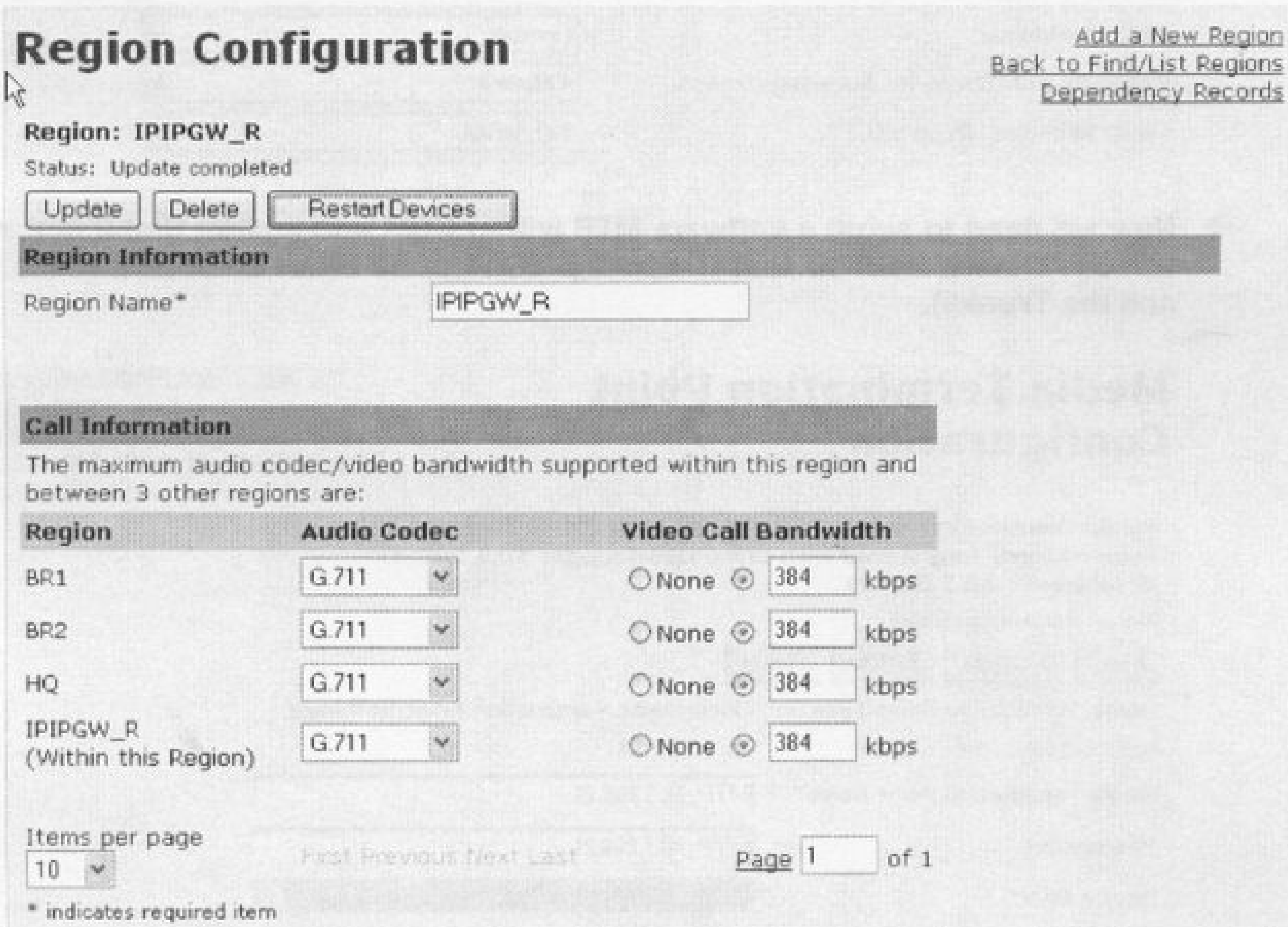
Register Call Manager to the HQ-RTR gatekeeper.

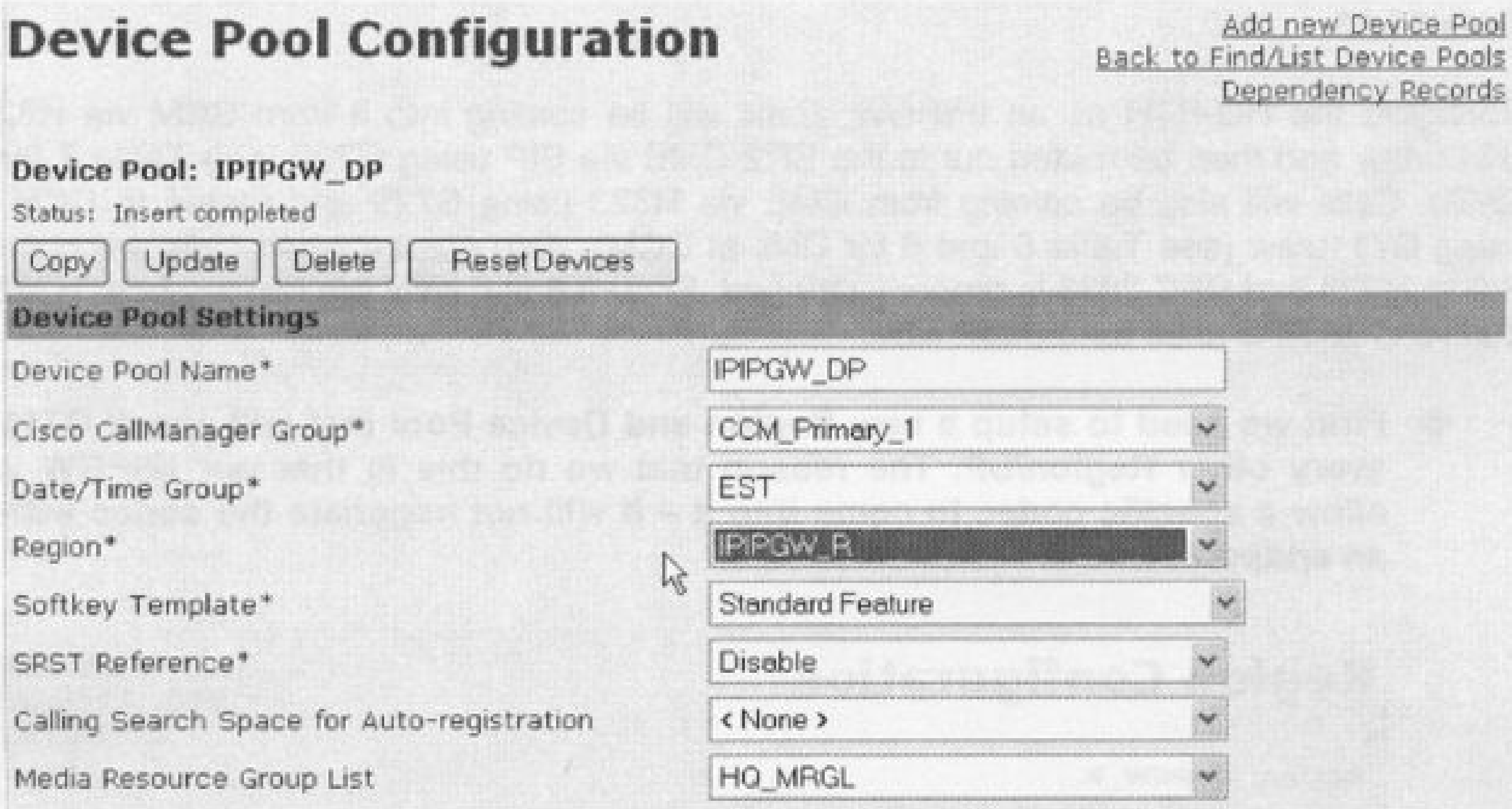
```
gatekeeper
zone local HQ-RTR ipexpert.net 172.2.100.1
zone remote PSTN-WAN ipexpert.net 10.2.200.2 1719
zone prefix PSTN-WAN 011*
no shutdown
```


Task 25.13

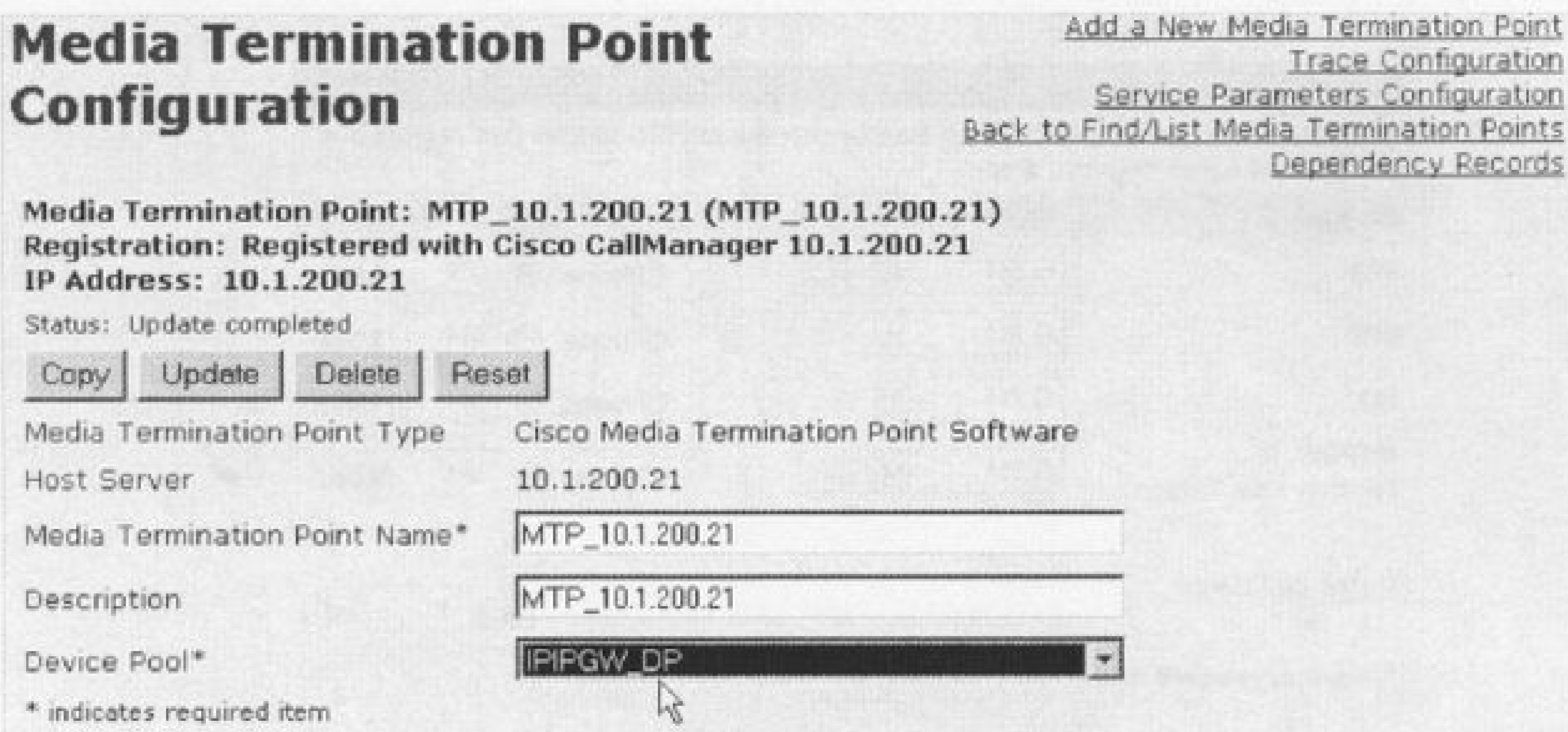
Configure the HQ-RTR as an IPIPGW. Calls will be coming into it from CCM via H323 using G711ulaw and then be routed out to the BR2 CME via SIP using G729 (see Table 7 for DNs at CME). Calls will also be coming from CME via H323 using G729 and routed to CCM via SIP using G711ulaw (see Table 5 and 6 for DNs at CCM). Also ensure when calls are coming from SIP to H323 that RFC 2833 is properly stripped. Ensure that if calls are coming from H323 to SIP, that RFC 2833 is used for the SIP side.

➔ **First we need to setup a new Region and Device Pool that will speak G711ulaw to every other Region/DP. The reason that we do this is that our IPIPGW will only allow a specific codec to come into it – it will not negotiate the codec with us like an endpoint would.**

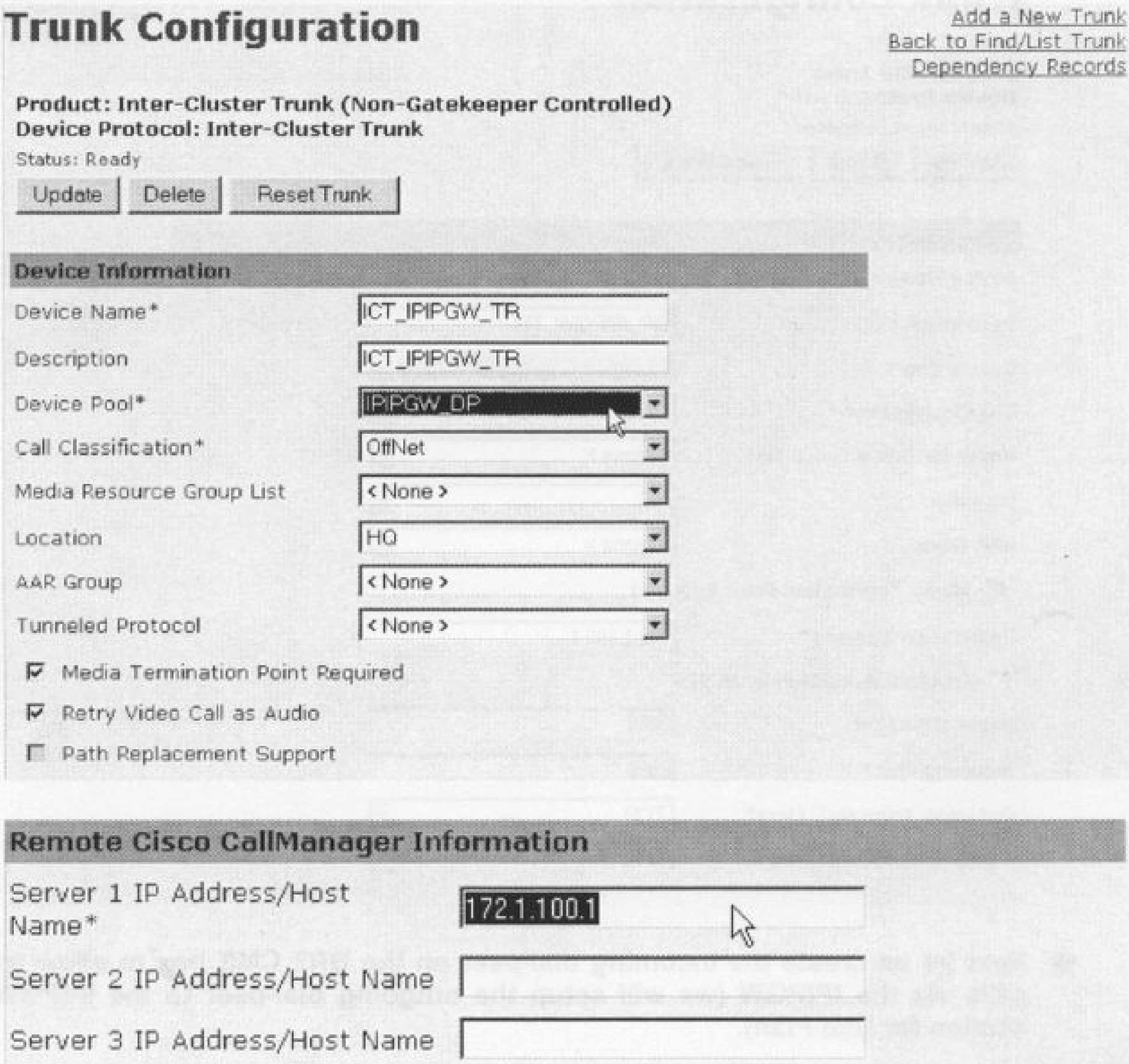




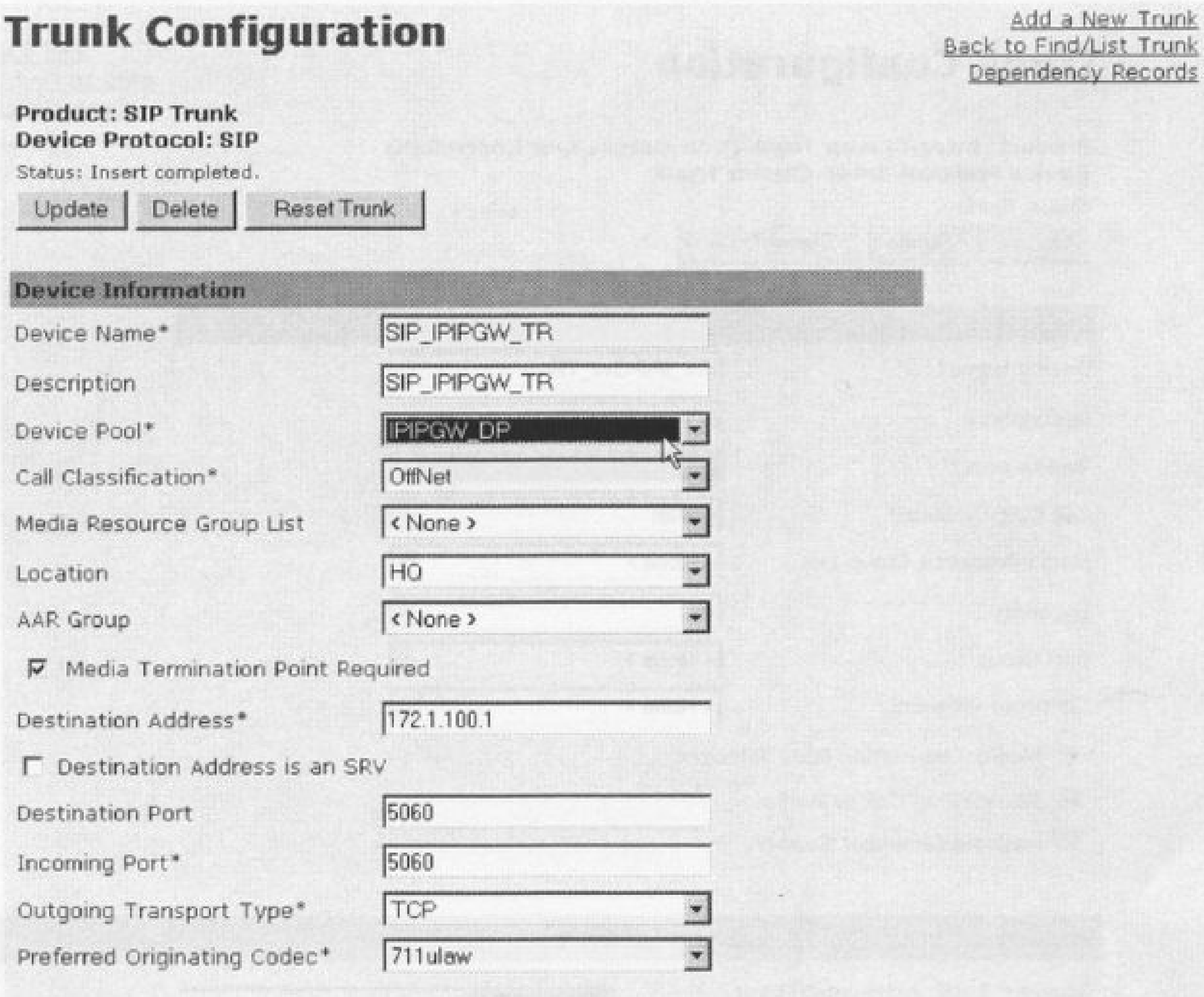
➔ **Now we need to setup a software MTP within CCM and ensure that it is part of the IPIPGW Device Pool so that it 'speaks' G711 to all other devices (i.e. the Phones and the Trunks).**



➔ **We now create our H323 non-GK controlled Inter-Cluster Trunk to be used on the outgoing leg from CCM to CME via the IPIPGW and of course point the destination to the HQ IPIPGW – not to the CME box.**



➔ **We now create our SIP Trunk to allow calls to come in from the CME via the IPIPGW.**



➔ **Next let us create the incoming dial-peer on the BR2 CME box to allow incoming calls via the IPIPGW (we will setup the outgoing dial-peer to the IPIPGW in the section for Dial Plan).**

➔ **On BR2 RTR:**

```
dial-peer voice 10 voip
 incoming called-number 3…
 session protocol sipv2
 dtmf-relay rtp-nte
```

➔ **Finally we need to setup our IPIPGW keeping in mind that we have 2 different codecs coming in and going out of our box – therefore we will need to setup a Transcoder and register it locally to a SCCP server. An instance of CME or SRST will do just fine as a SCCP server.**

➔ **On HQ-RTR:**

```
voice-card 2
 dspfarm
 dsp services dspfarm
!
!
!
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 h323
 sip
!
interface Loopback0
 ip address 172.1.100.1 255.255.255.255
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 172.1.100.1
!
sccp local FastEthernet0/0.210
sccp ccm 172.1.100.1 identifier 1
sccp ip precedence 3
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCODER
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 codec g729br8
 maximum sessions 2
 associate application SCCP
!
```



```
!
telephony-service
 max-conferences 12 gain -6
 ip source-address 172.1.100.1 port 2000
 max-ephones 10
 max-dn 10
 sdspfarm tag 1 XCODER
 sdspfarm units 1
 sdspfarm transcode sessions 1
!
dial-peer voice 10 voip                         ←(Incoming Dial-Peer for CCM-to-CME)
 incoming called-number 3...
 codec g711ulaw
dtmf-relay h245-alphanumeric
!
dial-peer voice 11 voip                         ←(Outgoing Dial-Peer for CCM-to-CME)
 destination-pattern 3...
 session protocol sipv2
 session target ipv4:10.1.202.1
 dtmf-relay rtp-nte digit-drop h245-alphanumeric
!
dial-peer voice 20 voip                         ←(Incoming Dial-Peer for CME-to-CCM)
 incoming called-number [12]...
dtmf-relay h245-alphanumeric
!
dial-peer voice 21 voip                         ←(Outgoing Dial-Peer for CME-to-CCM)
 destination-pattern [12]...
 session protocol sipv2
 session target ipv4:10.1.200.21
 codec g711ulaw
 dtmf-relay rtp-nte
!
```

Task 25.14

Configure Branch 2 gateway for CallManager Express. Allow maximum of 10 phones and 20 DNs.

➔ **This should be self-explanatory from previous examples.**

Task 25.15

Configure Branch 2 gateway as H.323 gateway for CallManager. Use the loopback address as the source address. Assuming there is another CallManager (10.x.200.20) in the cluster, configure the redundant dial-peers and reduce the H.225 timeout value to 3 seconds.

```
interface Loopback0
 ip address 172.2.102.1 255.255.255.255
 h323-gateway voip bind srcaddr 172.2.102.1
!
voice class h323 1
 h225 timeout tcp establish 3
!
dial-peer voice 2000 voip
 destination-pattern 2...
 session target ipv4:10.2.200.21
 dtmf-relay h245-alphanumeric
 voice-class h323 1
!
dial-peer voice 2001 voip
 destination-pattern 2...
 session target ipv4:10.2.200.20
 dtmf-relay h245-alphanumeric
 preference 1
 voice-class h323 1
```

Task 25.16

Allow that if a user dials *67 and then a pattern (PSTN or Internal), that the caller's ANI will not show up on the other side.

➔ **This should be self-explanatory from previous examples – See Task 14.4.**

Task 25.17

Ensure that any conference call at BR2 in which the conference initiator hangs up – that the conference terminates upon that person's leaving. However Phone 3 should be allowed to hang up or press the 'end-call' softkey and leave a conference but allow it to continue running.

➔ **This should be self-explanatory from previous examples – See Task 14.7.**

Task 25.18

Configure phones 1 and 2 at BR2 so that they can intercom each other and have an immediate 2-way conversation – security should be in place so that no one else can dial their respective intercom numbers. Use whatever DNs you wish for this. Also, if another intercom call happened to be present on phone 1 when phone 2 places the intercom call – the first call should be automatically put on hold.

➔ **This should be self-explanatory from previous examples – See Task 14.3.**

Task 25.19

Ensure that all calls that are placed internally (from IP Phone to IP Phone) receive not only CLID but also CNAM display with their respective names (you may name them whatever you wish).

➔ **This should be self-explanatory from previous examples – See Task 14.10.**

Task 25.20

Calls within the HQ and BR1 sites must use the G711 codec. Calls between the two sites must only be allowed to use G729 codec.

➔ **This should be self-explanatory from previous examples.**

Task 25.21

Use Locations CAC to limit the number of calls over the WAN between the HQ and BR1 to one call. Configure Call Manager so that Locations tracing is enabled.

➔ **This should be self-explanatory from previous examples.**

Task 25.22

Configure CallManager Express such that the codec selection is flexible between CME and CM.

➔ **Add the ICT Trunk in CCMAdmin in a Device Pool which contains a region which uses G711 to all other regions.**

➔ **Remember using a Region of G711 does NOT restrict usage of only that Codec – rather it allows any codec that has a bit rate of up to what G711 uses – which of course is 64kbps.**

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8

dial-peer voice 2000 voip
 destination-pattern 2...
 session target ipv4:10.2.200.21
 dtmf-relay h245-alphanumeric
 preference 0
 no huntstop
 voice-class h323 1
 voice-class codec 1
!
dial-peer voice 2001 voip
 destination-pattern 2...
 session target ipv4:10.2.200.20
 dtmf-relay h245-alphanumeric
 preference 1
no huntstop
 voice-class h323 1
 voice-class codec 1
```


Task 25.23

Configure the dial plan.

➔ **Create 8 new partitions:**

Find and List Partitions

11 matching record(s) for Partition Name begins with ""

Find Partitions where Partition Name begins with

and show 20 items per page

To list all items, click Find without entering any search text.

Partition Name	Description
pt-br1-911	pt-br1-911
pt-br1-intnl	pt-br1-intnl
pt-br1-ld	pt-br1-ld
pt-br1-loc	pt-br1-loc
pt-hq-911	pt-hq-911
pt-hq-intnl	pt-hq-intnl
pt-hq-ld	pt-hq-ld
pt-hq-loc	pt-hq-loc

➔ **Create 4 new CSS and assign relevant partitions into each partition.**

Find and List Calling Search Spaces

7 matching record(s) for CSS Name begins with ""

Find Calling Search Spaces where CSS Name begins with

and show 20 items per page

To list all items, click Find without entering any search te

Matching record(s) 1 to 7 of 7

CSS Name	Description
css-br1-911-loc	
css-br1-all	
css-hq-911-loc	
css-hq-all	

Task 25.24

Configure Call Manager to provide Class of Service such that phone 1 can call everywhere, phone 2 can call 911 and local, and all other phones (if applicable) can call 911, local and long distance. Configure device and line CSS to achieve this configuration. You cannot restrict any calls from the device CSS level.

➔ **Assign CSS to Line.**

Task 25.25

From HQ or Branch 1, dial 4 digits to reach Branch 2. Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed first out of the local Gatekeeper (which is expecting a e164 call with a 011 prefix) and then through the HQ-IPIPGW as a backup. (**Test both** call routing methods, one at a time, before moving on to the next question). All other calls from the HQ will be routed to local gateway only.

➔ **Task 25.28 has the solution.**

Task 25.26

Calls originating from BR2 to CallManager (both to HQ and to BR1) should use VoIP through the HQ IPIPGW as a first choice, directly to the CCM as a second choice, and to the PSTN as third choice backup. 4-digit dialing must be preserved all the way around. Also, you must use the minimum amount of dial-peers possible. All other calls will be routed via PSTN.

➔ **Task 25.28 has the solution.**

Task 25.27

Local calls from Branch 1 will be routed through local gateway first and use 6608 as backup. International calls will be routed through 6608 first and use local gateway as backup. 911 and Long Distance calls will be routed through local gateway only.

➔ **Task 25.28 has the solution.**

Task 25.28

When someone places the calls from Branch 1 to the area code in HQ, calls should be hopped off using the 6608 and use local gateway as backup.

➔ **When implementing a dial plan it is a good idea to look at all the tasks together rather than treat each question as a separate question.**

➔ **Digit Manipulation should be done in the Route List.**

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-GK	GK TRUNK	1
RG-IPIPGW-ICT	H323 (non-GK Controlled InterCluster Trunk)	1
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1	RG-HQ RG-BR1	PREDOT PREDOT
RL-BR1-HQ	RG-BR1 RG-HQ	PREDOT PREDOT + PREFIX 1617
RL-TOLLBY-2-HQ	RG-HQ RG-BR1	PREDOT PREDOT + PREFIX 1212
RL-GK-ICT	RG-GK RG-IPIPGW-ICT	PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1
91212.xxxxxxx	PT-BR1-LD	RL-TOLLBY-2-HQ
9.011! 9.011!#	PT-HQ-INTERNATIONAL	RL-HQ
9.011! 9.011!#	PT-BR1-INTERNATIONAL	RL-HQ-BR1
3xxx	PT-INTERNAL (or Null-PT)	RL-GK-ICT

➔ **For CCME use the following dial-peers (Don't forget in your dial-peers that there are TWO CCM servers).**

➔ **In CCM you will need to setup a 2nd H323 non-GK Controlled ICT with the IP address of the CME H323 bound interface to 'receive' calls should the IPIPGW option fail.**

```
voice translation-rule 1
 rule 1 /^(1...\)/ /1212222\1/
 rule 2 /^(2...\)/ /1617522\1/
!
voice translation-profile PSTN-OUT
 translate called 1
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 destination-pattern 9911
 corlist outgoing css-911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
```

```
 corlist outgoing css-loc
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1000 voip
 destination-pattern [12]...
 session target ipv4:172.1.100.1
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1001 voip
 destination-pattern [12]...
 session target ipv4:10.1.200.21
 preference 1
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1001 voip
 destination-pattern [12]...
 session target ipv4:10.1.200.20
 preference 2
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1002 pots
 preference 3
 destination-pattern [12]...
 port 0/0/0:0
 translation-profile outgoing PSTN-OUT
!
```

Task 25.29

Configure Survivable Remote Site Telephony for Branch 1. Allow maximum of 5 phones and 10 DNs. Ensure that by the time IP Phones register to this SRST device, that the necessary certificate exchange has occurred in order to continue to keep Phones capable of a secure conversation as such.

➔ **This should be self-explanatory from previous examples – for security portion see Task 17.2.**

Task 25.30

When "Message" button is pressed, users should be able to hear the general greeting from Unity.

```
call-manager-fallback
 voicemail <voicemail pilot number>
```

Task 25.31

Configure SRST to provide calling restriction as specified in question #22.

➔ **This should be self-explanatory from previous examples.**

Task 25.32

Configure Branch 1 gateway such that users at Branch 1 can dial 4 digits to reach the HQ.

➔ **This should be self-explanatory from previous examples.**

Task 25.33

Configure AAR between the HQ and Branch 1.

➔ **This should be self-explanatory from previous examples.**

Task 25.34

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 25.35

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 25.36

Configure conference bridge on BR1 router. Use a maximum of 1 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 25.37

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 25.38

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should use the IOS resources and the 6608 resources as backup.

➔ **This should be self-explanatory from previous examples.**

Task 25.39

Configure a Music on Hold server on the Publisher Call Manager. Add another music source which can be found on the C: drive of your Call Manager. Ensure that the default (Sample) audio source is used when a User presses the 'Hold' button on his/her phone. For all other events that require music to be played use the newly added music source.

➔ **Transcoding MOH will only work for Unicast so in the next task change the IP Media Streaming Application. The idea is to verify the transcoder is working – use the following command on the Cat 6K.**

```
sh port voice active transcode
```

Task 25.40

Configure the Call Manager such that HQ phones will receive music using the G711 codec and BR1 phones will receive music using the G729 codec. You cannot use the transcoder to achieve this task.

➔ **This should be self-explanatory from previous examples.**

Task 25.41

Ensure that the HQ and BR1 phones receive multicast music on hold.

➔ **This should be self-explanatory from previous examples.**

Task 25.42

Configure music on hold on the BR2 CME.

➔ **This should be self-explanatory from previous examples.**

Task 25.43

Assume the single cable solution is used, configure the switches to trust the IP phones and not the attached PC.

➔ **This should be self-explanatory from previous examples.**

Task 25.44

Configure the Catalyst 6500 to move VOIP control traffic to the 2nd queue and 1st threshold.

➔ **This should be self-explanatory from previous examples.**

Task 25.45

Configure the Catalyst 6500 and 3550 to map the CoS to DSCP value.

➔ **This should be self-explanatory from previous examples.**

Task 25.46

Configure the Catalyst 6500 to mark all VOIP control traffic from the CallManager as AF31.

➔ **This should be self-explanatory from previous examples.**

Task 25.47

Assume one of Gigabit Ethernet connections is used for the uplink to the distribution switch, configure the Catalyst 6500 such that the tagged packets will have access to PQ in the receive queue.

➔ **10/100 Ports are 2q2t for TX and 1q4T for RX.**

➔ **GE ports are as follows:**

```
PL-VoicePod-6500> (enable) sh port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.

Port  Interface Type Interface Type Policy Source Policy Source
        config        runtime        config        runtime
----- -------------- -------------- ------------- -------------
1/1     vlan-based     vlan-based     COPS          local

Port  TxPort Type  RxPort Type  Trust Type  Trust Type  Def CoS Def CoS
                                config      runtime
----- ------------ ------------ ------------ ------------ ------- -------
1/1    1p2q2t       1p1q4t      untrusted   untrusted     0       0
```


➔ **The RX port type for the GE port is 1p1q4t. Let's see which packets will use the PQ:**

```
PL-VoicePod-6500> (enable) sh qos info config 1p1q4t rx
QoS setting in NVRAM for 1p1q4t receive:
QoS is enabled
Queue and Threshold Mapping for 1p1q4t (rx):
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
1     3         4 6
1     4         7
2     -         5
```

➔ **Let's move packets with COS 3 to use the PQ on the RX ports.**

```
PL-VoicePod-6500> (enable) set qos map 1p1q4t rx 2 1 cos 3
```

➔ **Now verify:**

```
PL-VoicePod-6500> (enable) sh qos info config 1p1q4t rx
QoS setting in NVRAM for 1p1q4t receive:
QoS is enabled
Queue and Threshold Mapping for 1p1q4t (rx):
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2
1     3         4 6
1     4         7
2     -         3 5
```

➔ **We must now trust cos on the uplink port. Note the hardware restriction of not being able to trust-cos directly on the port only applies to the 10/100 ports on the 6348 linecard.**

```
PL-VoicePod-6500> (enable) set port qos 1/1 trust trust-cos
Port 1/1 qos set to trust-cos.
```

➔ **In theory we would have to change the HQ-RTR set the cos values (but remember the HQ-RTR isn't actually plugged onto the GE port).**

```
class-map match-any RTP
 match ip dscp ef
class-map match-any SIG
 match ip dscp af31
!
!
policy-map L3-L2
 class RTP
  set cos 5
 class SIG
  set cos 3

interface FastEthernet0/0.2
 encapsulation dot1Q 220
 ip address 10.2.200.3 255.255.255.0
 ip pim dense-mode
 service-policy output L3-L2
```

Task 25.48

The speed of the PVC between the HQ and Branch 2 is 768 kbps. Configure FRTS and apply to the PVC.

➔ **This should be self-explanatory from previous examples.**

Task 25.49

Configure FRF.12 between the HQ and Branch 2. Configure such that the serialization delay is 10 ms.

➔ **This should be self-explanatory from previous examples.**

Task 25.50

Configure Low Latency Queuing (LLQ) for the HQ and Branch 2. Allocate 33% of the total bandwidth to Priority Queue and 2% as one of the CBWFQ for the control traffic.

➔ **This should be self-explanatory from previous examples.**

Task 25.51

Configure Voice Mail Integration for Call Manager. The information is provided below.

- Pilot Number: 1600
- Unity Port Number: 1601 – 1604
- Set the default password to 54321
- MWI Light – 1998 off
- MWI Light – 1999 on

➔ **This should be self-explanatory from previous examples.**

Task 25.52

Integrate the Branch 2 CME with Unity Express (IP address in **Table 16**)with the following information and provide MWI and voice mail boxes for Phone 1 and 2 in the Branch 2 CME. Also ensure that callers receive the CallerID for whomever left the message.

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

➔ **This should be self-explanatory from previous examples – See Task 15.1 – 3.**

Task 25.53

Create 4 subscribers shown below in Unity using the Bulk ExchangeTool.

➔ **This should be self-explanatory from previous examples.**

Task 25.54

HQ needs Auto Attendant feature. Configure Unity to provide such functionality. Use 1570 as the extension for the call handler. User should hear a greeting saying "Press 1 for directory handler, 2 for HQ phone 1". When caller press 1, send the call to directory handler. When caller press 2, send the call to phone 1 at HQ. Any other entry should take the caller back to the original greeting.

➔ **This should be self-explanatory from previous examples.**

Task 25.55

Configure Unity to be an Inbound and an Outbound Fax Server. Create the necessary VM box for BR1 Phone 2 and ensure that Faxes coming in from the BR1 Gateway arrive in the appropriate user's mailbox. Ensure that Faxes going out to the PSTN number in **Table 18** from the BR1 Gateway arrive and are viewable. Also setup the BR1 Gateway as an OnRamp and an OffRamp Faxing GW. Unity needs to be able to accept in-bound faxes at the mailbox of IncomingFax@voip.lab . Unity also be your DNS server for this task. Refer to **Table 17** of this section for FaxDN ranges. All the files you will need are in BR1 Flash memory.

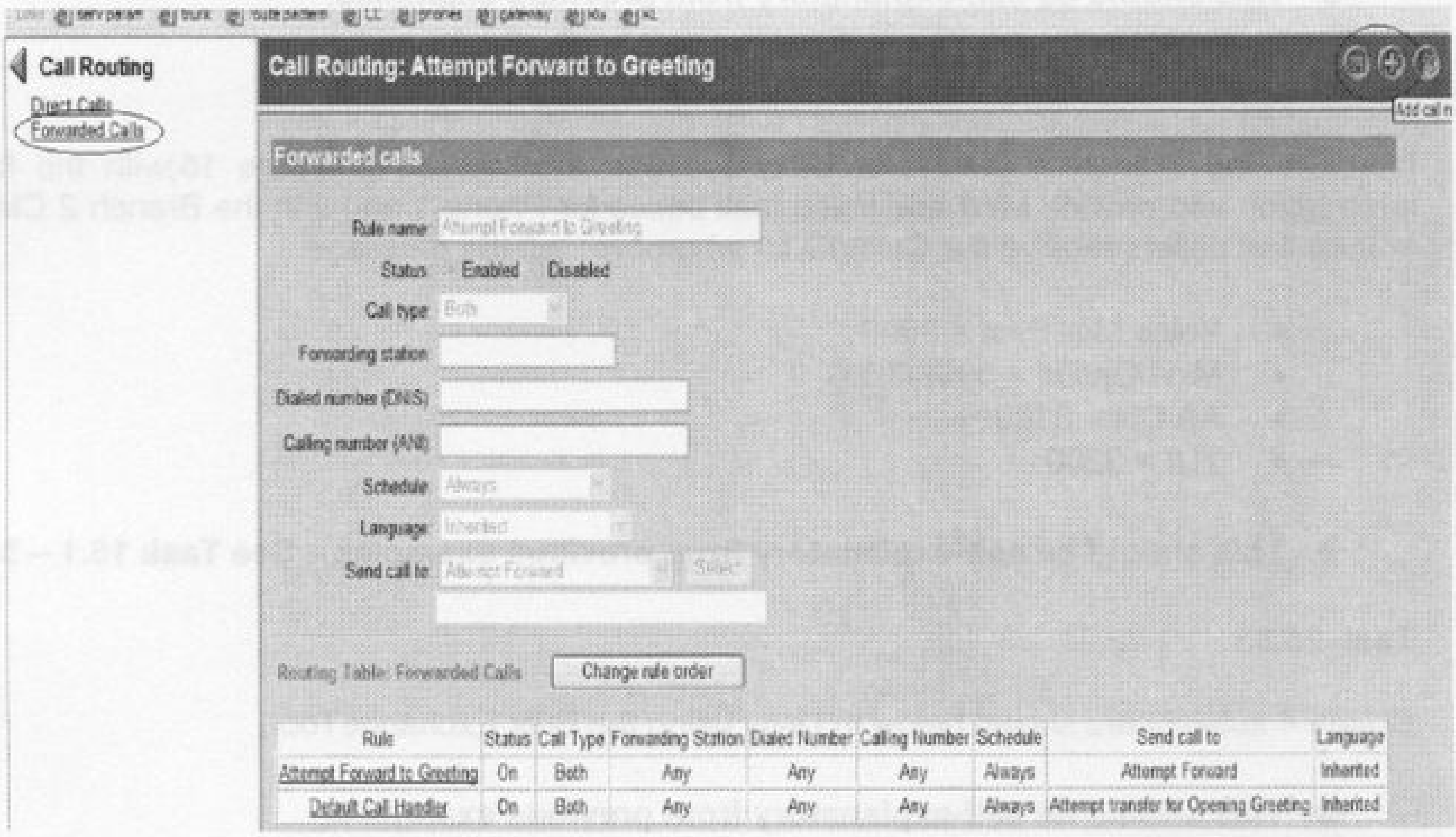
➔ **This should be self-explanatory from previous examples – Starting with Tasks 4.8 and 4.10 and finishing with Tasks 9.9 and 9.10.**

Task 25.56

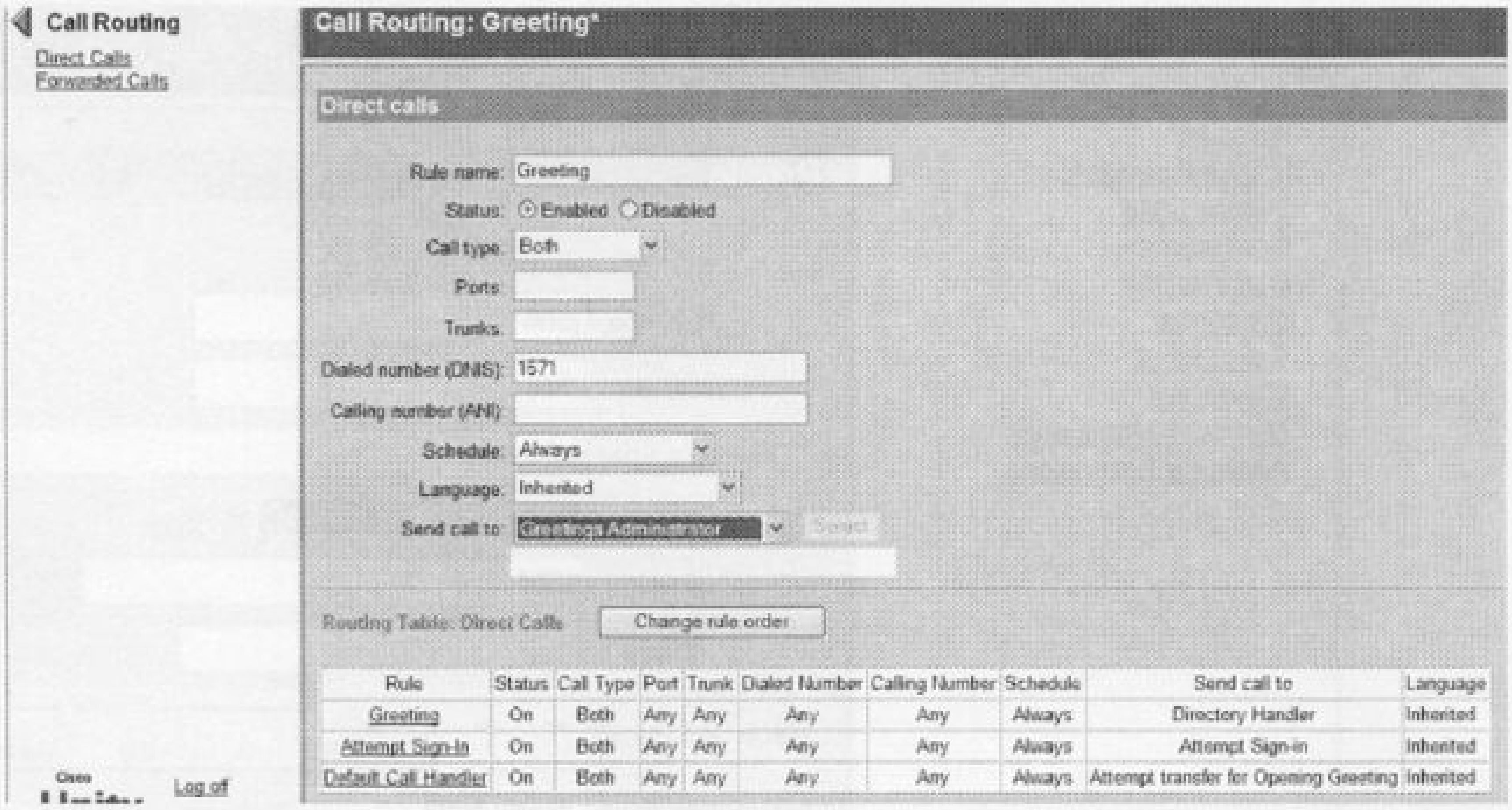
Configure Unity so that only "John Bee" and "Bill Dee" can manage the greeting using TUI and they have access to the call handler (1570) only.

Correction: Configure Unity so that "John Bee" can manage the greeting using TUI and he has access to the call handler (1570) only. John can dial 1571 to manage the greeting.

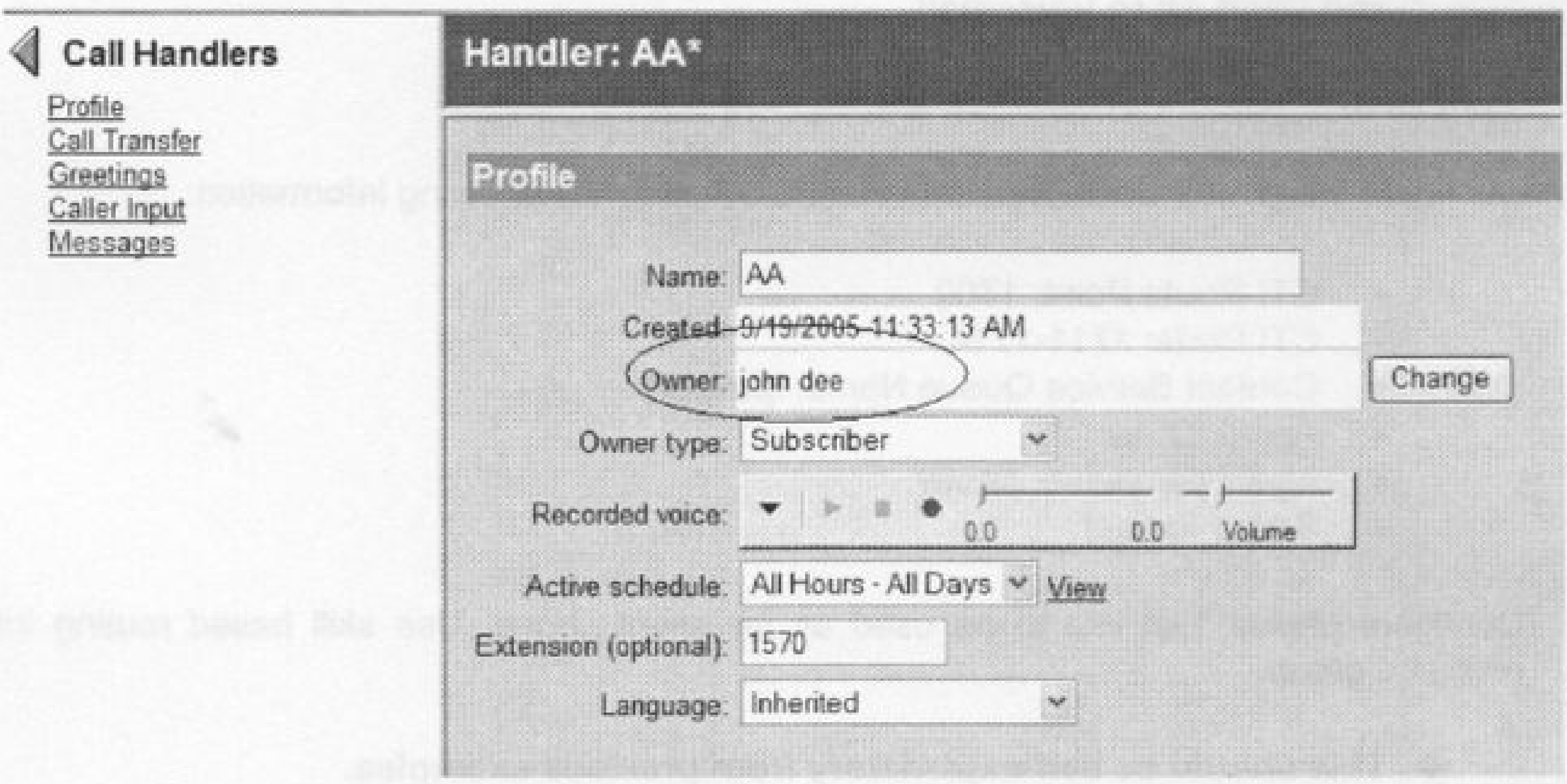
➔ **From the Unity Admin page click on Call Routing – Forward Calls and a new Forwarded Call Routing Rule.**



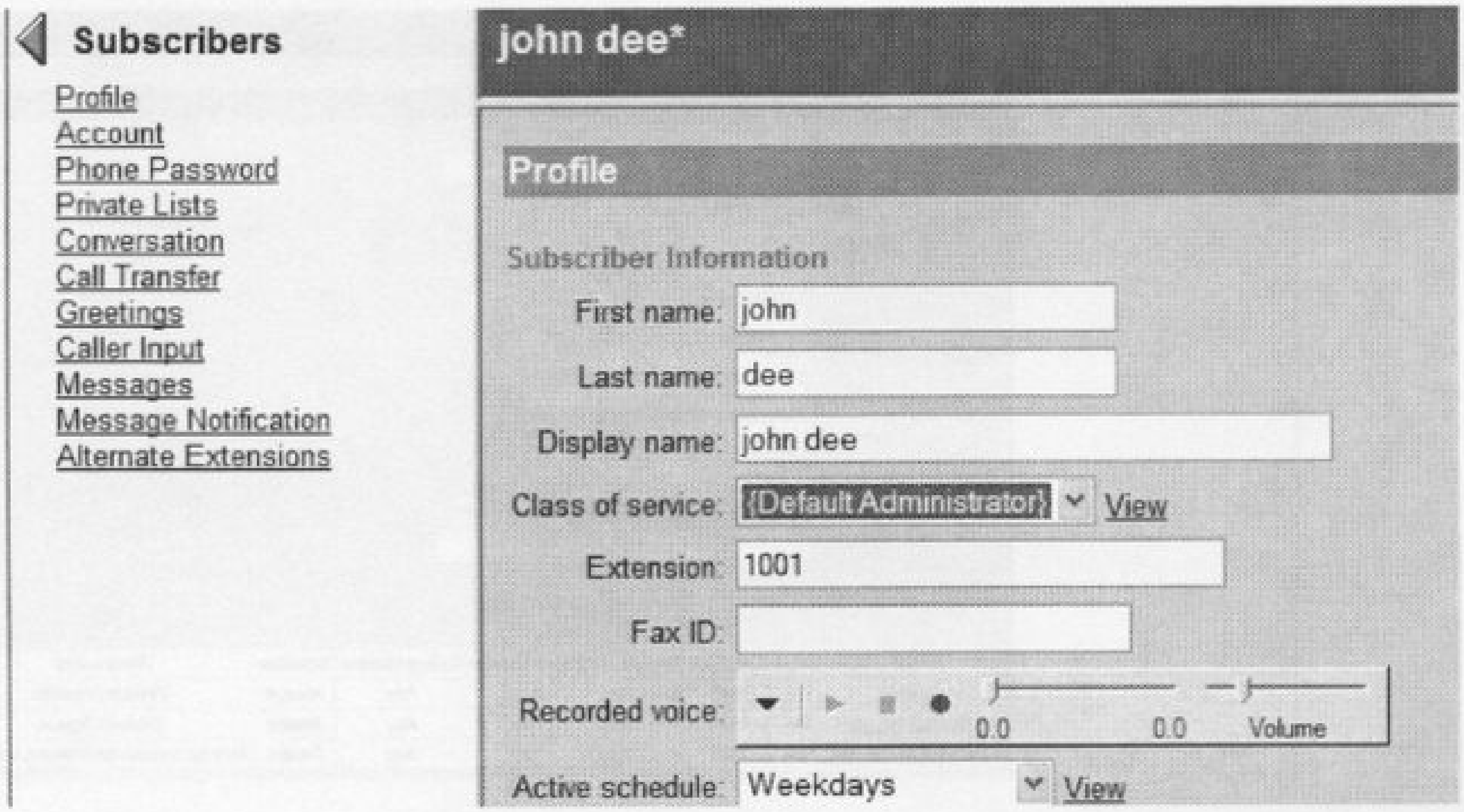
➔ **Define the DNIS and send the call to Greetings Administrator – then Save.**



➔ **Make the subscriber the owner of the Call Handler.**



➔ **Give the Administrator COS to the subscriber.**



➔ **In CCMAdmin create a CTI RP (or phone with dummy MAC Address) with DN=1571 and Cfwd All to Voicemail.**

Task 25.57

Configure Integrated Contact Distribution (ICD) using the following information:

- CTI Route Point: 1700
- CTI Ports: 1711-1714
- Contact Service Queue Name: ipexpert
- Agent ID: tw
- Agent password: jmptw
- Script: icd.aef

Configure phone 1 at HQ to be used as an agent phone. Use skill based routing instead of resource group.

➔ **This should be self-explanatory from previous examples.**

Task 25.58

Configure Extension Mobility as follows:

- Username: ptw
- Password: gjmpt

- HQ Device Profile: 1666
- Branch 2 Device Profile: 3666

➔ **This should be self-explanatory from previous examples – see Task 20.37.**

Task 25.59

Configure Phone 3 at HQ and Phone 2 at Branch 2 to support Extension Mobility. User's calling restriction should be preserved. Long distance call should be routed through 6608. All other calls should be routed through local gateway only.

➔ **This should be self-explanatory from previous examples – see Task 20.38.**

Task 25.60

Create a DN of 1005 for Tech Support. Make HQ phone 3 and BR1 Phone 3 ring simultaneously when this DN is called. You may not use a shared line to accomplish this task. DN 1005 should forward directly to VM anytime outside of normal business hours with no user intervention needed. Check Table 11 for a time schedule. Also, all members of this HuntGroup should get the message in their VM box and see their MWI for any message left for 1005. Finally create a new DN of 1010. When this DN is called, all calls should be directed to the DN of 1005. The call should ring this DN for approximately 2 rings. If for any reason this DN does not answer, the call should then be forwarded to VM if the call originated from an internal number, however if the call originated from an external number, the call should then be forwarded to the PSTN phone at '221-1111'.

➔ **This should be self-explanatory from multiple previous examples – See Task 2.12 to begin, Task 6.7 to continue, and Task 23.26 to complete.**

Task 25.61

Configure FAX Passthrough for 6608, ATA-186, VG248 and Branch 2 gateway.

➔ **This should be self-explanatory from previous examples.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 26: Multiprotocol Challenge I

Estimated Time to Complete: 7 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 26 Multiprotocol Challenge I

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 26 Configuration Tasks

Task 26.1

Configure OSPF as a routing protocol in the network so that all the router interfaces including loopback interfaces are reachable from anywhere in the network. Use area 0.

➔ **This should be self-explanatory from previous examples.**

Task 26.2

Configure each switch port connecting to IP phones and ATA to support both data and voice traffic according to VLAN IDs specified in Table 2.

➔ **This should be self-explanatory from previous examples.**

Task 26.3

Configure each switch port connecting to router/gateway in each site to only allow traffic from data and voice VLANs and not from any other VLANs.

➔ **On Cat6500 in HQ:**

```
clear trunk 2/1 1-119,121-219,221-1005,1025-4094
```

➔ **On Cat3550 in Branch 2:**

```
int fa0/1
switchport trunk allowed vlan remove 2-119,121-219,221-1001,1006-4094
```

Task 26.4

In the HQ site, configure MS DHCP server to enable DHCP service for IP phones to get IP addresses and download phone loads.

➔ **This should be self-explanatory from previous examples.**

Task 26.5

In each branch site, configure each router/gateway to provide DHCP service. Configure the lease time to be 8 hours.

➔ **This should be self-explanatory from previous examples.**

Task 26.6

Configure HQ and BR1 phones with 4 digit extensions as shown in Tables 5 and 6.

➔ **This should be self-explanatory from previous examples.**

Task 26.7

Configure each phone forward calling name and number. When calling PSTN, each phone should forward full DID DN to PSTN phone and calling names.

➔ **This should be self-explanatory from previous examples.**

Task 26.8

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **This should be self-explanatory from previous examples.**

Task 26.9

Configure BR1 as an MGCP gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed. Ensure that RTP packets as well as signaling packets on this GW are encrypted so that a sniffer would not be able to decode the traffic.

➔ **This should be self-explanatory from previous examples – for security portion see Tasks 17.4 – 5.**

Task 26.10

Ensure that the correct transport for DTMF digits is used for the BR1 gateway.

➔ **This should be self-explanatory from previous examples.**

Task 26.11

Configure BR2 as an E1 R2 gateway based on the information in Table 8.

➔ **This should be self-explanatory from previous examples.**

Task 26.12

Configure the E1 R2 such that calls to the PSTN are set up 3 seconds quicker (where possible) than the default. You may assume the maximum length digit string is 11 digits.

➔ **This should be self-explanatory from previous examples.**

Task 26.13

Configure gatekeeper on HQ-RTR with the following information:

Local zone= CCM-GK
domain name = ipexpert.com
[use loopback interface for local zone]
Register CallManager to this zone.

Local zone= BR2-GK
domain name = ipexpert.com
Register the BR2 CME to this zone.

Local zone= VGK
domain name = ipexpert.com
Register the IPIPGW to this zone.

➔ **We are departing from the Gatekeeper model where we route calls through this GK – sending an LRQ out to the PSTN GK (e.g. We will not be using the PSTN-GK in this model).**

➔ **We instead will register CME directly to the GK to its own Local Zone BR2-GK, CCM to its own Local Zone CCM-GK, and an IP to IP Gateway to its own Local Zone VGK (standing for ViaGK) and then route all calls between CCM and CME zones through the VGK zone and thus through the IPIPGW using the GK commands in-via and out-via.**

➔ **For now we will only setup the basic 3 zones and later we will introduce the necessary commands to get the IPIPGW to work for us.**

```
gatekeeper
 zone local VGK ipexpert.com 172.1.100.1
 zone local BR2-GK ipexpert.com
 zone local CCM-GK ipexpert.com
 zone prefix BR2-GK 3...
 no shutdown
```

Task 26.14

Configure a shared line of 3010 on Phone 1 and Phone 2. When a call comes into this number, it should only ring Phone 1, but not Phone 2.

➔ **Configure silent ring on phone 2.**

```
ephone-dn  1  dual-line
 number 3001
!
!
ephone-dn  2  dual-line
 number 3002
!
!
```



```
ephone-dn  3  dual-line
 number 3010
!
!
ephone  1
 mac-address 0011.BBEF.6901
 type 7940
 button  1:1 2:3
!
!
!
ephone  2
 mac-address 0011.BBE0.5775
 type 7940
 button  1:2 2s3
```

Task 26.15

A call from another site supporting only G729 may ring into a BR2 site CME phone, and that phone may be busy and have set to forward busy calls into CUE VM. If this is the case, ensure that G729 call into CUE will not fail.

➔ **We are here setting up an IOS transcoder much the same way that we would if we were going to register it to CallManager – only here we will be registering it to the local CME.**

```
voice-card 0
 dspfarm
 dsp services dspfarm
!
interface FastEthernet0/0.2
 encapsulation dot1Q 210
 ip address 10.1.202.1 255.255.255.0
 no snmp trap link-status
!
sccp local FastEthernet0/0.2
sccp ccm 10.1.202.1 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register mtp00128031d058        ←MAC Add of FastEth 0/0.2
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
```



```
 codec gsmfr
 maximum sessions 6
 associate application SCCP
!
telephony-service
 max-ephones 20
 max-dn 48
 ip source-address 10.1.202.1 port 2000
 sdspfarm units 1
 sdspfarm transcode sessions 6
 sdspfarm tag 1 mtp00128031d058
```

Task 26.16

Calls CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 26.17

Use a CallManager CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **This should be self-explanatory from previous examples – See Task 2.2.**

Task 26.18

In the HQ gatekeeper, allow only two concurrent G.711 calls to the gatekeeper.

➔ **Add the following command inside the gatekeeper.**

```
bandwidth total 256
```

Task 26.19

Configure the following Dial Plan and Classes of Restrictions.

➔ **This should be self-explanatory from previous examples.**

Task 26.20

Configure the international call route pattern to account for dialing # at the end of their number to avoid a long inter-digit timeout. International calls should also complete without dialing # at the end.

➔ **This should be self-explanatory from previous examples.**

Task 26.21

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

➔ **This should be self-explanatory from previous examples.**

Task 26.22

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

➔ **This should be self-explanatory from previous examples.**

Task 26.23

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed out of the HQ-RTR gatekeeper while terminating their RTP streams at the IPIPGW on the HQ-RTR, with the appropriate local gateway acting as backup. Users must be able to dial the BR2 site using access-code of 7 and the users' 4 digit extensions. Seeing as we are using a Gatekeeper for our primary route, calls use H323 signaling end-to-end. Calls will leave using codec G711ulaw but arrive at BR2 CME as G729.

➔ **When implementing a dial plan it is a good idea to look at all the tasks together rather than treat each question as a separate question.**

➔ **Digit Manipulation should be done in the Route List.**

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-GK	GK-TRUNK	1
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1	RG-HQ	PREDOT
	RG-BR1	PREDOT
RL-BR1-HQ	RG-BR1	PREDOT
	RG-HQ	PREDOT
RL-TOLLBY-2-HQ	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-GK-HQ	RG-GK	PREDOT
	RG-HQ	PREDOT + PREFIX 01133132X
RL-GK-BR1	RG-GK	PREDOT
	RG-BR1	PREDOT + PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1
91212.xxxxxxx	PT-BR1-LD	RL-TOLLBY-2-HQ
9.011! 9.011!#	PT-HQ-INTERNATIONAL	RL-HQ
9.011! 9.011!#	PT-BR1-INTERNATIONAL	RL-HQ-BR1
7.3xxx	PT-HQ-911	RL-GK-HQ
7.3xxx	PT-BR1-911	RL-GK-BR1

➔ **On HQ-RTR:**

```
voice-card 2
 no dspfarm
 dsp services dspfarm
!
sccp local vlan210
sccp ccm 10.1.201.1 identifier 1
sccp ip precedence 3
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCODER
 keepalive retries 5
 switchover method immediate
 switchback interval 15
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g729r8
 maximum sessions 2
 associate application SCCP
 no shutdown
!
call-manager-fallback
 ip source-address 10.1.201.1 port 2000
 max-ephones 10
 max-dn 10
 sdspfarm units 1
 sdspfarm transcode sessions 2
!
voice service voip
 allow-connections h323 to h323
!
interface Loopback0
 ip address 172.1.100.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id VGK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip bind srcaddr 172.1.100.1
!
dial-peer voice 10 voip
 destination-pattern [12]...
 codec g711ulaw
 session target ras
```



```
!
dial-peer voice 11 voip
 destination-pattern 3...
 session target ras
!
gateway
!
gatekeeper
 zone local VGK ipexpert.com 172.1.100.1
 zone local BR2-GK ipexpert.com invia VGK outvia VGK enable-intrazone
 zone local CCM-GK ipexpert.com
 zone prefix BR2-GK 3...
 no shutdown
```

➔ **On BR2:**

```
interface Loopback0
 ip address 172.1.102.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id BR2-GK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id CME
 h323-gateway voip bind srcaddr 172.1.102.1
!
gateway
!
dial-peer voice 10 voip
 incoming called-number [12]...
```

➔ **Place the call and Verify on HQ-RTR.**

```
P1-HQ-RTR#debug gatek main 10
P1-HQ-RTR#
May 22 19:43:38.608: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.320: gk_process: got a TIMER event

May 22 19:43:39.320: gk_handle_timers

May 22 19:43:39.320: gk_handle_timers: managed timer expired 0x45AAE620

P1-HQ-RTR#
May 22 19:43:39.880: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.880: gk_rassrv_arq: arqp=0x45EEBE7C, crv=0x4, answerCall=0
May 22 19:43:39.880: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:39.880: gk_dns_query: No Name servers
May 22 19:43:39.880: rassrv_get_addrinfo: (3004) Tech-prefix match failed.
May 22 19:43:39.880: rassrv_get_addrinfo: (3004) Matched zone prefix 3 and remainder 004
May 22 19:43:39.880: gk_rassrv_get_ingress_network: returning default ingress network = 1
May 22 19:43:39.880: rassrv_arq_select_viazone: about to check the source side,
src_zonep=0x476A44B0
```

May 22 19:43:39.880: rassrv_arq_select_viazone: matched zone is CCM-GK, and z_invianamelen=0
May 22 19:43:39.880: rassrv_arq_select_viazone: about to check the destination side, dst_zonep=0x45E91474
May 22 19:43:39.880: rassrv_arq_select_viazone: matched zone is BR2-GK, and z_outvianamelen=3
May 22 19:43:39.880: rassrv_arq_select_viazone and z_outvianamep=VGK
May 22 1
P1-HQ-RTR#9:43:39.880: rassrv_arq_select_viazone: Received ARQ for a zone (BR2-GK) that has an outviazone (VGK) specified. Pick an IP-IP gateway in that viazone.
May 22 19:43:39.880: gk_gw_select_ipipgw: zonep: 0x4724ED54, tpp: 0x0, current_endpt: 1
May 22 19:43:39.880: gk_gw_select_ipipgw: Selecting any IPIPGW. qelemp.head=0x472C0BB0, use_count=1, current_endpt=1
May 22 19:43:39.880: gk_gw_select_ipipgw: Gateway selection will start at the top of the linked list. use_count=1, current_endpt=0
May 22 19:43:39.880: gk_gw_select_ipipgw: qelemp=0x472C0BB0, loop_count=0
May 22 19:43:39.880: gk_gw_select_ipipgw: Examining tgwp 0x472B0E60, g_supp_prots: 0x50 qelemp: 0x472C0BB0, loop_count: 1
May 22 19:43:39.880: gk_gw_select_ipipgw: Found an IPIPGW. tgwp: 0x472B0E60, endptsigIP: 172.1.100.1, endptrasIP: 172.1.100.1, zone: VGK
May 22 19:43:39.884: gk_gw_select_ipipgw: Selected an IPIPGW.
May 22 19:43:39.884: rassrv_get_addrinfo: (3004) successfully resolved IPIPGW and returning with return code 0
May 22 19:43:39.904: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.904: gk_rassrv_arq: arqp=0x45EAD3AC, crv=0x33, answerCall=1
May 22 19:43:39.904: gk_rassrv_dep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:39.920: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.920: gk_rassrv_arq: arqp=0x45E9B960, crv=0x34, answerCall=0
May 22 19:43:39.920: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:39.920: gk_dns_query: No Name servers
May 22 19:43:39.920: rassrv_get_addrinfo: (3004) Tech-prefix match failed.
May 22 19:43:39.920: rassrv_get_addrinfo: (3004) Matched zone prefix 3 and remainder 004
May 22 19:43:39.920: gk_rassrv_get_ingress_network: ARQ non-std ingress network = 2
May 22 19:43:39.920: rassrv_arq_select_viazone: about to check the destination side, dst_zonep=0x45E91474
May 22 19:43:39.924: rassrv_arq_select_viazone: matched zone is BR2-GK, and z_outvianamelen=3
May 22 19:43:39.924: rassrv_arq_select_viazone and z_outvianamep=VGK
May 22 19:43:39.924: rassrv_arq_select_viazone: Received ARQ for a zone (BR2-GK) that has an outviazone (VGK) specified, but I am that viazone. Continue normal ARQ processing
May 22 19:43:39.924: gk_zone_get_proxy_usage: local zone= BR2-GK, remote zone= VGK, call direction= 0, eptype= 2050 be_entry= 0
May 22 19:43:39.924: gk_zone_get_proxy_usage: returns proxied = 0
May 22 19:43:39.924: gk_gw_select_px: Source and destination endpoints in different local zones
May 22 19:43:39.924: gk_zone_get_proxy_usage: local zone= VGK, remote zone= BR2-GK, call direction= 1, eptype= 2114 be_entry= 0
May 22 19:43:39.924: gk_zone_get_proxy_usage: returns proxied = 0
May 22 19:43:39.924: rassrv_get_addrinfo: (3004) successfully resolved the alias locally and returning with 0x0
May 22 19:43:39.924: rassrv_get_addrinfo: We know this alias

May 22 19:43:39.952: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.952: gk_rassrv_arq: arqp=0x45E9B960, crv=0x3A, answerCall=1
May 22 19:43:39.952: gk_rassrv_dep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:41.264: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:41.268: gk_rassrv_irr: irrp=0x45E9B960, from 172.1.102.1:58652


```
May 22 19:43:41.404: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:41.404: gk_rassrv_irr: irrp=0x45EA1C30, from 172.1.100.1:53849
May 22 19:43:41.412: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:41.412: gk_rassrv_irr: irrp=0x45EA1C30, from 172.1.100.1:53849
```

```
P1-HQ-RTR#sh voip rtp connections
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP       RemoteIP
1   72      73         18336    24618  172.1.100.1   10.1.200.21
2   73      72         19556    17460  172.1.100.1   172.1.102.1
3   74      75         17516    2000   10.1.200.3    10.1.200.3
4   76      75         18502    2000   10.1.200.3    10.1.200.3
Found 4 active RTP connections
```

```
P1-HQ-RTR#sh sdspfarm sessions sum

max-mtps:1, max-streams:4, alloc-streams:4, act-streams:2
 ID  MTP  State   CallID confID Usage                Codec/Duration
==== ==== ======= ====== ====== ==================== ==============
1    1    IDLE    -1     0                          G711Ulaw64k /20ms
2    1    IDLE    -1     0                          G711Ulaw64k /20ms
3    1    START   73     3      Ip-Ip               G729 /20ms
4    1    START   72     3      Ip-Ip               G711Ulaw64k /20ms
```

Task 26.24

In the Branch 2 site, use an access-code of 7 and the users' 4 digit extensions to call other sites (HQ and BR1). Primary route must be via an IPIPGW on the BR1 router inbound as a SIP call, outbound to CCM as H323. If the IPIPGW were to fail for some reason, try a direct call to both CallManagers using H323. Finally if this method were to fail then you must send the calls out the local PSTN trunk. Accomplish this with the **minimum** number of dial-peers. Use the local gateway for all other PSTN calls.

➔ **On BR1 Router:**

```
voice service voip
 allow-connections sip to h323
!
voice-card 2
 no dspfarm
 dsp services dspfarm
!
sccp local vlan210
sccp ccm 10.1.201.1 identifier 1
sccp ip precedence 3
sccp
!
sccp ccm group 1
```



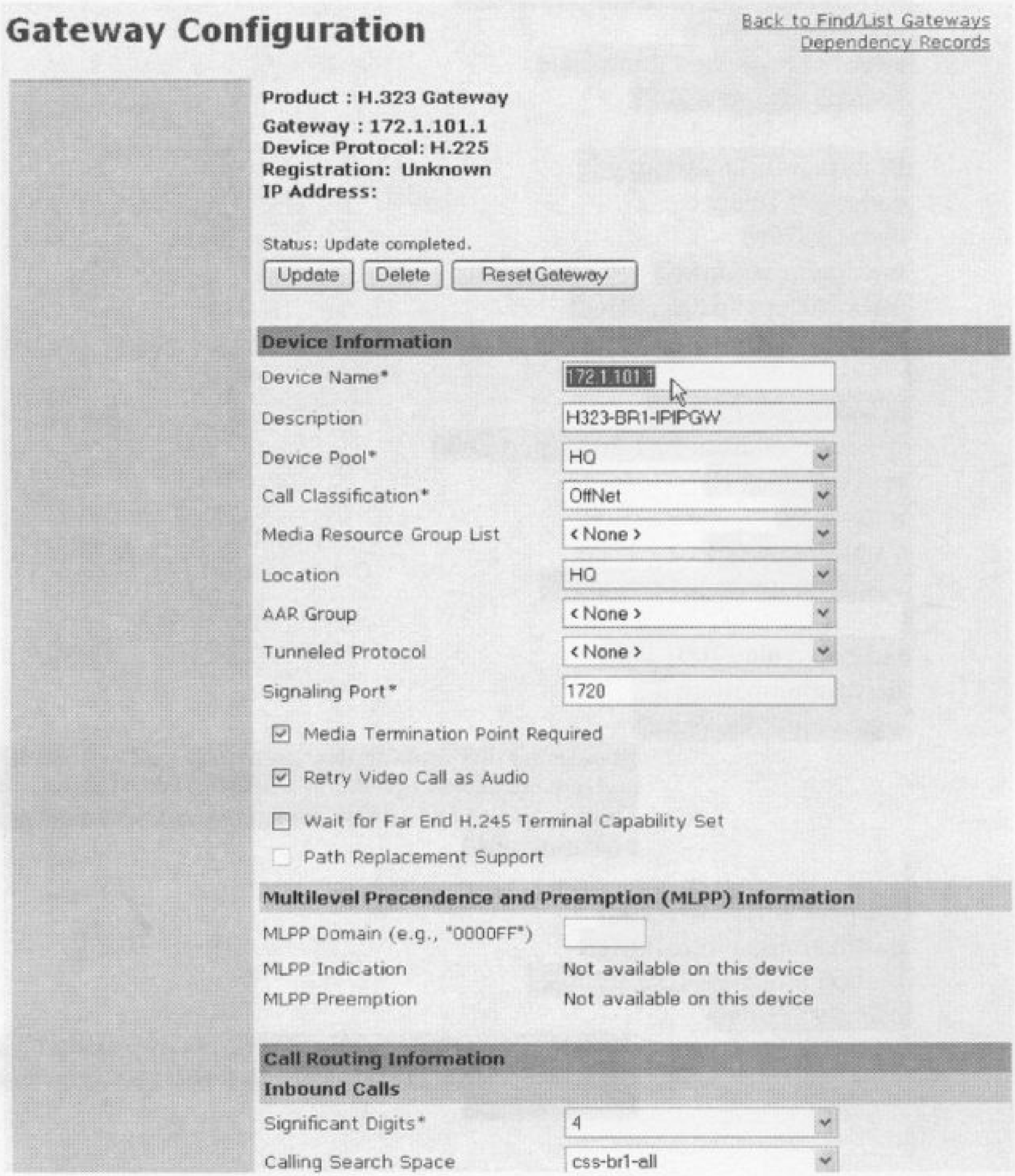
```
 associate ccm 1 priority 1
 associate profile 1 register XCODER
 keepalive retries 5
 switchover method immediate
 switchback interval 15
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g729r8
 maximum sessions 2
 associate application SCCP
 no shutdown
!
call-manager-fallback
 ip source-address 10.1.201.1 port 2000
 max-ephones 10
 max-dn 10
 sdspfarm units 1
 sdspfarm transcode sessions 2
!
dial-peer voice 1001 voip
 destination-pattern 3...
 session protocol sipv2
```

(Remember that while destination-pattern cmd matches DNIS on an Outbound Call Leg – that it also matches ANI on an Inbound Call Leg – so on an IPIPGW config – we can minimize our dial-peers with such)

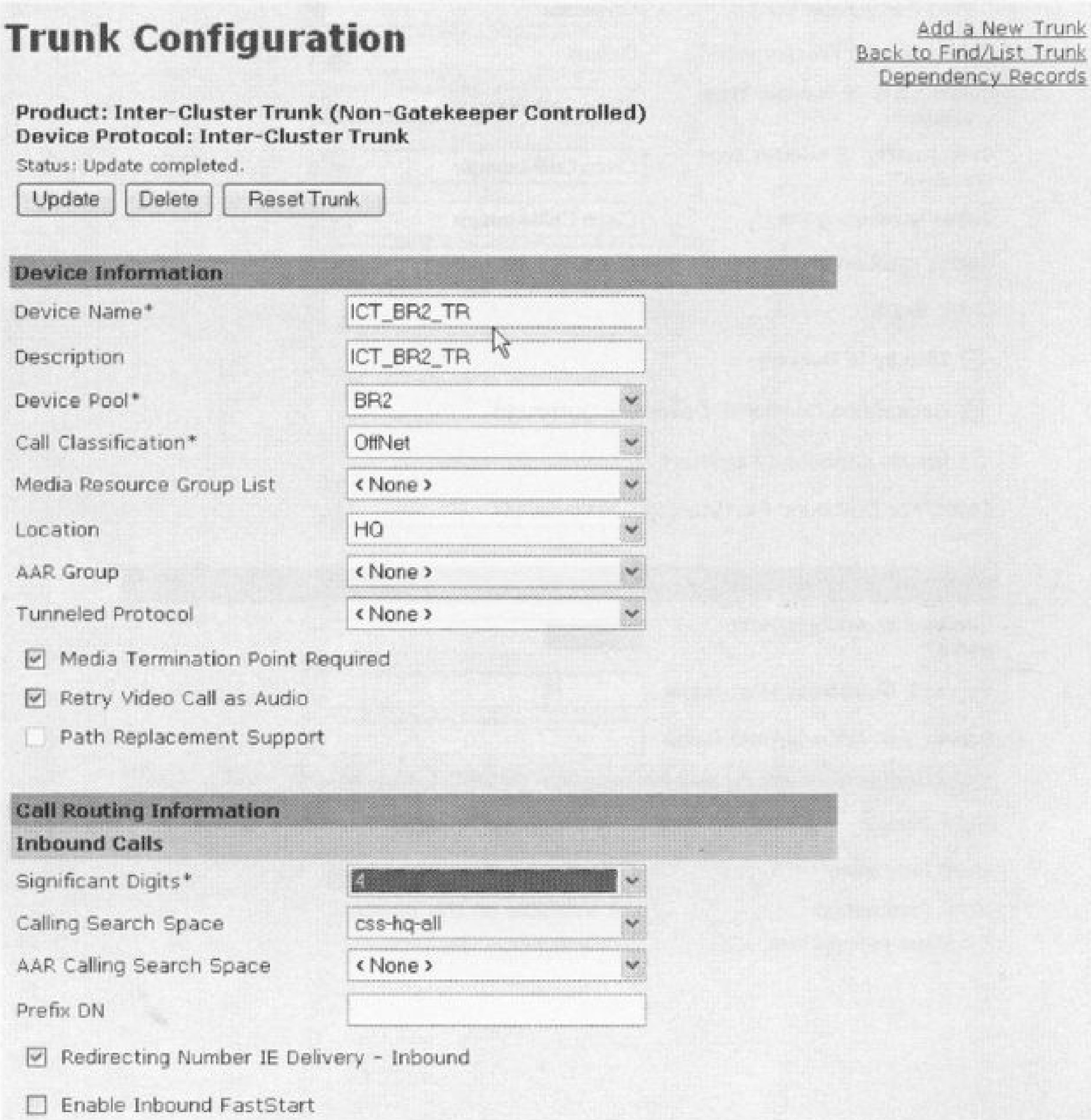
```
!
dial-peer voice 1002 voip
 destination-pattern 7[12]...
 session target ipv4:10.1.200.21
 codec g711ulaw
```

(We will strip the 7 off in the CCM H323 GW with the Significant Digits command in the Inbound Call Routing Rules section of the H323 GW Page)

➔ **Add the BR1 IPIPGW as a H323 GW in CCM for the first inbound route.**



➔ Add CME as a H323-nonGKcontrolled-ICT in CCM as the second inbound route.



Outbound Calls

Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Caller ID DN	

☑ Display IE Delivery

☑ Redirecting Number IE Delivery - Outbound

☐ Enable Outbound FastStart

Codec For Outbound FastStart*	G711 u-law 64K

Remote Cisco CallManager Information

Server 1 IP Address/Host Name*	10.1.202.1
Server 2 IP Address/Host Name	
Server 3 IP Address/Host Name	

Multilevel Precendence and Preemption (MLPP) Information

MLPP Domain	(e.g., "0000FF")
MLPP Indication	Default
MLPP Preemption	Not available on this device

* indicates required item

➔ **On BR2 Router - Add the following dial-peers:**

```
dial-peer voice 1000 voip
 destination-pattern 7[12]...
 session target ipv4:172.1.101.1
 session protocol sipv2
 preference 0
 no huntstop
!
dial-peer voice 1001 voip
 destination-pattern 7[12]...
 session target ipv4:10.1.200.21
 dtmf-relay h245-alphanumeric
 preference 1
 no huntstop
!
dial-peer voice 1001 voip
 destination-pattern 7[12]...
 session target ipv4:10.1.200.20
 dtmf-relay h245-alphanumeric
 preference 2
 no huntstop
!
translation-rule 1
 Rule 1 71... 12122211
 Rule 2 72... 16175212
!
dial-peer voice 1002 pots
 destination-pattern 7[12]...
 preference 3
 port 0/0/0:0
 translate-outgoing called 1
```

Task 26.25

Enable DID for PSTN users dialing into the CM/CME (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits.

➔ **This should be self-explanatory from previous examples.**

Task 26.26

Configure in Call Manager such that if there is not enough bandwidth to make calls to and from Branch 1, use PSTN to complete the calls.

➔ **This should be self-explanatory from previous examples.**

Task 26.27

Create a circular hunt group for Support with a DN of 3210 at BR2 between phones 1 and 3, and ensure that those phones can login-to and out-of the hunt group in order to receive calls. Allow the call to ring at around 3 times before searching for the next member.

➔ **This should be self-explanatory from previous examples – See Task 14.7.**

Task 26.28

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 26.29

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 26.30

Configure conference bridge on BR1 router. Use a maximum of 1 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 26.31

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 26.32

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should load share between the IOS resources and the 6608 resources.

➔ **This should be self-explanatory from previous examples.**

Task 26.33

Configure G.711 unicast MoH for HQ. Configure G729 multicast for Branch 1. Configure MoH for the Branch 1 so that the gateway provides MoH instead of CM.

➔ **The MRG for HQ should NOT have the Enable Multicast checkbox enabled.**

➔ **Max Hops on the Server should be set to 1.**

➔ **The SRST gateway should have the "multicast moh" command configured.**

Task 26.34

In the HQ site Cat 6500, Configure on the HQ router to set the CoS of voice RTP to 5 and CoS of voice control traffic to 3 on traffic sent to Catalyst 6500 in voice VLAN. Configure the switch ports connected to IP phones not to trust COS marking from PCs connected to the phones.

➔ **On the HQ-RTR:**

```
class-map match-any RTP
 match ip dscp ef
class-map match-any SIG
 match ip dscp af31
!
!
policy-map L3-L2
 class RTP
  set cos 5
 class SIG
  set cos 3

interface FastEthernet0/0.2
 encapsulation dot1Q 220
 ip address 10.2.200.3 255.255.255.0
 ip pim dense-mode
 service-policy output L3-L2
```

➔ **On the 6500:**

```
set qos enable

set port qos 2/7-8 vlan-based
set port qos 2/7-8 trust-ext untrusted
set qos acl ip POD12_IP-PHONES trust-cos ip any any
commit qos acl POD12_IP-PHONES
set qos acl map POD12_IP-PHONES 220
```

Task 26.35

In the Branch 2 Cat 3550, configure the port connected to IP phones not to trust CoS marking from PCs connected to the phones.

```
int range fa0/23 - 24
switchport priority extend cos 0
```


Task 26.36

Assume that ATA does not mark voice RTP packets correctly to CoS of 5. Configure the switch port connected to ATA to correct this problem.

```
set port qos 2/27 port-based
set qos acl ip POD12_ATA dscp 26 tcp any range 2000 2002 any
commit qos acl POD12_ATA
set qos acl map POD12_ATA 2/42
```

Task 26.37

Configure MLPPP between HQ Site and Branch 2. Assume the PVC speed between HQ and BR2 is 256Kbps.

➔ **This should be self-explanatory from previous examples.**

Task 26.38

From HQ Site to Branch 2, reserve 128 kbps for voice RTP traffic on a priority queue and reserve minimum guaranteed bandwidth of 8kbps for voice control traffic.

➔ **This should be self-explanatory from previous examples.**

Task 26.39

From Branch 2 to HQ Site, reserve 128 kbps for voice RTP traffic on a priority queue and reserve minimum guaranteed bandwidth of 8kbps for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queueing.

➔ **This should be self-explanatory from previous examples.**

Task 26.40

From the HQ site to the BR1 site, reserve 50% of bandwidth for voice RTP traffic on a high priority queue and 5 % of bandwidth for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queueing. The link speed between HQ and BR1 is 1544Kbps.

➔ **This should be self-explanatory from previous examples.**

Task 26.41

Setup Unity voice mail boxes for Phone 1 in HQ, and Branch 1. Ensure you can call and reach mailboxes as well as leave messages. Ensure you can light the MWI light.

- Pilot Number: 1600
- Unity Port Number: 1601 – 1604
- Set the default password to 54321
- MWI Light – 1998 off
- MWI Light – 1999 on

➔ **This should be self-explanatory from previous examples.**

Task 26.42

Integrate the Branch 2 CME with Unity Express with the following information (Table 16).

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

Provide voice mail boxes for Phone 1 and Phone 3 at Branch 2.

➔ **This should be self-explanatory from previous examples – See Task 15.1.**

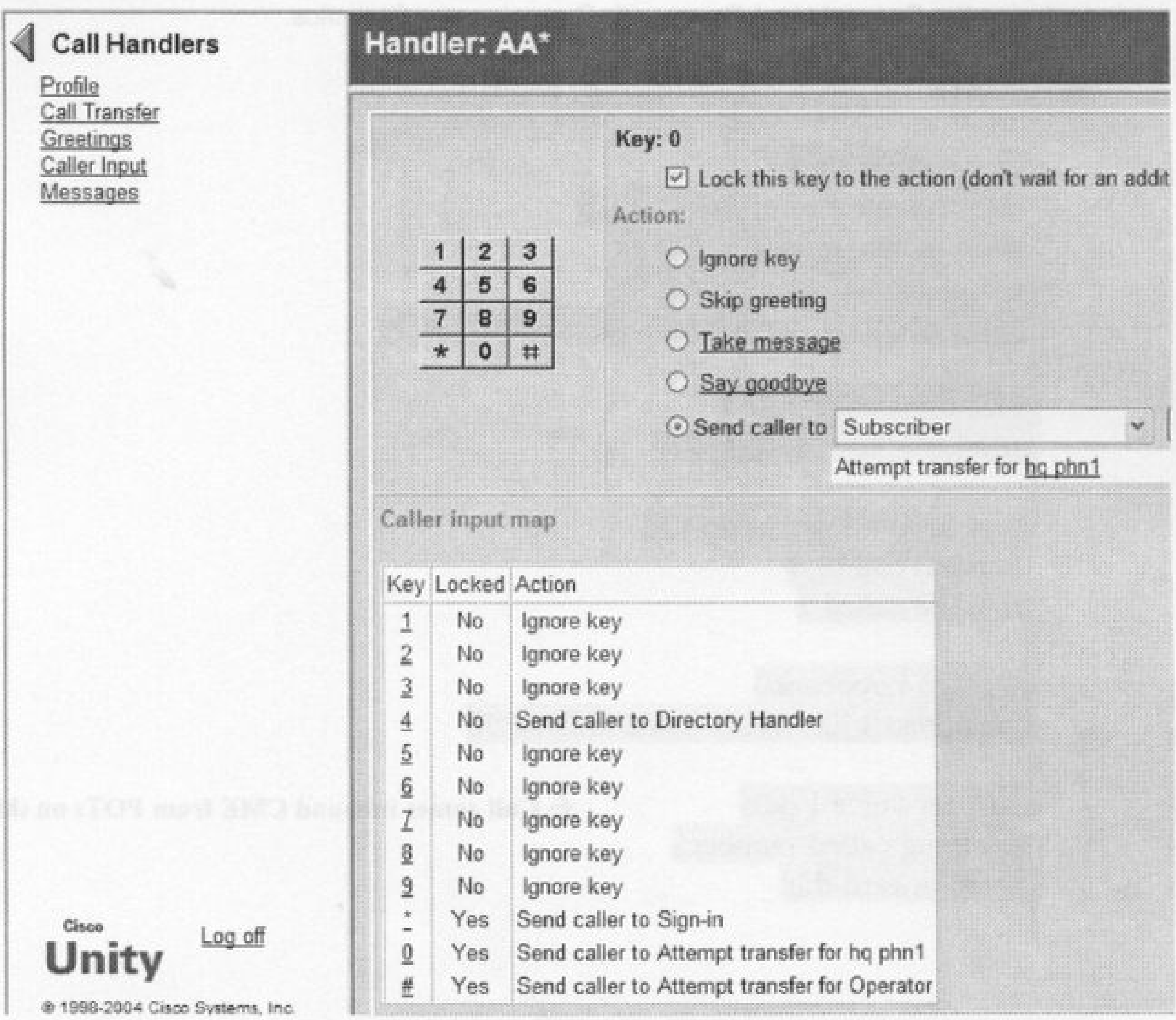
Task 26.43

When dialing 1570, configure Unity and CM such that a caller hears a custom greeting. After hearing the greeting, if a caller dials 0, the call should be transferred to HQ Phone 1 (1001).

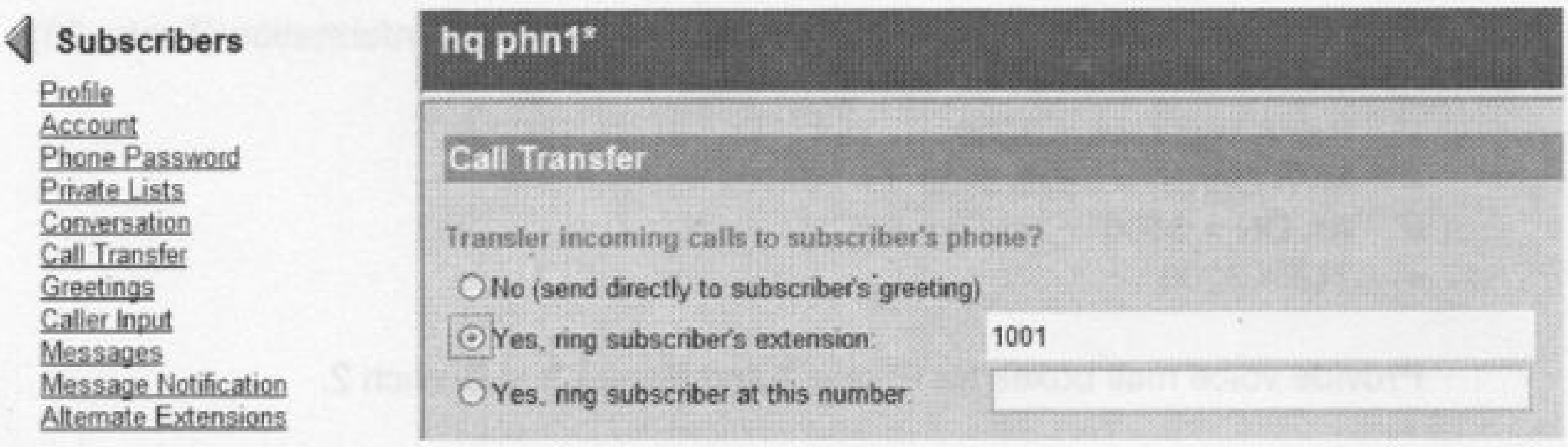
➔ **Create a Call handler in Unity with DN=1570.**

➔ **Record a Greeting saying "Welcome to IPExpert – press 0 to be transferred".**

➔ **On Caller Input, for 0 transfer call to HQ Phone 1.**



➔ **On the subscriber ring extension.**



Task 26.44

Ensure that when users listen to their voicemail messages in CUE, that they hear the ANI announced of the phone who left them the message.

➔ **This should be self-explanatory from previous examples – See Task 15.3.**

Task 26.45

Create an Auto-Attendant application using CUE. The incoming DN will be 3313213000 or 3000 and the AA should give the option to dial-by-name by pressing 1, dial-by-extension at any time during the prompt, and be transferred into a B-ACD TCL Queue at DN 3500 by pressing 2 and be connected to the Support Hunt Group with Queueing and Statistics.

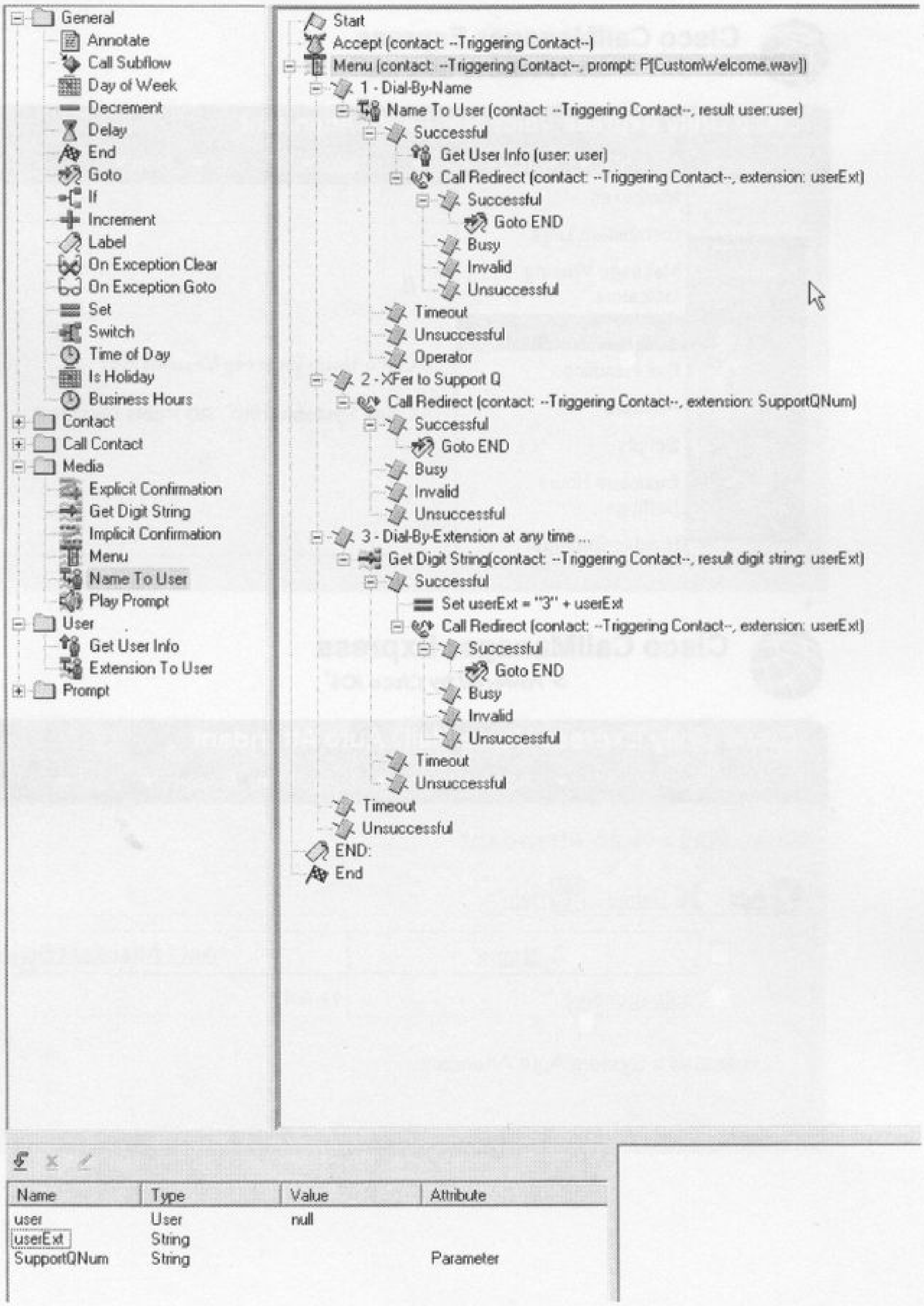
➔ **On BR2:**

```
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 supplementary-service h450.12 advertise-only
!
voice translation-rule 1
 rule 1 /^331321\(3...\)/ /\1/
!
voice translation-profile VM
 translate calling 1
 translate called 1
!
interface Loopback0
 ip address 172.1.102.1 255.255.255.255
!
dial-peer voice 1 pots          ← Call comes inbound CME from POTs on this Dial-Peer
 incoming called-number .
 direct-inward-dial
!
```

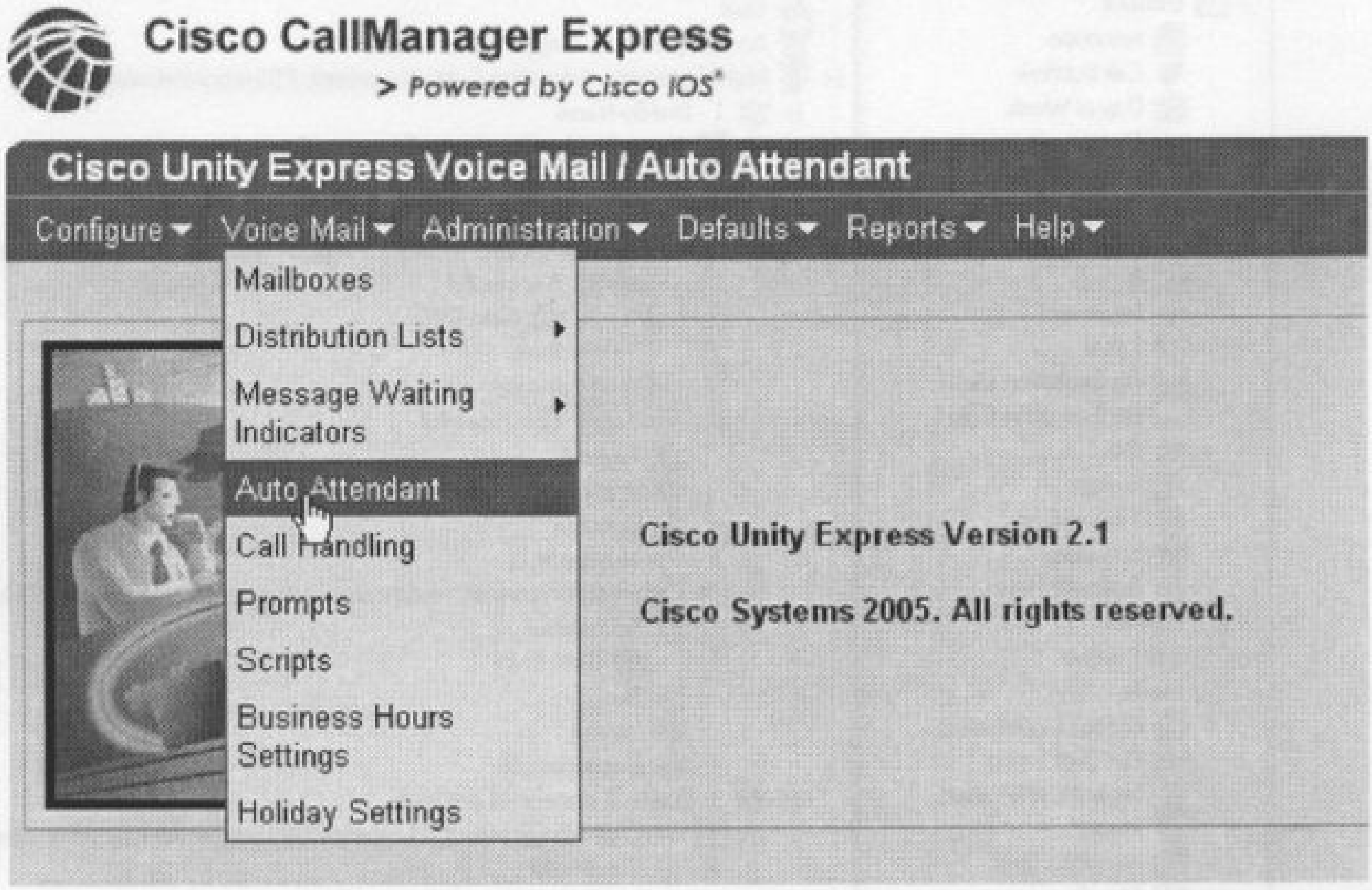
```
dial-peer voice 3601 voip                  ← Call goes outbound to CUE on this Dial-Peer
 translation-profile outgoing VM           ← When script transfers call – call comes back inbound to
 destination-pattern                         router from CUE on this Dial-Peer
3313213[126]00
 incoming called-number .
 session protocol sipv2
 session target ipv4:10.1.202.2
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 3500 voip                  ← Call then routes outbound via this Dial-Peer to DN 3500
 destination-pattern 3500                    – only this dial-peer points to our own Loopback so .......
 session target ipv4:172.1.102.1
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
!
dial-peer voice 3501 voip                  ← Finally call comes back into router via its own loopback
 service aa                                  (even though it never really left the router) and is finally
 incoming called-number 3500                 handed off to the AA service application
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
!
!
application
 service queue flash:app-b-acd-2.1.0.0.tcl
  param queue-len 20
  param queue-manager-debugs 1
  param aa-hunt2 3210
  param number-of-hunt-grps 1
 !
 service aa flash:app-b-acd-aa-2.1.0.0.tcl
  paramspace english index 1
  param number-of-hunt-grps 1
  param handoff-string aa
  param dial-by-extension-option 3
  param operator 3001
  paramspace english language en
  param max-time-vm-retry 2
  param aa-pilot 3500
  param max-extension-length 4
  paramspace english location flash:
  param second-greeting-time 30
  param welcome-prompt en_bacd_welcome.au
```

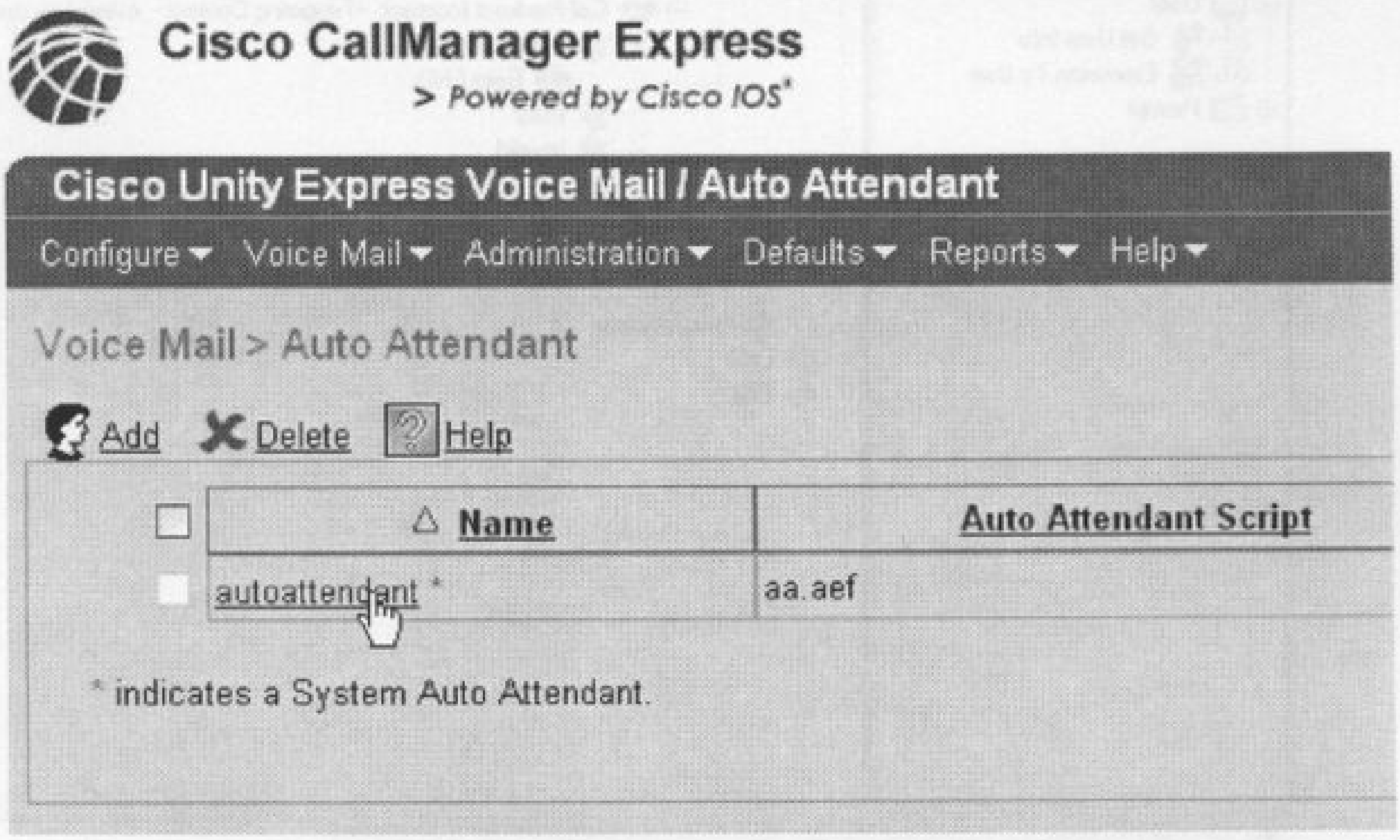
```
 param call-retry-timer 15
 paramspace english prefix en
 param max-time-call-retry 45
 param voice-mail 3215
 param service-name queue
 !
!
ephone-hunt 1 peer
 pilot 3210
 list 3001, 3003
 timeout 12
 statistics collect
```

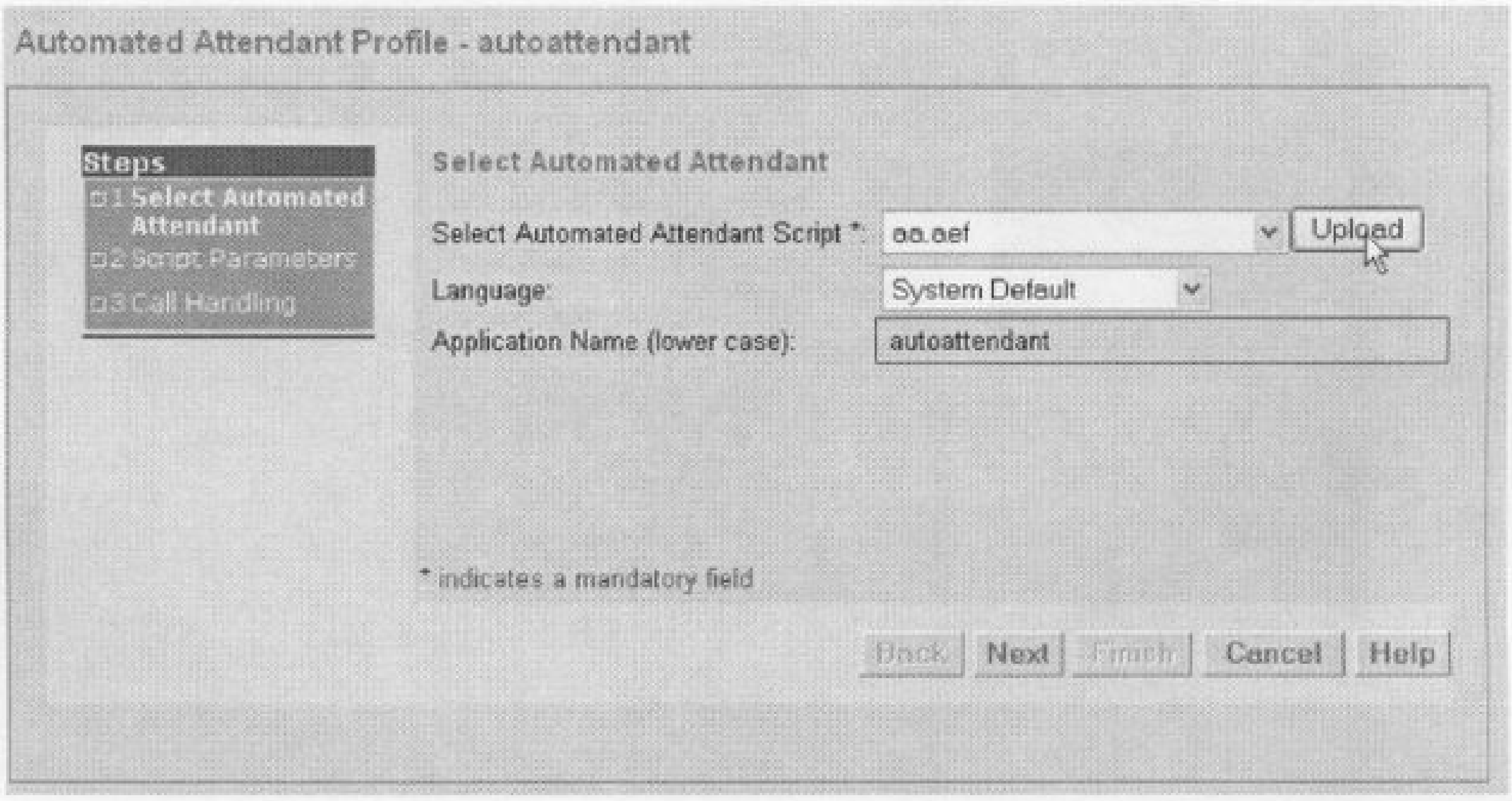

➔ **Using the CUE Editor:**

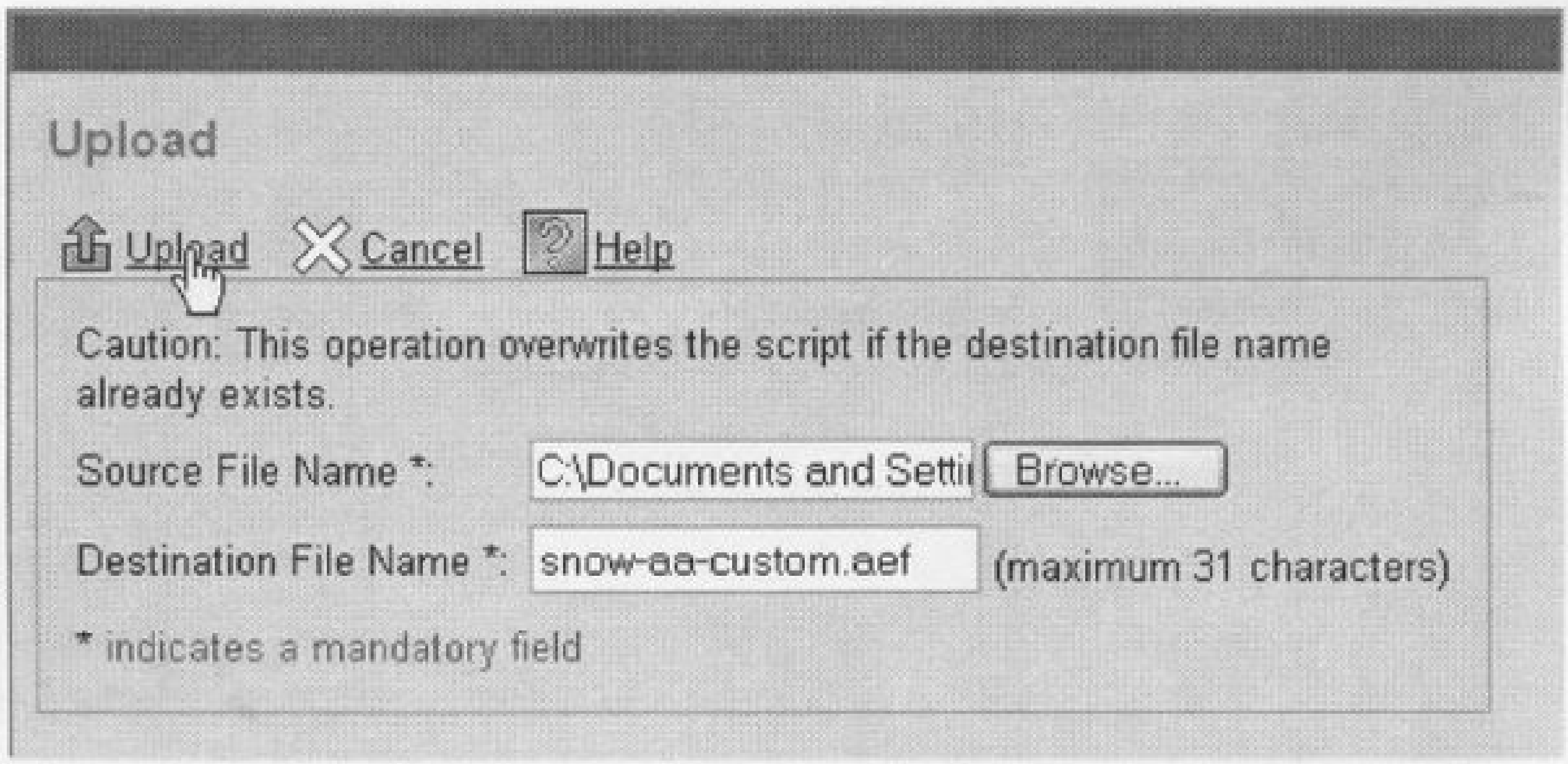


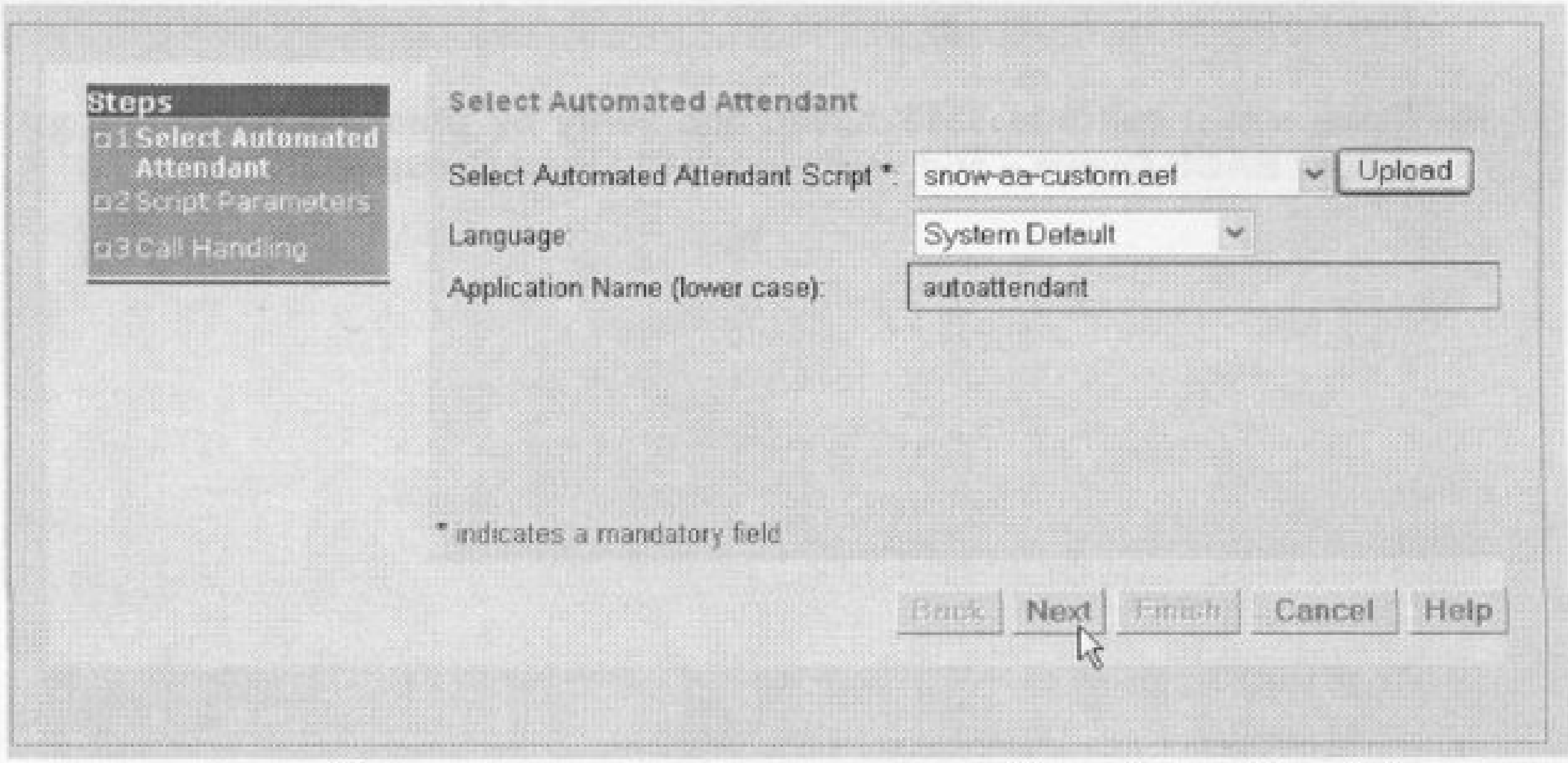
➔ **From Internet Explorer browse to http://10.1.202.2/Web.**

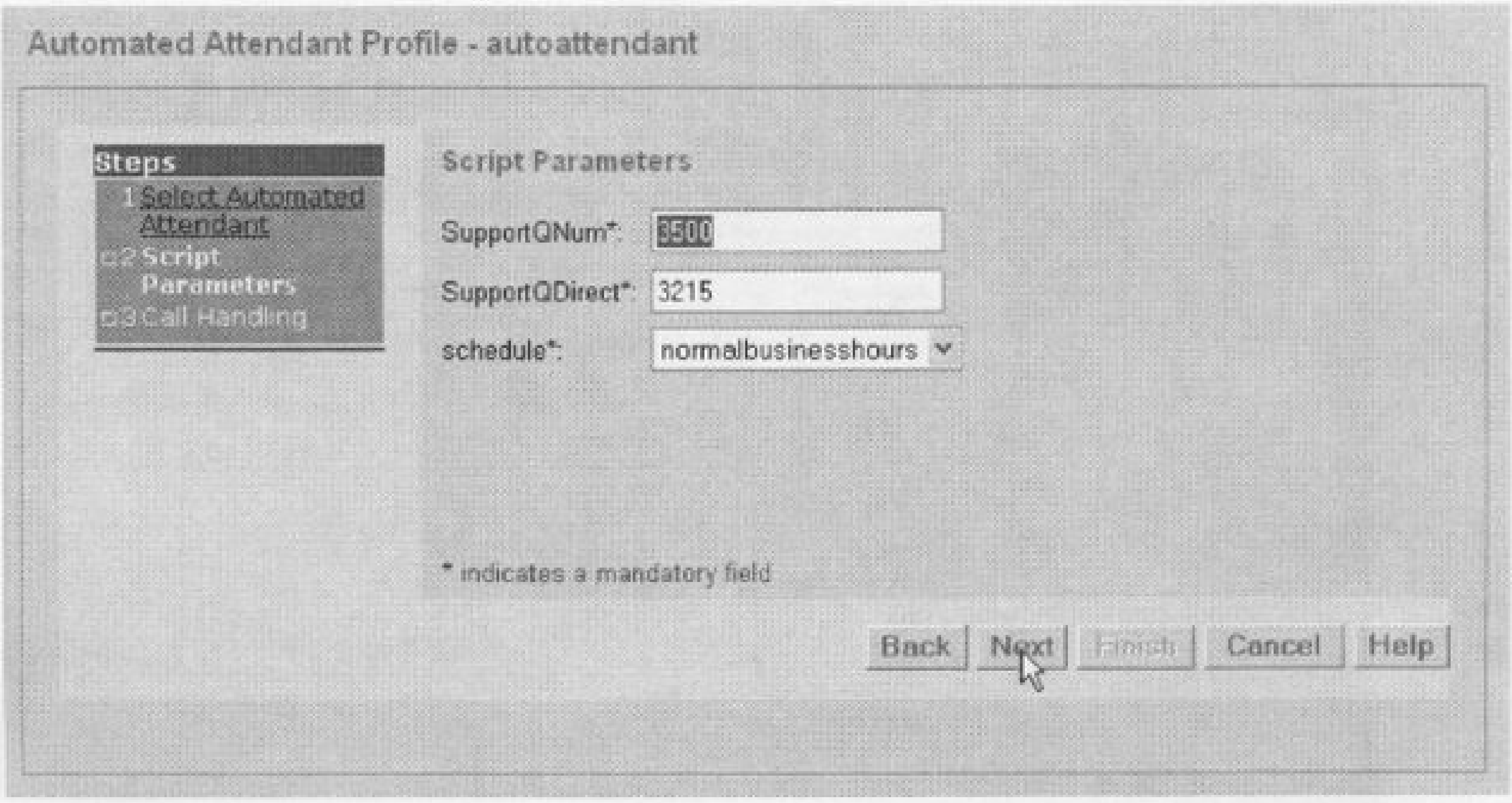


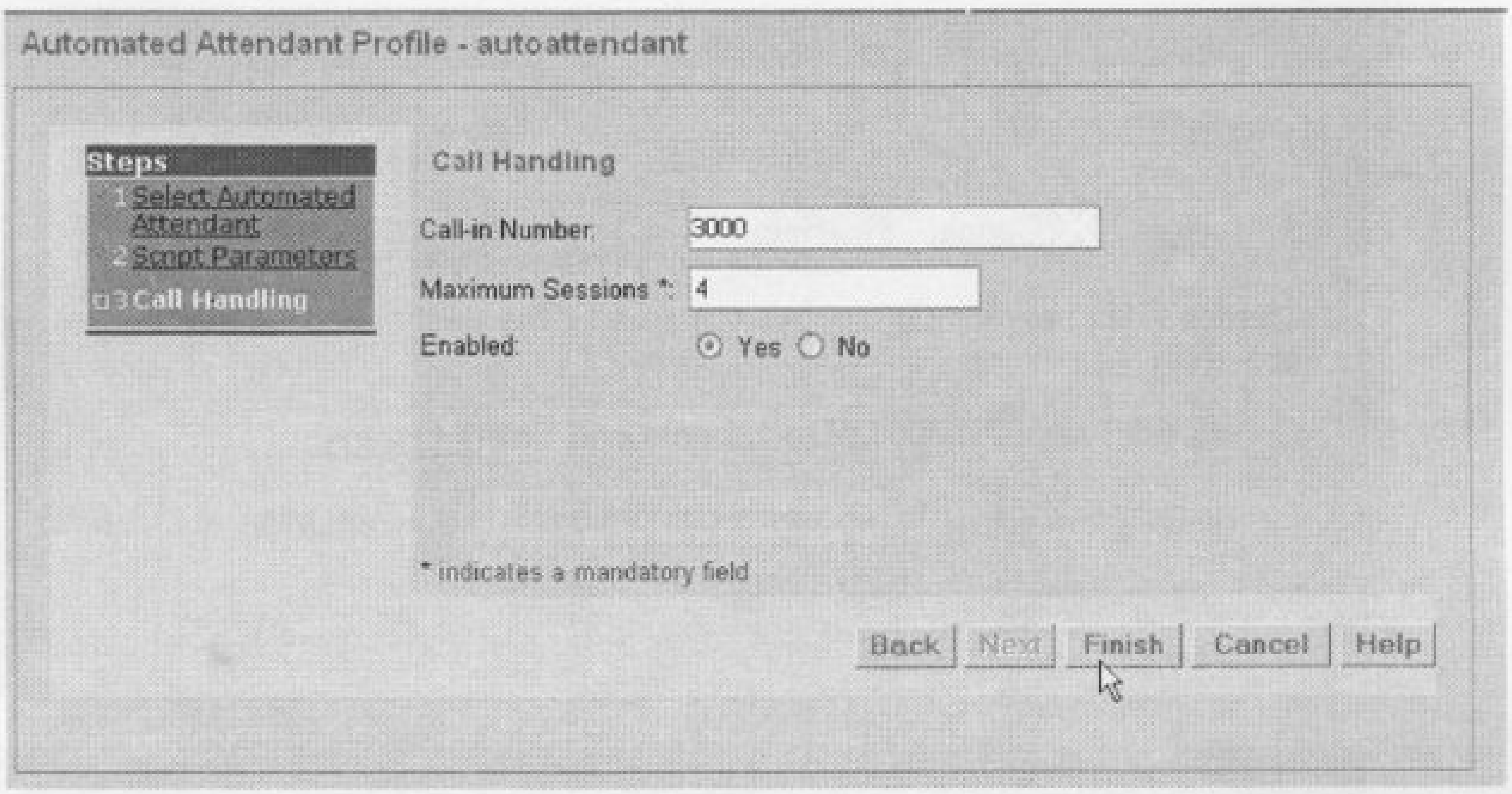



Automated Attendant Profile - autoattendant
Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Select Automated Attendant
Select Automated Attendant Script *:
aa.aef
Upload
Language:
System Default
Application Name (lower case):
autoattendant
* indicates a mandatory field
Back
Next
Finish
Cancel
Help


Upload
Upload
Cancel
Help
Caution: This operation overwrites the script if the destination file name already exists.
Source File Name *:
C:\Documents and Setti
Browse...
Destination File Name *:
snow-aa-custom.aef
(maximum 31 characters)
* indicates a mandatory field


Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Select Automated Attendant
Select Automated Attendant Script *:
snow-aa-custom.aef
Upload
Language:
System Default
Application Name (lower case):
autoattendant
* indicates a mandatory field
Back
Next
Finish
Cancel
Help





➔ **Place a test call into 33132X3000 and verify by pressing 2 that you go into the proper BACD Queue – and verify using CLI Hunt Group stats.**

Task 26.46

Configure Auto-attendant and ICD with the following information:

- AA Route Point = 1710
- Script = aa.aef
- CTI Ports = 1711, 1712

- ICD Route Point = 1700
- Script = icd.aef
- CTI Ports = 1701, 1702

Create the following users that will be used in this task:

- "**jtapi**" to be used for the JTAPI Subsystem.
- "**rmjtapi**" to be used for the ICD Subsystem.
- "**telecaster**" to be used for the ICD Subsystem and enterprise data.
- "**crsadmin**" which must be the designated administrator for IPCC Express.
- **agent1** [assigned device HQ Phone 3 with ICD ext="1003"].
- **agent2** [assigned device BR Phone 2 with ICD ext="2003"]

[all passwords must be 'cisco' and PIN numbers set to '12345' except of course 'telecaster']

For the ICD application you must use skills based routing with the following information:

- CSQ: "GeneralQ"
- Skills: "sales" & "support"
- 'agent1' shall have the skill of 'support' at a proficiency level of 9 and the skill of 'sales' at a proficiency level of 10
- 'agent2' shall have the skill of 'support' at a proficiency level of 10 and the skill of 'sales' at a proficiency level of 9
- The CSQ 'GeneralQ' should have both skills assigned to it with a proficiency level of at least 5 or better for each
- With this stated, the engine should always choose agent1 over agent2 if agent1 is available (you may use whatever method you wish to accomplish this in the engine)
- The engine should also send every agent into a automatic state of 'Work' for 30 seconds before then automatically returning them to a state of 'Ready' (this should happen regardless of whether the call is routed to a specific agent or through the GeneralQ)

➔ **This should be self-explanatory from previous examples – See Task 10.1.**

Task 26.47

Modify the "icd.aef" script with the following information (you may wish to rename it to avoid loosing the original script)

- You must determine if the call is coming from the PSTN from anywhere in the area code of '617' and if the call is coming from the 617 area code then the call must check to see if 'agent1' is available and route the call directly to that agent without queuing the call, however if agent1 is not available, send the call to the 'GeneralQ'

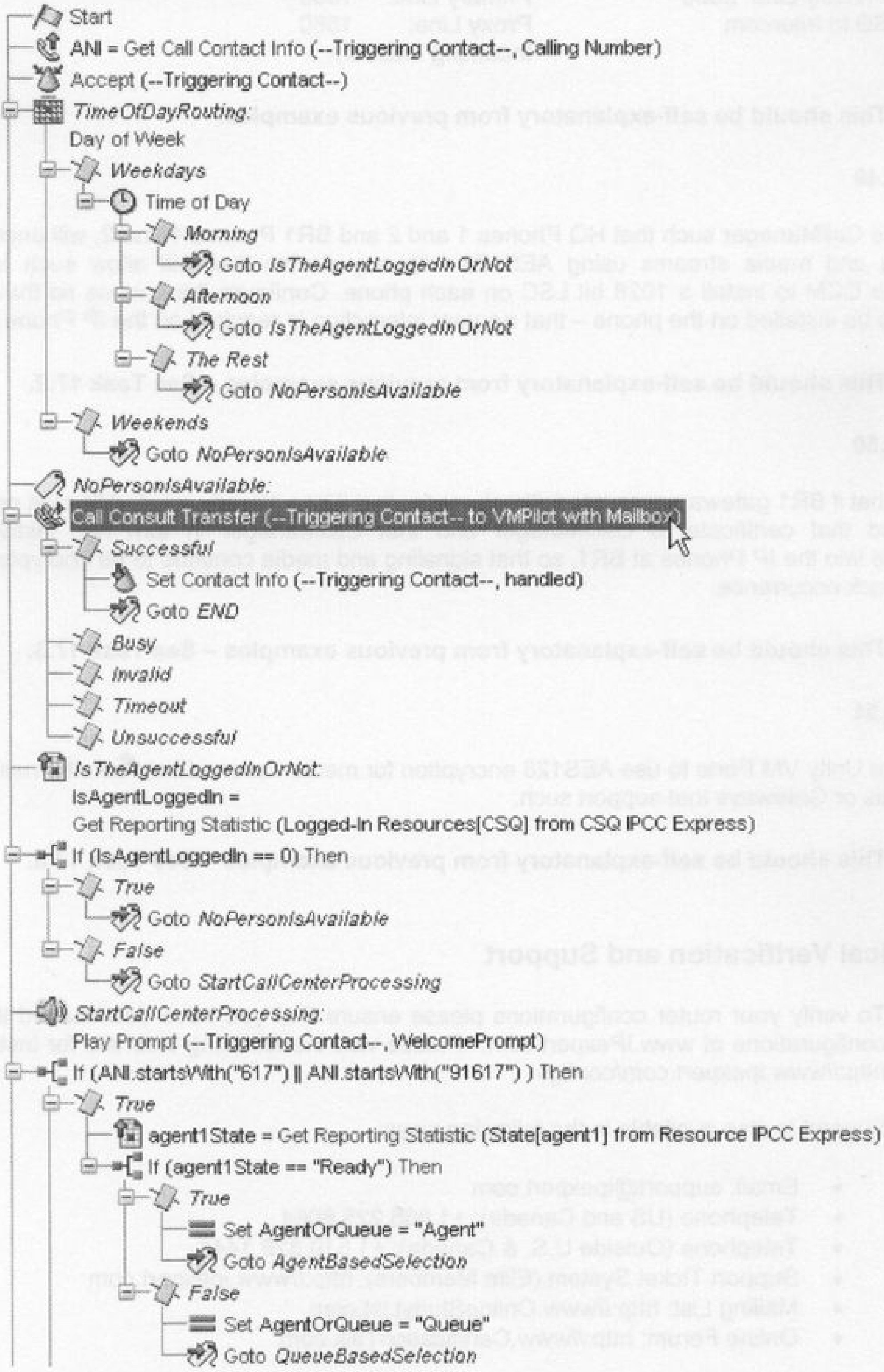
- If the call goes to the GeneralQ, music should be played to the caller while waiting in Q and the caller should also hear the 'QueuePrompt' every 30 seconds

- Regardless of whether the call is routed to a specififc agent or through the GeneralQ, the agent receiving the call should be presented with Enterprise Data showing both the ANI of the call and a disposition of how the call was routed (a string showing 'Agent' or 'Queue')

➔ **This task is partially covered in previous examples – See Task 10.2.**

➔ **The new script is shown below – but also you may click on the paper clip in the PDF containing the Solutions to extract the actual .aef file for a much closer look.**

➔ **The Time of Day routing and GetReportingStatistic is certainly a change but the biggest part of this question comes with what we are told we are NOT allowed to use to get the call to the right Mailbox in Unity, should we find ourselves outside of normal business hours. We must use a "Call Consult Transfer" in the script in order to ring the VM pilot point of 1600, and then enter the additional digits of the mailbox we wish to enter – 1580.**



Task 26.48

Configure IPMA with the following information: BR1 phone 3 will be used as the manager phone and HQ phone 3 will be used as the assistant phone.

Username: Manager	**Username: Assistant**
Primary Line: 2003	Primary Line: 1003
SD to Intercom	Proxy Line: 1560
	Incoming Intercom

➔ **This should be self-explanatory from previous examples.**

Task 26.49

Configure CallManager such that HQ Phones 1 and 2 and BR1 Phones 1 and 2, will encrypt their signaling and media streams using AES128 with any device that will allow such to occur. Configure CCM to install a 1028 bit LSC on each phone. Configure the phones so that when a LSC is to be installed on the phone – that **no** user interaction is required on the IP Phone.

➔ **This should be self-explanatory from previous examples – See Task 17.2.**

Task 26.50

Ensure that if BR1 gateway goes into fallback mode, that it has already created its own certificate, forwarded that certificate to CallManager and that CallManager in turn has installed that certificate into the IP Phones at BR1, so that signaling and media continue to be encrypted during any fallback occurrence.

➔ **This should be self-explanatory from previous examples – See Task 17.3.**

Task 26.51

Configure Unity VM Ports to use AES128 encryption for media traversal between themselves and IP Phones or Gateways that support such.

➔ **This should be self-explanatory from previous examples – See Task 17.6.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 27: Multiprotocol Challenge J

Estimated Time to Complete: 10 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 27 Multiprotocol Challenge J

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 27 Configuration Tasks

Task 27.1

Configure OSPF as a routing protocol in the network so that all the router interfaces including loopback interfaces are reachable from anywhere in the network. Use area 0.

➔ **This should be self-explanatory from previous examples – see Task 1.2.**

Task 27.2

Configure each switch port connecting to IP phones and ATA to support both data and voice traffic according to VLAN IDs specified in Table 2.

➔ **This should be self-explanatory from previous examples – see Task 1.2.**

Task 27.3

Configure each switch port connecting to router/gateway in each site to only allow traffic from data and voice VLANs and not from any other VLANs.

➔ **On Cat6500 in HQ:**

```
clear trunk 2/1 1-119,121-219,221-1005,1025-4094
```

➔ **On Cat3550 in Branch 2:**

```
int fa0/1
switchport trunk allowed vlan remove 2-119,121-219,221-1001,1006-4094
```

Task 27.4

In the HQ site, configure MS DHCP server to enable DHCP service for IP phones to get IP addresses and download phone loads.

➔ **This should be self-explanatory from previous examples.**

Task 27.5

In each branch site, configure each router/gateway to provide DHCP service. Configure the lease time to be 8 hours.

➔ **This should be self-explanatory from previous examples.**

Task 27.6

Configure HQ and BR1 phones with 4 digit extensions as shown in Tables 5 and 6. Security must be enforced on these phones so that one using a sniffer would not be able to decipher signaling or voice packets.

➔ **Looking ahead to Task 27.49, you will see that there is Calling Restriction between phones. This means we must not put the phones in the <Null> Partition, but instead configure per the directions for that task.**

➔ **The security portion of this task is also covered in previous examples – see Task 17.2.**

Task 27.7

Configure each phone forward calling name and number. When calling PSTN, each phone should forward full DID DN to PSTN phone and calling names.

➔ **This should be self-explanatory from previous examples.**

Task 27.8

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **This should be self-explanatory from previous examples.**

Task 27.9

Configure BR1 as an MGCP gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed. Security must be enforced on this gateway so that one using a sniffer would not be able to decipher signaling or voice packets.

➔ **This should be self-explanatory from previous examples.**

➔ **See Task 17.4 – 5 for security setup.**

Task 27.10

Configure the HQ-RTR as an IPIPGW. Calls will be coming into it from CCM via H323 using G711ulaw and then be routed out to the BR2 CME via SIP using G729 (see Table 7 for DNs at CME). Calls will also be coming from CME via H323 using G729 and routed through the IPIPGW to CCM via SIP using G711ulaw (see Table 5 and 6 for DNs at CCM). Also ensure when calls are coming from SIP to H323 that RFC 2833 is properly stripped. Ensure that if calls are coming from H323 to SIP, that RFC 2833 is used for the SIP side.

➔ **This should be self-explanatory from previous examples – See Task 4.9.**

Task 27.11

Configure BR2 as an E1 R2 gateway based on the information in Table 8.

➔ **This should be self-explanatory from previous examples.**

Task 27.12

Configure the E1 R2 such that calls to the PSTN are set up 3 seconds quicker (where possible) than the default. You may assume the maximum length digit string is 11 digits.

➔ **This should be self-explanatory from previous examples.**

Task 27.13

Configure gatekeeper on HQ-RTR with the following information:

Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Register Call Manager to the HQ-RTR gatekeeper with a default technology prefix.
Register CME to the gatekeeper with 4 digit extension numbers only.

➔ **Create Gatekeeper and H225 trunk with Tech-Prefix and Zone.**

➔ **On HQ-RTR:**

```
gatekeeper
zone local HQ-RTR ipexpert.com 172.2.100.1
gw-type-prefix 1#* default-technology
no shutdown
```


➔ **On BR2:**

```
interface Loopback0
 ip address 172.5.102.1 255.255.255.255
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id HQ-RTR ipaddr 172.5.100.1 1719
 h323-gateway voip h323-id BR2
 h323-gateway voip bind srcaddr 172.5.102.1

P5-BR2-RTR(config)#telephony-service
P5-BR2-RTR(config-telephony)#dialplan-pattern 1 3313253... exte 4 no-reg
P5-BR2-RTR(config)#gateway
Aug 23 16:02:44.696: %CCH323-6-REGSTR: Gateway BR2 registered with Gatekeeper
HQ-RTR
```

Task 27.14

Configure the router in Branch 2 for CallManager Express. Register the devices and configure the DNs described in Table 7. Assign the appropriate restrictions.

➔ **This should be self-explanatory from previous examples.**

Task 27.15

Configure paging for the two IP phones located in Branch One, use line 2 as the intercom so that when ephone 1 presses line 2, a call is placed to line 1 of ephone 2. When ephone 2 presses line 2, a call is placed to line 1 of ephone 1. Assign 3101 to line 2 on IP Phone 1 and 3102 on line 2 of IP Phone 2.

```
telephony-service
 max-ephones 4
 max-dn 6
 ip source-address 192.1.201.1 port 2000
 auto assign 1 to 4
 create cnf-files version-stamp 7960 Mar 02 2004 17:02:20
 dialplan-pattern 1 1321.... extension-length 5
 max-conferences 4
 moh music-on-hold.au
!
!
ephone-dn  1
 number 15001
 call-forward busy 15101
 description 13215001
!
!
ephone-dn  2
 number 15002
```



```
 description 13215002
!
!
ephone-dn  3
 number 15101
!
!
ephone-dn  4
!
!
ephone-dn  5
 number A15001
 name "Intercom"
 intercom A15002
!
!
ephone-dn  6
 number A15002
 name "Intercom"
 intercom A15001

ephone  1
 mac-address 0007.50A4.D602
 type 7960
 button  1:1  2:3  3:5
!
!
ephone  2
 mac-address 0030.94C2.8595
 type 7960
 button  1:2  2s3  3:6
```

Task 27.16

Specify the maximum entries and minutes of the call history to 500.

```
call-history-mib retain-timer 500
call-history-mib max-size 500
```

Task 27.17

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 27.18

Use CallManager's only CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **This should be self-explanatory from previous examples – See Task 2.2.**

Task 27.19

In the HQ gatekeeper, allow only two concurrent G.729 calls to the gatekeeper.

```
bandwidth remote 32
```

Task 27.20

Configure Calling Restriction using the Table below. All phones are allowed to call each other except for HQ phone 4 which is a lobby phone which can only call HQ phone 1 and BR1 phone 1.

➔ **Create the following partitions.**

- PT-HQ-911
- PT-HQ-LOC
- PT-HQ-LD
- PT-HQ-INTERNATIONAL
- PT-BR1-911
- PT-BR1-LOC
- PT-BR1-LD
- PT-BR1-INTERNATIONAL
- PT-INTERNAL

➔ **Put all the phones (except HQ phn1 and BR1 Phn 1) in the partition PT-INTERNAL.**

➔ **Create the following CSS:**

- CSS-HQ-INTERNAL-911-LOC
- CSS-HQ-INTERNAL-ALL
- CSS-BR1-INTERNAL-911-LOC
- CSS-BR1-INTERNAL-ALL

➔ **Assign CSS to Devices. HQ phone 4 should not have any CSS assigned.**

➔ **This phone will have the null CSS assigned and will only be able to see devices in the null Partition (i.e. HQ phone 1 and BR1 phone 1).**

Task 27.21

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the BR1 gateway with the HQ gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

➔ **See Task 27.25.**

Task 27.22

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway.

➔ **See Task 27.25.**

Task 27.23

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed first out of the local Gatekeeper and then through the HQ-IPIPGW as a backup. Users must be able to dial the BR2 site using extension (4 digit) dialing. (**Test both** call routing methods, one at a time, before moving on to the next question).

➔ **See Task 27.25.**

➔ **This task also covered in previous examples – see task 6.1 – 6.**

Task 27.24

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway.

➔ **See Task 27.25.**

Task 27.25

Calls originating from BR2 to CallManager (both HQ and BR1) should use VoIP through the HQ IPIPGW and the PSTN as backup. 4-digit dialing must be preserved. Also, you must use the minimum amount of dial-peers possible.

➔ **When implementing a dial plan it is a good idea to look at all the tasks together rather than treat each question as a separate question.**

➔ **Digit Manipulation should be done in the Route List.**

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-GK	GK TRUNK	1
RG-IPIPGW-ICT	H323 (non-GK controlled) InterCluster Trunk	1
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1-LOC	RG-HQ RG-BR1	PREDOT PREDOT + PREFIX 1212
RL-BR1-HQ-LOC	RG-BR1 RG-HQ	PREDOT PREDOT + PREFIX 1617
RL-HQ-BR1-LD-INT	RG-HQ RG-BR1	PREDOT PREDOT
RL-BR1-HQ-LD-INT	RG-BR1 RG-HQ	PREDOT PREDOT
RL-TOLLBY-2-BR1	RG-BR1 RG-HQ	PREDOT PREDOT + PREFIX 1617
RL-GK-ICT	RG-GK RG-IPIPGW-ICT	PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ-BR1-LOC
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ-LOC
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ-BR1-LD-INT
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1-HQ-LD-INT
91617.xxxxxxx	PT-HQ-LD	RL-TOLLBY-2-BR1
9.011! 9.011!#	PT-HQ-INT	RL-HQ-BR1-LD-INT
9.011! 9.011!#	PT-BR1-INT	RL-BR1-HQ-LD-INT
3xxx	(Null or Internal PT)	RL-GK-ICT

➔ **For CCME use the following dial-peers:**

```
voice translation-rule 1
  rule 1 /^(1...\)/ /1212222\1/
  rule 2 /^(2...\)/ /1617522\1/
!
voice translation-profile PSTN-OUT
  translate called 1
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 destination-pattern 9911
corlist outgoing css-911
 no digit-strip
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
```

```
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1000 voip
 destination-pattern [12]...
 session target ipv4:172.1.100.1
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1001 pots
 preference 1
 destination-pattern [12]...
 port 0/0/0:0
 translation-profile outgoing PSTN-OUT
!
```

Task 27.26

Unity needs to be able to accept in-bound faxes at the mailbox of IncomingFax@voip.lab. Unity will also be your DNS server. Configure the BR1 GW to intercept these faxes from the PSTN PRI as an On-Ramp gateway and email all incoming faxes to this mailbox. Refer to Table 17 of this section for FaxDN ranges. All the files you will need are in BR1 Flash memory. Unity also needs to be able to send out-bound faxes to the PSTN (we will configure Unity for this task later). Configure the BR1 GW to accept these faxes via email from Unity and then to send them out through the PSTN PRI as an Off-Ramp gateway. Refer to Table 18 of this section for PSTN FaxDN ranges. Again, all the files you will need are in BR1 Flash memory.

➔ **This should be self-explanatory from previous examples – See Task 4.8 and 4.10.**

Task 27.27

All users with a class of service that includes access to PSTN numbers should be given access to Toll Free Services. Block access to all 1-900 and 1-976 numbers.

➔ **Click Route Plan --> Route Pattern.**

➔ **Under the Route Pattern, enter 9.1900XXXXXXX and place in the default partition.**

➔ **Under the Gateway, select any gateway.**

➔ **Under Route Option, select Block this pattern.**

➔ **Then Insert the route pattern.**

➔ **You can block 976 numbers as well by doing the same as above except create a Route Pattern for 9.1976xxxx.**

➔ **On BR2:**

```
telephony-service
after-hours block pattern 1 91900....... 7-24
after-hours block pattern 2 91976....... 7-24
```

Task 27.28

Configure the Branch 1 router to provide SRST service. Only allow three phones to register. In this exercise to block calls you must use a super set of COR lists applied for outgoing calls and subset of COR lists applied for incoming calls. Use descriptive names like Restricted, LD, INTL, Manager and Employee. Route Patterns must be transparent to the users.

```
call-manager-fallback
 ip source-address 10.1.201.1 port 2000
 max-ephones 3
 max-dn 6


dial-peer cor custom
 name restricted
 name local
 name longdistance
 name international
!
dial-peer cor list restricted
 member restricted
!
dial-peer cor list local
 member local
!
dial-peer cor list longdistance
 member longdistance
!
dial-peer cor list international
 member international
!
dial-peer cor list Manager
 member restricted
 member local
 member longdistance
 member international
!
```

```
dial-peer cor list Employee
 member restricted
 member local
 member longdistance
!
dial-peer voice 1 pots
 destination-pattern 911
 port 2/0/0:23
 cor outgoing restricted
 forward-digits All
!
dial-peer voice 2 pots
 destination-pattern 9[2-9]......
 port 2/0/0:23
 cor outgoing local
 forward-digits 7
!
dial-peer voice 3 pots
 destination-pattern 91[2-9]..[2-9]......
 port 2/0/0:23
 cor outgoing longdistance
 forward-digits 11
!
dial-peer voice 4 pots
 destination-pattern 9011T
 port 2/0/0:23
 cor outgoing international
 prefix 011
!
call-manager-fallback
 cor incoming Manager 1 2001
 cor incoming Employee 2 2002
```

Task 27.29

Configure AAR for Headquarters and Branch 1.

➔ **This should be self-explanatory from previous examples.**

Task 27.30

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 27.31

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 27.32

Configure conference bridge on BR1 router. Use a maximum of 1 sessions. Do not allow any G729 annexes to be configured as supported codecs. Configure only G729r8.

➔ **This should be self-explanatory from previous examples.**

Task 27.33

Configure transcoder on BR1 router. Use a maximum of 2 sessions. Do not allow any G729 annexes to be configured as supported codecs. Configure only G729r8.

➔ **This should be self-explanatory from previous examples.**

Task 27.34

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should load share the IOS resources and 6608 resources.

➔ **Create a MRG called HQ-MRG. Put HQ media resources – 6608 conference bridge, 6608 transcoder and MOH Server – into the MRG.**

➔ **Create a MRG called IOS-MRG. Put IOS media resources into this MRG.**

➔ **Create a third MRG called BR1-MRG – put ALL media resources into this group.**

➔ **Create a MRGL called HQ-MRGL and put HQ-MRG and IOS-MRG into this MRGL – HQ-MRG should be listed above IOS-MRG.**

➔ **Create a MRGL called BR1-MRGL – put BR1-MRG into this MRGL.**

Task 27.35

Configure a Music on Hold server on the Publisher Call Manager. Add another music source which can be found on the C: drive of your Call Manager. Ensure that the default (Sample) audio source is used when a User presses the 'Hold' button on his/her phone. For all other events that require music to be played use the newly added music source. You may not configure music sources on line, device or device pool to accomplish this task.

➔ **This should be self-explanatory from previous examples.**

Task 27.36

Configure the Call Manager such that HQ phones will receive music using the G711 codec and BR1 phones will receive music using the G729 codec. You must use the transcoder to achieve this task.

➔ **Transcoding MOH will only work for Unicast so in the next task change the IP Media Streaming Application. The idea is to verify the transcoder is working – use the following command on the Cat 6K.**

```
sh port voice active transcode
```

Task 27.37

Ensure that the HQ and BR1 phones receive multicast music on hold.

➔ **Check perfmon on Call Manager.**

Task 27.38

Configure music on hold on the BR2 CME.

➔ **This should be self-explanatory from previous examples.**

Task 27.39

Create a meet-me conference with DN=1900.

➔ **This should be self-explanatory from previous examples.**

Task 27.40

Configure the CoS-to-DSCP Mappings for the Catalyst 6500 and the Catalyst 3550 switches. The recommended settings are DSCP of AF31 for VoIP control plane and DSCP of EF for VoIP bearer plane.

➔ **This should be self-explanatory from previous examples.**

Task 27.41

Configure LLQ between Headquarters and BR1 site – configure 32kbps control traffic and 256kbps bearer traffic. From BR1 to Headquarters configure 6% control traffic and 40% bearer traffic. Link speed is 1544Kbps.

➔ **This should be self-explanatory from previous examples.**

Task 27.42

Setup Unity voice mail boxes for Phone 1 in HQ, and Branch 1. Ensure you can call and reach mailboxes as well as leave messages. Ensure you can light the MWI light.

- Pilot Number: 1600
- Unity Port Number: 1601 – 1604
- Set the default password to 54321
- MWI Light – 1998 off
- MWI Light – 1999 on

➔ **This should be self-explanatory from previous examples.**

Task 27.43

Integrate the Branch 2 CME with Unity with the following information.

- Pilot Number: 3600
- Unity Port Number: 3600 – 3603
- Set the default password to 54321
- MWI Light – 3998 off
- MWI Light – 3999 on

Provide voice mail boxes for Phone 1 and Phone 3 at Branch 2.

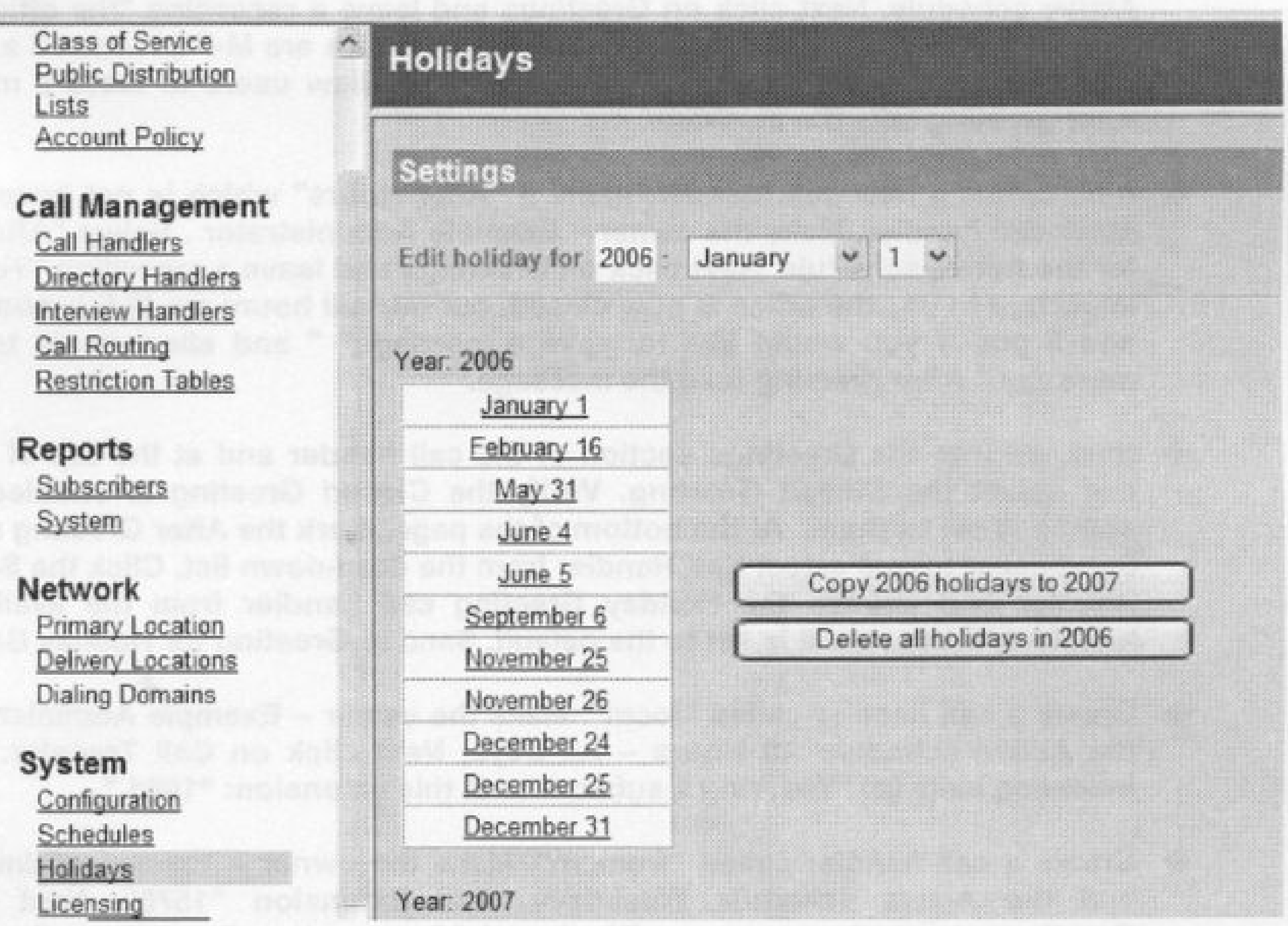
➔ **This should be self-explanatory from previous examples.**

Task 27.44

Configure Unity to observe holidays for the next five years.

New Year's Day	January 1
President's Day	February 16
Memorial Day	May 31
Independence Day	July 4-5
Labor Day	September 6
Thanksgiving	November 25-26
Christmas	December 24-25
New Year's Eve	December 31

➔ **Create the holidays in Unity and Copy for the next 5 years.**



Task 27.45

Setup a Unity Call Handler for each site with DN 1570/2570/3570. During active hours (8-5pm) Monday through Friday, a standard transfer will release the call to phone 1 at each site. During closed business hours send the caller to a standard greeting that says a message like "Your call is important to us...the office is now closed, our normal hours are M-F between 8 a.m. and 5 pm. If you would like to leave a message" and allow users to leave a message. During a holiday schedule send the call to a standard greeting that says a message like "Your call is important to us...the office is now closed due to holiday observance, our normal hours are M-F between 8 a.m. and 5 pm if you would like to leave a message" and allow users to leave a message.

➔ **In this exercise we will create 2 schedules (Holidays and After Hours) and create four CallHandlers (fromcm, tocm, Holidays, After Hours).**

➔ **Click on Schedules. The Weekdays (def) schedule is set for 8am to 5pm. Verify the Observe Holidays checkbox, at the top of the screen, is checked. Click on PLUS/add button. Name: Holidays -> Based on All Hours-All DaysMake sure to uncheck the Observe Holidays checkbox for the Holiday Schedule and save.**

➔ **Create another custom schedule "After Hours". This schedule must be the opposite of the Weekdays (Def) schedule. All hours that are checked in the Weekdays (Def) schedule above should be unchecked in this schedule. All blank hours in the Weekdays (Def) schedule above should be checked in this schedule. The quickest way to complete this part is to create this schedule based on All Hours-All Days and deselect M-F 8am – 5pm. Verify the Observe Holidays checkbox, at the top of the screen, is checked.**

➔ **Next create a new call handler, name it "Holidays" which is not based on any other call handler. Make the owner – Example Administrator . Select "Holidays" for the Active schedule. Next click on Greetings and leave a recording "the office is now closed due to holiday observance, our normal hours are M-F between 8 a.m. and 5 pm if you would like to leave a message" and allow users to leave a message." After greeting take the message.**

➔ **Next create a new call handler, name it "After Hours" which is not based on any other call handler. Make the owner – Example Administrator . Select "After Hours" for the Active schedule. Next click on Greetings and leave a recording "Your call is important to us...the office is now closed, our normal hours are M-F between 8 a.m. and 5 pm. If you would like to leave a message" " and allow users to leave a message." After greeting take the message.**

➔ **Next, go into the Greetings section of the call hander and at the top of the page and select the Closed Greeting. Verify the Closed Greeting is enabled and its source is set to Blank. At the bottom of the page, mark the After Greeting setting to Send caller to and select Call Handler from the drop-down list. Click the Select Call Handler and choose the Holiday Greeting call handler from the available call handlers. Make sure it is set to the default, Send to Greeting for Holiday Greeting.**

➔ **Create a call handler called "tocm". Make the owner – Example Administrator and the Active schedule All Hours – All Days. Next click on Call Transfer. Transfer incoming calls to: "Yes, ring a subscriber at this extension: "1001."**

➔ **Create a call handler called "fromcm". Make the owner – Example Administrator and the Active schedule Weekdays. Add Extension "1570". Next click on Greetings, leave the source as Blank and After greeting Send the caller to a Call Handler. Select Attempt transfer for "tocm".**

➔ **Repeat for BR1 and BR2.**

Task 27.46

Configure Unity to be an Inbound/Outbound Fax Server. Ensure that Faxes going out to the PSTN number in Table 18 from the BR1 Gateway arrive and are viewable.

➔ **This task started back with 27.26 and was answered by tasks 4.8 and 4.10.**

➔ **This should be self-explanatory from previous finished examples – See Task 9.9 and 9.10.**

Task 27.47

Configure Unity so that if a IP Phone caller conferences in Ext 1650, that Unity will record the conversation and forward that recording to the mailbox of the IP Phone that initiated the conference.

➔ **This should be self-explanatory from previous finished examples – See Task 9.8.**

Task 27.48

Configure the CallManager IP Phones with idle URL using the Cisco Logo image. (Graphic provided on the Desktop: ciscologo.cip)

➔ **Open Internet Services Manager from Programs > Administrative Tools**

Expand CiscoIPServices > idleurl (right click and Explore.)

➔ **Edit the following information:**

```
var callManagerUserId = "administrator";
var callManagerPassword = "ipexpert";
var callManager = "10.2.200.21";
var fontfile = "c:\\CiscoIPServices\\ASP\\includes\\usenglishfont.xml";
var logofile = "c:\\CiscoIPServices\\ASP\\idleurl\\cisco.xml";
var refresh = 30;
```

➔ **Save**

➔ **Open Enterprise Parameter in CallManager.**

1. **Set Idle URL to: http://10.2.200.21/CiscoIPServices/idleurl/idleurl.asp**
2. **Set Idle Time to something greater than 0 seconds. Ex. 10**
3. **Reset phone(s)**

Task 27.49

Restrict internal callers from BR1 only, so that they may not see CNAM information only regarding who they are calling or who is calling them, however ensure that BR1 Phone 3 can see all CNAM information.

➔ **This should be self-explanatory from previous examples – See Task 11.14.**

Task 27.50

Configure CCM to 'appear' as an older KSU would have appeared at a remote site – so that if a BR1 Phone3 was to pick up their handset and select what they believed to be a "line" to dial out of, that they would not need to first dial a 9 in order to access a trunk. Make this "Line" access separate from their main extension DN. Also ensure that the Caller does **not** see the 9 before their dialed number when they place the call.

➔ **This should be self-explanatory from previous examples – See Task 11.13.**

Task 27.51

Make sure that if during a call, the user presses the Transfer softkey, dials the extension, and hangs up, that the transfer succeeds without having to press the transfer key a second time.

➔ **This should be self-explanatory from previous examples – See Task 11.11.**

Task 27.52

Enable support for a VTA camera on HQ Phone 3.

➔ **This should be self-explanatory from previous examples – See Task 11.12.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 28: Multiprotocol Challenge K

Estimated Time to Complete: 10 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 28 Multiprotocol Challenge K

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 28 Configuration Tasks

Task 28.1

Ensure that the link between the HQ/BR1/BR2 routers and appropriate switches are configured as DOT1Q trunks. Give the voice sub-interface the appropriate ip address from Table 1. Check connectivity between all sites and to Call Manager/Unity.

➔ **This should be self-explanatory from previous examples.**

Task 28.2

Configure Voice and Data VLAN for all IP Phones including ATA and VG248. VLAN IDs are defined in Table 2. Use Table 3 for HQ site 6500 port assignment. For BR1 and BR2 port allocation you are required to find out port allocation by your own methods.

➔ **This should be self-explanatory from previous examples.**

Task 28.3

Configure all phone ports such that they bypass the spanning-tree listening and learning states.

➔ **This should be self-explanatory from previous examples.**

Task 28.4

Set the clock on the BR2 router to be an authoritative time source.

➔ **From enable mode:**

```
set clock
```

➔ **From global config mode:**

```
clock timezone EST -5
ntp master
```

Task 28.5

For Headquarter and Branch 1, use Microsoft DHCP server to allocate IP address for all Devices. For Branch 2, use IOS DHCP to allocate IP address for the IP phones. For each voice subnet, allocate the IP address from .50 to .69.

➔ **This should be self-explanatory from previous examples.**

Task 28.6

Configure Call Manager to allow devices to register manually using CDP information. Assign directory number to devices based on Tables 5 and 6.

➔ **This should be self-explanatory from previous examples.**

Task 28.7

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 28.8

Use CallManager's only CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **This should be self-explanatory from previous examples – See Task 2.2.**

Task 28.9

Assume a Publisher exists (**Table 1**) and every phone is registered in a CCM Group first to a Subscriber, and then to the Publisher. Configure the keepalive interval between any IP Phone and the Publisher server CallManager to be set to 40 seconds.

➔ **This should be self-explanatory from previous examples – See Task 2.6.**

Task 28.10

Configure Calling Restriction using the Table below.

➔ **This should be self-explanatory from previous examples.**

Task 28.11

Set the phones that reside in the POD (all 79XX not physically accessible to you) to auto-answer. Phones must only auto-answer after 5 seconds.

➔ **This should be self-explanatory from previous examples.**

Task 28.12

Register phones at BR2 based on Table 7.

➔ **This should be self-explanatory from previous examples.**

Task 28.13

Create a shared line on Branch 2 phones 1 and 2 with DN 3010. The first call coming into the shared line must ring both phones. When a second call comes into the shared line it must ring the unused phone while at the same time displaying 'call waiting' on the first phone. Ensure that the shared lines have the second channel enabled.

```
ephone-dn 1 dual-line
 number 3001
!
ephone-dn 2 dual-line
 number 3002
!
ephone-dn 3 dual-line
 number 3010
 huntstop channel
 no huntstop
!
ephone-dn 4 dual-line
 number 3010
 preference 1
 huntstop channel
 no huntstop
!
ephone 1
 mac-address 0011.BBEF.6901
 type 7940
 button 1:1 2c3,4
!
ephone 2
 mac-address 0011.BBE0.5775
 type 7940
 button 1:2 2c3,4
```


Task 28.14

BR2 should use the same class of restriction as the other sites.

```
dial-peer cor custom
 name pt-911
 name pt-loc
 name pt-ld
 name pt-internl
!
!
dial-peer cor list css-911
 member pt-911
!
dial-peer cor list css-loc
 member pt-loc
!
dial-peer cor list css-ld
 member pt-ld
!
dial-peer cor list css-intnl
 member pt-internl
!
dial-peer cor list css-911-loc
 member pt-911
 member pt-loc
!
dial-peer cor list css-ALL
 member pt-911
 member pt-loc
 member pt-ld
 member pt-internl
!
dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
```

```
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 9011T
 port 0/0/0:0
 prefix 011

ephone-dn 1 dual-line
 number 3001
 cor incoming css-911-loc
!
!
ephone-dn 2 dual-line
 number 3002
 cor incoming css-ALL
```

Task 28.15

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **This should be self-explanatory from previous examples.**

Task 28.16

Configure BR1 as an MGCP gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed. Secure all MGCP signaling and RTP stream packets from being decoded by a sniffer of any sort.

➔ **This should be self-explanatory from previous examples – See Task 17.4 – 5 for security setup.**

Task 28.17

Configure the HQ-RTR as a IPIPGW for any possible dial-peer scenario to come.

➔ **On HQ-RTR**

```
voice service voip
 allow connections h323 to h323
 allow connections h323 to sip
 allow connections sip to h323
 allow connections sip to sip
!
interface Loopback0
 ip address 172.1.100.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id ???? ipaddr 172.1.100.1 1719
```

← We don't know what Zone we will register with just yet – so we will have to wait till later to find out

```
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip bind srcaddr 172.1.100.1
```

Task 28.18

Configure BR2 as an H323 gateway based on the information in Table 8.

```
controller E1 0/0/0
 ds0-group 0 timeslots 1-3 type r2-digital r2-semi-compelled ani
```

Task 28.19

Configure the E1 R2 such that calls to the PSTN are set up 3 seconds quicker (where possible) than the default. You may assume the maximum length digit string is 11 digits.

```
controller E1 0/0/0
ds0-group 0 timeslots 1-3 type r2-digital r2-semi-compelled ani
cas-custom 0
 dnis-digits min 3 max 11
```

Task 28.20

Unity will later need to be able to accept in-bound faxes at the mailbox of IncomingFax@voip.lab. Unity will also be your DNS server. Configure the BR1 GW to intercept these faxes from the PSTN PRI as an On-Ramp gateway and email all incoming faxes to this mailbox. Refer to Table 17 of this section for FaxDN ranges. Unity will also need to be able to send out-bound faxes to the PSTN. Configure the BR1 GW to accept these faxes via email from Unity and then to send them out through the PSTN PRI as an Off-Ramp gateway. Refer to Table 18 of this section for PSTN FaxDN ranges. All of the files you will need are in BR1 Flash memory.

➔ **This should be self-explanatory from previous examples – See Task 4.8 and 4.10.**

Task 28.21

Configure gatekeeper on HQ-RTR with the following information:

Local zone= HQ-RTR
domain name = ipexpert.com
Register CCM with this zone.
[use loopback interface for local zone]

Local zone= VGK
domain name = ipexpert.com
Register IPIPGW on loopback interface with this zone.

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.1.100.1
 zone local VGK ipexpert.com
 zone remote PSTN-WAN ipexpert.com 10.1.200.2 1719
 zone prefix PSTN-WAN 011*
 no shutdown
!
interface Loopback0
 ip address 172.1.100.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id VGK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip bind srcaddr 172.1.100.1
```

Task 28.22

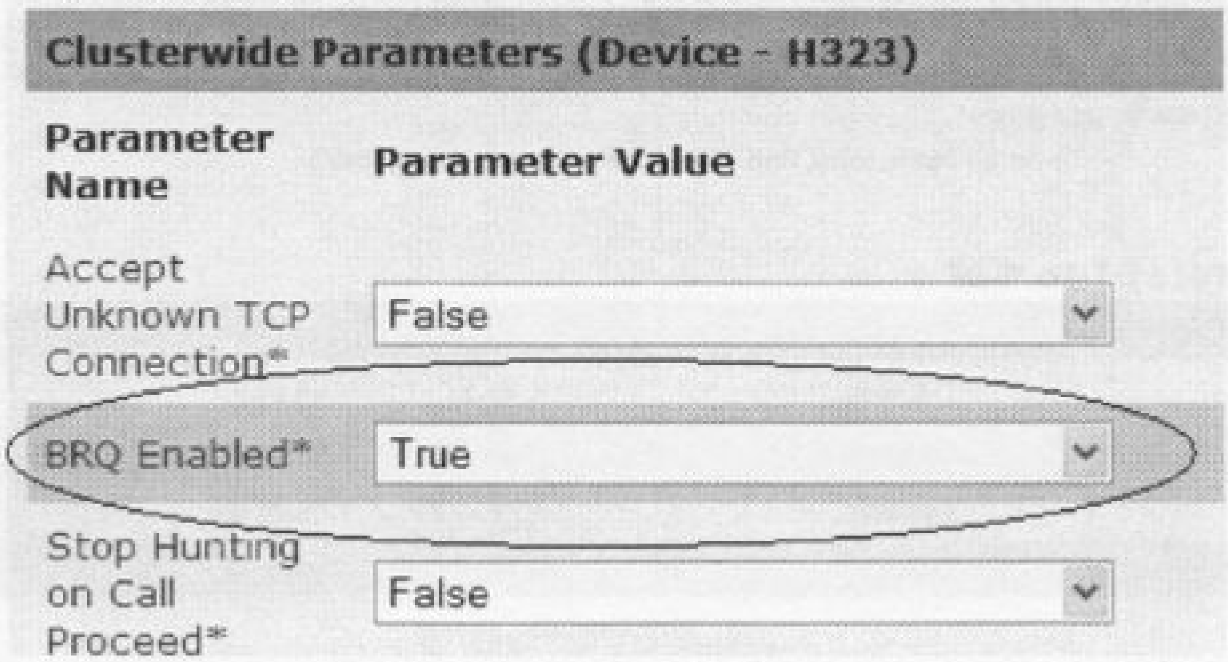
Configure CAC to allow one G711 call plus one G729 call.

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.2.100.1
 zone remote PSTN-WAN ipexpert.com 10.2.200.2 1719
 bandwidth remote 144
 no shutdown
```

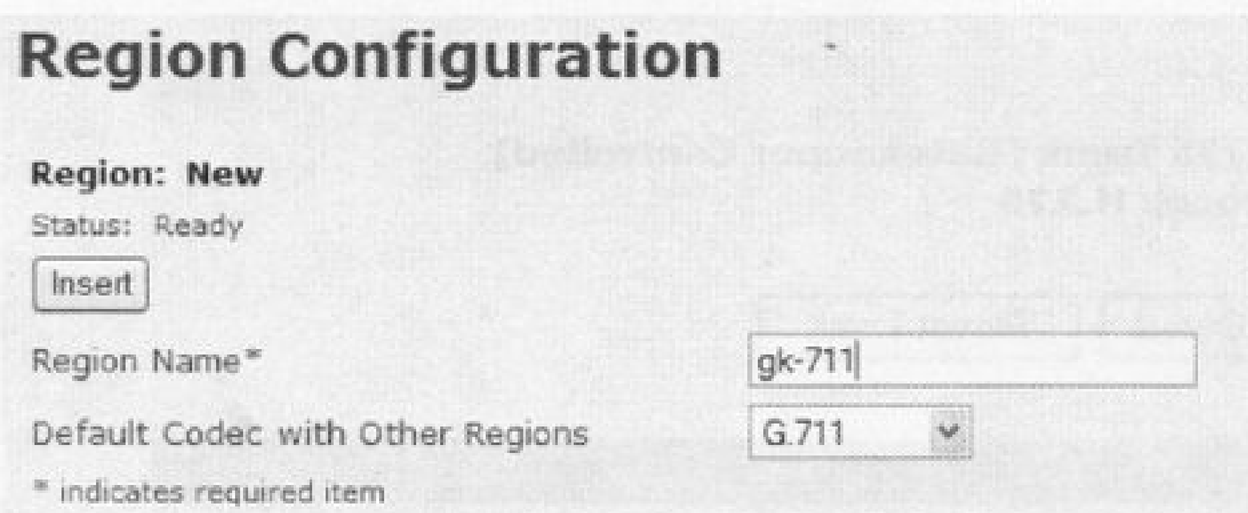
Task 28.23

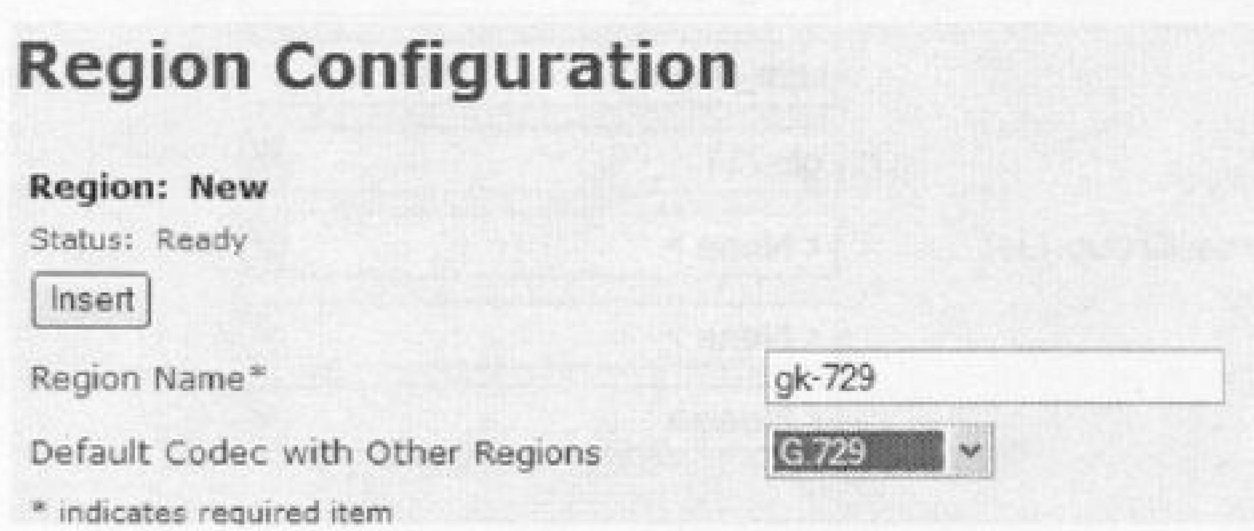
Calls should attempt to use G711. If the call fails due to there not being enough bandwidth over the WAN provisioned, then the G729 codec should be selected.

➔ **Change the BRQ Enabled CCM Service Parameter and restart the CCM Service.**

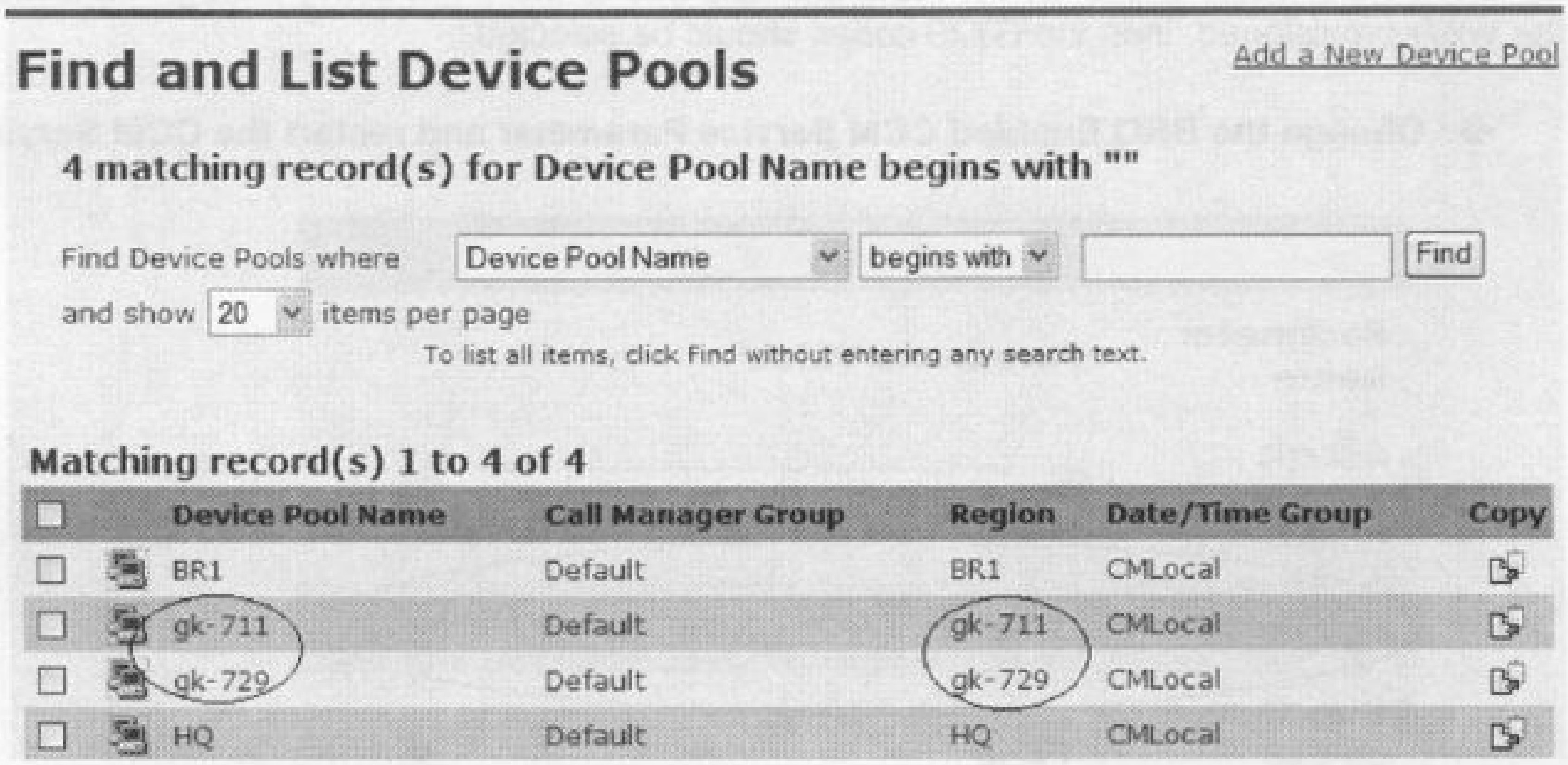


➔ **Create two new Regions and Device Pools – one that uses G711 to other Regions and one that uses G729 to other Regions.**

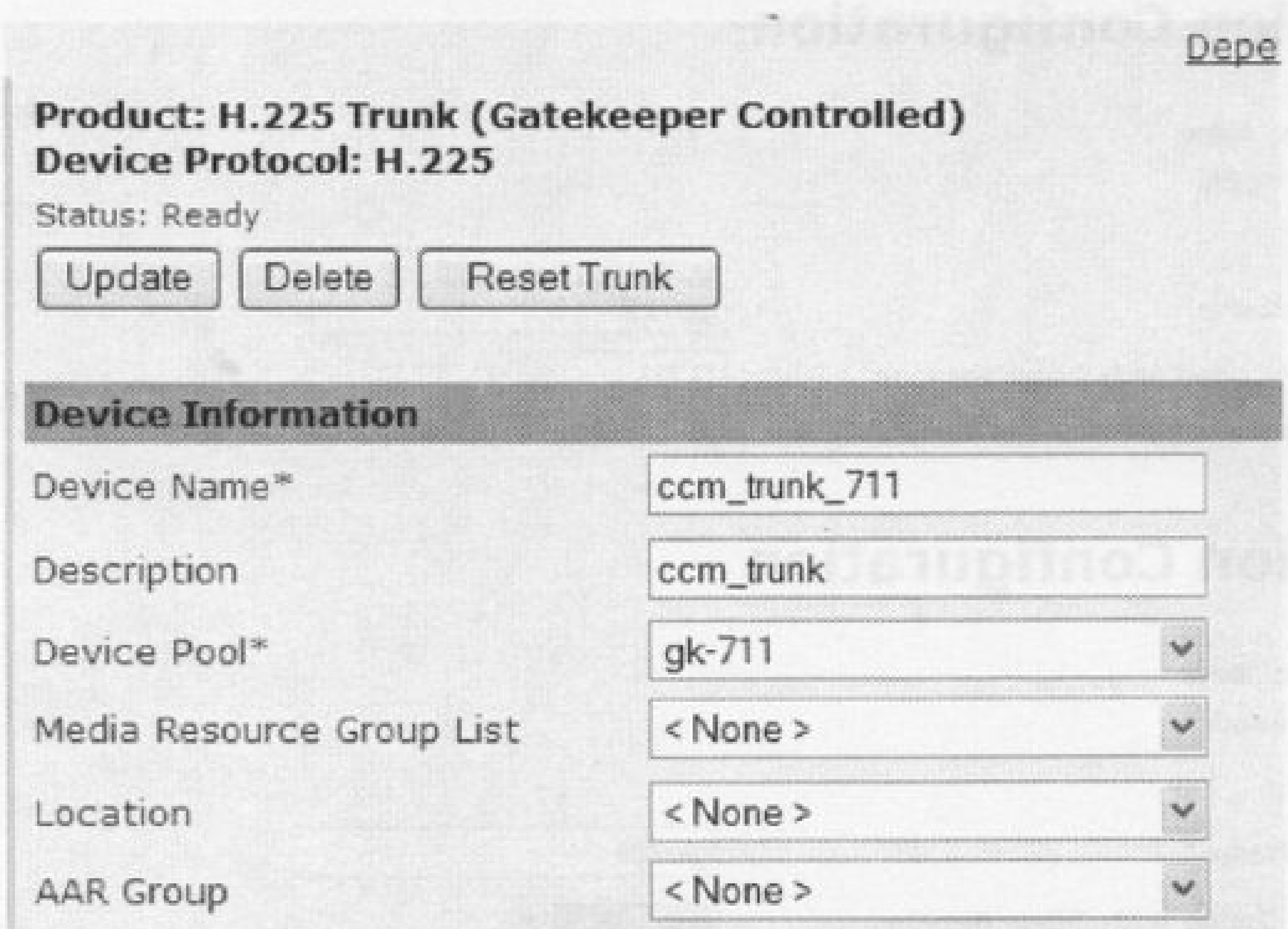


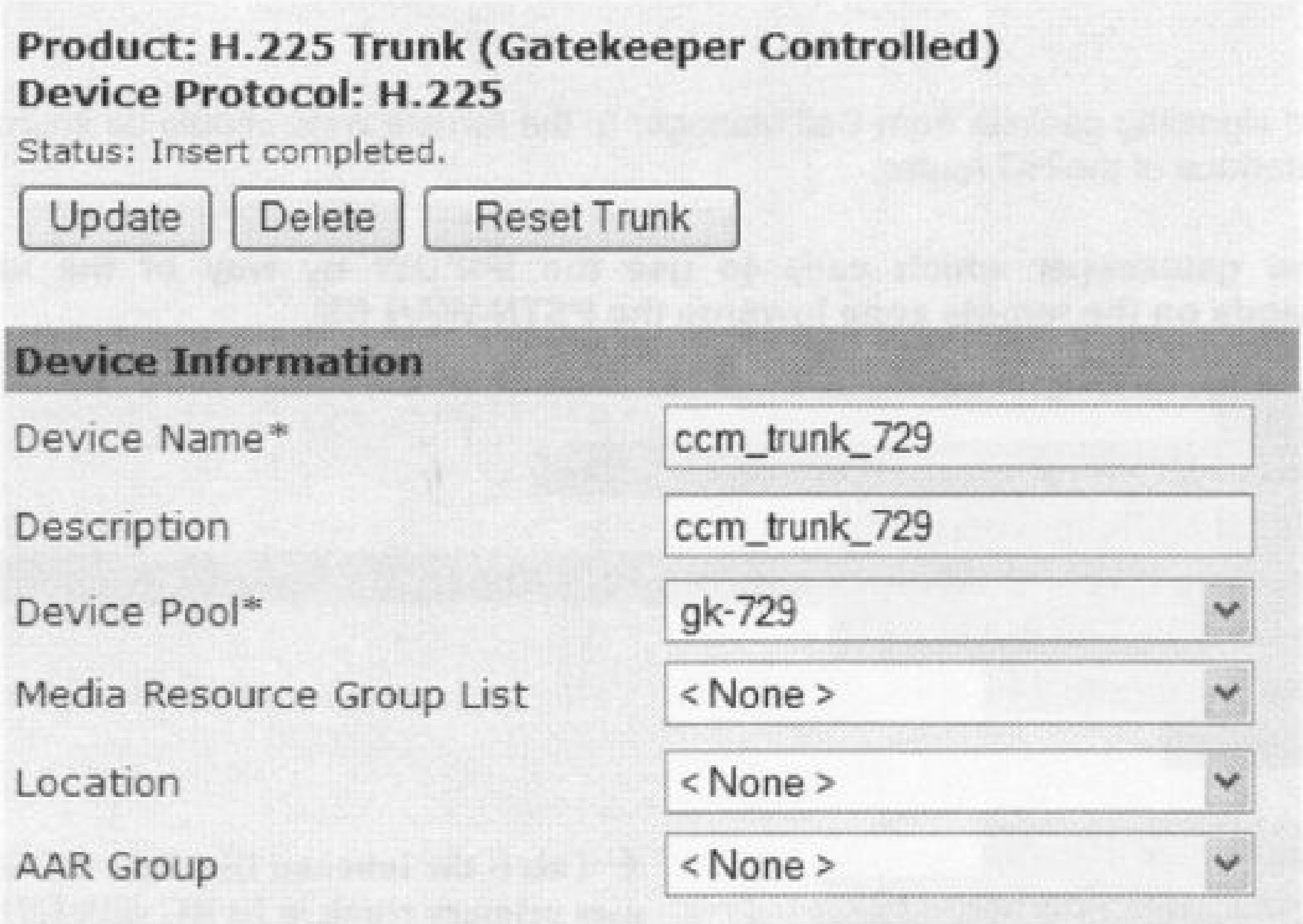


➔ **Assign these Regions to the new Device Pools – call the Device Pools GK-711 and GK-729.**

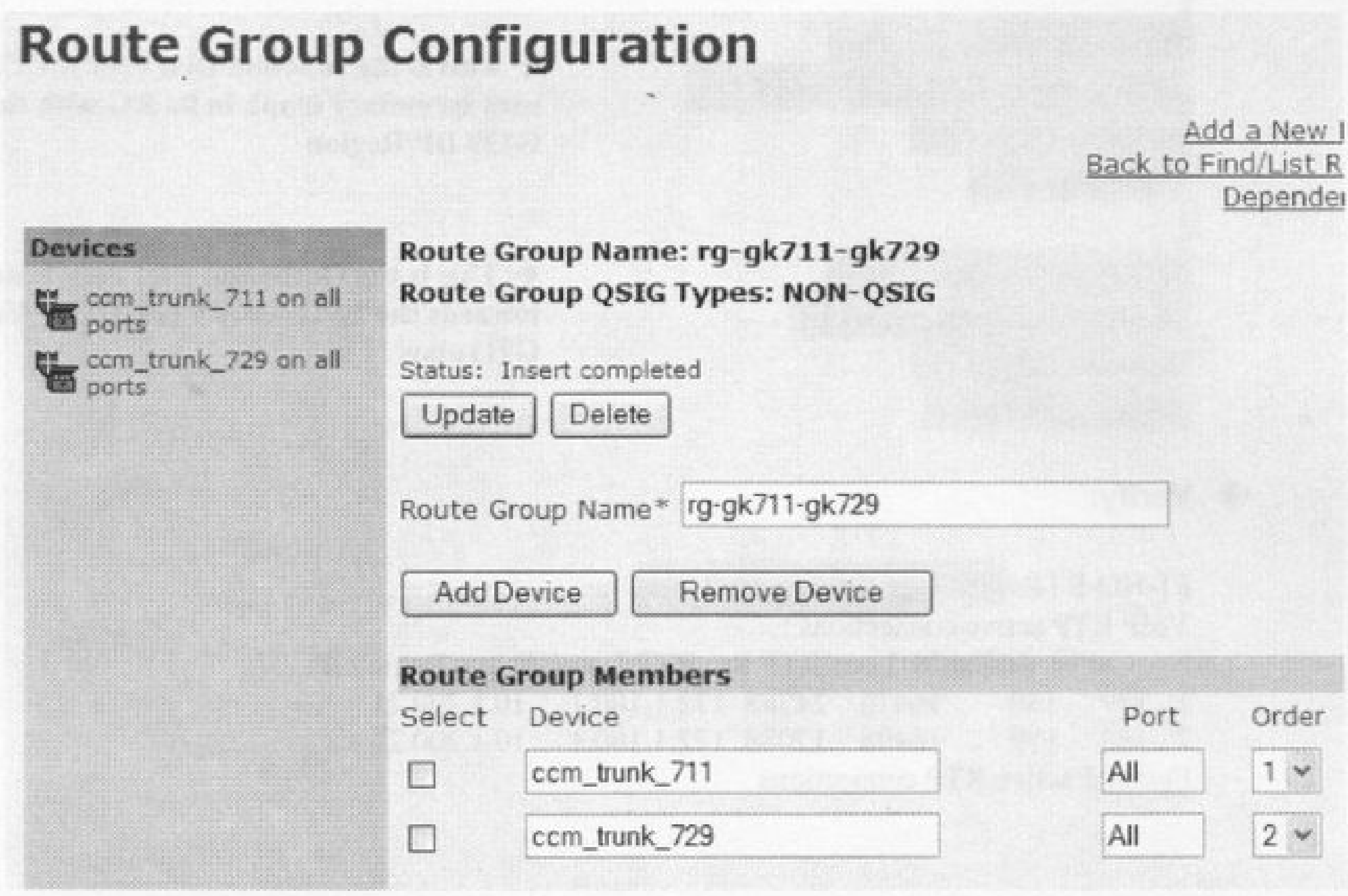


➔ **Rename the existing trunk to "ccm_trunk_711" and create another trunk called "ccm_trunk_729". Assign the ccm_trunk_711 to the gk-711 Device Pool, assign the ccm_trunk_729 to the gk-729 Device Pool. Other parameters in the new trunk should be identical to the trunk created in the earlier task within this section.**





➔ **Create a Route Group as follows:**



Task 28.24

Both media and signaling packets from Call Manager to the remote zone should be sourced from the loopback interface of the HQ router.

➔ **Tell the gatekeeper which calls to use the IPIPGW by way of the via zone commands on the remote zone towards the PSTN-WAN GK.**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.1.100.1
 zone local VGK ipexpert.com
 zone remote PSTN-WAN ipexpert.com 10.1.200.2 1719 invia VGK outvia VGK
 zone prefix PSTN-WAN 011*
 bandwidth remote 144
 no shutdown
!
dial-peer voice 10 voip                     ← This is the Inbound Dial Peer if CCM
 incoming called-number [12]...               uses primary trunk in its RG with G711ulaw
 session target ras                           DP/Region
 codec g711ulaw
!
dial-peer voice 10 voip                     ← This is the Inbound Dial Peer if CCM
 incoming called-number [12]...               uses secondary trunk in its RG with the
 session target ras                           G729 DP/Region
 codec g729r8
!
dial-peer voice 12 voip                     ← This is the Outbound Dial Peer headed off
 destination-pattern 011T                     towards the PSTN-WAN GK/GW – Use
 session target ras                           G711ulaw
 codec g711ulaw
```

➔ **Verify:**

```
P1-HQ-RTR#sh voip rtp connections
VoIP RTP active connections :
No. CallId dstCallId LocalRTP RmtRTP LocalIP     RemoteIP
1   179    180       16470    24788  172.1.100.1 10.1.200.21
2   180    179       16408    17088  172.1.100.1 10.1.200.2
Found 2 active RTP connections
```

Task 28.25

Enable security on the local gatekeeper such that only devices that need to register CAN register (e.g. Call Manager) – other rogue devices should be prevented from registering.

```
gatekeeper
zone local HQ-RTR ipexpert.net 172.1.100.1
zone remote PSTN-WAN ipexpert.net 10.1.200.2 1719 invia VGK outvia VGK
no zone subnet HQ-RTR default enable
zone subnet HQ-RTR 10.1.200.21/32 enable
zone subnet HQ-RTR 10.1.200.20/32 enable
zone subnet HQ-RTR 172.1.100.1/32 enable
bandwidth remote 144
no shutdown
```

Task 28.26

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

➔ **See Task 28.31.**

Task 28.27

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

➔ **See Task 28.31.**

Task 28.28

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed out of the local gatekeeper with the appropriate local gateway acting as backup. Users must be able to dial the BR2 site using extension (4 digit) dialing. **NOTE**: The gatekeeper is expecting the full E164 number, i.e. international prefix '011' plus 10 digits.

```
gatekeeper
zone local HQ-RTR ipexpert.net 172.1.100.1
zone local VGK ipexpert.com
zone remote PSTN-WAN ipexpert.net 10.1.200.2 1719 invia VGK outvia VGK
zone prefix PSTN-WAN 011*
no zone subnet HQ-RTR default enable
zone subnet HQ-RTR 10.1.200.21/32 enable
zone subnet HQ-RTR 10.1.200.20/32 enable
zone subnet HQ-RTR 172.1.100.1/32 enable
bandwidth remote 144
no shutdown
```


➔ **See Task 28.31 for the remainder**

Task 28.29

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway. You must use 4 different methods of digit manipulation to send calls to the PSTN (e.g. one method is by using the 'forward-digits' command inside the POTS dial-peer).

➔ **We are going to use all four of the following: translation-rules, num-exp, prefix, and forward-digits.**

➔ **See Task 28.31 for the completion of this task.**

Task 28.30

Calls originating from BR2 to CallManager (both HQ and BR1) should use VoIP and PSTN as backup. If you decide to register the CME to the gatekeeper use your local HQ-RTR gatekeeper as opposed to the PSTN-WAN gatekeeper. 4-digit dialing must be preserved.

➔ **See Task 28.31.**

Task 28.31

Enable DID for PSTN users dialing into the CM/CME (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits. At BR2, you are not allowed to use translation rules or the 'num-exp' command.

You are not allowed to use translation rules/num-exp for the inbound call, you ARE allowed to use them to achieve Task 28.29!

➔ **When implementing a dial plan it is a good idea to look at all the tasks together rather than treat each question as a separate question.**

➔ **Digit Manipulation should be done in the Route List.**

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-GK	G711 TRUNK G729 TRUNK	1 2
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1-LOC	RG-HQ RG-BR1	PREDOT PREDOT + PREFIX 1212
RL-BR1-HQ-LOC	RG-BR1 RG-HQ	PREDOT PREDOT + PREFIX 1617
RL-HQ-BR1-LD-INT	RG-HQ RG-BR1	PREDOT PREDOT
RL-BR1-HQ-LD-INT	RG-BR1 RG-HQ	PREDOT PREDOT
RL-HQ-TOLLBY	RG-BR1 RG-HQ	PREDOT PREDOT + PREFIX 1617
RL-BR1-TOLLBY	RG-HQ RG-BR1	PREDOT PREDOT + PREFIX 1212
RL-GK-HQ	RG-GK RG-HQ	PREFIX 01133132X PREFIX 01133132X
RL-GK-BR1	RG-GK RG-BR1	PREFIX 01133132X PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ-BR1-LOC
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ-LOC
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ-BR1-LD-INT
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1-HQ-LD-INT
91212.xxxxxxx	PT-BR1-LD	RL-BR1-TOLLBY
91617.xxxxxxx	PT-HQ-LD	RL-HQ-TOLLBY
9.011! 9.011!#	PT-HQ-INT	RL-HQ-BR1-LD-INT
9.011! 9.011!#	PT-BR1-INT	RL-BR1-HQ-LD-INT
3xxx	PT-HQ-911	RL-GK-HQ
3xxx	PT-BR1-911	RL-GK-BR1

➔ **For CCME use the following dial-peers.**

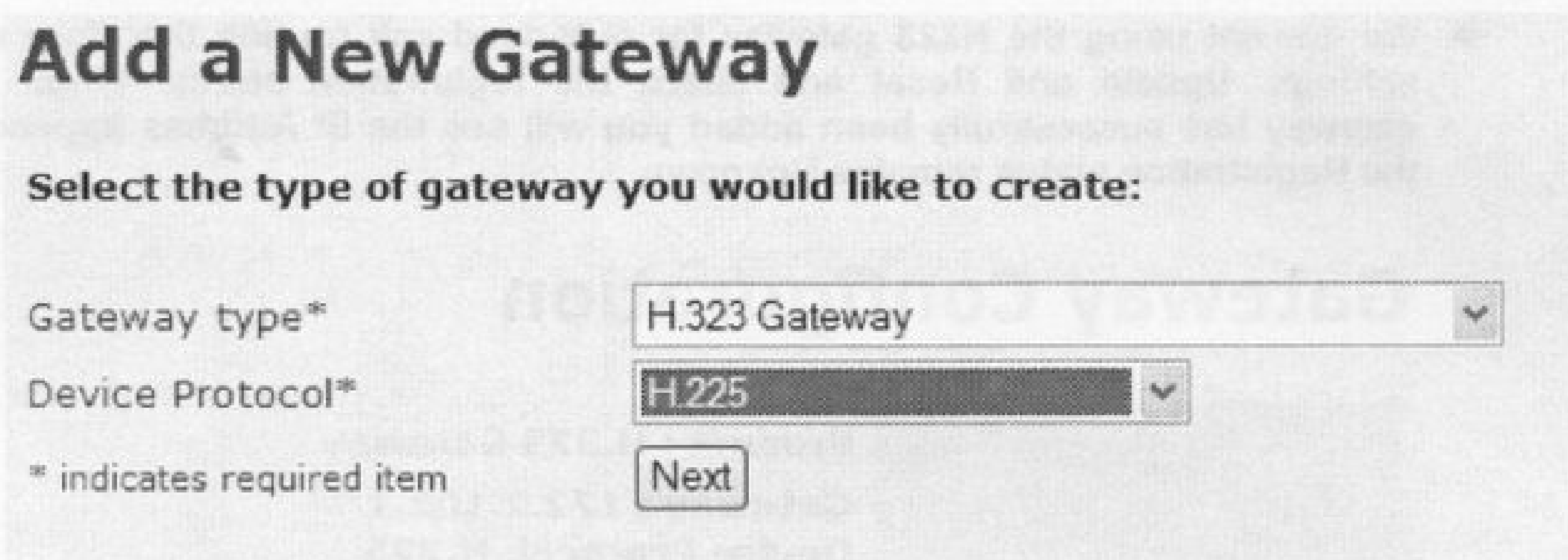
```
translation-rule 1
 rule 0 91 1

dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 translate-outgoing called 1
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1000 voip
 destination-pattern 1...
 session target ipv4:10.1.200.21
 dtmf-relay h245-alphanumeric
 nu huntstop
!
dial-peer voice 1001 pots
 preference 1
 destination-pattern 1...
 no digit-strip
 port 0/0/0:0
 prefix 1212222
!
dial-peer voice 2000 voip
 destination-pattern 916175222...
 session target ipv4:10.1.200.21
 dtmf-relay h245-alphanumeric
```

```
!
dial-peer voice 2001 pots
 preference 1
 destination-pattern 916175222...
 port 0/0/0:0
 forward-digits 11
!
num-exp 2... 916175222...
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
telephony-service
 dialplan-pattern 1 3313213… extension-length 4
```

➔ **We are sending calls directly from CCME to CCM in this particular case (registering CCME to GK is covered in a later section). We must therefore add the CCME as an H323 gateway or an ICT Trunk in CCM otherwise CCM will ignore Call attempts from CCME (since it is an unregistered gateway). We must bind H323 to an interface first – in this example the Loopback.**

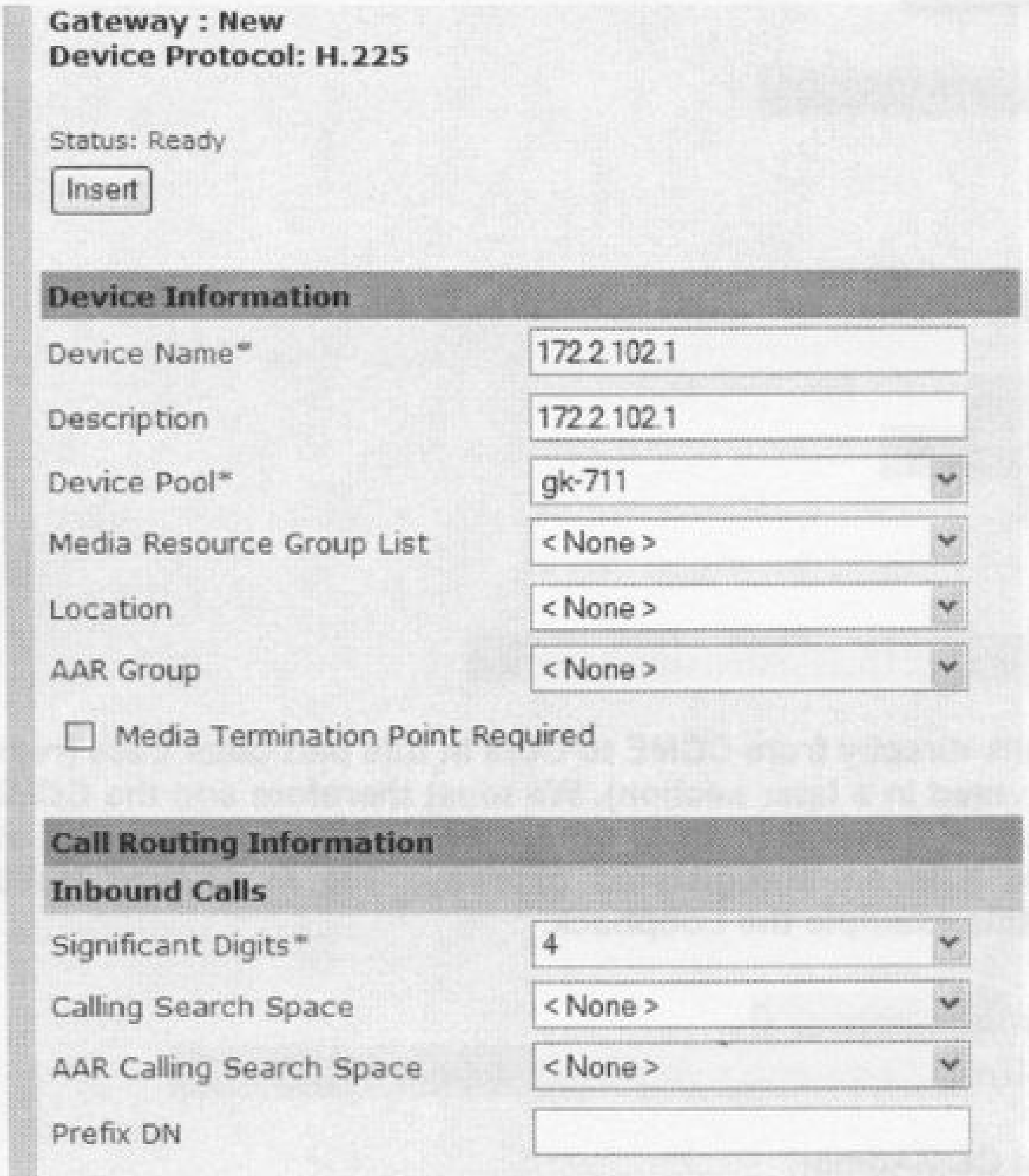
```
P2-BR2-RTR(config)#int loopback 0
P2-BR2-RTR(config-if)#h323-gateway voip bind srcaddr 172.2.102.1
```

➔ **Add the gateway in CCMAdmin.**



➔ **Configure settings on gateway page. Ensure you use the IP Address of the interface you specified as the source Address for H323. Codec and CAC is not specified in the question therefore use the Device Pool which supports all codecs (G711 and G729) and no Locations CAC.**

➔ **For inbound Call Routing set Significant Digits to 4 and assign CSS if required.**



➔ **We are not using the H323 gateway for outbound call routing therefore use any settings. Update and Reset and check the registration status. When a H323 gateway has successfully been added you will see the IP Address appear – Note the Registration status remains Unknown.**

Task 28.32

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 28.33

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 28.34

Configure conference bridge on BR1 router. Use a maximum of 1 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 28.35

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 28.36

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should use the IOS resources and the 6608 resources as backup.

➔ **Put 6608 Media Resources into HQ-MRG.**

➔ **Put IOS Media Resources into BR1-MRG.**

➔ **In HQ-MRGL HQ-MRG should be above BR1-MRG.**

➔ **In BR-MRGL BR1-MRG should be above HQ-MRG.**

➔ **Assign MRG to device pools.**

Task 28.37

Configure a Music on Hold server on the Publisher Call Manager. Add another music source which can be found on the C: drive of your Call Manager. Ensure that the default (Sample) audio source is used when a User presses the 'Hold' button on his/her phone. For all other events that require music to be played use the newly added music source.

➔ **This should be self-explanatory from previous examples.**

Task 28.38

Configure the Call Manager such that HQ phones will receive music using the G711 codec and BR1 phones will receive music using the G729 codec. You cannot use the transcoder to achieve this task.

➔ **This should be self-explanatory from previous examples.**

Task 28.39

Ensure that the HQ and BR1 phones receive multicast music on hold.

➔ **This should be self-explanatory from previous examples.**

Task 28.40

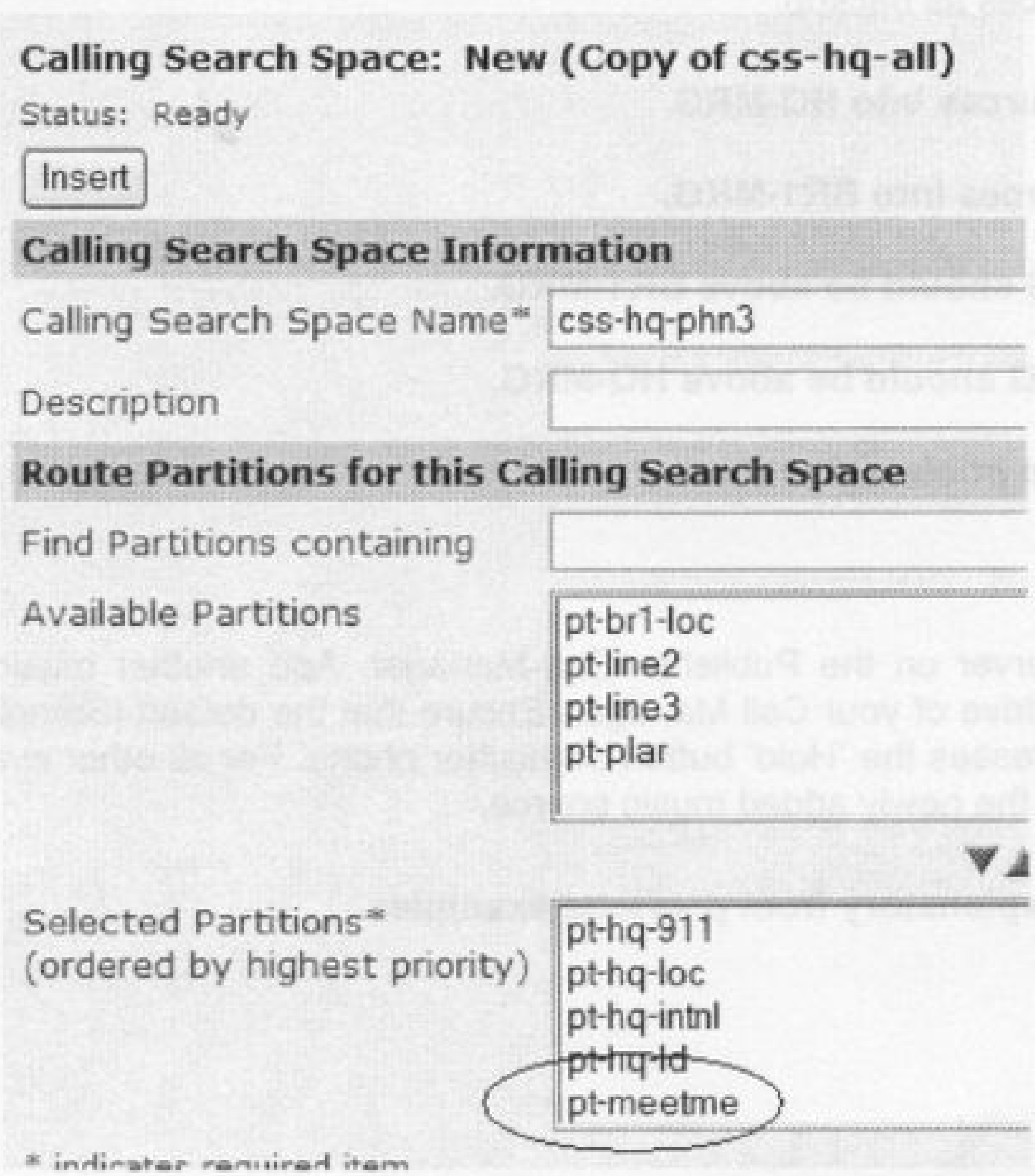
Configure music on hold on the BR2 CME.

➔ **This should be self-explanatory from previous examples.**

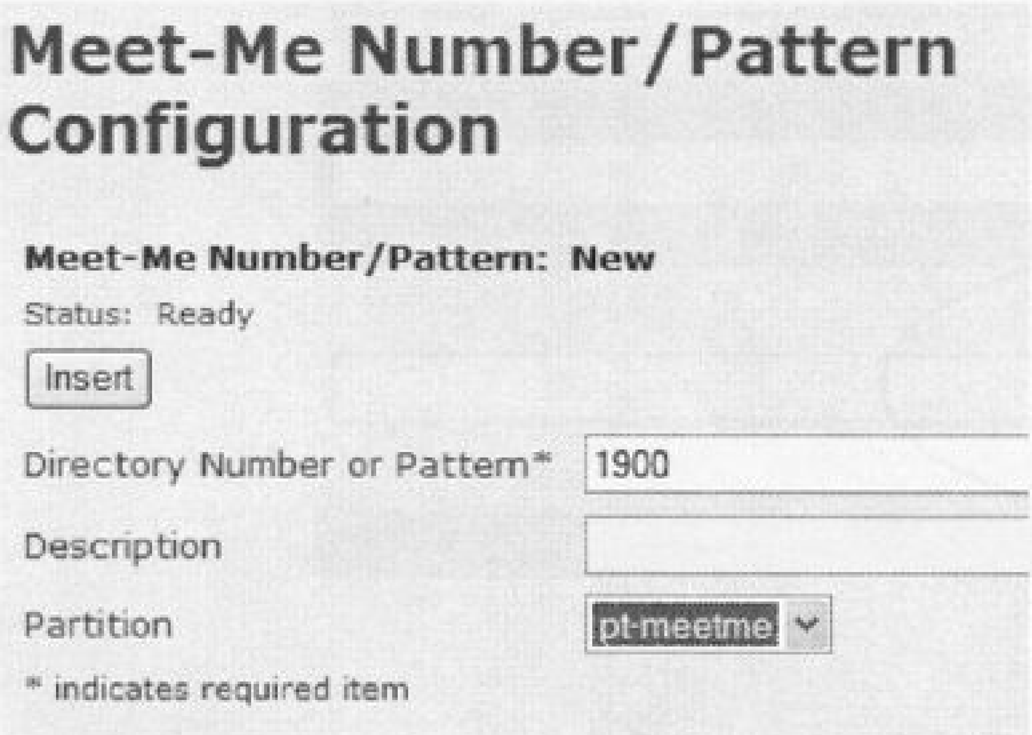
Task 28.41

Create a meet-me conference with DN=1900. Only HQ Phone 3 should be able to initiate the conference – other devices should be able to join/initiate this conference using DN=1901. Set the maximum number of participants of a single Meet-me conference to 6 conferencees.

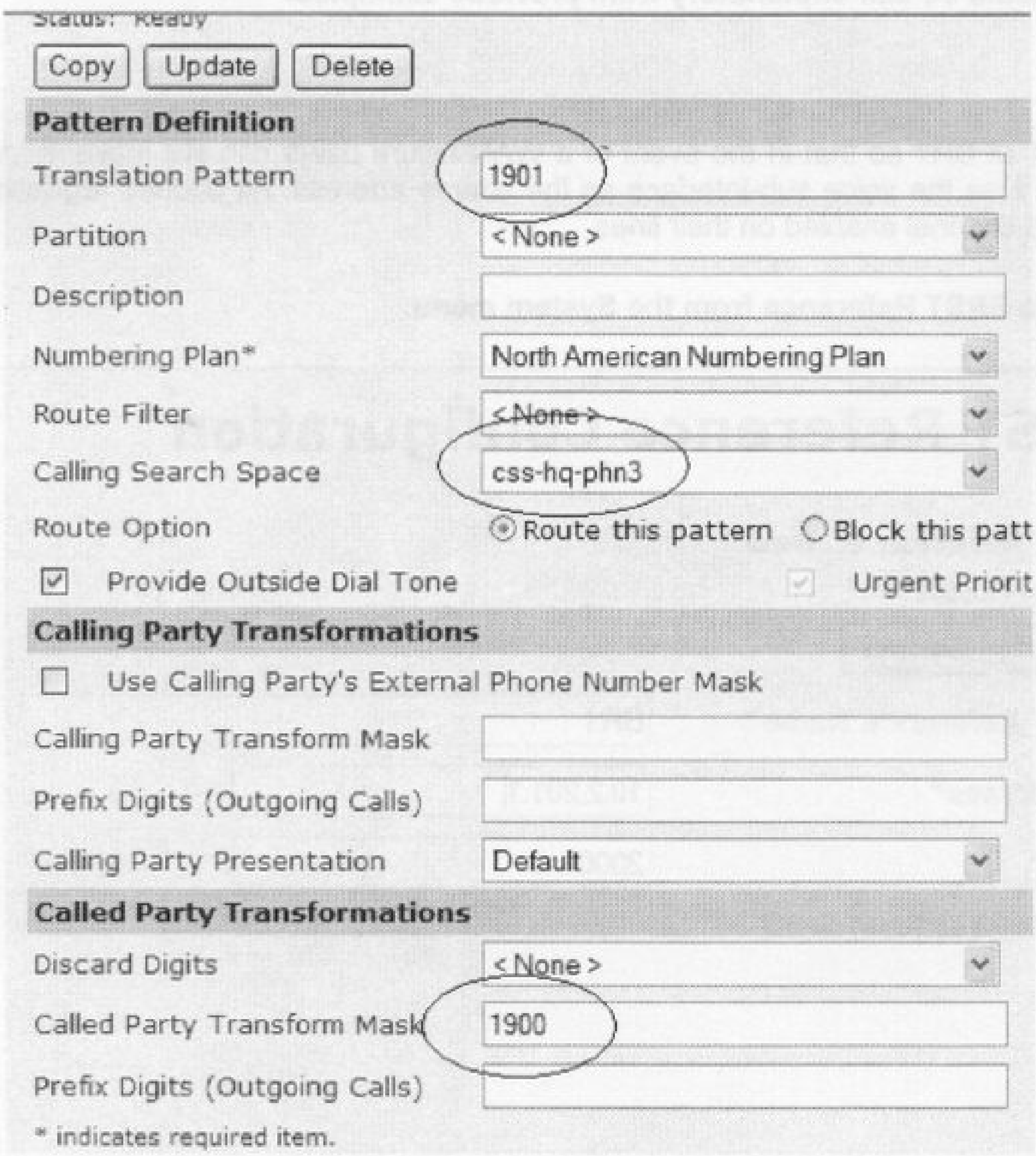
➔ **Create a new partition called PT-MEETME and a new CSS called CSS-HQ-PHN3. Configure the new CSS as below and assign to the Device settings on HQ Phone 3.**



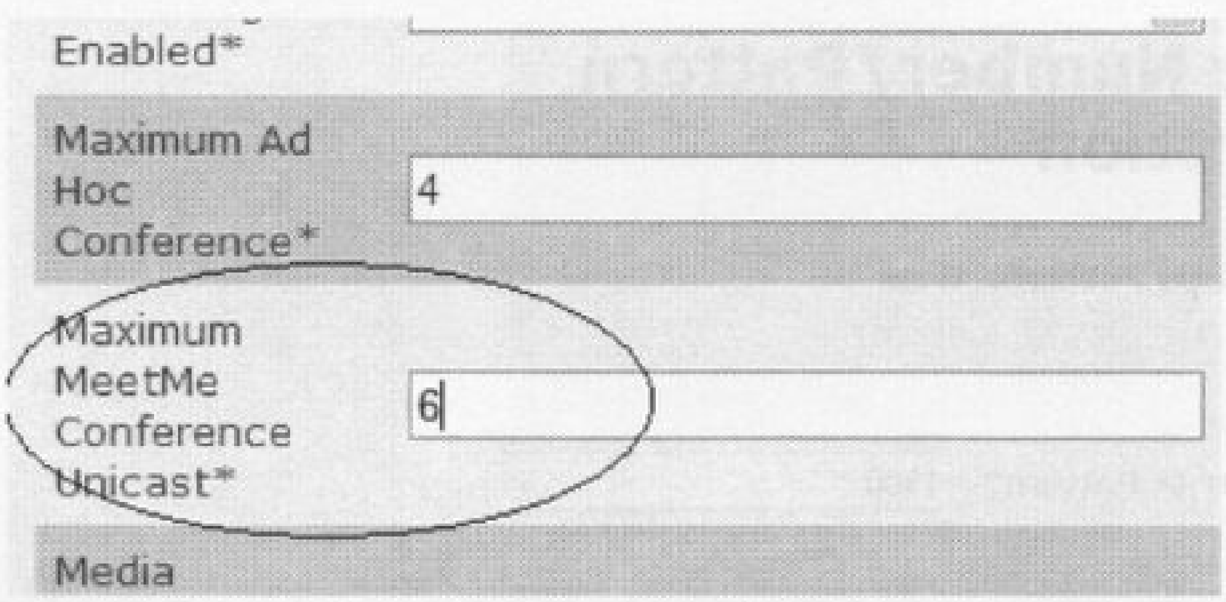
➔ **Create a Meet-me Conference number and place it in the new partition.**



➔ **Create a translation pattern in the Null Partition and Mask the Called Number as shown below. The Translation Pattern must be assigned a CSS with the Meet-me partition visible.**



➔ **Change the following CCM Service Parameter.**



Task 28.42

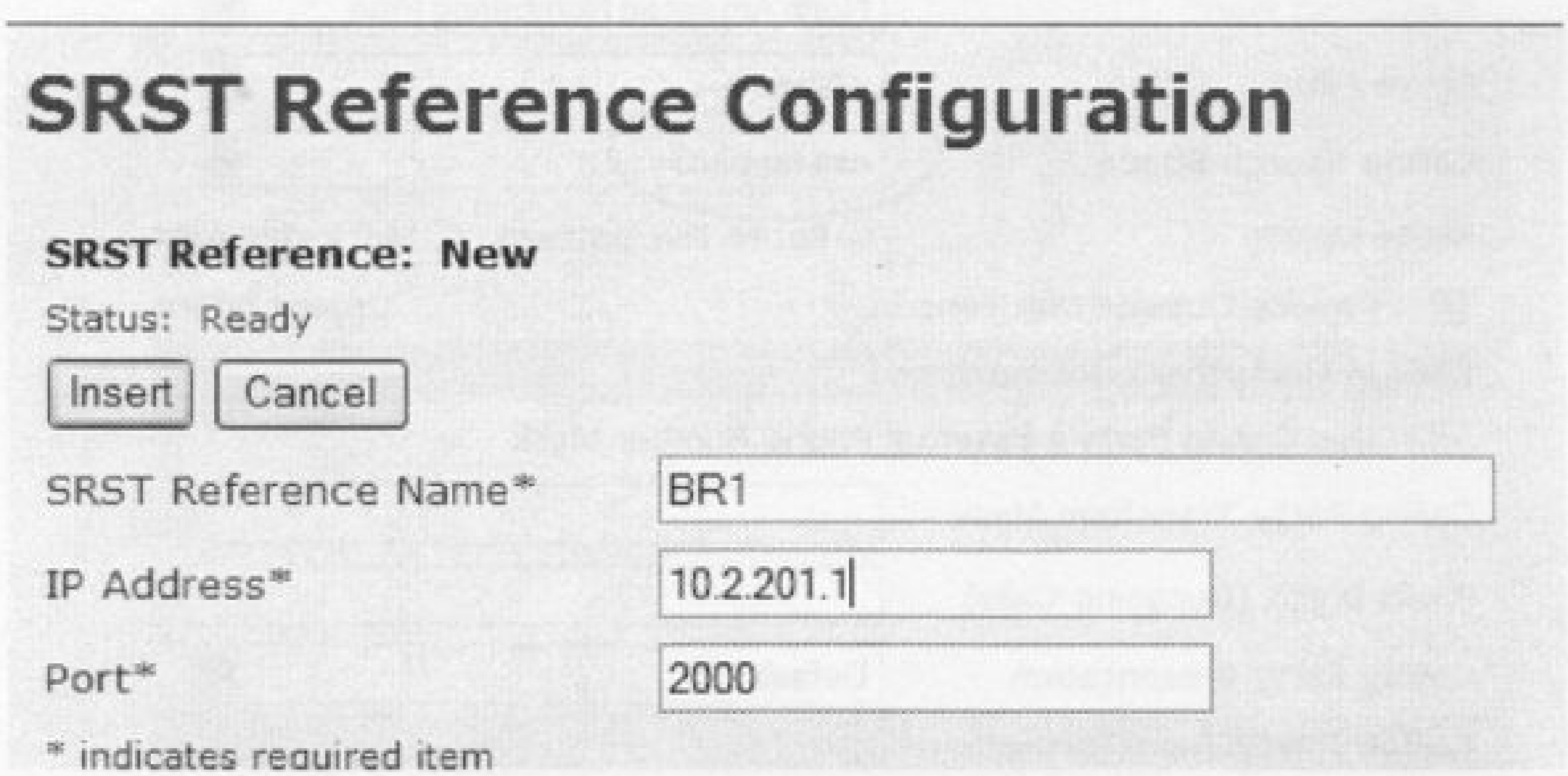
Configure AAR such that calls between HQ and BR1 will be rerouted over the PSTN when there is not enough bandwidth over the WAN. You must preserve 10 digit Calling Number display. The text "*Network Congestion, Rerouting*!!!" must be displayed on the phone when AAR is being used.

➔ **This should be self-explanatory from previous examples.**

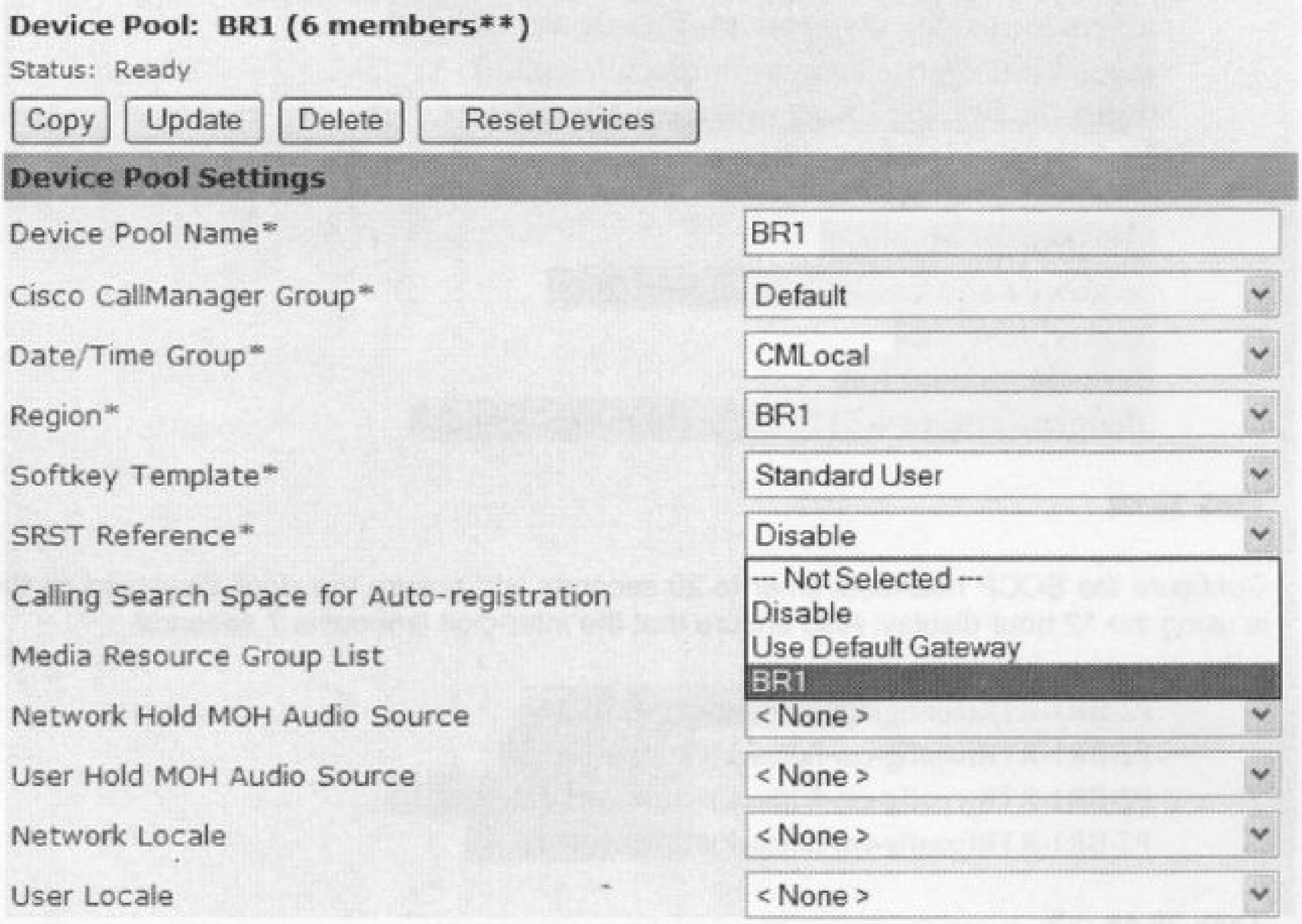
Task 28.43

Configure SRST at BR1 so that in the event of a WAN failure users can still make/receive calls from the PSTN. Use the voice sub-interface as the source address. All phones registered must have the second channel enabled on their lines.

➔ **Create a SRST Reference from the System menu.**



➔ **Assign the SRST Reference to the BR1 Device Pool and reset the BR1 devices.**



➔ **On BR1:**

```
isdn switch-type primary-ni
!
ccm-manager fallback-mgcp
ccm-manager mgcp
!
!
controller T1 2/0/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-3,24 service mgcp
!
!
interface Serial2/0/0:23
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager
 no cdp enable
call application alternate default
!
!
```



```
mgcp
mgcp call-agent 10.2.200.21 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp bind control source-interface Vlan220
mgcp bind media source-interface Vlan220
!
!
call-manager-fallback
 ip source-address 10.2.201.1 port 2000
 max-ephones 24
 max-dn 48 dual-line
 dialplan-pattern 1 6175222... extension-length 4
```

Task 28.44

Configure the SCCP heartbeat timer to 20 seconds and ensure the clock displayed on the phone is using the 12 hour display. Also ensure that the inter-digit timeout is 7 seconds.

```
P2-BR1-RTR(config)#call-manager-fallback
P2-BR1-RTR(config-cm-fallback)#keepalive 20
P2-BR1-RTR(config-cm-fallback)#timeouts interdigit 7
P2-BR1-RTR(config-cm-fallback)#time-format 12
```

Task 28.45

Secure SRST such that phones with existing LSCs will continue to communicate in a secure fashion when in fallback mode.

➔ **This should be self-explanatory from previous examples – See Task 17.3.**

Task 28.46

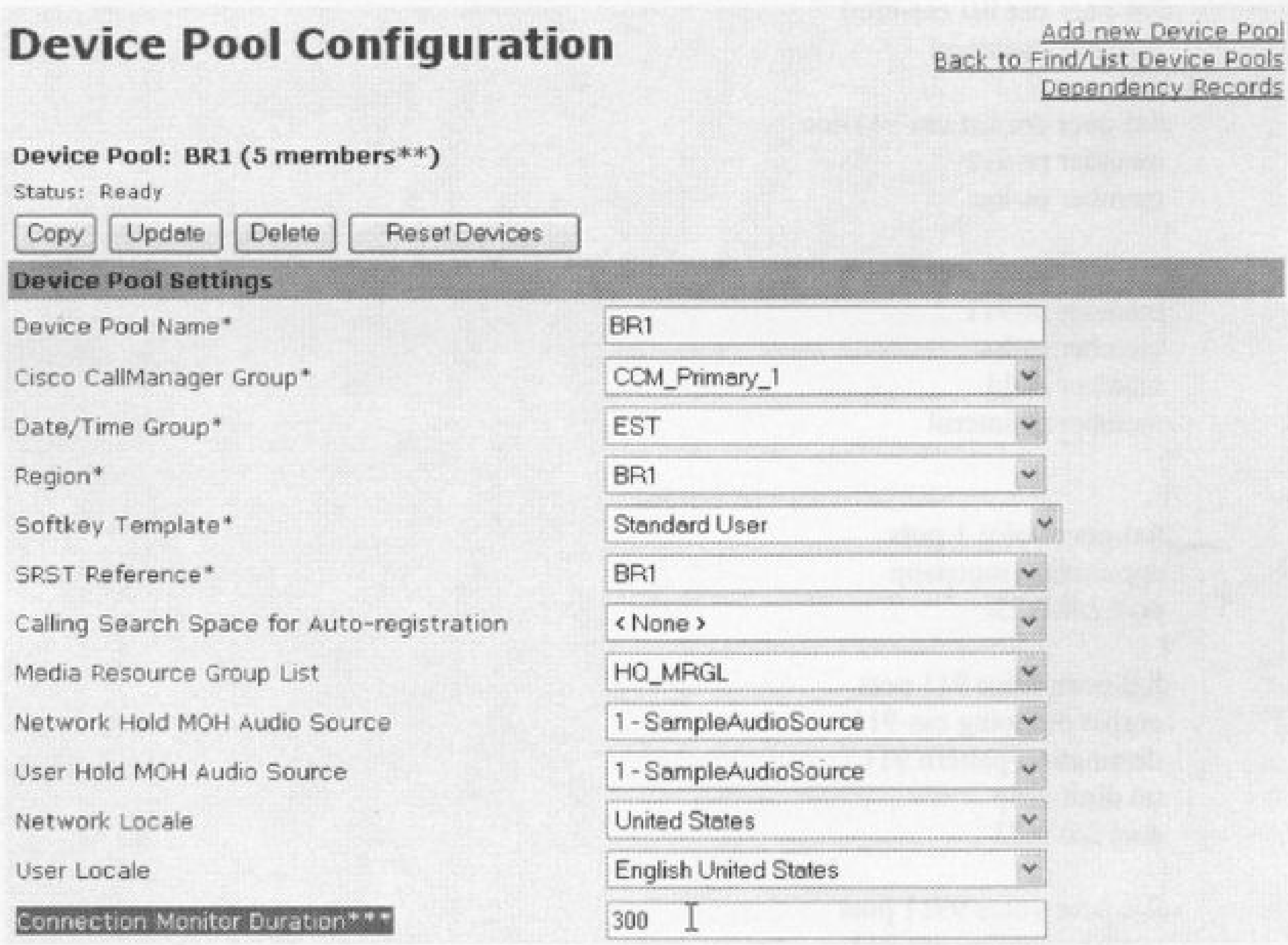
Configure Music on Hold for all phones in SRST fallback.

```
P2-BR1-RTR(config-cm-fallback)#moh music-on-hold.au
```

Task 28.47

Configure SRST such that the phones will only re-register back to CallManager after normal service has been resumed for 5 minutes. (normal service is defined as the WAN is operational and CallManager is running).

➔ **In CCM for the DP that contains devices to register to BR1 SRST.**



Task 28.48

Calls to HQ and BR2 must be preserved using 4 digit dialing.

➔ **See next Task.**

Task 28.49

Ensure that the same Class of restriction is preserved when phones are in SRST fallback.

```
num-exp 1... 12122221...
num-exp 3... 0113313223...

dial-peer cor custom
 name pt-911
 name pt-loc
 name pt-ld
 name pt-interml
!
!
dial-peer cor list css-911
```



```
 member pt-911
!
dial-peer cor list css-loc
 member pt-loc
!
dial-peer cor list css-ld
 member pt-ld
!
dial-peer cor list css-intnl
 member pt-internl
!
dial-peer cor list css-911-loc
 member pt-911
 member pt-loc
!
dial-peer cor list css-ALL
 member pt-911
 member pt-loc
 member pt-ld
 member pt-internl
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 2/0/0:23
!
dial-peer voice 911 pots
 corlist outgoing css-911
 destination-pattern 911
 no digit-strip
 port 2/0/0:23
!
dial-peer voice 9911 pots
 corlist outgoing css-911
 destination-pattern 9911
 no digit-strip
 forward-digits 3
 port 2/0/0:23
!
dial-peer voice 7 pots
 corlist outgoing css-loc
 destination-pattern 9[2-9]......T
 port 2/0/0:23
 forward-digits 7
!
dial-peer voice 11 pots
 corlist outgoing css-ld
 destination-pattern 91[2-9]..[2-9]......
 port 2/0/0:23
 forward-digits 11
!
dial-peer voice 110 pots
 corlist outgoing css-intnl
 destination-pattern 9011T
 port 2/0/0:23
 prefix 011
```

```
!
dial-peer voice 1001 pots
 destination-pattern 12122221...
 no digit-strip
 port 2/0/0:23
!
dial-peer voice 3001 pots
 destination-pattern 0113313223...
 no digit-strip
 port 2/0/0:23
!
dial-peer voice 2 pots
 incoming called-number .
corlist incoming css-911
 direct-inward-dial

call-manager-fallback
 max-conferences 1
 timeouts interdigit 7
 ip source-address 10.2.201.1 port 2000
 max-ephones 24
 max-dn 48 dual-line
 dialplan-pattern 1 6175222... extension-length 4
 keepalive 20
 moh music-on-hold.au
 cor incoming css-911-loc 1 2002 - 2003
 cor incoming css-ALL 2 2002
 cor outgoing css-intnl 3 2002
```

Task 28.50

Configure Class of Restriction such that no PSTN caller can dial BR1 phone 2.

➔ **See previous task.**

Task 28.51

Integrate Call Manager with Unity with the following information:

- Voice Mail Pilot = 1600
- Voice Mail Ports = 1601-1604
- MWI On/Off = 1999/1998

➔ **This should be self-explanatory from previous examples.**

Task 28.52

Configure the BR2 router to support the CUE module using information from Table 16. Setup the basic information needed to work the CUE module including what is needed to access the web-based GUI to manipulate user's extensions and mailboxes:

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

Finally setup mailboxes for all 3 phones at BR2.

Also ensure that when Callers leave Voicemail, that their callerID will be read to the recipient.

➔ **This should be self-explanatory from previous examples – See Tasks 15.1 and 15.3.**

Task 28.53

Configure Unity to be an Inbound and Outbound Fax Server. Create the necessary VM box for BR1 Phone 2 and ensure that Faxes coming in from the BR1 Gateway arrive in the appropriate user's mailbox (Table 17). Ensure that Faxes going out to the PSTN number in Table 18 from the BR1 Gateway arrive and are viewable.

➔ **This should be self-explanatory from previous examples – See Task 9.9 and 9.10.**

Task 28.54

Phone 1 at HQ should be configured with a Unity subscriber account with DN=1001. You must create this subscriber account using the Bulk Import Tool and a CSV file. Record a subscriber greeting.

➔ **This should be self-explanatory from previous examples - see section 9 for further information.**

Task 28.55

Phone 3 at HQ should use the corresponding subscriber account of Phone 1 (i.e. extension '1003' will use the voicemail account for '1001'). Ensure the Phone 1 subscriber greeting is heard when Phone 3 is forwarded to voicemail and that MWI lights up both phones.

➔ **This should be self-explanatory from previous examples – see section 9 for further information.**

Task 28.56

Create a Unity subscriber account for BR1 phone 1 with DN = 22001. Record a subscriber greeting. When Call Forward occurs from extension '2001' the correct subscriber greeting must be heard and MWI must be working correctly. You may NOT use Alternate Extension or Alternate MWI to achieve this task.

➔ **This should be self-explanatory from previous examples – see section 9 for further information.**

Task 28.57

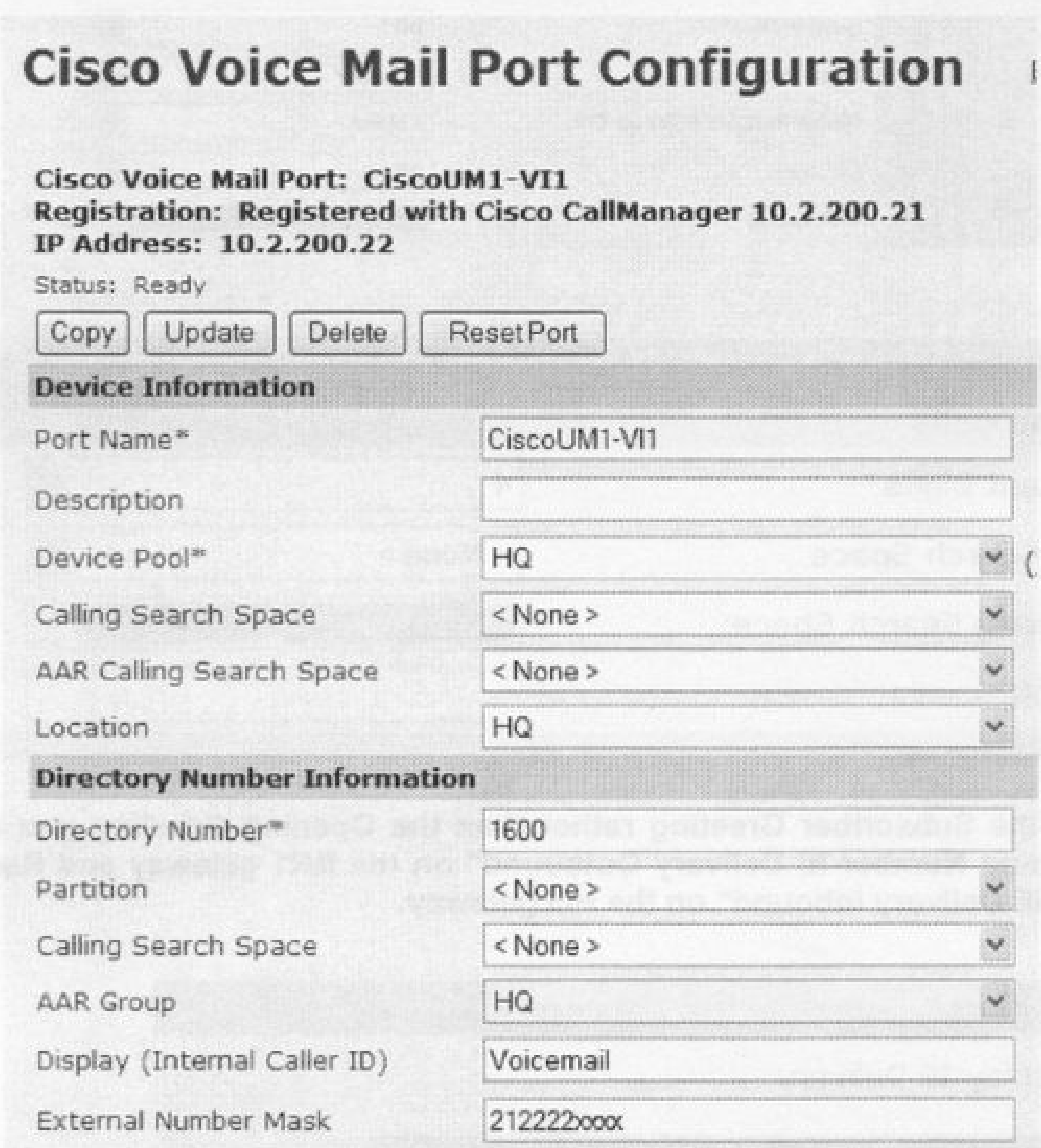
Configure Unity so that if a IP Phone caller conferences in Ext 1650, that Unity will record the conversation and forward that recording to the mailbox of the IP Phone that initiated the conference.

➔ **This should be self-explanatory from previous examples – See Section 9.8.**

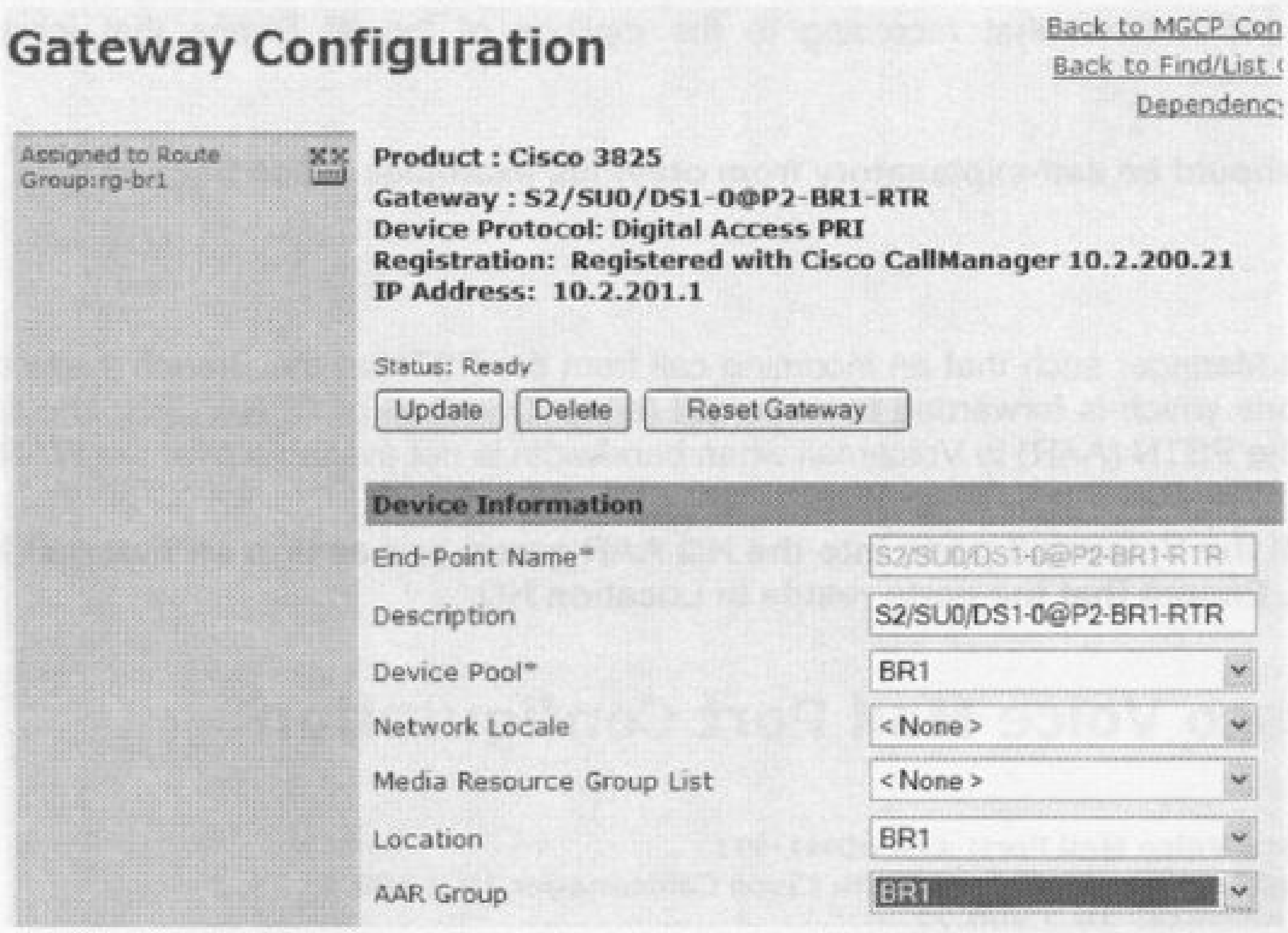
Task 28.58

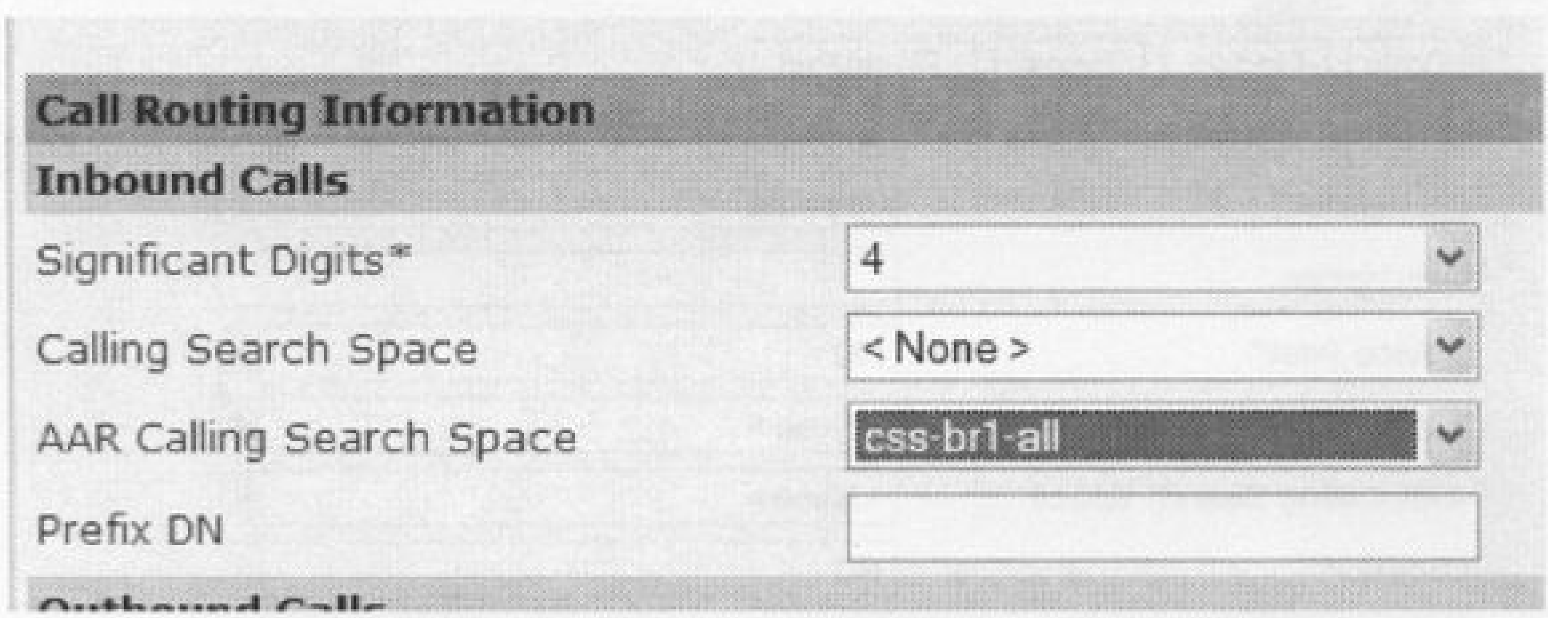
Configure Call Manager such that an incoming call from the PSTN at the Branch 1 site destined for a BR1 phone which is forwarded to voicemail (either Divert all or CFNA/CFB) should be re-routed out of the PSTN (AAR) to Voicemail when bandwidth is not available over the WAN.

➔ **Put all the Voicemail ports into the HQ AAR group and assign an External Number Mask. Ensure that the ports reside in Location HQ.**

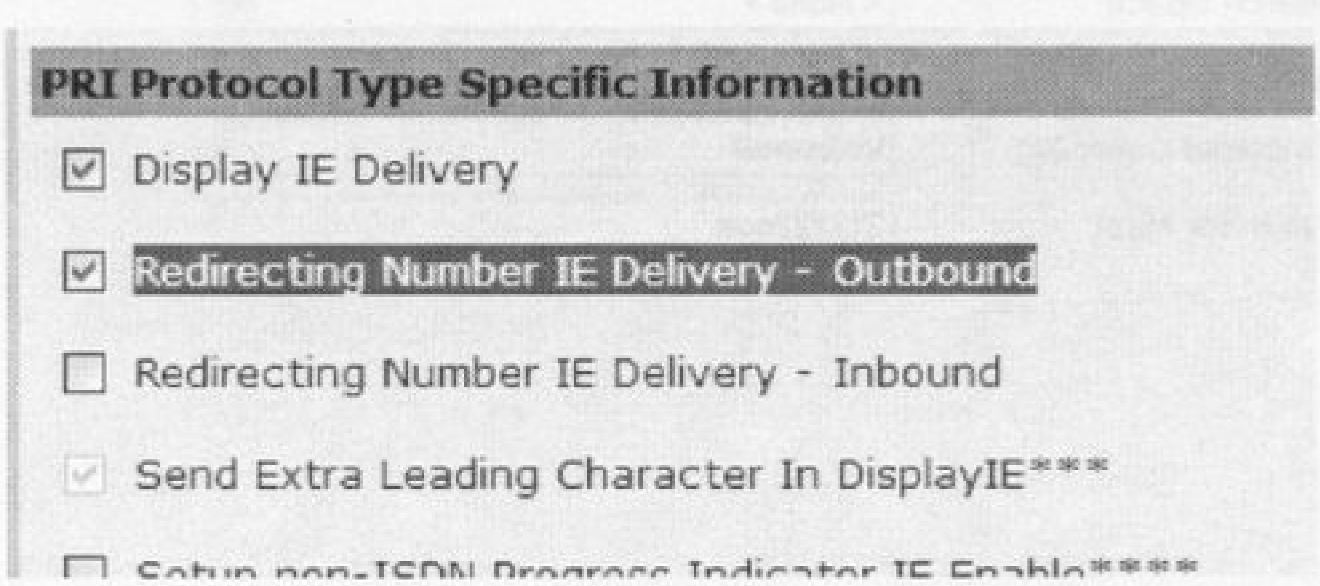


➔ **Put the BR1 IOS MGCP gateway into the BR1 AAR Group and assign an AAR CSS. Ensure that the GW resides in Location BR1.**





➔ **To hear the Subscriber Greeting rather than the Opening Greeting you must set "Redirecting Number IE Delivery Outbound" on the BR1 gateway and Redirecting Number IE Delivery Inbound" on the HQ gateway.**



PRI Protocol Type Specific Information

- [x] Display IE Delivery
- [ ] Redirecting Number IE Delivery - Outbound
- [x] Redirecting Number IE Delivery - Inbound
- [x] Send Extra Leading Character In DisplayIE***

Task 28.59

Configure Auto-attendant and ICD with the following information:

- AA Route Point = 1710
- Script = aa.aef
- CTI Ports = 1711, 1712

- ICD Route Point = 1700
- Script = icd.aef
- CTI Ports = 1701, 1702

Create the following users that will be used in this task:

- "**jtapi**" to be used for the JTAPI Subsystem.
- "**rmjtapi**" to be used for the ICD Subsystem.
- "**telecaster**" to be used for the ICD Subsystem and enterprise data.
- "**crsadmin**" which must be the designated administrator for IPCC Express.
- **agent1** [assigned device HQ Phone 3 with ICD ext="1003"].
- **agent2** [assigned device BR Phone 2 with ICD ext="2003"]

[all passwords must be 'cisco' and PIN numbers set to '12345' except of course 'telecaster']

For the ICD application you must use skills based routing with the following information:

- CSQ: "GeneralQ"
- Skills: "sales" & "support"
- 'agent1' shall have the skill of 'support' at a proficiency level of 9 and the skill of 'sales' at a proficiency level of 10
- 'agent2' shall have the skill of 'support' at a proficiency level of 10 and the skill of 'sales' at a proficiency level of 9
- The CSQ 'GeneralQ' should have both skills assigned to it with a proficiency level of at least 5 or better for each
- With this stated, the engine should always choose agent1 over agent2 if agent1 is available (you may use whatever method you wish to accomplish this in the engine)
- The engine should also send every agent into a automatic state of 'Work' for 30 seconds before then automatically returning them to a state of 'Ready' (this should happen regardless of whether the call is routed to a specific agent or through the GeneralQ.

➔ **This should be self-explanatory from previous examples – See Tasks 10.1.**

Task 28.60

Modify the "icd.aef" script with the following information (you may wish to rename it to avoid loosing the original script:

- You must determine if the call is coming from the PSTN from anywhere in the area code of '617' and if the call is coming from the 617 area code then the call must check to see if 'agent1' is available and route the call directly to that agent without queuing the call, however if agent1 is not available, send the call to the 'GeneralQ'.
- If the call goes to the GeneralQ, music should be played to the caller while waiting in Q and the caller should also hear the 'QueuePrompt' every 30 seconds.
- Regardless of whether the call is routed to a specififc agent or through the GeneralQ, the agent receiving the call should be presented with Enterprise Data showing both the ANI of the call and a disposition of how the call was routed (a string showing 'Agent' or 'Queue').

➔ **This should be self-explanatory from previous examples – See Tasks 10.2.**

Task 28.61

Configure IPCC Phone Agent for both phones and also ensure that they only have to press the services button once (i.e. that they don't have to provide User/Ext/Pin information on the phone when logging in).

➔ **This should be self-explanatory from previous examples – See Tasks 10.3.**

Task 28.62

Configure Attendant Console with Pilot number = '1550'. Add HQ phone 3 and BR1 phone 3 into the huntgroup. Enable Circular Hunting within the AC huntgroup. Also ensure that if there are up to 20 callers simultaneously calling 1550, and both IP Phones are presently taking calls, that callers will not be dropped but any number greater that 20 callers will be dropped and not sent to VM. Also, a call should not be dropped no matter how long it remains waiting.

➔ **This should be self-explanatory from previous examples – See Tasks 11.1 and 11.3.**

Task 28.63

Configure calls such that a HQ user must enter a forced auth code with a level of at least 20 or better in order to be allowed to dial an LD number and one of 30 or better in order to be allowed to dial an International number. See Table 19 for Auth Codes.

➔ **This should be self-explanatory from previous examples – See Tasks 11.15.**

Task 28.64

Restrict internal callers from BR1 only, so that they may not see CNAM information only regarding who they are calling or who is calling them, however ensure that BR1 Phone 3 **can** see all CNAM information.

➔ **This should be self-explanatory from previous examples – See Tasks 11.14.**

Task 28.65

Enable support for a VTA camera on HQ Phone 3.

➔ **This should be self-explanatory from previous examples – See Tasks 11.12.**

Task 28.66

Configure IPMA with the following information: BR1 phone 3 will be used as the manager phone and HQ phone 3 will be used as the assistant phone.

Username: br1phn3	**Username: Assistant**
Primary Line: 2003	Primary Line: 1003
SD to Intercom	Proxy Line: 1560
	Incoming Intercom

➔ **This should be self-explanatory from previous examples.**

Task 28.67

Assume the single cable solution is used, configure the switches to trust the Layer 2 QoS classification of the IP phones but not the attached PC.

➔ **On 6500:**

```
set qos enable

set port qos 2/7-8 vlan-based
set port qos 2/7-8 trust-ext untrusted
set qos acl ip POD12_IP-PHONES trust-cos ip any any
commit qos acl POD12_IP-PHONES
set qos acl map POD12_IP-PHONES 220
```

➔ **On the 3550 enable QoS globally and enter the interface commands.**

```
3550G-Access(config)#mls qos
3550G-Access(config)#interface range FastEthernet0/23 - 24
Switch(config-if-range)# mls qos trust cos
Switch(config-if-range)# switchport priority extend cos 0
```

➔ **On the 3825 Etherswitch same as 3550 except no need to enable qos globally.**

Task 28.71

Configure FRTS and apply to the PVC between HQ and BR2, however do so in such a way that the traffic shaper only engages when Voice traffic is present on the link. For this task you may assume that the FR port speed is 768kbps and that the CIR provided by the carrier is 384. A proper LFI mechanism should be engaged at all times and should be relevant to the CIR not the Port speed.

➔ **This should be self-explanatory from previous examples – See Tasks 12.10.**

Task 28.72

Assume that CUE does not mark any of its traffic with correct DSCP bits. Ensure that in the router, this traffic is marked correctly as soon as it comes from CUE and ensure that it follows the same standards of marking set from CCM regarding voice and call control.

➔ **This should be self-explanatory from previous examples – See Tasks 15.5.**

Task 28.73

Configure Low Latency Queuing (LLQ) for the HQ and Branch 2. Allocate 33% of the total bandwidth to Media and 2% as one of the CBWFQ for the control traffic.

➔ **On both the HQ-RTR and BR2 router configure class-maps and policy maps shown below.**

```
class-map match-any RTP
 match ip dscp ef
class-map match-any SIG
 match ip dscp af31
!
!
policy-map LLQ
 class RTP
  priority percent 33
 class SIG
  bandwidth percent 2
 class class-default
  fair-queue
```

➔ **Apply the service policy to the frame-relay map-class on both routers.**

➔ **On BR2:**

```
P2-BR2-RTR(config)#map-class frame-relay FRTS
P2-BR2-RTR(config-map-class)#service-policy output LLQ
```

➔ **On HQ-RTR:**

```
P2-HQ-RTR(config)#map-class frame-relay FRTS
P2-HQ-RTR(config-map-class)#service-policy output LLQ
```

```
P2-HQ-RTR#sh policy-map interface Serial0/1/0:0.2
 Serial0/1/0:0.2: DLCI 202 -

  Service-policy output: LLQ

    Class-map: RTP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp ef
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 72
        Bandwidth 33 (%)
        Bandwidth 252 (kbps) Burst 6300 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: SIG (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Output Queue: Conversation 73
        Bandwidth 2 (%)
        Bandwidth 15 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      1 packets, 84 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 64
        (total queued/total drops/no-buffer drops) 0/0/0
```

Task 28.74

Configure LLQ between the HQ and Branch 1 sites. Allocate 256Kbps for media and 8Kbps for signaling. Assume the speed of the PVC between HQ and Branch 1 is 1544 Kbps.

- ➔ **As before, create class-maps and policy-maps to fit the requirement.**
- ➔ **Apply the Service Policy enabling LLQ in the PVC.**

➔ **On HQ-RTR:**

```
policy-map LLQ-BR1
 class RTP
  priority 256
 class SIG
  bandwidth 8
 class class-default
  fair-queue

map-class frame-relay FRTS
 frame-relay cir 1466800
 frame-relay bc 14668
 frame-relay be 0
 frame-relay mincir 1466800
 service-policy output LLQ-BR1

interface Serial0/1/0:0.1
ip address 162.2.101.1 255.255.255.0
 ip ospf mtu-ignore
ip pim sparse-dense-mode
frame-relay interface-dlci 201
 class FRTS
```

➔ **On BR1:**

➔ **As before, create class-maps and policy-maps to fit the requirement.**

➔ **Apply the Service Policy enabling LLQ in the *map-class*.**

```
interface Serial0/1/0
 no ip address
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0/1/0.1 point-to-point
 ip address 162.2.101.2 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf mtu-ignore
 frame-relay interface-dlci 101
  class FRTS

map-class frame-relay FRTS
 frame-relay cir 1466800
 frame-relay bc 14668
 frame-relay be 0
 frame-relay mincir 1466800
 service-policy output LLQ-BR1
```


NOTE:

- In policy-map statements the PQ and CBWFQ should both be specified as a percentage or both be explicitly stated – you can't mix 'n match.
- If the table in the QoS SRND does not have an entry for the PVC speed, CIR should be set to 95% of the PVC speed to take into account FR headers.
- To verify issue the command *sh policy-map interface*

Task 28.75

Use the Catalyst 6500 policer to police all control traffic originating from Call Manager to 32 Kbps – the exceed action should be to drop excess control traffic.

➔ **In the Cat 6000:**

➔ **Define the policer - either microflow or aggregate. The name of the policer given in this example is "remark-sig". The policed rate is 64Kbps with a burst size of 13Kbits. The exceed action (all packets on the VLAN/Interface which are in excess of 32Kbps traffic) is to remark the DSCP value.**

➔ **The DSCP will be marked down to DSCP=10 – this step is performed in global configuration.**

➔ **Apply the policer to the ACL we created earlier. Commit and apply to the CCM port.**

```
PL-VoicePod-6500> (enable) set qos policer aggregate remark-sig rate 32 burst 13 policed-dscp
QoS policer for aggregate remark-sig updated successfully.
PL-VoicePod-6500> (enable) set qos policed-dscp-map 26:10
QoS policed-dscp-map set successfully.
PL-VoicePod-6500> (enable) set qos acl ip POD12_SERVER dscp 26 aggregate remark-sig any
POD12_SERVER editbuffer modified. Use 'commit' command to apply changes.
PL-VoicePod-6500> (enable) commit qos acl POD12_SERVER

QoS ACL 'POD12_SERVER' successfully committed.
PL-VoicePod-6500> (enable) set qos acl map POD12_SERVER 2/42
ACL POD12_SERVER is successfully mapped to port 2/42.
```

NOTE:

- To determine the burst parameter, use this equation:

  Burst = (Rate [bps]) * 0.00025 [sec/interval]) *or* (maximum packet size [bits]), whichever is greater.

- For example, if you want to calculate the minimum burst value needed to sustain a rate of 1 Mbps on an Ethernet network, the rate is defined as 1 Mbps and the maximum Ethernet packet size is 1518 bytes. The equation is:

  Burst = (1,000,000 bps * 0.00025) *or* (1518 bytes * 8 bits/byte) = 250 *or* 12144.

- The larger result is 12144, which you round to 13 kbps.

Task 28.76

Configure Fax Passthru throughout the network.

➔ **This should be self-explanatory from previous examples.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 29: Multiprotocol Challenge L

Estimated Time to Complete: 10 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 29 Multiprotocol Challenge L

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 29 Configuration Tasks

Task 29.1

Ensure that the link between the HQ/BR1/BR2 routers and appropriate switches are configured as DOT1Q trunks. Give the voice sub-interface the appropriate ip address from Table 1. Check connectivity between all sites and to Call Manager/Unity.

➔ **This should be self-explanatory from previous examples.**

Task 29.2

Configure Voice and Data VLAN for all IP Phones including ATA and VG248. VLAN IDs are defined in Table 2. Use Table 3 for HQ site 6500 port assignment. For BR1 and BR2 port allocation you are required to find out port allocation by your own methods.

➔ **This should be self-explanatory from previous examples.**

Task 29.3

Set the clock on the HQ router to poll and set its time from the PSTN-WAN router (See Table 1 for IP address). Configure the BR1 and BR2 routers to be able to poll and update their times from the HQ router loopback interface.

➔ **On HQ-RTR:**

```
ntp peer 10.1.200.2
ntp source loopback0
```

➔ **On BR1 and BR2 routers:**

```
ntp server 10.1.200.3
```

Task 29.4

For Headquarter and Branch 1, use Microsoft DHCP server to allocate IP address for all Devices. For Branch 2, use IOS DHCP to allocate IP address for the IP phones. For each voice subnet, allocate the IP address from .50 to .69.

➔ **This should be self-explanatory from previous examples.**

Task 29.5

Configure CallManager and register devices manually using CDP information. Assign directory number to devices based on Tables 5 and 6. Also Assume a Publisher exists (Table 1) and every phone is registered in a CCM Group first to a Subscriber, and then to the Publisher. Configure the keepalive interval between any IP Phone and the Publisher server CallManager to be set to 40 seconds.

→ **This should be self-explanatory from previous examples – See Task 2.6.**

Task 29.6

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

→ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 29.7

Use CallManager's only CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

→ **This should be self-explanatory from previous examples – See Task 2.2.**

Task 29.8

Ensure that when a user presses the 'Services' or 'Directories' button the error message is not displayed.

→ **This should be self-explanatory from previous examples.**

Task 29.9

Configure Calling Restriction using the Table below.

→ **This should be self-explanatory from previous examples.**

Task 29.10

Set the phones that reside in the POD (all 79XX not physically accessible to you) to auto-answer. Phones must only auto-answer after 5 seconds.

→ **This should be self-explanatory from previous examples.**

Task 29.11

Register phones at BR2 based on Table 7.

➔ **This should be self-explanatory from previous examples.**

Task 29.12

Create a shared line on Branch 2 phones 1 and 2 with DN 3010. The first call coming into the shared line must ring both phones. When a second call comes into the shared line it must ring both phones again but this time ringing in as a Call Waiting call on the active phone.

```
ephone-dn 1 dual-line
 number 3001
!
ephone-dn 2 dual-line
 number 3002
!
ephone-dn 3 dual-line
 number 3010
 no huntstop
 huntstop channel
!
ephone-dn 4 dual-line
 number 3010
 preference 1
 huntstop channel
!
ephone 1
 mac-address 0011.BBEF.6901
 type 7940
 button 1:1 2c3,4
!
ephone 2
 mac-address 0011.BBE0.5775
 type 7940
 button 1:2 2c3,4
```

Task 29.13

BR2 should use the same class of restriction as the other sites.

➔ **This should be self-explanatory from previous examples.**

Task 29.14

International calls should be blocked from all phones Mon-Fri outside office hours. Office hours are 9am-5pm. Allow phone 3 at BR2 to be able to enter a code in order to make International calls after hours, and make phone 2 to never be restricted for after hours international calls.

```
telephony-service
 after-hours block pattern 1 9011
 after-hours day Sun 23:59 12:00
 after-hours day Mon 17:01 08:59
 after-hours day Tue 17:01 08:59
 after-hours day Wed 17:01 08:59
 after-hours day Thu 17:01 08:59
 after-hours day Fri 17:01 08:59
after-hours day Sat 23:59 12:00
!
ephone 3
  pin 12345
!
ephone 2
  after-hour exempt
```

Task 29.15

A call from another site supporting only G729 may ring into a BR2 site CME phone, and that phone may be busy and have set to forward busy calls into CUE VM. If this is the case, ensure that G729 call into CUE will not fail.

➔ **This should be self-explanatory from previous examples – See Task 3.8.**

Task 29.16

Create a circular hunt group for Support with a DN of 3210 at BR2 between phones 1 and 3, and ensure that those phones can login-to and out-of the hunt group in order to receive calls. Allow the call to ring at around 3 times before searching for the next member. Now Create an incoming AutoAttendant at the DN of 3000. Also Create a Basic ACD using the support team hunt group you just created (The necessary TCL scripts are already loaded in BR2 router's flash memory). Have the AA script automatically hand-off the callers into the support ACD hunt group when a user presses 2. Allow no more than 20 callers in the Q at any one point. Play a prompt for the user every 30 seconds to let them know that all agents are busy. Allow the users to dial-by-extension by pressing 4. Ensure that the Q is collecting statistics and view them as part of your troubleshooting.

➔ **On BR2:**

```
ephone-hunt 1 peer
 pilot 3210
 list 3001, 3003
 timeout 12
 statistics collect
!
!
application
 service queue flash:app-b-acd-2.1.0.0.tcl
  param queue-len 20
  param aa-hunt2 3210
  param number-of-hunt-grps 1
 !
 service aa flash:app-b-acd-aa-2.1.0.0.tcl
  paramspace english index 1
  param number-of-hunt-grps 1
  param handoff-string aa
  param dial-by-extension-option 3
  paramspace english language en
  param aa-pilot 3313213000
  param max-extension-length 4
  paramspace english location flash:
  param second-greeting-time 30
  param welcome-prompt en_bacd_welcome.au
  param call-retry-timer 15
  param max-time-call-retry 600
  param service-name queue
 !
!
dial-peer voice 5 pots
 service aa
 incoming called-number 3313213000
```

Task 29.17

Configure the HQ 6608 T1 PRI gateway based on Table 8. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **Add the gateway as covered in previous sections.**

➔ **The fact that you are not allowed to use External Number Mask on the LINES means that you must use some other method to display 10 digit Calling Party DN.**

➔ **One method is to use the Prefix DN on the Outbound Calls section of the gateway.**

Outbound Calls	
Calling Party Presentation*	Allowed
Calling Party Selection*	Originator
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Number of digits to strip*	0
Caller ID DN	212222XXXX
SMDI Base Port*	0

➔ **This should not be used however if the gateway will be used for Toll-bypass.**

➔ **Instead to configure 10 digit Calling Party Number on the Route Pattern.**

➔ **Remember for Calling Name mark the Display IE Delivery Checkbox.**

Calling Party Transformations	
☐ Use Calling Party's External Phone Number Mask	
Calling Party Transform Mask	
Prefix Digits (Outgoing Calls)	212222
Calling Party Presentation	Allowed
Called Party Transformations	

Task 29.18

Configure BR1 as an MGCP gateway, based on information in Table 8. Calling Number (10 digits) and Calling Name should be displayed. Secure the signaling and RTP transport traffic (RTP if allowed by phone) back and forth to this gateway.

➔ **This should be self-explanatory from previous examples – See Task 17.4 – 5 for security setup.**

Task 29.19

Configure the BR1 Router as an IPIPGW.

➔ **To begin thinking like the exam requires – we would have needed to look ahead in the exam (hopefully reading the entire exam before beginning any configuration) to determine all the necessary variables to complete this question's config.**

➔ **On BR1 Router (why put an IPIPGW on Branch 1 instead of HQ you may ask? Doesn't seem to logical does it? Well it's not logical in terms of packet flow – but it is possible and does make your configuration (and your mind) work a little harder – and after all, this is an Expert level exam. So why BR1? Simply because it is possible!)**

➔ **On BR1 Router:**

```
voice service voip
 allow connections h323 to sip
!
interface Loopback0
 ip address 172.1.101.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id VGK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip bind srcaddr 172.1.101.1
!
dial-peer voice 10 voip
 incoming called-number [12]...
 session target ras
 codec g711ulaw
!
dial-peer voice 12 voip
 destination-pattern 011T
 session target ras
 codec g711ulaw
```

Task 29.20

Configure BR2 as an H323 gateway based on the information in Table 8.

➔ **This should be self-explanatory from previous examples.**

Task 29.21

Configure gatekeeper on HQ-RTR with the following information:

Local zone= CCM-GK
domain name = ipexpert.com
[use loopback interface for local zone]
Register CallManager to this zone.

Local zone= VGK
domain name = ipexpert.com
Register the IPIPGW to this zone.

Remote zone= PSTN-WAN
domain name= ipexpert.com
ip address= 10.X.200.2 [X=Last digit of POD number]

➔ **On HQ-RTR:**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.1.100.1
 zone local VGK ipexpert.com
 zone remote PSTN-WAN ipexpert.com 10.1.200.2 1719 invia VGK outvia VGK
 no shutdown
```

Task 29.22

Configure CAC such that one G711 call is allowed through the gatekeeper to all zones.

➔ **On HQ-RTR:**

```
gatekeeper
 bandwidth total default 128
```


Task 29.23

Enable security on the local gatekeeper such that only devices that need to register CAN register (e.g. Both CallManagers, IPIPGW) – other rogue devices should be prevented from registering.

➔ **On HQ-RTR:**

```
gatekeeper
zone local HQ-RTR ipexpert.com 172.1.100.1
 zone local VGK ipexpert.com
 zone local BR2-GK ipexpert.com
 zone remote PSTN-WAN ipexpert.com 10.1.200.2 1719 invia VGK outvia VGK
 no zone subnet HQ-RTR default enable
 zone subnet HQ-RTR 10.1.200.21/32 enable  ← CCM Sub IP Address
 zone subnet HQ-RTR 10.1.200.20/32 enable ← CCM Pub IP Address
 no zone subnet VGK default enable
 zone subnet VGK 172.1.101.1/32 enable  ← IPIPGW IP Address
no shutdown
```

Task 29.24

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

➔ **See Task 29.29.**

Task 29.25

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

➔ **See Task 29.29.**

Task 29.26

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed out through the local gatekeeper to the PSTN gatekeeper, with the appropriate local gateway acting as backup. Users must be able to dial the BR2 site using extension (4 digit) dialing. **NOTE**: The gatekeeper is expecting the full E164 number, i.e. international prefix '011' plus 10 digits. All signaling traffic for these calls to the PSTN GK should be sourced out of the BR1 Loopback interface, however RTP should not be terminated on BR1 at all.

➔ **NOTE: Although the CME is sending calls through the IPIPGW on BR1, we are still routing calls from CCM to CME via the PSTN-WAN GK.**

➔ **On HQ-RTR:**

```
gatekeeper
 zone prefix PSTN-WAN 011*
```
← This will send a LRQ to the PSTN-WAN GK to route the call

```
 zone remote PSTN-WAN ipexpert.com 10.1.200.2 1719 invia VGK outvia VGK
```
← This will ensure that any calls routed out to the PSTN-WAN GK must loop through the VGK zone – which only has an IP-to-IP-Gateway (IPIPGW) associated to it – this will force all calls to terminate their signaling on this IPIPGW (and media if configured though not in this case – see next bullet point)

➔ **On BR1 Router – we already configured some of this in task 29.19 – but we must ensure that signaling goes through but media (RTP) does not – we can do this from the Dial-Peer or Globally as we choose to do here:**

```
voice service voip
 media flow-around
```

➔ **Later on after we finish the rest of our configuration we can test this to ensure that RTP is not being terminated here on the BR1 Router with this command while in the middle talking after placing a successful call:**

```
P1-BR1-RTR#sh voip rtp connections
No active connections :
```

➔ **The rest of the call routing from CCM is in Task 29.29.**

Task 29.27

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway.

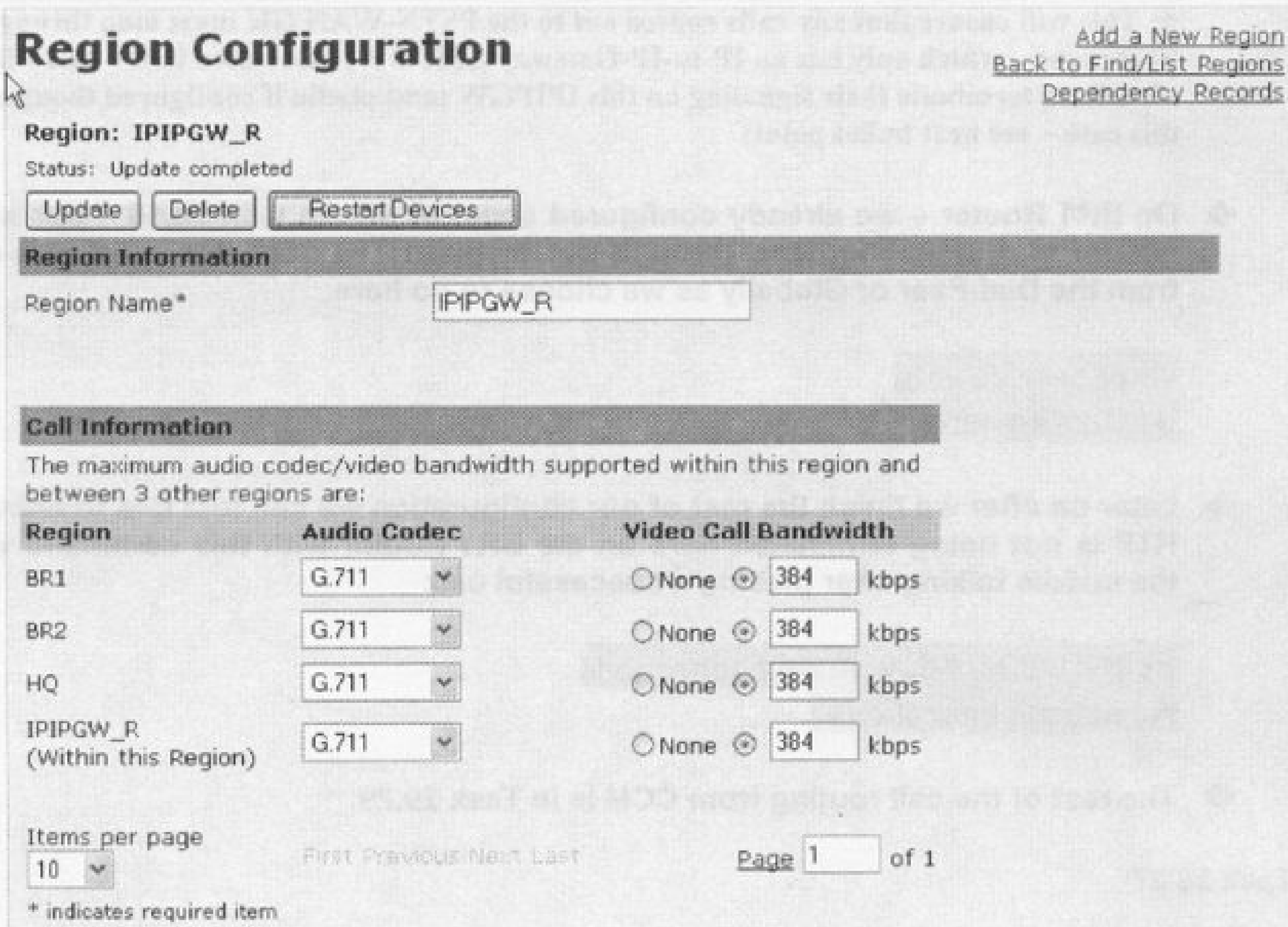
➔ **See Task 29.29.**

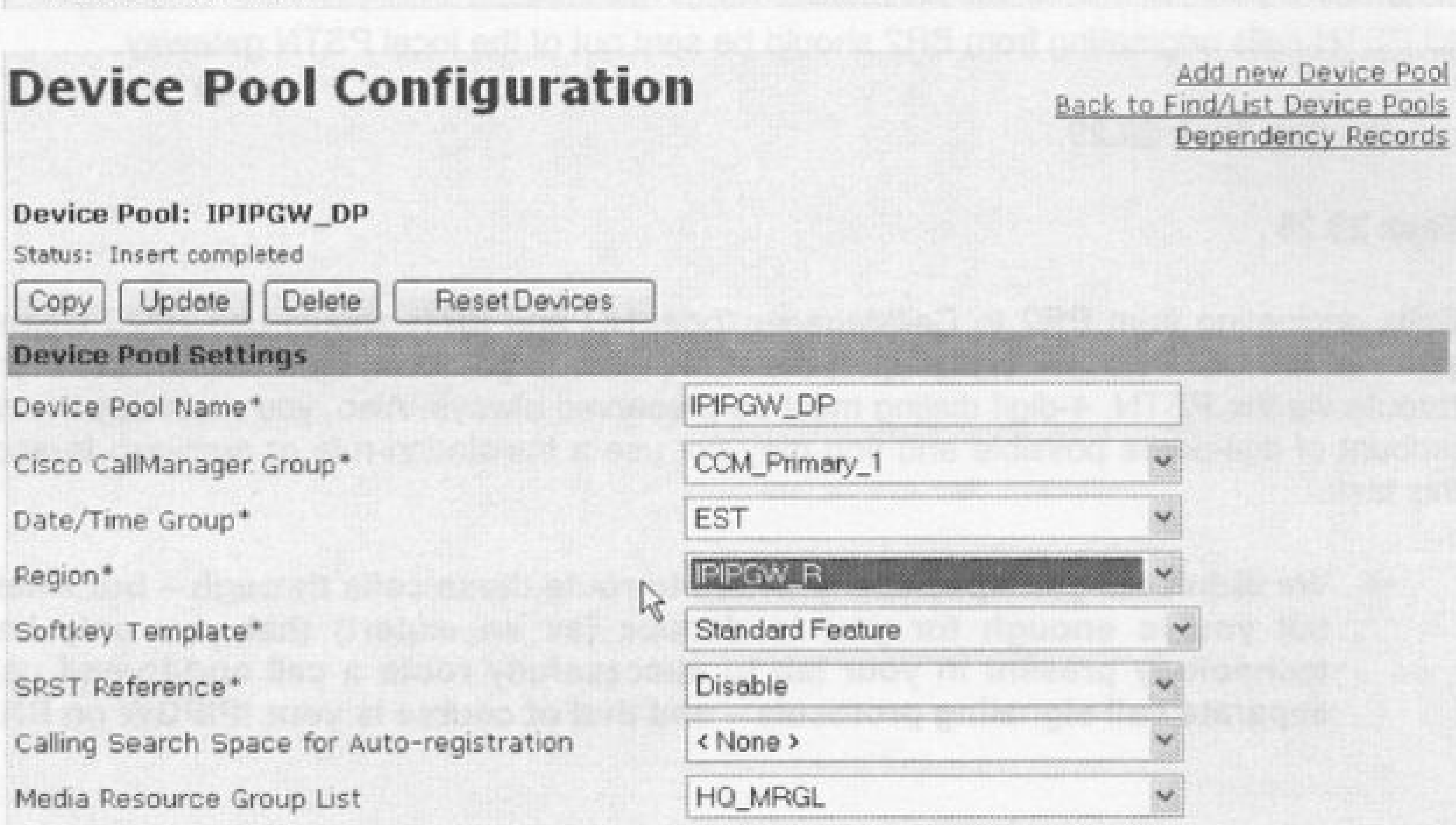
Task 29.28

Calls originating from BR2 to CallManager (both HQ and BR1) should use H323 signaling and arrive at the CCM via SIP signaling. If the WAN were to go down, then calls must automatically reroute via the PSTN. 4-digit dialing must be preserved always. Also, you must use the minimum amount of dial-peers possible and you may not use a translation-rule or num-exp to accomplish this task.

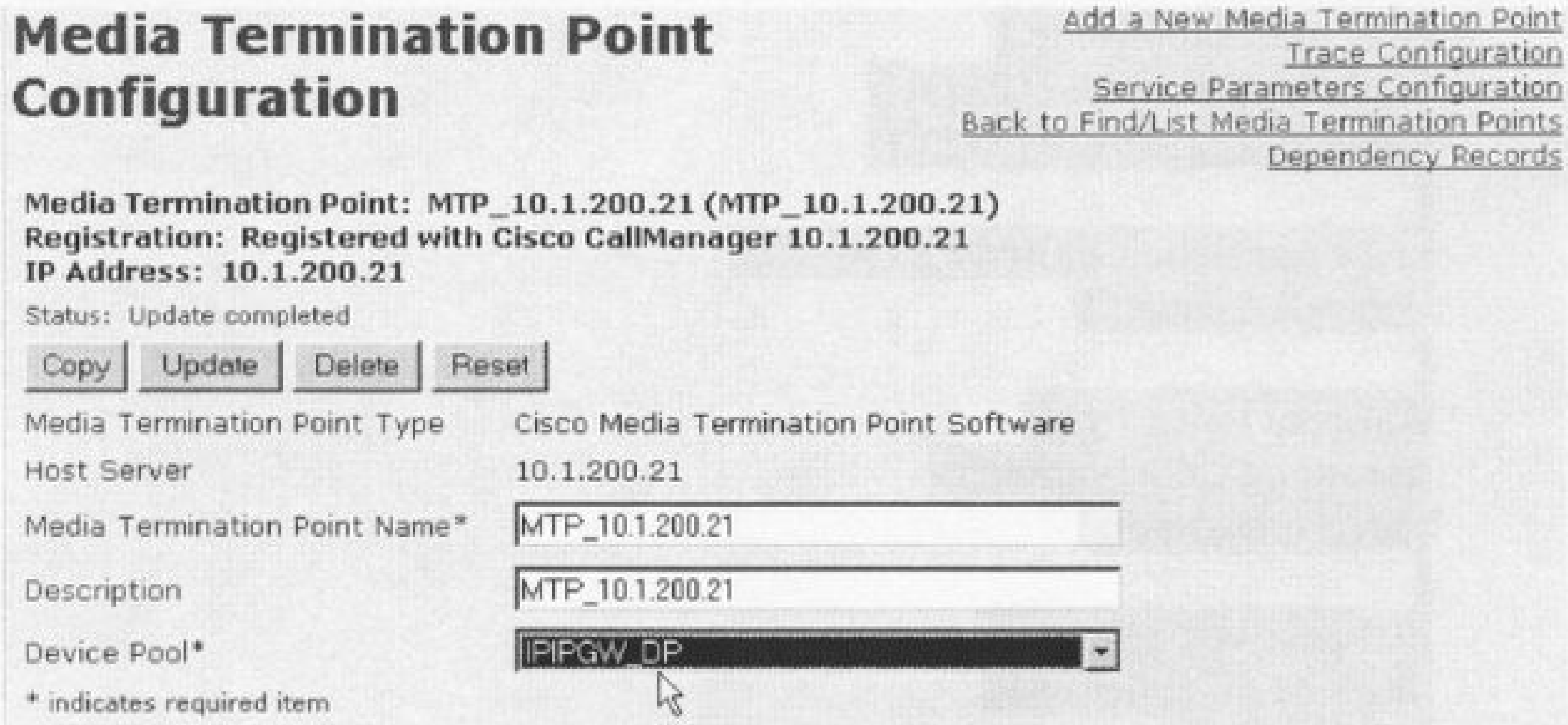
➔ **We didn't tell you specifically where to route these calls through – but what we did tell you is enough for you to deduce (as an expert) that you only have one technology present in your lab to successfully route a call end-to-end using two separate call signaling protocols – and that of course is your IPIPGW on BR1.**

➔ **First we need to setup a new Region and Device Pool that will speak G711ulaw to every other Region/DP. The reason that we do this is that our IPIPGW will only allow a specific codec to come into it – it will not negotiate the codec with us like an endpoint would. And even though we are only receiving calls into us from the CME (sending them goes through the HQ-GK and ultimately through the PSTN-GK).**

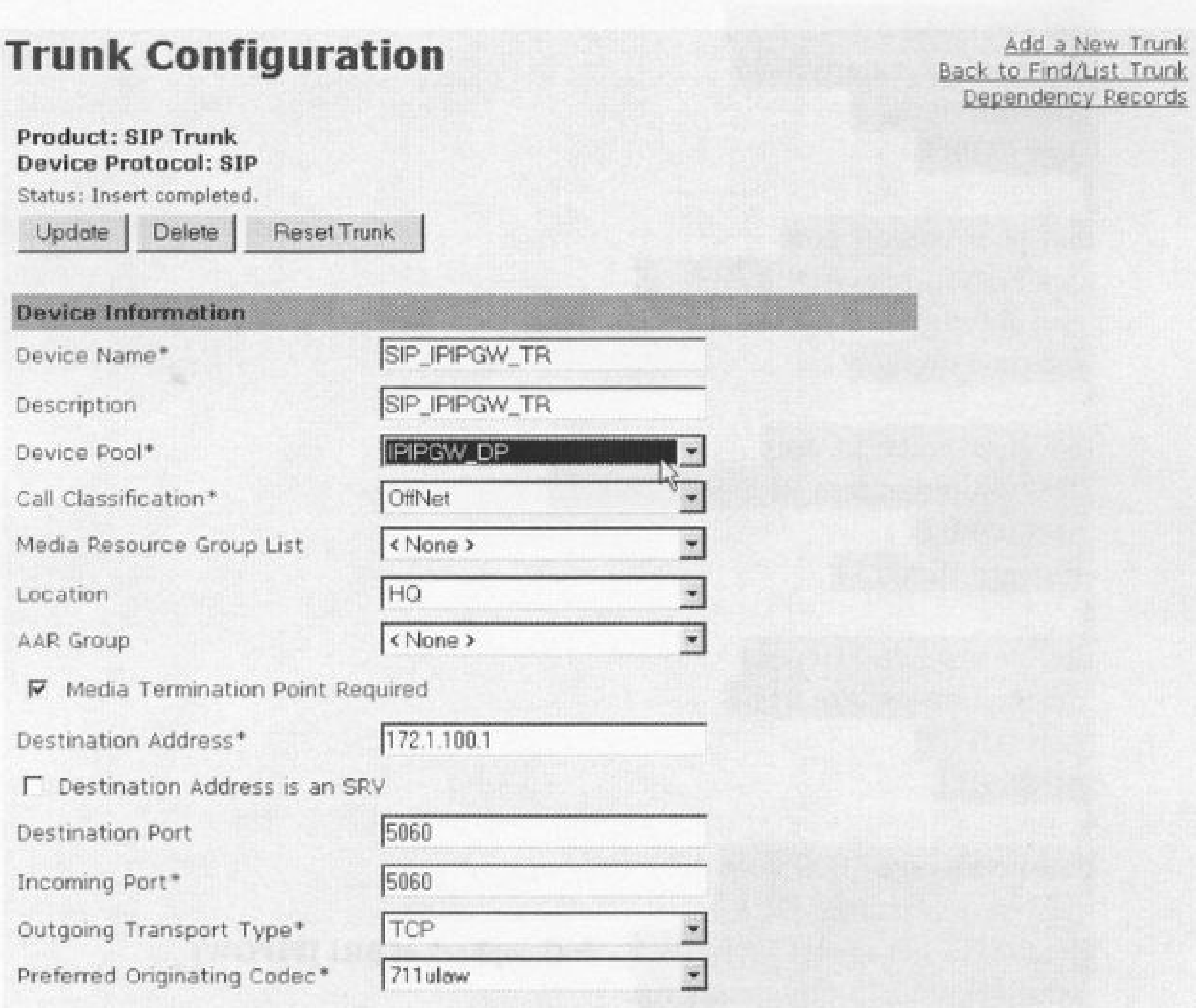




➔ **Now we need to setup a software MTP within CCM and ensure that it is part of the IPIPGW Device Pool so that it 'speaks' G711 to all other devices (i.e. the Phones and the Trunks).**



➔ **We now create our SIP Trunk to allow calls to come in from the CME via the IPIPGW.**



➔ **For CME use the following dial-peers on BR2: (Note that while we stated that you could not use a translation-rule we did NOT state that you could not use a Voice Translation-Rule which is a very different command altogether) ;)**

```
voice translation-rule 1
  rule 1 /\(^1...\)/ /1212222\1/
  rule 2 /\(^2...\)/ /1617522\1/
!
voice translation-profile PSTN-OUT
  translate called 1
!
dial-peer voice 1 pots
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 911 pots
 destination-pattern 911
 no digit-strip
 port 0/0/0:0
!
dial-peer voice 9911 pots
 destination-pattern 9911
 forward-digits 3
 port 0/0/0:0
!
dial-peer voice 7 pots
 destination-pattern 9[2-9]......T
 port 0/0/0:0
 forward-digits 7
!
dial-peer voice 11 pots
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:0
 forward-digits 11
!
dial-peer voice 110 pots
 destination-pattern 011T
 port 0/0/0:0
 prefix 011
!
dial-peer voice 1000 voip
 destination-pattern [12]...
 session target ipv4:172.1.101.1   ← (Loopback of BR1 IPIPGW)
 dtmf-relay h245-alphanumeric
!
dial-peer voice 1001 pots
 preference 1
```

```
destination-pattern [12]...
port 0/0/0:0
translation-profile outgoing PSTN-OUT
```

Task 29.29

Enable DID for PSTN users dialing into the CM/CME (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits.

➔ **Digit Manipulation should be done in the Route List.**

➔ **Calling Party Prefix DN should be done in Route Pattern.**

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-GK	GK-TRUNK	1
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1-LOC	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-BR1-HQ-LOC	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617
RL-HQ-BR1-LD-INT	RG-HQ	PREDOT
	RG-BR1	PREDOT
RL-BR1-HQ-LD-INT	RG-BR1	PREDOT
	RG-HQ	PREDOT
RL-HQ-TOLLBY	RG-BR1	PREDOT
	RG-HQ	PREDOT + PREFIX 1617
RL-BR1-TOLLBY	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-GK-HQ	RG-GK	PREFIX 01133132X
	RG-HQ	PREFIX 01133132X
RL-GK-BR1	RG-GK	PREFIX 01133132X
	RG-BR1	PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ-BR1-LOC
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ-LOC
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ-BR1-LD-INT
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1-HQ-LD-INT
91212.xxxxxxx	PT-BR1-LD	RL-BR1-TOLLBY
91617.xxxxxxx	PT-HQ-LD	RL-HQ-TOLLBY
9.011! 9.011!#	PT-HQ-INT	RL-HQ-BR1-LD-INT
9.011! 9.011!#	PT-BR1-INT	RL-BR1-HQ-LD-INT
3xxx	PT-HQ-911	RL-GK-HQ
3xxx	PT-BR1-911	RL-GK-BR1

Task 29.30

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 29.31

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 29.32

Configure conference bridge on BR1 router. Use a maximum of 1 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 29.33

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 29.34

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should load share the IOS resources and 6608 resources.

➔ **This should be self-explanatory from previous examples.**

Task 29.35

Configure a Music on Hold server on the Publisher Call Manager. Add another music source which can be found on the C: drive of your Call Manager. Ensure that the default (Sample) audio source is used when a User presses the 'Hold' button on his/her phone. For all other events that require music to be played use the newly added music source. You may not configure music sources on line, device or device pool to accomplish this task.

- ➔ **This should be self-explanatory from previous examples.**

Task 29.36

Configure the Call Manager such that HQ phones will receive music using the G711 codec and BR1 phones will receive music using the G729 codec. You must use the transcoder to achieve this task.

- ➔ **Transcoding MOH will only work for Unicast so in the next task change the IP Media Streaming Application. The idea is to verify the transcoder is working - use the following command on the Cat 6K.**

```
sh port voice active transcode
```

Task 29.37

Ensure that the HQ and BR1 phones receive multicast music on hold.

- ➔ **This should be self-explanatory from previous examples.**

- ➔ **Being clever you may note that we have an IPSec tunnel defined between CCM and the BR1 Router, and you may or may not know that without some other helping protocol (such as GRE) Multicast traffic is not supported in the IPSec RFC – so that may lead you to the question, "how will the MoH stream originating from the CCM – get out to my FastEthernet interfaces in order to be heard by my IP Phones at BR1?" That would be an excellent question – but wait, take a second look at the configuration we used for our IPSec tunnel – from the CCM side, the IPSec tunnel was ONLY configured to encrypt traffic that originates from the CCM (10.x.200.21) and is destined for the IP Address of the SERIAL interface of the BR1 Router. So any traffic originating from the CCM (10.x.200.21) destined for any other interface (Loopback, FastEth) will NOT be encrypted – thus our MoH stream should work just fine.**

Task 29.38

Configure music on hold on the BR2 CME.

- ➔ **This should be self-explanatory from previous examples.**

Task 29.39

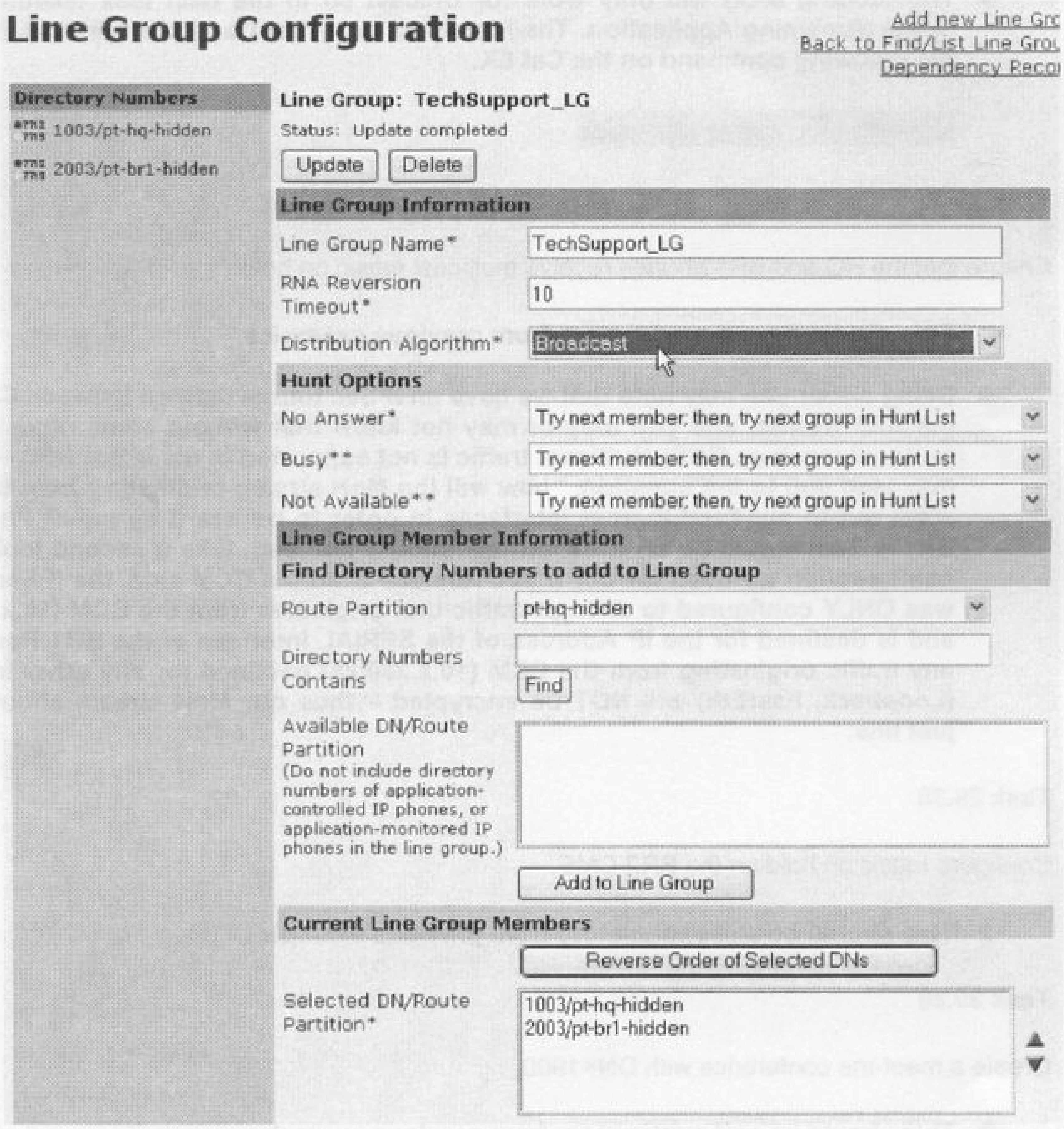
Create a meet-me conference with DN=1900.

- ➔ **This should be self-explanatory from previous examples.**

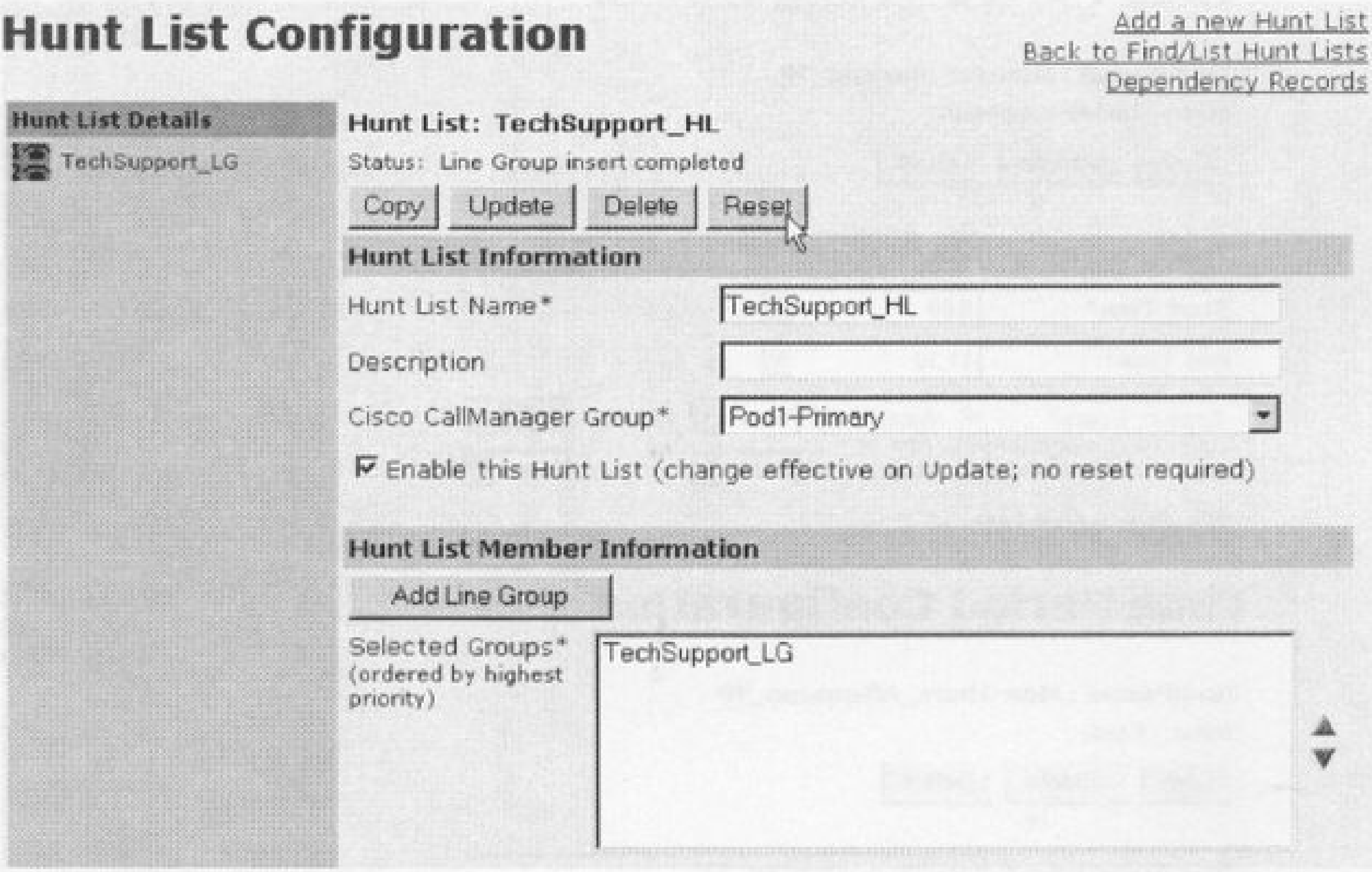
Task 29.40

Create a DN of 1005 for Tech Support. Make HQ phone 3 and BR1 Phone 3 ring simultaneously when this DN is called. You may not use a shared line to accomplish this task. DN 1005 should forward directly to VM anytime outside of normal business hours with no user intervention needed. Check Table 11 for a time schedule. Also, all members of this HuntGroup should get the message in their VM box and see their MWI for any message left for 1005. Finally Create a new DN of 1010. When this DN is called, all calls should be directed to the DN of 1005. The call should ring this DN for approximately 2 rings. If for any reason this DN does not answer, the call should then be forwarded to VM if the call originated from an internal number, however if the call originated from an external number, the call should then be forwarded to the PSTN phone at '221-1111.

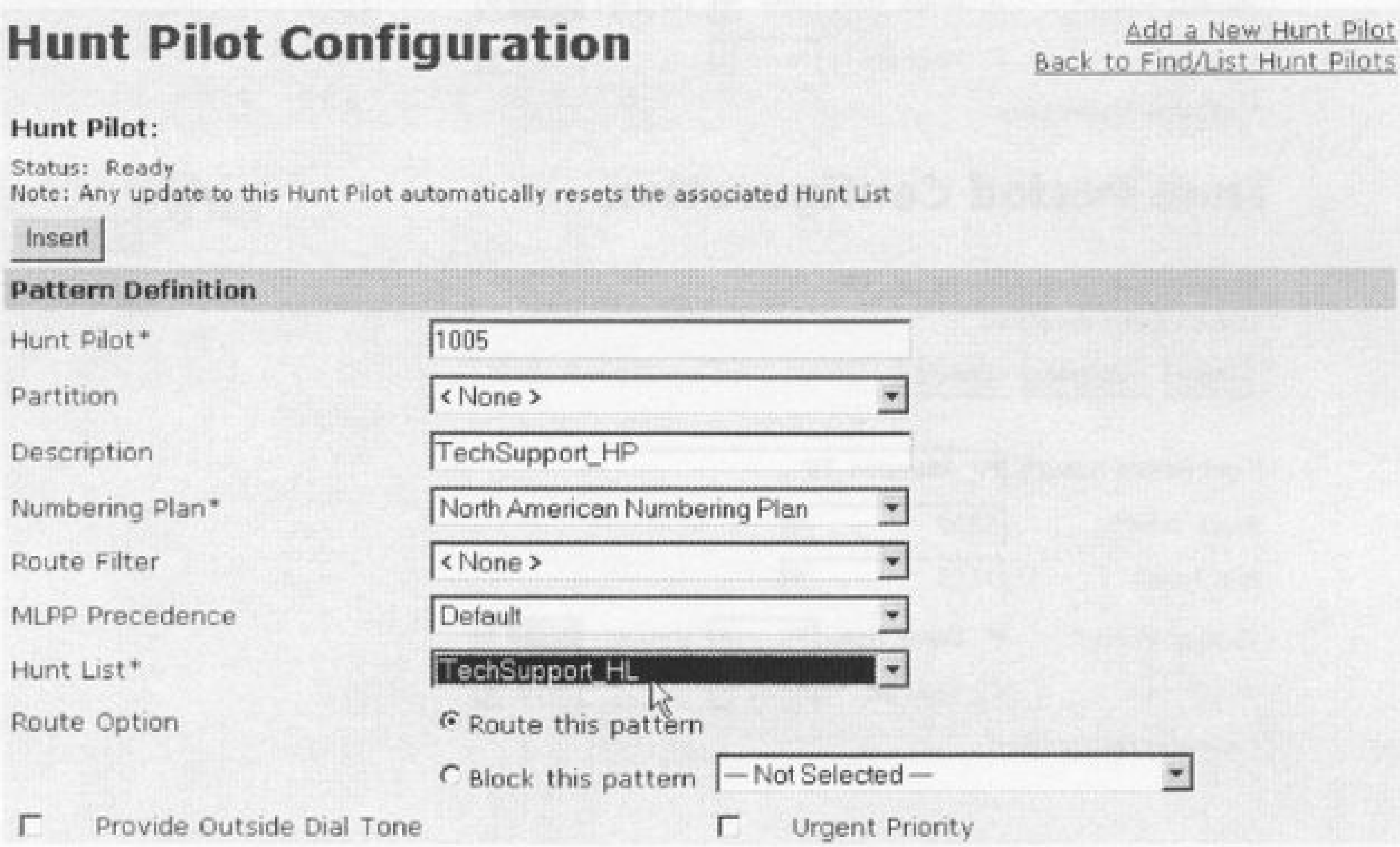
➔ **Add a new Line Group called TechSupport_LG, ensure that it follows a Top Down Distribution Algorithm, and include the DNs 1001, 1002, and 1003 as members and ensure their order.**



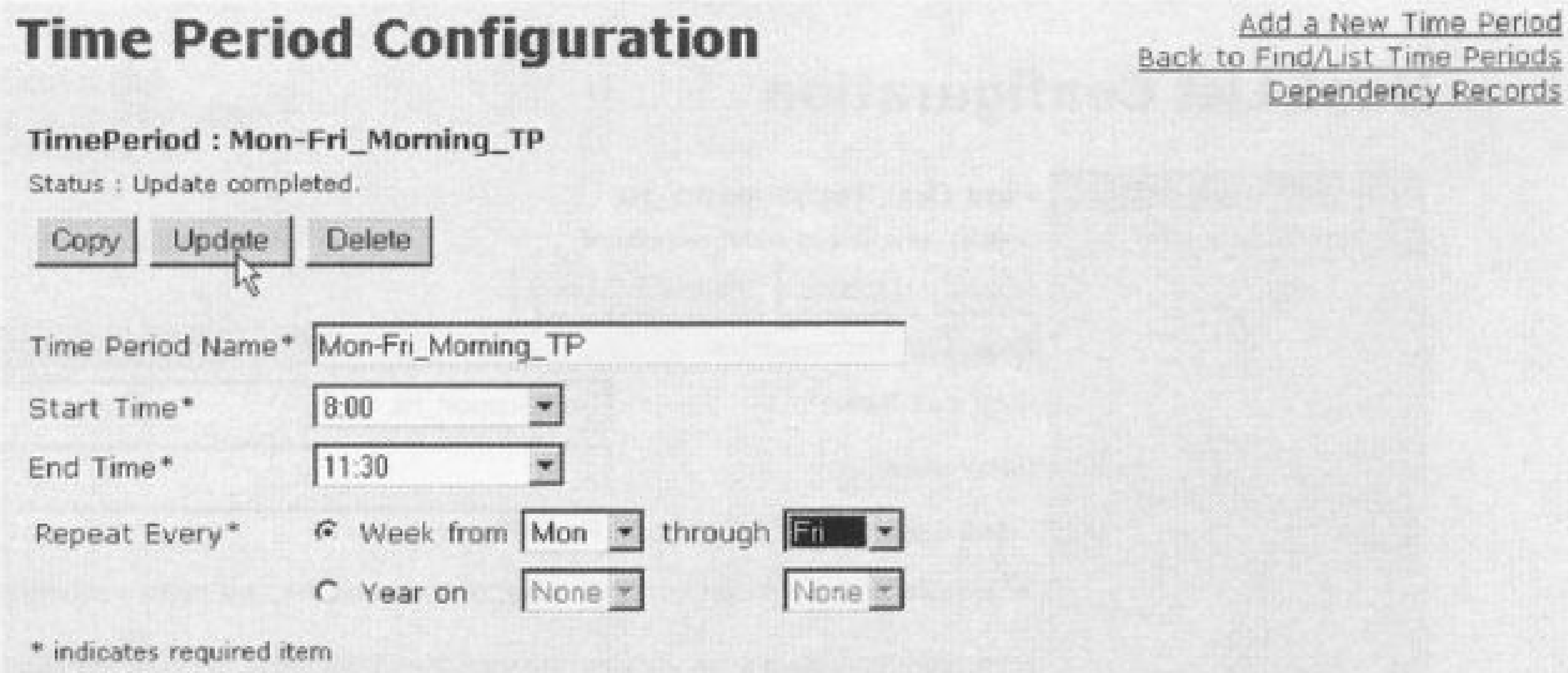
➔ **Add a new Hunt List called TechSupport_HL, add the Line Group you just created, and be sure to reset the Hunt List once you've inserted it.**

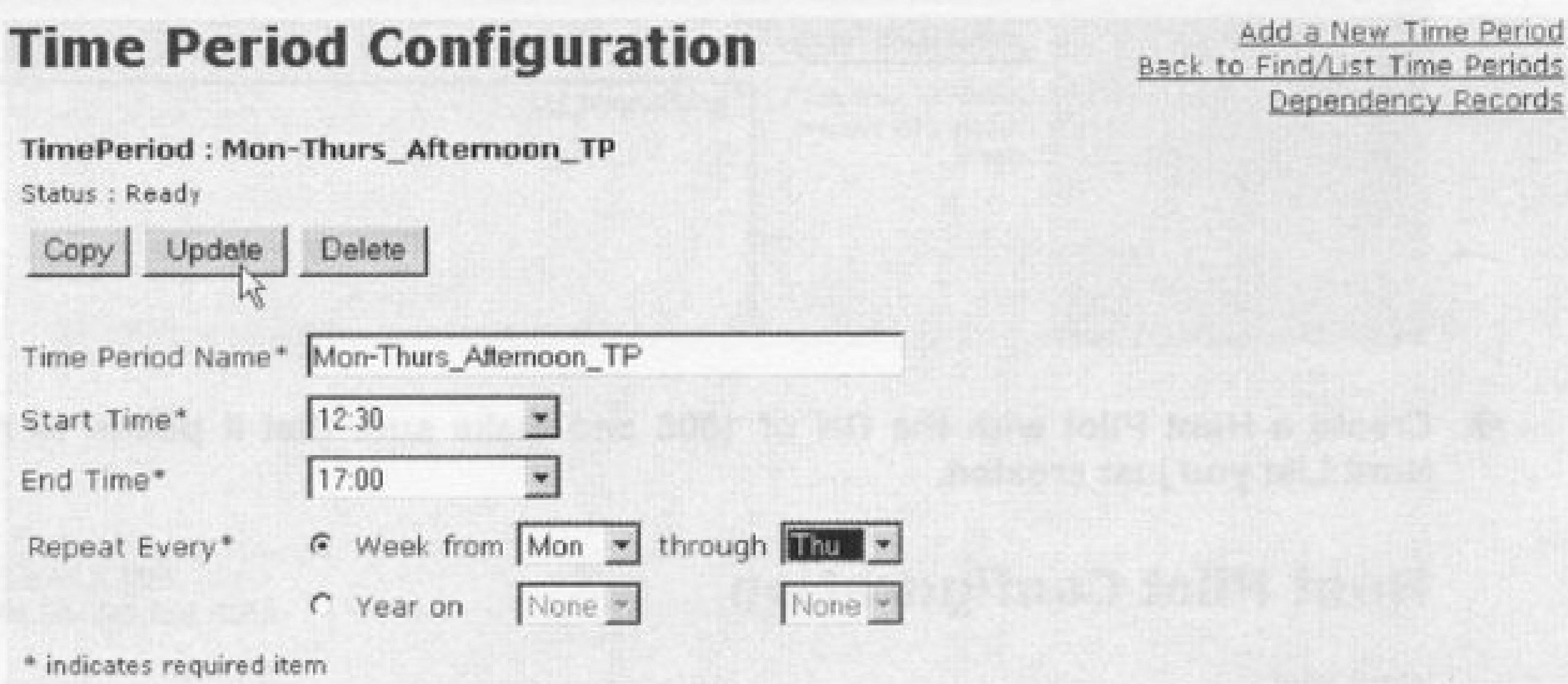


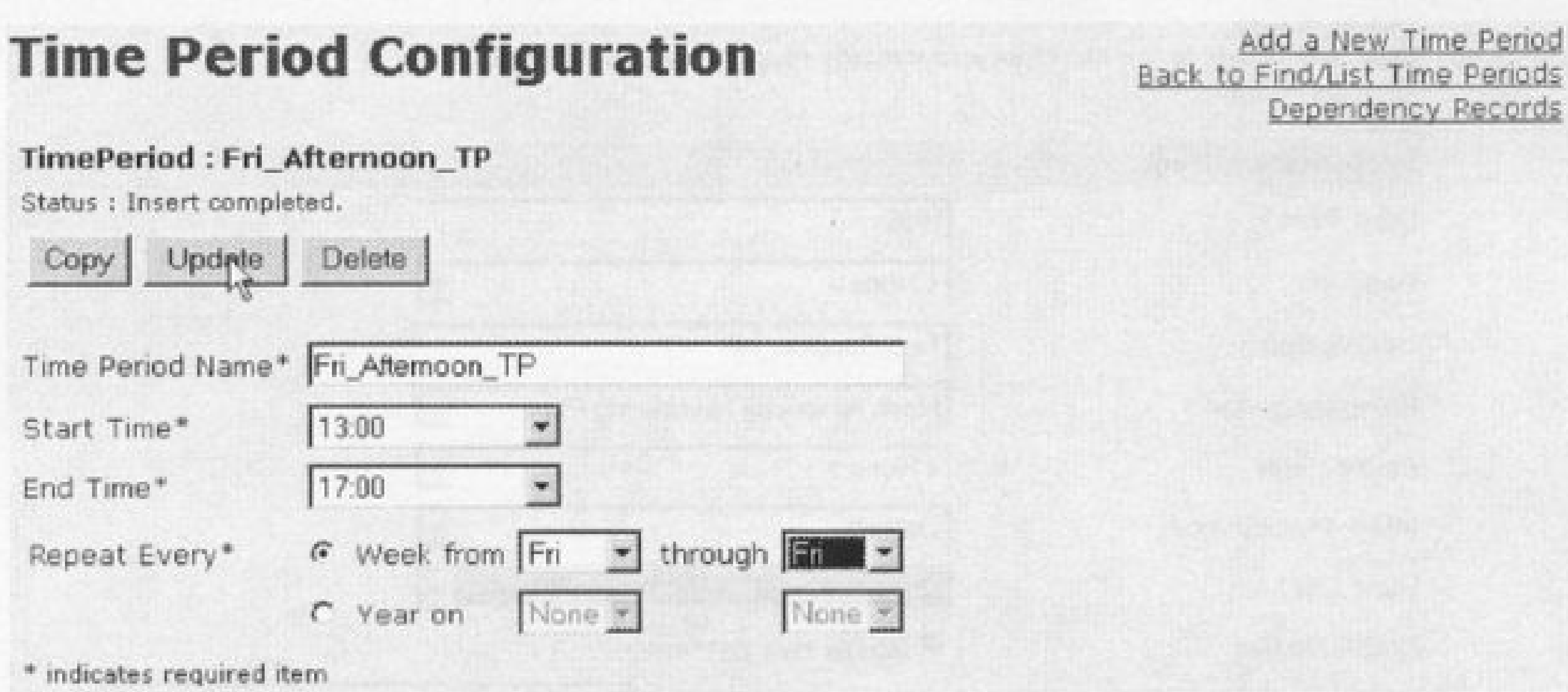
➔ **Create a Hunt Pilot with the DN of 1005 and make sure that it points to ring the Hunt List you just created.**

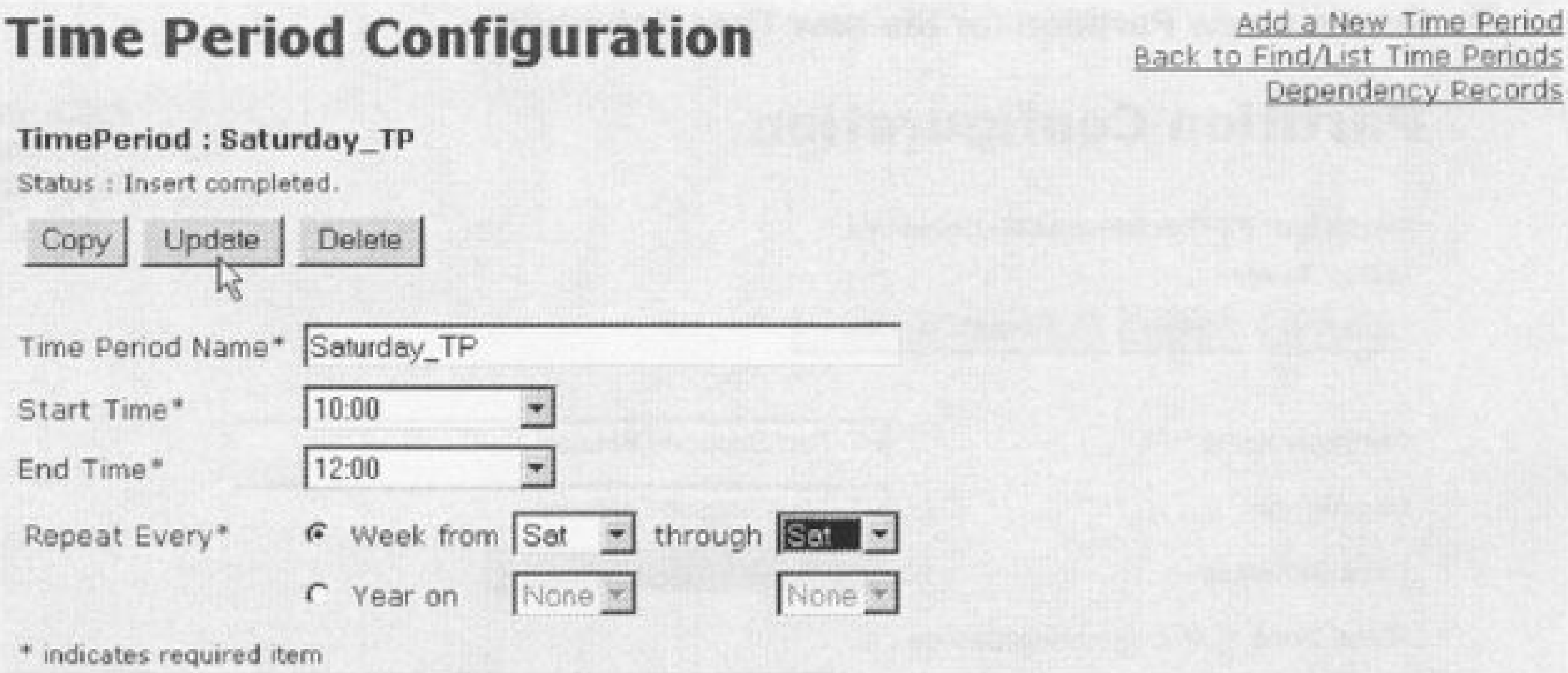


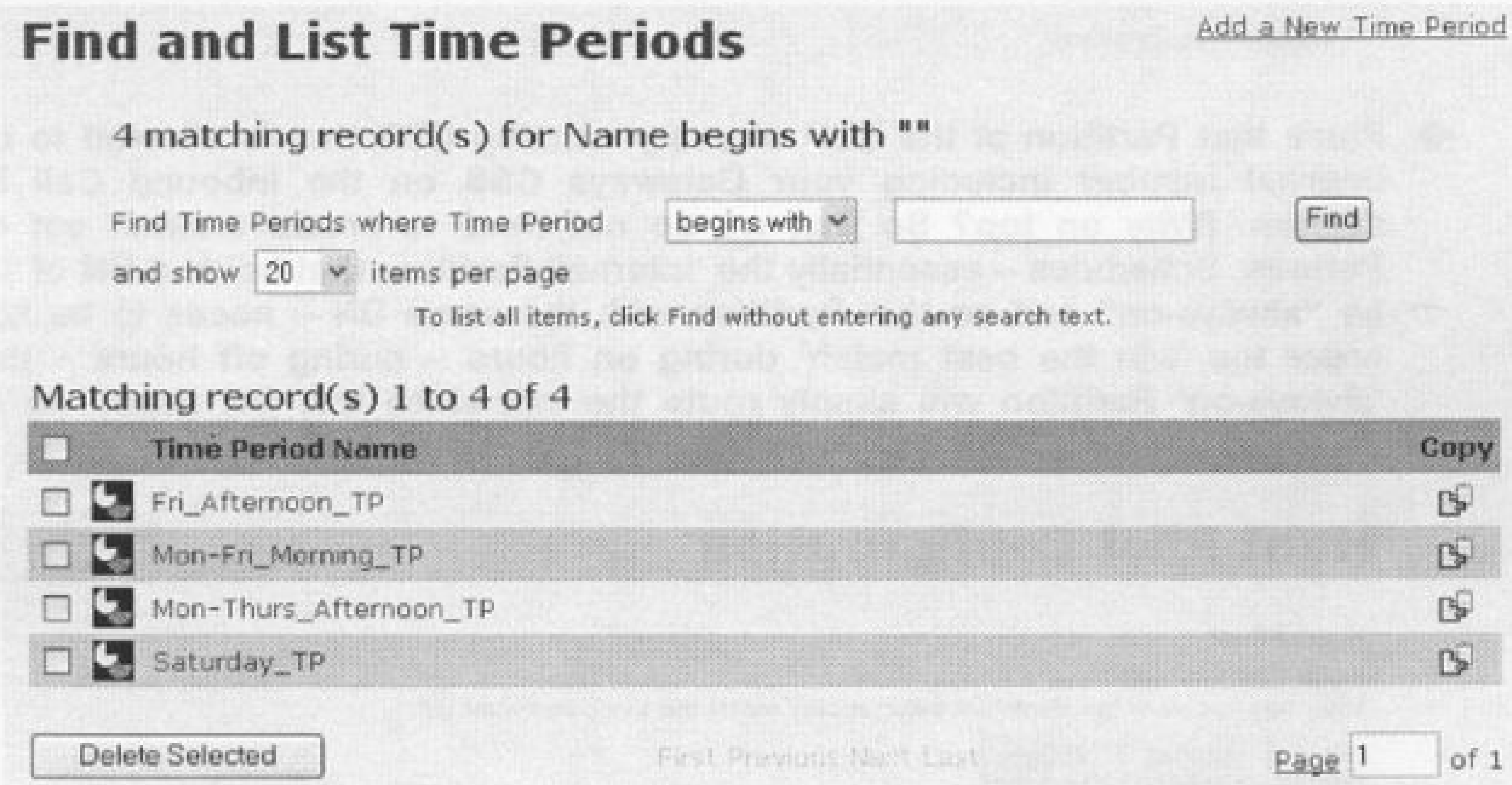
➔ **Now we will create our Time of Day based Call Routing.**

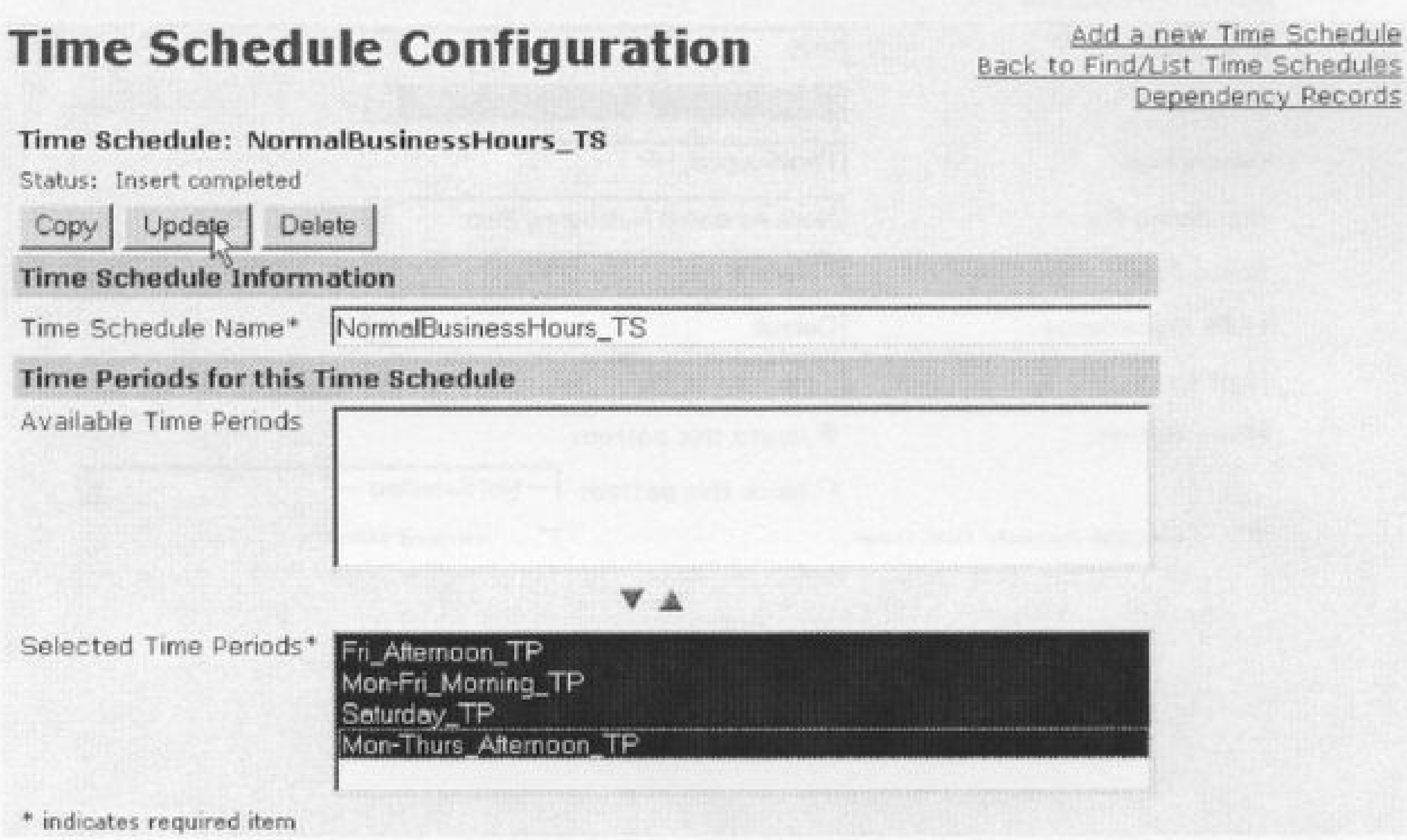




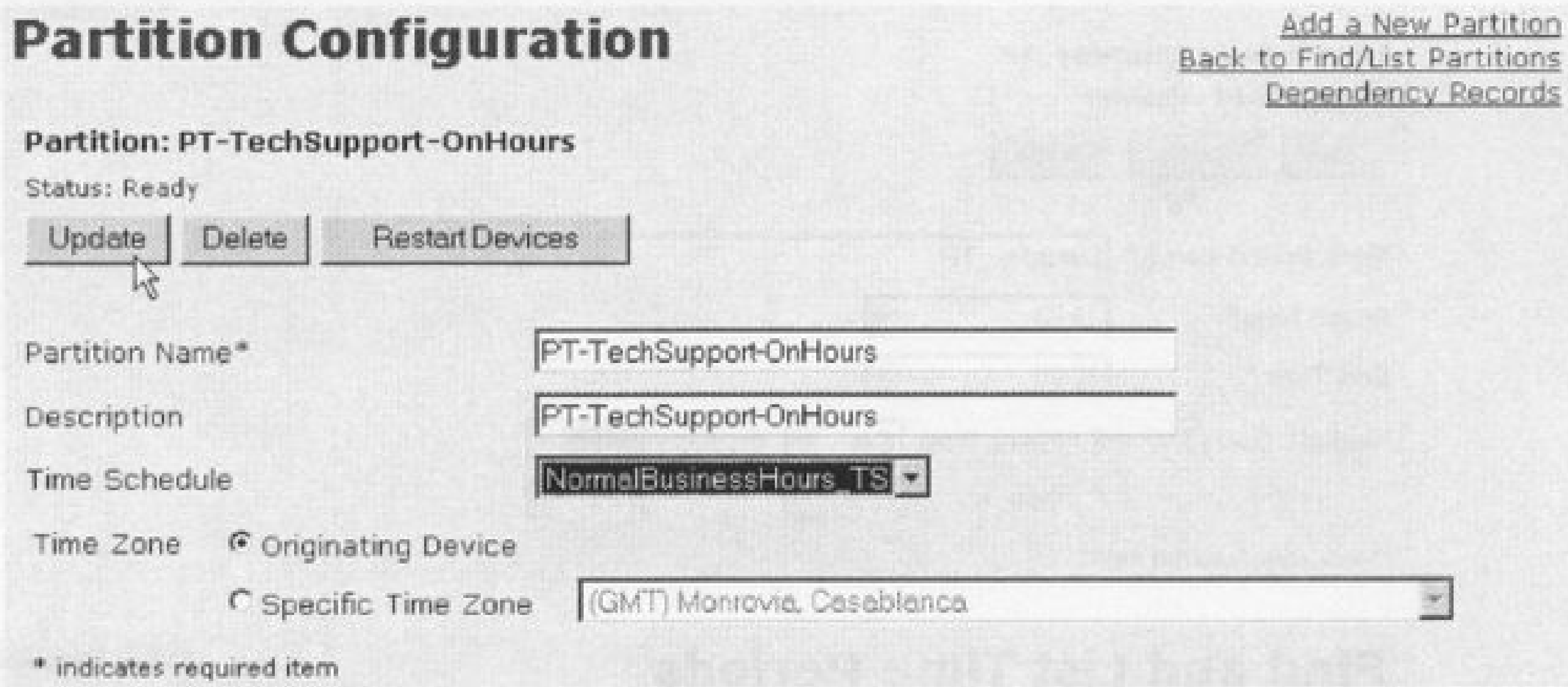



Time Period Configuration
Add a New Time Period
Back to Find/List Time Periods
Dependency Records
TimePeriod : Saturday_TP
Status : Insert completed.
Copy
Update
Delete
Time Period Name* Saturday_TP
Start Time* 10:00
End Time* 12:00
Repeat Every* Week from Sat through Sat
Year on None None
* indicates required item

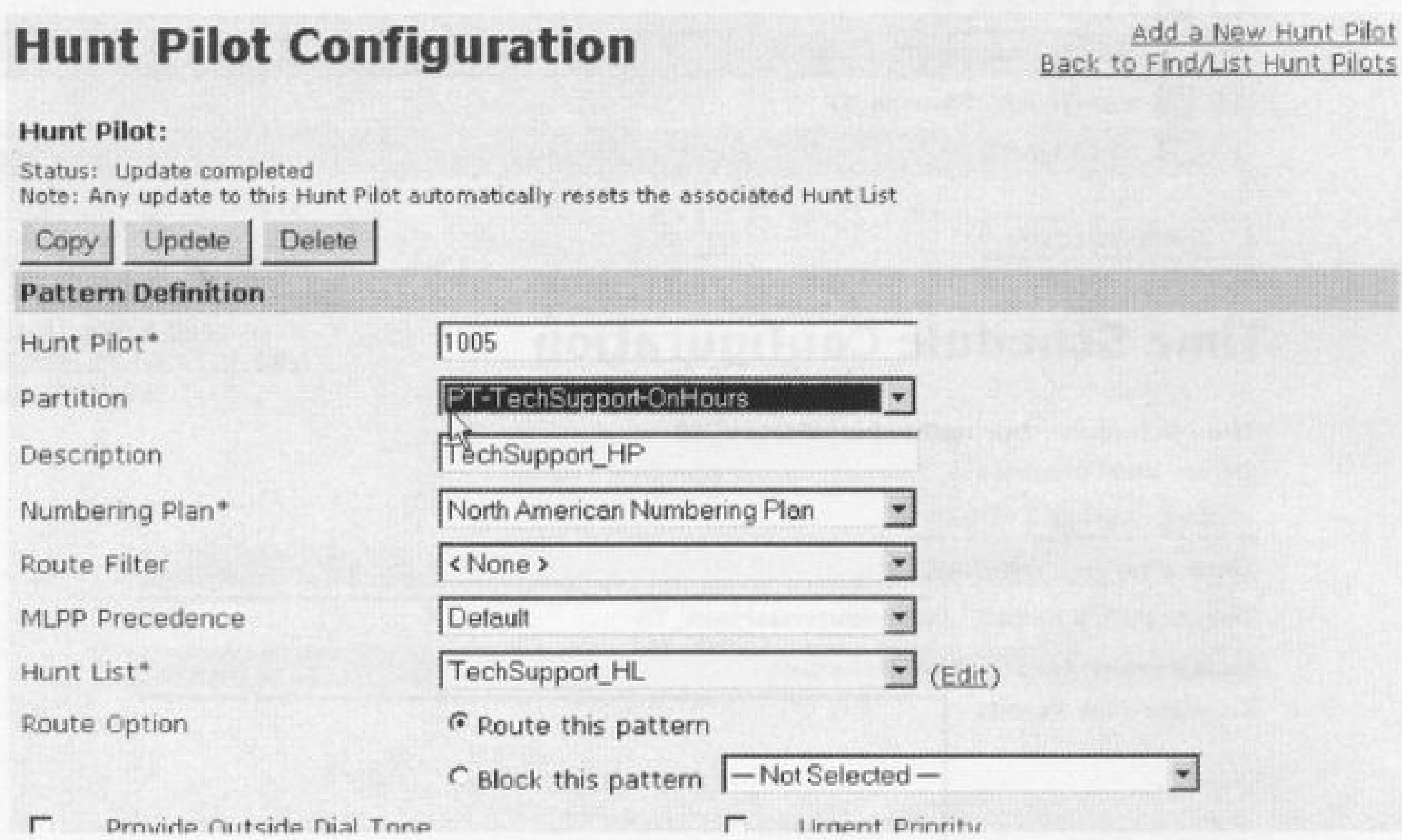

Find and List Time Periods
Add a New Time Period
4 matching record(s) for Name begins with ""
Find Time Periods where Time Period begins with
Find
and show 20 items per page
To list all items, click Find without entering any search text.
Matching record(s) 1 to 4 of 4
Time Period Name
Copy
Fri_Afternoon_TP
Mon-Fri_Morning_TP
Mon-Thurs_Afternoon_TP
Saturday_TP
Delete Selected
First Previous Next Last
Page 1 of 1


Time Schedule Configuration
Add a new Time Schedule
Back to Find/List Time Schedules
Dependency Records
Time Schedule: NormalBusinessHours_TS
Status: Insert completed
Copy
Update
Delete
Time Schedule Information
Time Schedule Name* NormalBusinessHours_TS
Time Periods for this Time Schedule
Available Time Periods
Selected Time Periods* Fri_Afternoon_TP
Mon-Fri_Morning_TP
Saturday_TP
Mon-Thurs_Afternoon_TP
* indicates required item

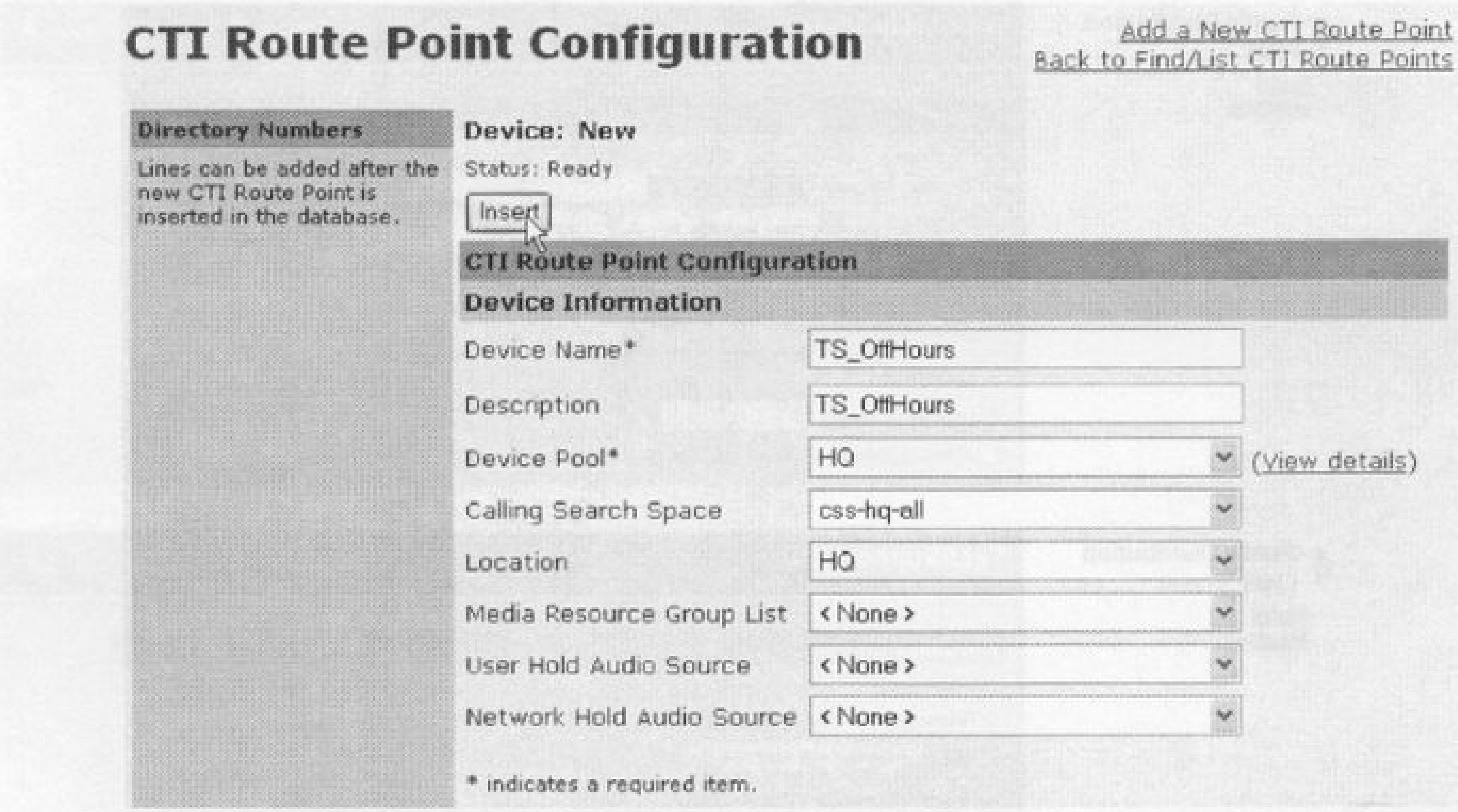
➔ **Create a new Partition for the new Time Schedule.**

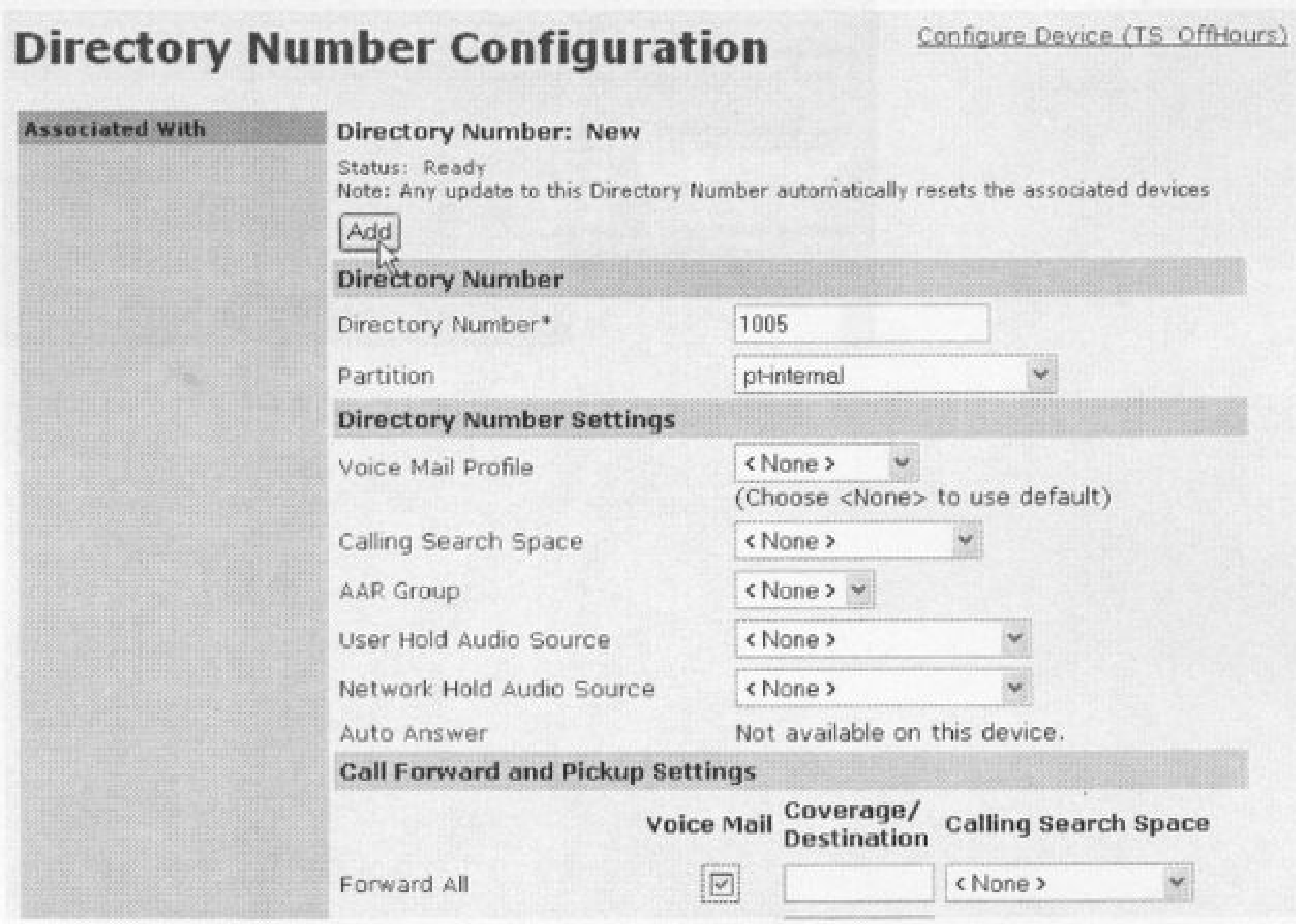


➔ **Place that Partition at the TOP of every existing CSS that is allowed to call that internal number including your Gateways CSS on the Inbound Call Routing section. (Why on top? So that we do not have to create another set of Time Periods, Schedules – essentially the 'Internal' Partition that holds a DN of 1005 will be "always-on" and so this Partition with the same DN – needs to be higher in order the 'win the best match' during on hours – during off hours – the other 'always-on' Partition will simply route the call since this DN based on its time schedule will simply be viewed as not even a part of the CSS).**

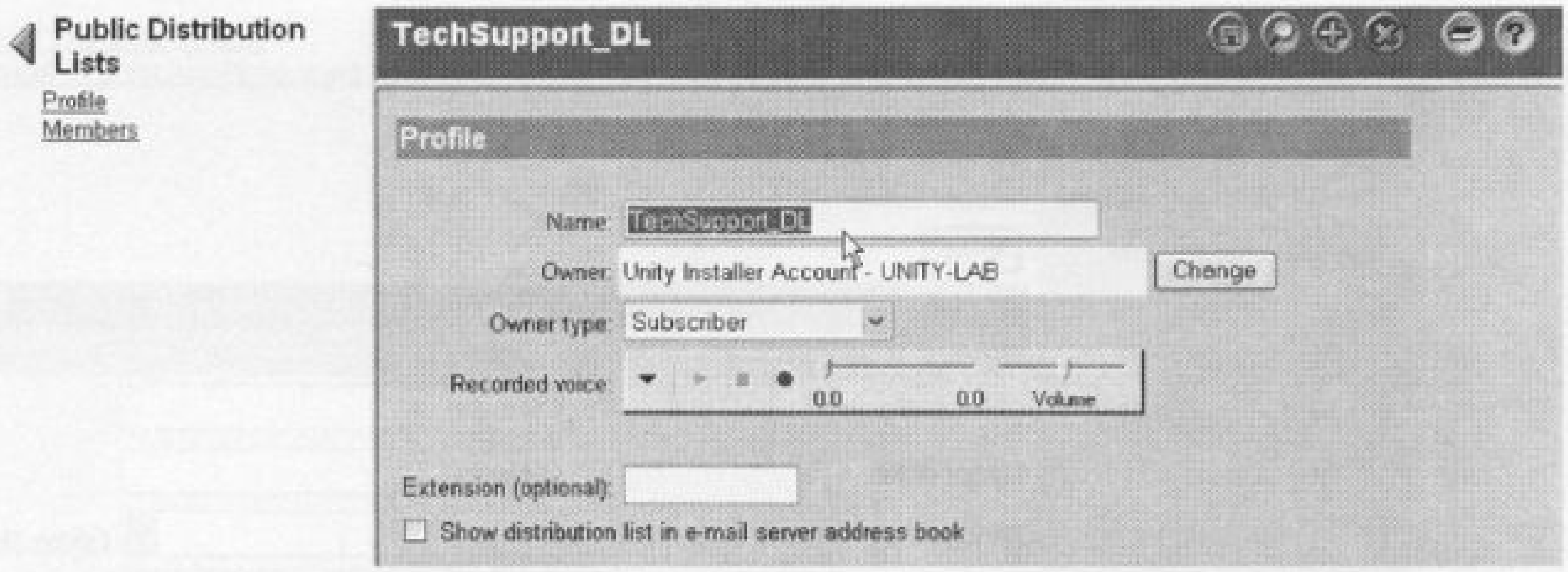


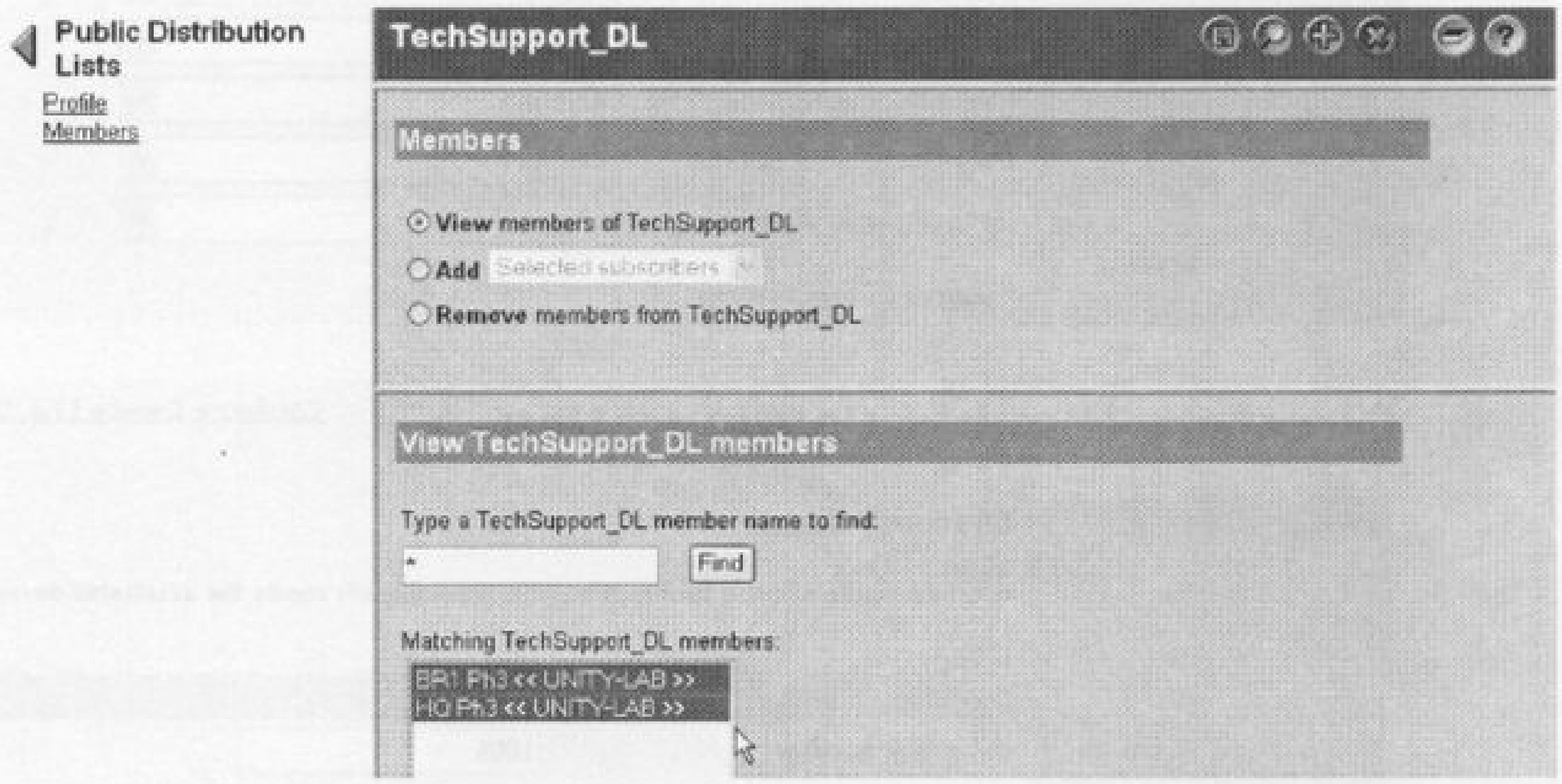
➔ **Create a CTI RP and assign it to the PT-Internal and forward it always to VM.**



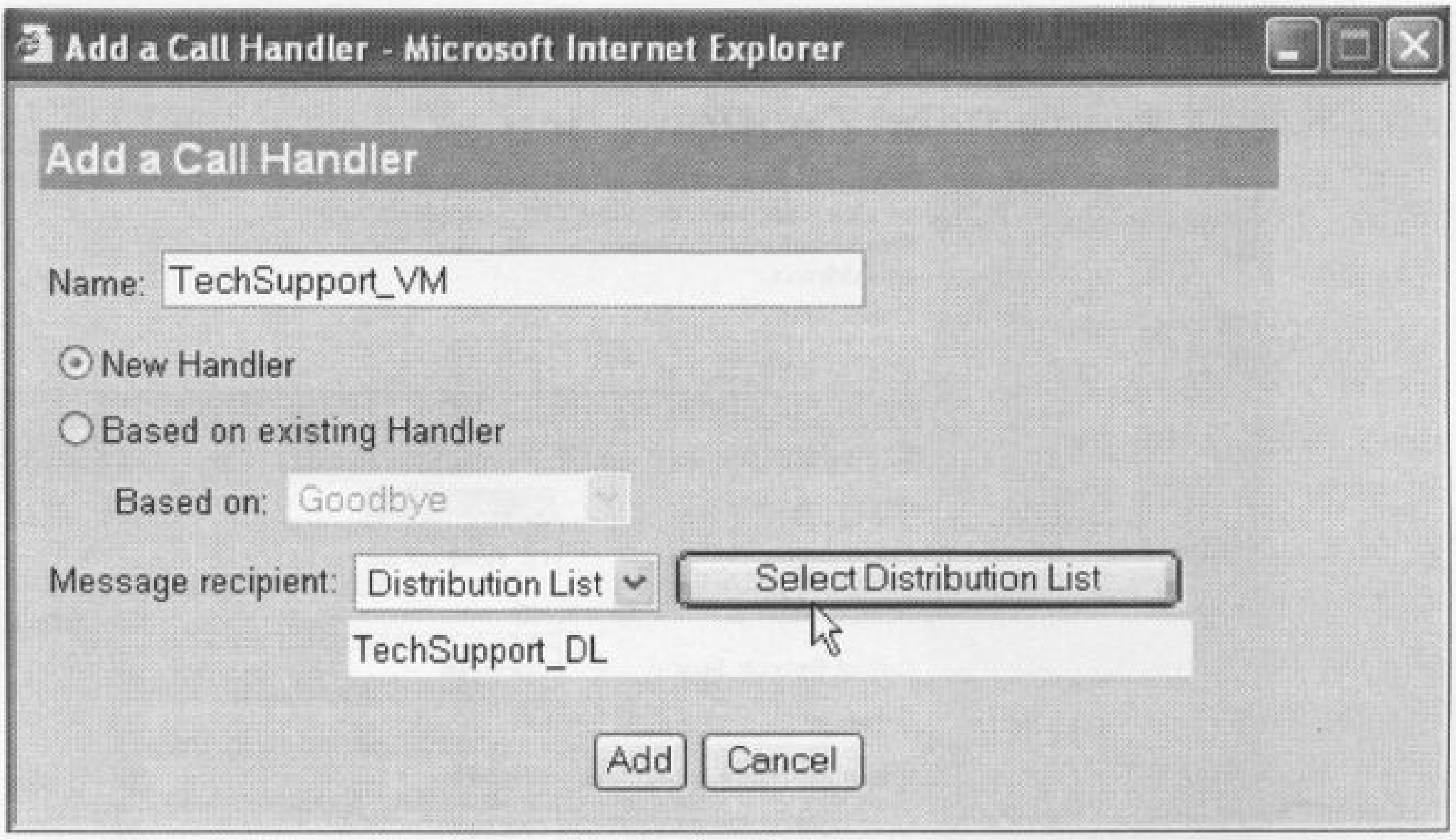


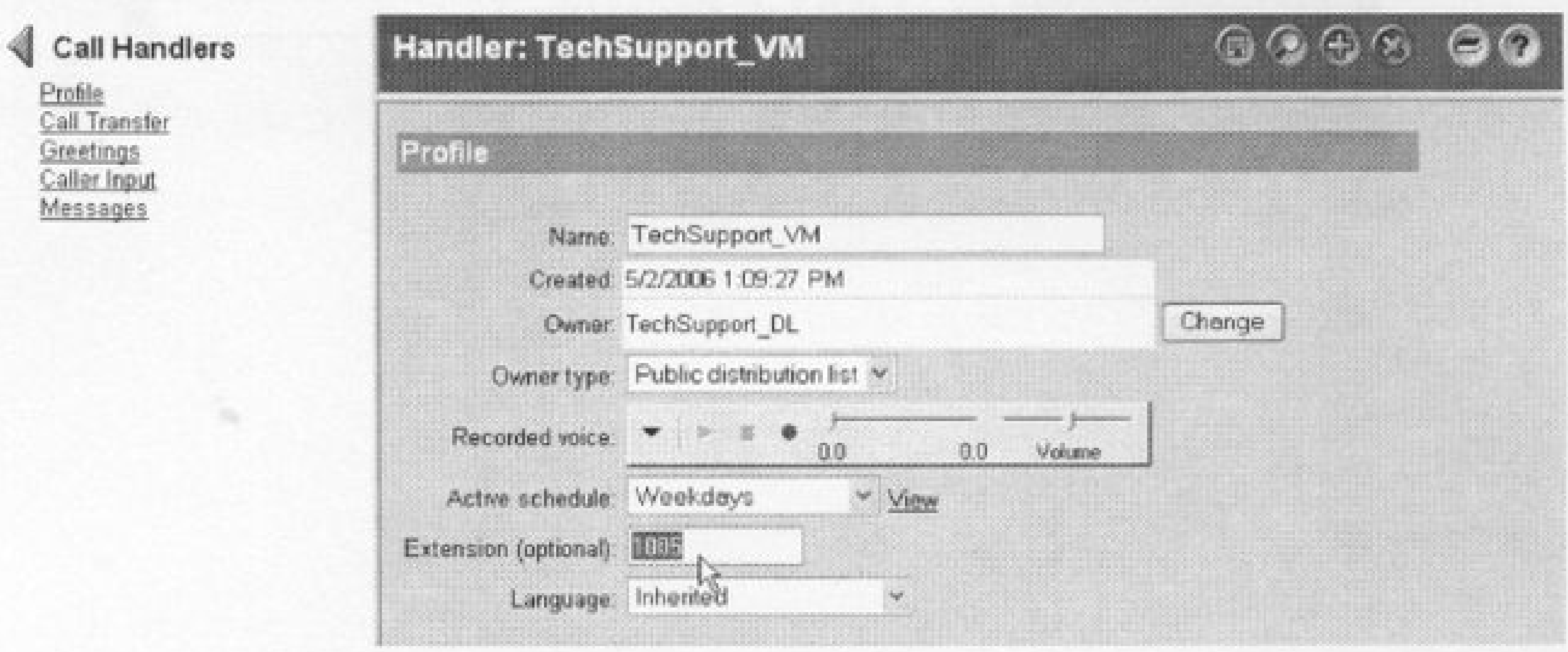
➔ **In Unity:**


Public Distribution Lists
Profile
Members
TechSupport_DL
Profile
Name: TechSupport_DL
Owner: Unity Installer Account - UNITY-LAB
Change
Owner type: Subscriber
Recorded voice:
0.0
0.0
Volume
Extension (optional):
Show distribution list in e-mail server address book

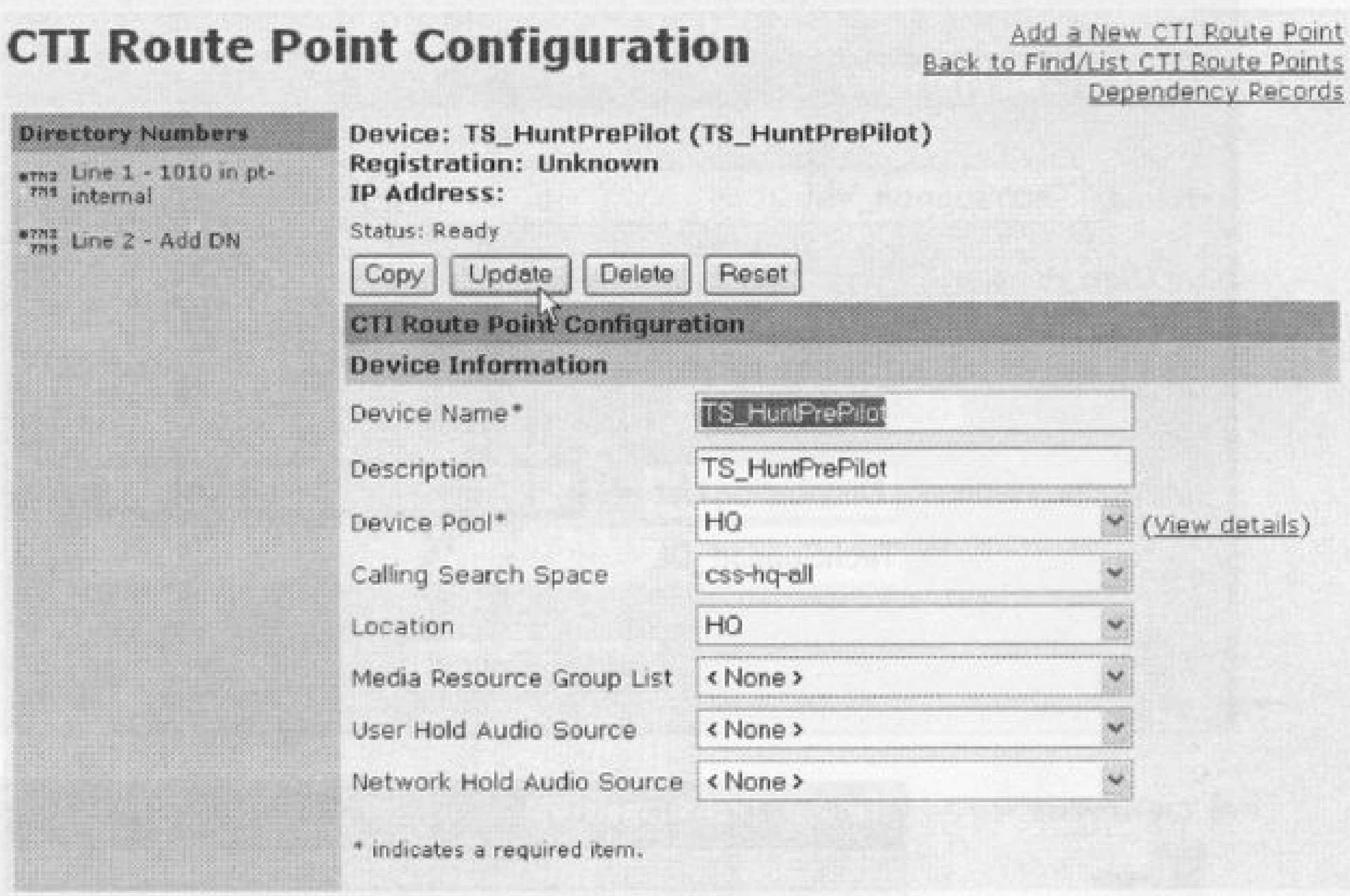

Public Distribution Lists
Profile
Members
TechSupport_DL
Members
View members of TechSupport_DL
Add Selected subscribers
Remove members from TechSupport_DL
View TechSupport_DL members
Type a TechSupport_DL member name to find:
*
Find
Matching TechSupport_DL members:
BR1 Ph3 << UNITY-LAB >>
HQ Ph3 << UNITY-LAB >>

➔ **Create a Call Handler with the message recipient as the Public Distribution list of TechSupport_DL.**



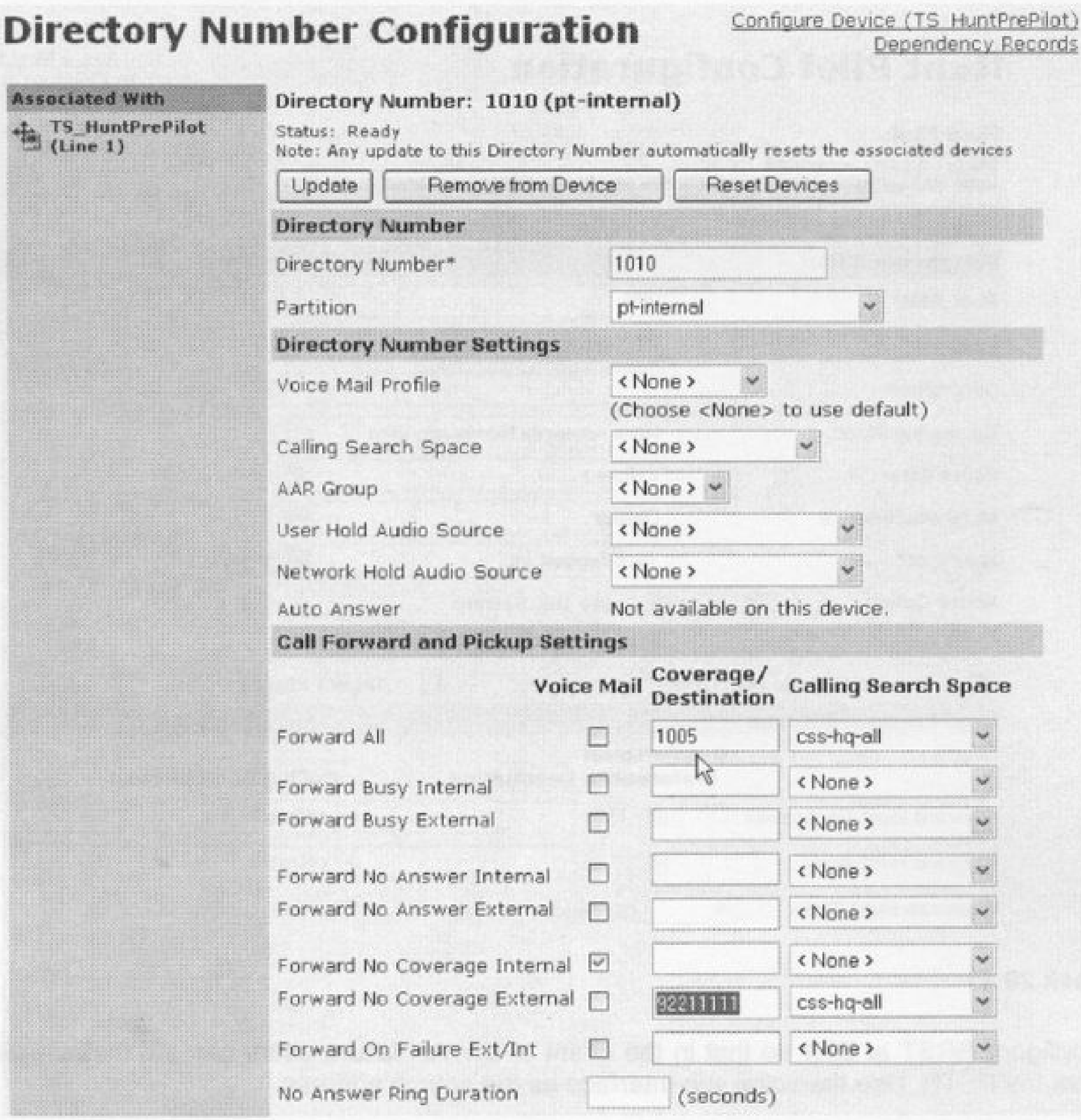


➔ **Now back in CCM – We need to create a CTI Route Point with the DN of 1010 in the PT-Internal or Null PT if you choose to use it. This will actually be the DN or DID that people call that will ring whichever DN of 1005 is available based on ToD Routing.**

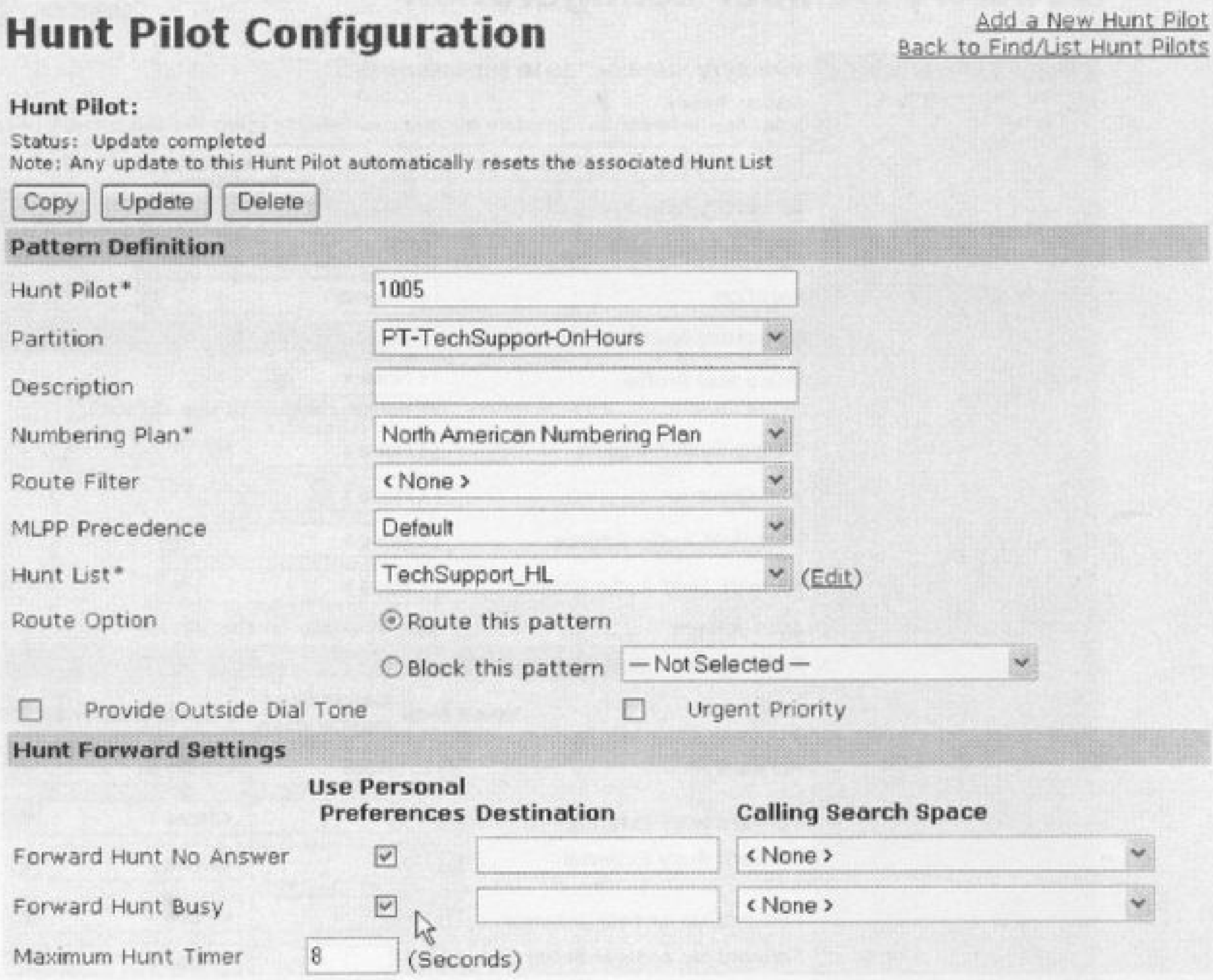


➔ **We will then configure this CTI RP DN with the setting to 'Forward All' to the DN of 1005 (our Hunt Pilot).**

➔ **Then configure the 'Forward No Coverage Internal' with the VM checkbox and the 'Forward No Coverage External' to '912211111' with a CSS allowing the call to go out the HQ gateway with Local privileges.**



➔ **Now we need to go back to our Hunt Pilot and configure it to only try the Hunt Group for 2 rings (which is approximately 8 seconds – 4 seconds per ring roughly) and then also tell the 'Forward Hunt No Answer' and 'Forward Hunt Busy' to 'Use Personal Preferences' which causes the Pilot number to revert back to the Call Coverage settings of whomever forwarded the call to it in the first place – which in this case is of course the CTI Route Point. This is what will enable the 'Forward No Coverage Internal/External' settings in the CTI RP DN page to take effect.**



Task 29.41

Configure SRST at BR1 so that in the event of a WAN failure users can still make/receive calls from the PSTN. Use the voice sub-interface as the source address.

➔ **This should be self-explanatory from previous examples.**

Task 29.42

Ensure that if BR1 gateway goes into fallback mode, that it has already created its own certificate, forwarded that certificate to CallManager and that CallManager in turn has installed that certificate into the IP Phones at BR1, so that signaling and media continue to be encrypted during any fallback occurrence.

➔ **This should be self-explanatory from previous examples – See Task 17.3.**

Task 29.43

Configure SRST such that one 3-party conference is allowed.

➔ **This should be self-explanatory from previous examples.**

Task 29.44

Configure Music on Hold for all phones in SRST fallback.

```
P2-BR1-RTR(config)#call-manager-fallback
P2-BR1-RTR(config-cm-fallback)#moh music-on-hold.au
```

Task 29.45

Configure SRST such that the phones will only re-register back to Call Manager after normal service has been resumed for 5 minutes. (normal service is defined as the WAN is operational and Call Manager is running).

➔ **See Task 8.6.**

Task 29.46

Calls to HQ and BR2 must be preserved using 4 digit dialing.

➔ **This should be self-explanatory from previous examples – use num-exp or prefix in POTS dial-peer.**

Task 29.47

Ensure that the same Class of restriction is preserved when phones are in SRST fallback.

➔ **This should be self-explanatory from previous examples.**

Task 29.48

Integrate Call Manager with Unity with the following information:

- Voice Mail Pilot = 1600
- Voice Mail Ports = 1601-1604
- MWI On/Off = 1999/1998

➔ **This should be self-explanatory from previous examples.**

Task 29.49

Configure the BR2 router to support the CUE module using information from Table 16. Setup the basic information needed to work the CUE module including what is needed to access the web-based GUI to manipulate user's extensions and mailboxes.

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

Finally setup mailboxes for all 3 phones at BR2 and ensure that they hear the CallerID of the person leaving the message when they go to retrieve messages.

➔ **This should be self-explanatory from previous examples – See Tasks 15.1 - 2.**

Task 29.50

Create a General Delivery Mailbox in CUE for the Support Queue but give it the extension of 3215. Ensure that any phone in the office can access this mailbox by pressing "9" after they sign into their VM box. Finally, modify the Support Queue (not the hunt group) so that if agents are un-available they will go to this GDM. Also ensure that all BR2 phones see if there is a message waiting in the GDM.

➔ **This should be self-explanatory from previous examples – See Task 16.2.**

Task 29.51

Create a Distribution List in CUE that allows users to be able to forward important messages to extension 3250 and all phones will receive the message in their own mailbox. The GDM must also receive the message in its box. You may NOT directly select phone extensions when creating this List.

➔ **This should be self-explanatory from previous examples – See Task 16.4.**

Task 29.52

Network CUE with Unity. Allow messages to be seamlessly forwarded back and forth.

➔ **This should be self-explanatory from previous examples – See Task 16.5.**

Task 29.53

Configure Unity VM Ports to use AES128 encryption for media traversal between themselves and IP Phones or Gateways that support such.

➔ **This should be self-explanatory from previous examples – See Task 17.6.**

Task 29.54

Configure a subscriber mailbox for phone 2 at each location. Record the subscriber's greeting to say "I am not in the office right now. If you need to reach me press 3 to be transferred to my cell phone otherwise please leave a message". Have callers transferred from Voicemail to the External Numbers listed in Table 10.

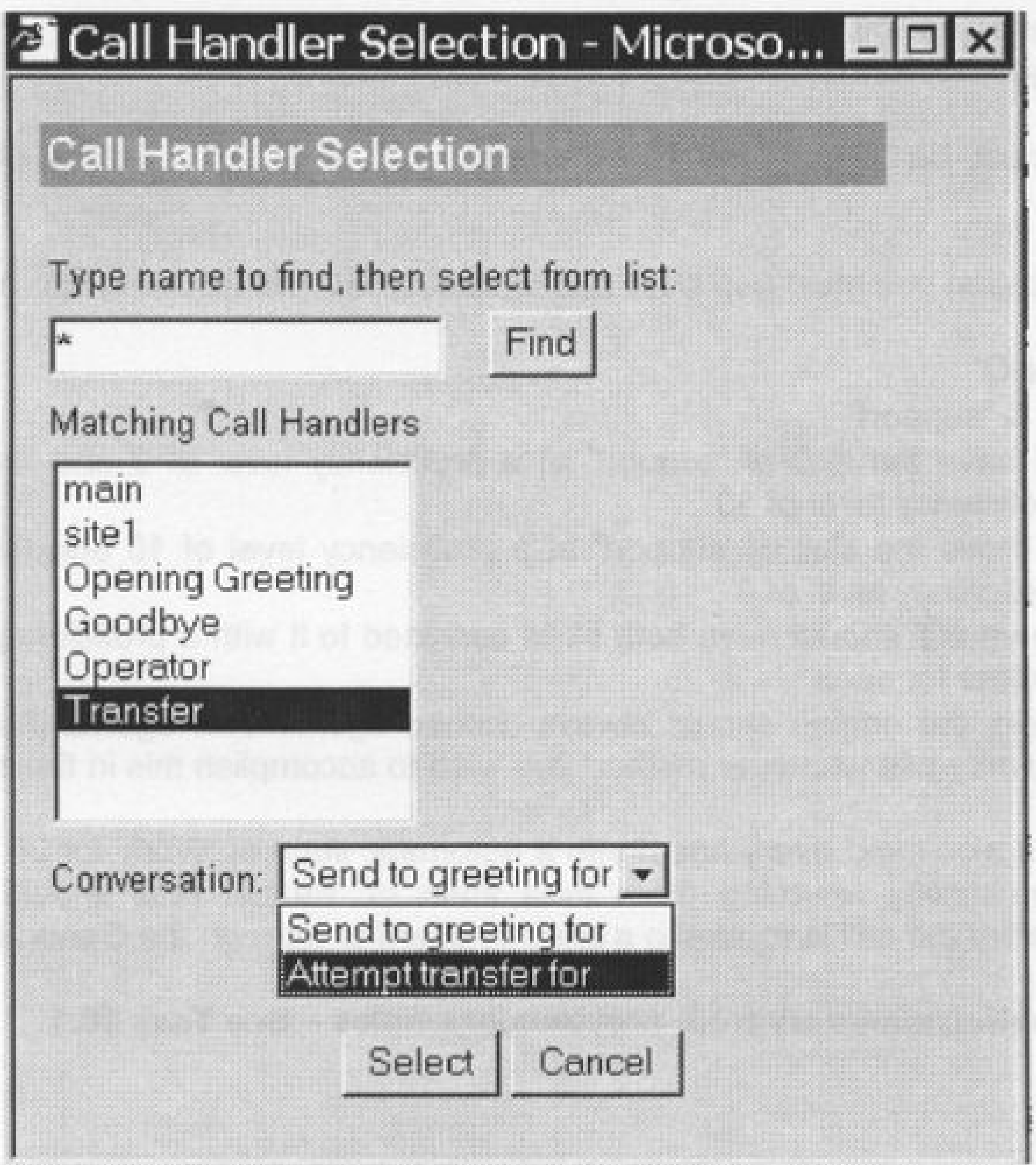
HQ phone 2 transfers to 212-22X-1111
BR1 phone 2 transfers to 617-52X-2222
BR2 phone 2 transfers to 011-33-1-32X-3333

➔ **Create a call handler. "Transfer". The purpose of this new call handler is to act as a transfer agent to the external phone.**

➔ **From the Call Transfer section under the Call Handlers heading, select Yes, Ring a subscriber at this extension - "912122221111".**

➔ **Now go to the subscriber (created in an earlier exercise) . From the Subscriber heading, select Caller Input and select the number you want callers to press in order to transfer to an external phone -"3".**

➔ **Select "Send caller to" using the pull down menu, choose the new Call handler. Click the find button to select your newly created call handler "Transfer".**



➔ **Under the Conversation menu of this screen select Attempt transfer for and save.**

➔ **Change your voicemail greeting to "I am not in the office right now. If you need to reach me press 3 to be transferred to my cell phone".**

Task 29.55

Configure Auto-attendant and ICD with the following information:

- AA Route Point = 1710
- Script = aa.aef
- CTI Ports = 1711, 1712

- ICD Route Point = 1700
- Script = icd.aef
- CTI Ports = 1701, 1702

Create the following users that will be used in this task:

- "**jtapi**" to be used for the JTAPI Subsystem.
- "**rmjtapi**" to be used for the ICD Subsystem.
- "**telecaster**" to be used for the ICD Subsystem and enterprise data.
- "**crsadmin**" which must be the designated administrator for IPCC Express.
- **agent1** [assigned device HQ Phone 3 with ICD ext="1003"].
- **agent2** [assigned device BR Phone 2 with ICD ext="2003"]

[all passwords must be 'cisco' and PIN numbers set to '12345' except of course 'telecaster']

For the ICD application you must use skills based routing with the following information:

- CSQ: "GeneralQ"
- Skills: "sales" & "support"
- 'agent1' shall have the skill of 'support' at a proficiency level of 9 and the skill of 'sales' at a proficiency level of 10
- 'agent2' shall have the skill of 'support' at a proficiency level of 10 and the skill of 'sales' at a proficiency level of 9
- The CSQ 'GeneralQ' should have both skills assigned to it with a proficiency level of at least 5 or better for each
- With this stated, the engine should always choose agent1 over agent2 if agent1 is available (you may use whatever method you wish to accomplish this in the engine)

The engine should also send every agent into a automatic state of 'Work' for 30 seconds before then automatically returning them to a state of 'Ready' (this should happen regardless of whether the call is routed to a specific agent or through the GeneralQ

➔ **This should be self-explanatory from previous examples – See Task 10.1.**

Task 29.56

Modify the "icd.aef" script with the following information (you may wish to rename it to avoid loosing the original script):

- You must determine if the call is coming from the PSTN from anywhere in the area code of '617' and if the call is coming from the 617 area code then the call must check to see if 'agent1' is available and route the call directly to that agent without queuing the call, however if agent1 is not available, send the call to the 'GeneralQ'
- If the call goes to the GeneralQ, music should be played to the caller while waiting in Q and the caller should also hear the 'QueuePrompt' every 30 seconds
- You must also determine what time the call is coming into the script – and if between the hours of 8 AM to 5 PM local server time – then you must determine if any agents are logged into the CSQ and if they are, continue processing the call in the script (do not worry about logged in agents for agent based routing here). If no agents are logged into the CSQ or if you determine that the time is outside of the specified hours, then the call must be routed to VM. You must route the call to the VM subscriber box of 1580 (create this mailbox), however you may **not** use any forwarding device in CCM (e.g. CTI Port, CTI RP, Phone, etc ...) **or** any Call Routing Rules in Unity to get this call to the correct mailbox.
- Regardless of whether the call is routed to a specififc agent or through the GeneralQ, the agent receiving the call should be presented with Enterprise Data showing both the ANI of the call and a disposition of how the call was routed (a string showing 'Agent' or 'Queue').

➔ **This should be self-explanatory from previous examples – See Task 26.47.**

Task 29.57

Configure CallManager such that HQ Phones 1 and 2 and BR1 Phones 1 and 2, will encrypt their signaling and media streams using AES128 with any device that will allow such to occur. Configure CCM to install a 1028 bit LSC on each phone. Configure the phones so that when a LSC is to be installed on the phone – that **no** user interaction is required on the IP Phone.

➔ **This should be self-explanatory from previous examples – See Task 17.2.**

Task 29.58

Configure Extension Mobility such that a Device Profile with DN = '1551' is assigned to the following user.

- UserID='em'
- Password='adgjm'
- PIN='12345'

This user must be allowed to log into any device in the BR1 site. The user should be allowed to log into the ICD and become a sales agent.

➔ **Set up Extension Mobility like in previous tasks such as 11.4.**

➔ **Assign all devices in Branch 1 to RMJTAPI.**

➔ **Assign the Device Profile created to RMJTAPI.**

➔ **Subscribe the ICD service to the Device Profile.**

Task 29.59

Configure IPMA with the following information: BR1 phone 3 will be used as the manager phone and HQ phone 3 will be used as the assistant phone.

Username: br1phn3	**Username: Assistant**
Primary Line: 2003	Primary Line: 1003
SD to Intercom	Proxy Line: 1560
	Incoming Intercom

The IPMA Assistant Console can be installed on the Call Manager.

Make sure that the IPMA can intercept the calls to the manager's primary extension.

Configure a Unity account for the manager. Make sure that on the manager's phone MWI still works correctly.

➔ **This should be self-explanatory from previous examples.**

Task 29.60

Assume the single cable solution is used, configure the switches to trust the Layer 2 QoS classification of the IP phones but not the attached PC.

➔ **This should be self-explanatory from previous examples.**

Task 29.61

Configure the Catalyst 6500 to mark all VOIP control traffic from the Call Manager to the appropriate L3 setting.

➔ **This should be self-explanatory from previous examples.**

Task 29.62

Configure the Catalyst 6500 to move VOIP control traffic to the 2nd queue and 1st threshold.

➔ **This should be self-explanatory from previous examples.**

Task 29.63

Configure the Catalyst 6500 and 3550 to map the CoS to DSCP value.

➔ **This should be self-explanatory from previous examples.**

Task 29.64

The link speed between HQ and Branch 2 is 256 Kbps. Employ the well-known technique to minimize serialization delay. There is no need to do this on the link between HQ and Branch 1 since its link speed is 1544kbps.

➔ **This should be self-explanatory from previous examples.**

Task 29.65

From HQ Site to Branch 2, reserve 33% of the bandwidth for voice RTP traffic on a priority queue and reserve 5% minimum guaranteed bandwidth for voice control traffic.

➔ **This should be self-explanatory from previous examples.**

Task 29.66

From Branch 2 to HQ Site, reserve 128 kbps for voice RTP traffic on a priority queue and reserve minimum guaranteed bandwidth of 12kbps for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queuing.

➔ **This should be self-explanatory from previous examples.**

Task 29.67

From the HQ site to the Branch 1 site (PVC speed is 1544 Kbps), reserve 25% of bandwidth for voice RTP traffic on a high priority queue and 5 % of bandwidth for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queuing.

➔ **This should be self-explanatory from previous examples.**

Task 29.68

Configure Fax Passthru throughout the network.

➔ **This should be self-explanatory from previous examples.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 30: Multiprotocol Challenge M

Estimated Time to Complete: 10 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 30 Multiprotocol Challenge M

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 30 Configuration Tasks

Task 30.1

Ensure that the link between the HQ/BR1/BR2 routers and appropriate switches are configured as DOT1Q trunks. Give the voice sub-interface the appropriate ip address from Table 1. Check connectivity between all sites and to Call Manager/Unity.

➔ **This should be self-explanatory from previous examples.**

Task 30.2

Configure Voice and Data VLAN for all IP Phones including ATA and VG248. VLAN IDs are defined in Table 2. Use Table 3 for HQ site 6500 port assignment. For BR1 and BR2 port allocation you are required to find out port allocation by your own methods.

➔ **This should be self-explanatory from previous examples.**

Task 30.3

Set the hardware clock on the HQ router (use EST as the time zone which is 5 hours behind GMT and setup Daylight Savings Time as well as EDT). Configure the HQ-RTR to become an authoritative time source which distributes the time via NTP. Configure the BR1 and BR2 routers to synchronize their clock with the HQ-RTR loopback interface.

➔ **On HQ-RTR:**

```
clock timezone EST -5
clock summer-time EDT reoccurring
ntp master
ntp source loopback0
```

➔ **On BR1 and BR2 routers:**

```
ntp server 10.1.200.3
```

Task 30.4

For the Headquarter site, use Microsoft DHCP server to allocate IP address for all Devices. For Branch 1 and 2, use IOS DHCP to allocate IP address for the IP phones. For each voice subnet, allocate the IP address from .50 to .69.

➔ **This should be self-explanatory from previous examples.**

Task 30.5

Assign directory number to devices based on Tables 5 and 6. Allow HQ devices to register manually and manually add BR1 devices to the Call Manager.

➔ **This should be self-explanatory from previous examples.**

Task 30.6

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 30.7

Use CallManager's only CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **This should be self-explanatory from previous examples – See Task 2.2.**

Task 30.8

Ensure that when a user presses the 'Services' or 'Directories' button the error message is not displayed.

➔ **This should be self-explanatory from previous examples.**

Task 30.9

Configure Calling Restriction using the Table below. Restrict internal callers from BR1 only, so that they may not see CNAM information only regarding who they are calling or who is calling them, however ensure that BR1 Phone 3 **can** see all CNAM information.

➔ **See Task 2.2 for CNAM restrictions.**

- PT-HQ-911
- PT-HQ-LOC
- PT-HQ-LD
- PT-HQ-INTERNATIONAL
- PT-BR1-911
- PT-BR1-LOC
- PT-BR1-LD
- PT-BR1-INTERNATIONAL
- PT-INTERNAL

➔ **Put all the phones (except HQ phn1 and BR1 Phn 1) in the partition PT-INTERNAL.**

➔ **Create the following CSS:**

- CSS-HQ-INTERNAL-911-LOC
- CSS-HQ-INTERNAL-ALL
- CSS-BR1-INTERNAL-911-LOC
- CSS-BR1-INTERNAL-ALL

➔ **Assign CSS to Devices. HQ phone 4 should not have any CSS assigned.**

➔ **This phone will have the null CSS assigned and will only be able to see devices in the null Partition (i.e. HQ phone 1 and BR1 phone 1).**

Task 30.10

Set the phones that reside in the POD (all 79XX not physically accessible to you) to auto-answer. Phones must only auto-answer after 5 seconds.

➔ **This should be self-explanatory from previous examples.**

Task 30.11

Register phones at BR2 based on Table 7.

➔ **This should be self-explanatory from previous examples.**

Task 30.12

Create a circular hunt group for Support with a DN of 3210 at BR2 between phones 1 and 3, and ensure that those phones can login-to and out-of the hunt group in order to receive calls. Allow the call to ring at around 3 times before searching for the next member.

➔ **On BR2:**

```
ephone-hunt 1 peer
 pilot 3210
 list 3001, 3003
 timeout 12
```

➔ **Use the 'DND' softkey to log a user out of the hunt group.**

Task 30.13

BR2 should use the same class of restriction as the other sites.

➔ **This should be self-explanatory from previous examples.**

Task 30.14

Configure CME such that outbound calls to 1 900 XXX-XXXX from Phone 1 and 2 are blocked.

```
P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)# after-hours block pattern 1 91900  7-24
```

Task 30.15

Configure CME such that outbound calls from Phone 2 do not forward caller ID. All other phones from CME should forward caller IDs. However allow that if a user dials *67 and then a pattern (PSTN or Internal), that caller ID will not show up on the receiving phone.

```
telephony-service
 caller-id block code *67
!
ephone-dn  2
 number 3002
 description 3313223002
 caller-id block
```

Task 30.16

Configure the inter-digit timeout to be 3 seconds on CME.

```
P2-BR2-RTR(config)#telephony-service
P2-BR2-RTR(config-telephony)# timeout interdigit 3
```

Task 30.17

Configure phones 2 and 3 at BR2 so that they can intercom each other and have an immediate 2-way conversation – security should be in place so that no one else can dial their respective intercom numbers. Use whatever DNs you wish for this. Also, if another intercom call happened to be present on phone 1 when phone 2 places the intercom call – the first call should be automatically put on hold.

➔ **This task can only be performed on 7960 phones given that each phone in the POD is a 7940 and already has two lines assigned. To perform use IP Blue clients or remove the shared line added in previous tasks.**

➔ **On BR2:**

➔ **The A3002, A3003 alpha-numeric DNs make the intercom # so it is not dial-able from a phone.**

➔ **The barge-in feature puts any existing intercom calls on hold.**

```
ephone-dn 2
 number 3002
!
ephone-dn 3
 number 3003
!
ephone-dn 22
 number A3002
 name "Intercom Ph2"
 intercom A3003 barge-in
!
ephone-dn 23
 number A3003
name "Intercom Ph1"
 intercom A3002 barge-in
!
ephone 2
 button 1:2 2:22
!
ephone 3
 button 1:3 2:23
```

Task 30.18

Configure BR1 as an H323 gateway, based on information in Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed.

➔ **This should be self-explanatory from previous examples.**

Task 30.19

Configure BR1 as an MGCP gateway, based on information in Table 8. Calling Number (10 digits) and Calling Name should be displayed. Secure the signaling and RTP transport traffic (RTP if allowed by phone) back and forth to this gateway.

➔ **This should be self-explanatory from previous examples – See Task 17.4 – 5 for security setup.**

Task 30.20

Configure the HQ-RTR as an IPIPGW. Calls will be coming into it from CCM via H323 using G711ulaw and then be routed out to the BR2 CME via SIP using G729 (see Table 9 for DNs at CME). Calls will also be coming from CME via H323 using G729 and routed to CCM via SIP using G711ulaw (see Table 10 for DNs at CCM). Also ensure when calls are coming from SIP to H323 that RFC 2833 is properly stripped. Ensure that if calls are coming from H323 to SIP, that RFC 2833 is used for the SIP side.

➔ **This should be self-explanatory from previous examples – See Task 4.9.**

Task 30.21

Unity needs to be able to accept in-bound faxes at the mailbox of IncomingFax@voip.lab. Unity will also be your DNS server. Configure the BR1 GW to intercept these faxes from the PSTN PRI as an On-Ramp gateway and email all incoming faxes to this mailbox. Refer to Table 7 of this section for FaxDN ranges. Unity also needs to be able to send out-bound faxes to the PSTN. Configure the BR1 GW to accept these faxes via email from Unity and then to send them out through the PSTN PRI as an Off-Ramp gateway. Refer to Table 18 of this section for PSTN FaxDN ranges. All the files you will need are in BR1 Flash memory.

➔ **This should be self-explanatory from previous examples – See Task 4.8 and 4.10.**

Task 30.22

Configure the E1 R2 such that calls to the PSTN are set up 3 seconds quicker (where possible) than the default. You may assume the maximum length digit string is 11 digits.

➔ **This should be self-explanatory from previous examples.**

Task 30.23

Configure gatekeeper on HQ-RTR with the following information:

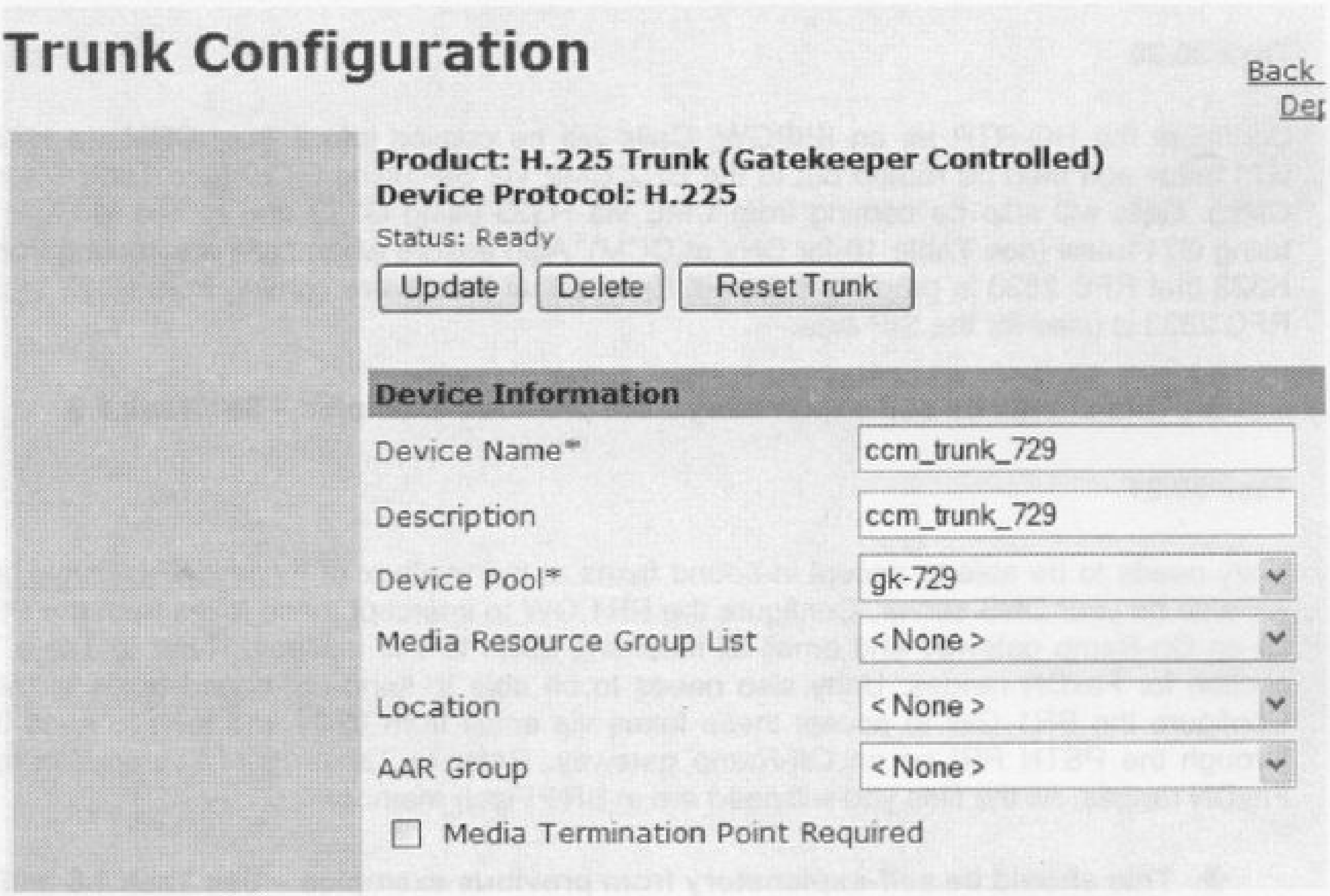
Local zone= HQ-RTR
domain name = ipexpert.com
[use loopback interface for local zone]

Allow 2 G729 calls through the gatekeeper. All calls involving the gatekeeper must use G729.

Register Call Manager to gatekeeper using a tech-prefix but not using "default-technology". Register CME to the gatekeeper. You MUST not register any DNs or E164 numbers configured on CME. The PSTN-WAN gatekeeper in the PSTN backbone IS NOT ALLOWED in this lab.

➔ **On CCM:**

➔ **Create the trunk in a device pool which only uses G729.**



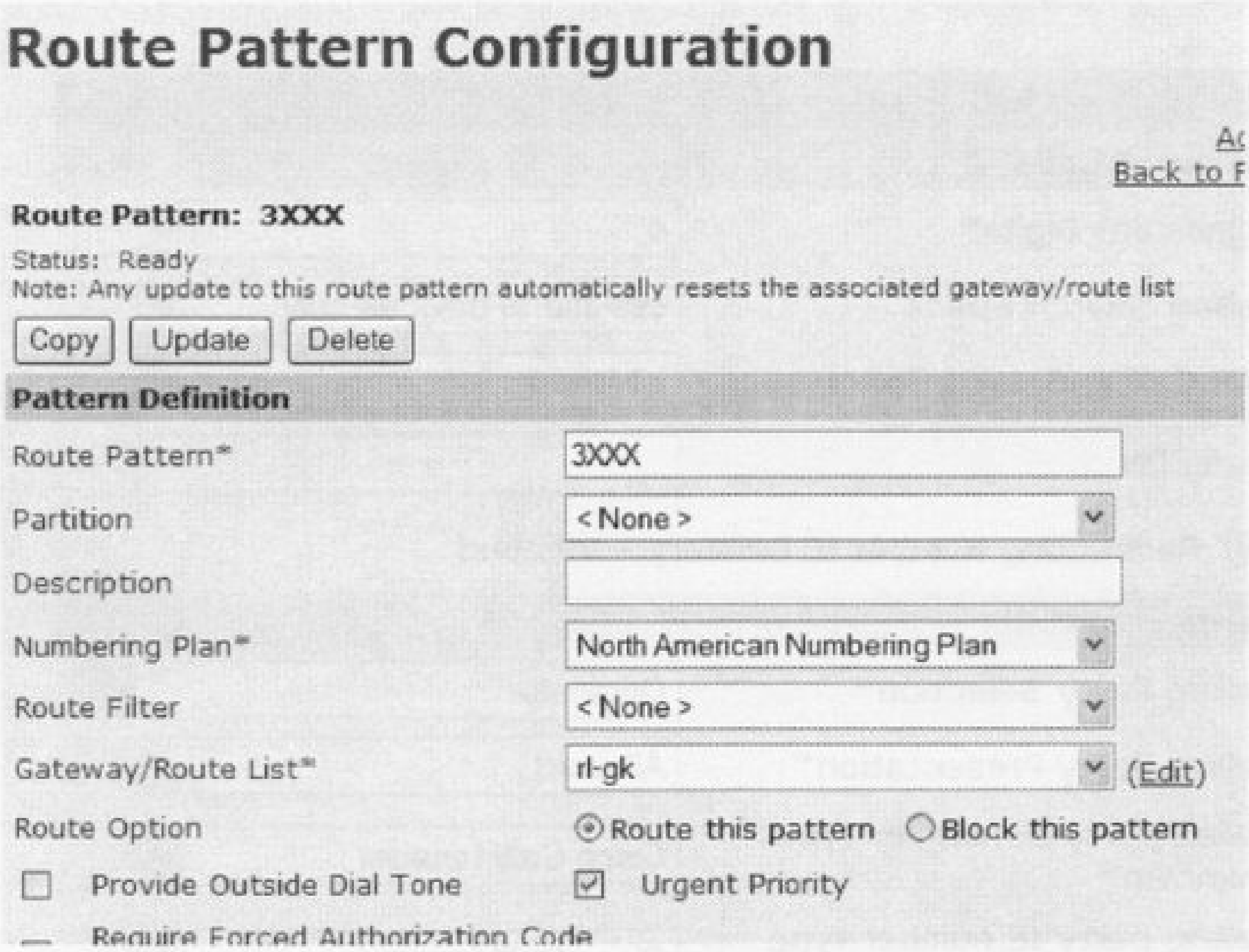
➔ **Ensure the IC Sig digits is set to 4 and assign a CSS which can see the devices (remembering that devices are in PT-INTERNAL and the null partition).**

Call Routing Information	
Inbound Calls	
Significant Digits*	4
Calling Search Space	css-interal-devices-only
AAR Calling Search Space	< None >
Prefix DN	
☑ Redirecting Number IE Delivery - Inbound	
Outbound Calls	
Calling Party Selection*	Originator
Calling Party Presentation*	Allowed
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Caller ID DN	
☑ Display IE Delivery	
☑ Redirecting Number IE Delivery - Outbound	

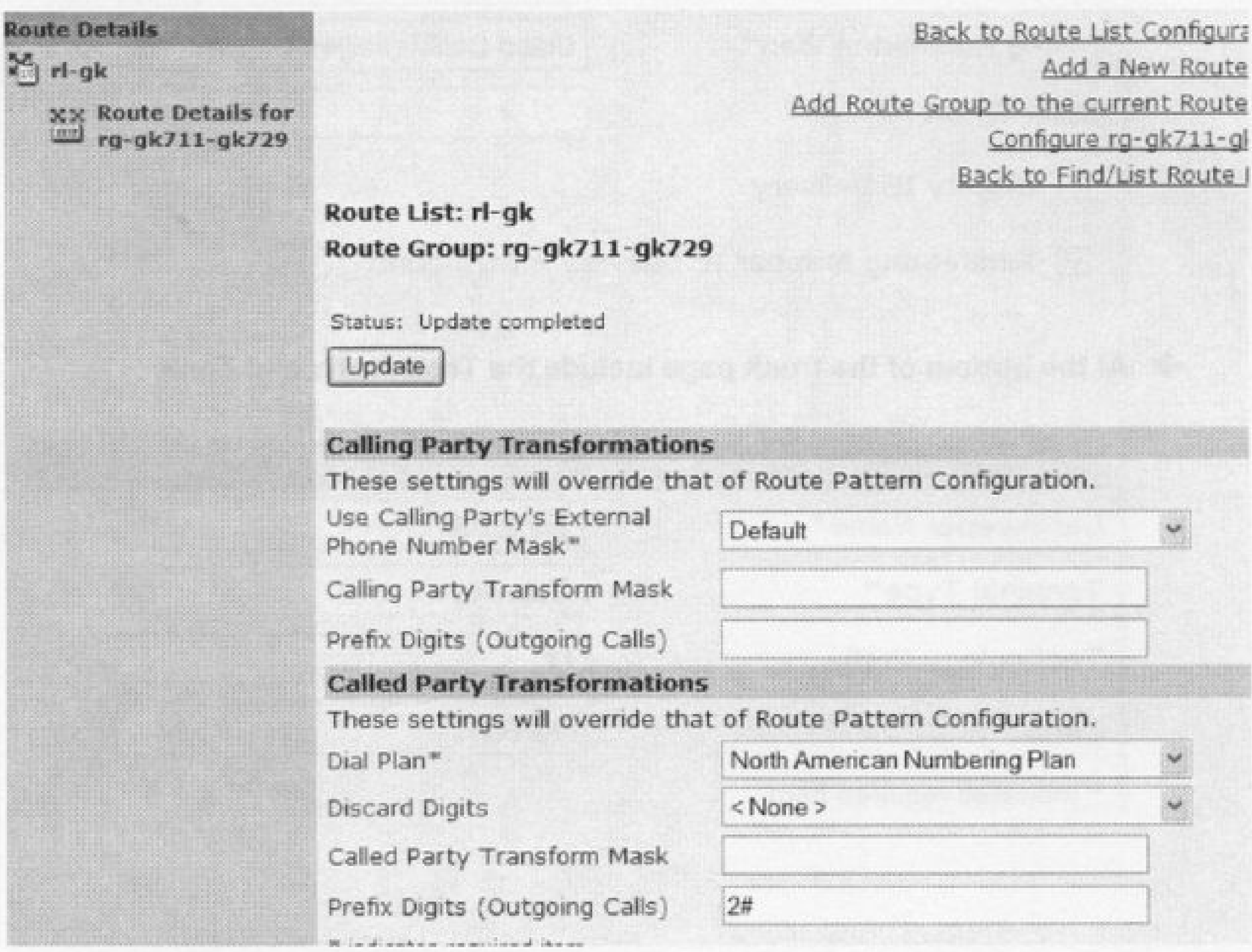
➔ **At the bottom of the trunk page include the Tech Prefix and Zone.**

Gatekeeper Information	
Gatekeeper Name*	172.2.100.1
Terminal Type*	Gateway
Technology Prefix	1#
Zone	HQ-RTR
* indicates required item	

➔ **Create a Route Pattern in the null partition and point to the GK Route List.**



➔ **Insert Tech-prefix of 2# in the Route List of GK.**



➔ **On HQ-RTR:**

```
gatekeeper
 zone local HQ-RTR ipexpert.com 172.2.100.1
 bandwidth total default 32
 no shutdown
```

➔ **On CME:**

```
interface Loopback0
 ip address 172.2.102.1 255.255.255.255
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id HQ-RTR ipaddr 172.2.100.1 1719
 h323-gateway voip h323-id CME
 h323-gateway voip tech-prefix 2#
 h323-gateway voip bind srcaddr 172.2.102.1
!
gateway
!
telephony-service
!
 dialplan-pattern 1 3313223... extension-length 4 no-reg
!
ephone-dn 1 dual-line
 number 3001 no-reg primary
!
ephone-dn 2 dual-line
 number 3002 no-reg primary
!
ephone-dn 3
 number 3010 no-reg primary
 no huntstop
!
ephone-dn 4
 number 3010 no-reg primary
 preference 1
!
ephone-dn 5 dual-line
 number 3003 no-reg primary
 description 3313223003
 name BR2Phn3
!
dial-peer voice 12 voip
 incoming called-number .
 dtmf-relay h245-alphanumeric
 no vad
!
num-exp 2#3... 3...
```

← Again, this tech prefix will dynamically register with the GK – there is no need to statically configure it on the GK

← This num-exp will strip off the 2# Tech Prefix from the DNIS on any inbound call

➔ Verification:

➔ On HQ GK:

```
P2-HQ-RTR#sh gatek end
            GATEKEEPER ENDPOINT REGISTRATION
            ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name       Type    Flags
--------------- ----- --------------- ----- ---------       ----    -----
10.2.200.21     62774 10.2.200.21     59712 HQ-RTR          VOIP-GW
  H323-ID: ccm_trunk_729_1
  Voice Capacity Max.=  Avail.=  Current.= 1
172.2.102.1     1720  172.2.102.1     56382 HQ-RTR          VOIP-GW
  H323-ID: CME
  Voice Capacity Max.=  Avail.=  Current.= 1
Total number of active registrations = 2
```

```
P2-HQ-RTR#sh gatek gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=========================
Prefix: 1#*
 Zone HQ-RTR master gateway list:
  10.2.200.21:62774 ccm_trunk_729_1
 Zone HQ-RTR prefix 3... priority gateway list(s):
  Priority 5:
   10.2.200.21:62774 ccm_trunk_729_1

Prefix: 2#*
 Zone HQ-RTR master gateway list:
  172.2.102.1:1720 CME
 Zone HQ-RTR prefix 3... priority gateway list(s):
  Priority 10:
   172.2.102.1:1720 CME
```

➔ Make the Call…

```
P2-HQ-RTR#sh gatek call
Total number of active calls = 1.
                    GATEKEEPER CALL INFO
                    ====================
LocalCallID                  Age(secs)  BW
7-170                        28         16(Kbps)
 Endpt(s): Alias             E.164Addr
  src EP: ccm_trunk_729_1    2003
       CallSignalAddr  Port  RASSignalAddr   Port
       10.2.200.21     62774 10.2.200.21     59712
 Endpt(s): Alias             E.164Addr
  dst EP: CME                2#3003
       CallSignalAddr  Port  RASSignalAddr   Port
       172.2.102.1     1720  172.2.102.1     56382
```


➔ **On BR2 CME:**

```
P2-BR2-RTR#sh call act v br

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
3B1D : 167 677729520ms.1 +2830 pid:12 Answer 2003 active
 dur 00:00:03 tx:118/2360 rx:0/0
 IP 10.0.200.32:24634 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
3B1D : 168 677729530ms.1 +2820 pid:20006 Originate 3003 active
 dur 00:00:03 tx:0/0 rx:118/2360
 Tele 50/0/5 (168) [50/0/5.0] tx:0/0/0ms g729r8 noise:0 acom:0  i/0:0/0 dBm

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Task 30.24

For the HQ site ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the BR1 gateway with the HQ gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of local gateway with HQ gateway acting as backup.

➔ **This should be self-explanatory from previous examples.**

Task 30.25

Configure calls such that a BR1 user is able to enter one of 2 client codes (see Table 19) when dialing a LD number.

➔ **This should be self-explanatory from previous examples – See Task 11.8.**

Task 30.26

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed out of the local gatekeeper as the primary route and directly through the IPIPGW as a secondary route. Users must be able to dial the BR2 site using extension (4 digit) dialing. (**Test both** call routing methods, one at a time, before moving on to the next question)

➔ **Primary route is covered previously in Task 30.23.**

➔ **Secondary route is covered in Tasks 6.1 – 6.**

Task 30.27

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway.

➔ **This should be self-explanatory from previous examples.**

Task 30.28

Calls originating from BR2 to CallManager (both HQ and BR1) should use the HQ gatekeeper as the primary route and directly through the IPIPGW as a secondary route. 4-digit dialing must be preserved. (**Test both** call routing methods, one at a time, before moving on to the next question.

➔ **Primary route is covered below:**

```
interface Loopback0
 ip address 172.1.102.1 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id HQ-RTR ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id CME
 h323-gateway voip bind srcaddr 172.1.102.1
!
gateway
!
dial-peer voice 1000 voip
 destination-pattern [1-2]...
 session target ras
 tech-prefix 1#
 dtmf-relay h245-alphanumeric
```

➔ **Secondary route is covered in Tasks 6.1 – 6.**

Task 30.29

Enable DID for PSTN users dialing into the CM/CME (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits.

➔ **This should be self-explanatory from previous examples.**

Task 30.30

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 30.31

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 30.32

Configure conference bridge on BR1 router. Use a maximum of 1 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 30.33

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 30.34

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should use the IOS resources first and then 6608 resources.

➔ **This should be self-explanatory from previous examples.**

Task 30.35

Configure a Music on Hold server on the Publisher Call Manager.

➔ **This should be self-explanatory from previous examples.**

Task 30.36

All sites must receive music using the G711 codec.

➔ **This should be self-explanatory from previous examples.**

Task 30.37

Ensure that the HQ and BR1 phones receive multicast music on hold. The IOS gateway must be the multicast source for music played to the BR1 phones and the CCM MOH server must be the multicast source for music played to the HQ phones.

➔ **This should be self-explanatory from previous examples.**

Task 30.38

Configure music on hold on the BR2 CME.

➔ **This should be self-explanatory from previous examples.**

Task 30.39

Create a meet-me conference with DN=1900. Nobody should be able to dial this number directly other than HQ Phone 1. The maximum number of participants of a single Meet-me conference should be 6 conferencees.

➔ **This should be self-explanatory from previous examples.**

Task 30.40

Integrate Call Manager with Unity with the following information:

- Voice Mail Pilot = 1600
- Voice Mail Ports = 1601-1604
- MWI On/Off = 1999/1998

➔ **This should be self-explanatory from previous examples.**

Task 30.41

Integrate CME into Unity Express with the following information (**Table 16**):

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

Also ensure that when users listen to their voicemail messages, that they hear the ANI announced of the phone who left them the message.

➔ **This should be self-explanatory from previous examples – See Tasks 15.1 and 3.**

➔ **Remember NOT to register your ephone-DNs to gatekeeper lest you miss points for that previous task.**

```
ephone-dn 10
number 3999…. no-reg
mwi on
!
ephone-dn 11
number 3998…. no-reg
mwi off
```

Task 30.42

Configure Unity VM Ports to use AES128 encryption for media traversal between themselves and IP Phones or Gateways that support such.

➔ **This should be self-explanatory from previous examples – See Task 17.6.**

Task 30.43

Phone 1 at all locations should be configured with a Unity account.

➔ **This should be self-explanatory from previous examples.**

Task 30.44

Configure Unity so that if a IP Phone caller conferences in Ext 1650, that Unity will record the conversation and forward that recording to the mailbox of the IP Phone that initiated the conference.

➔ **This should be self-explanatory from previous examples – See Task 9.8.**

Task 30.45

Configure Unity to be an Inbound and Outbound Fax Server. Create the necessary VM box for BR1 Phone 2 and ensure that Faxes coming in from the BR1 (Table 17). Ensure that Faxes going out to the PSTN number in Table 18 from the BR1 Gateway arrive and are viewable.

➔ **This should be self-explanatory from previous examples – See Task 9.9 – 10.**

Task 30.46

Configure an Auto-Attendant and ICD application with the following information.

- AA Route Point = 1710
- Script = aa.aef
- CTI Ports = 1711, 1712

- ICD Route Point = 1700
- Script = icd.aef
- CTI Ports = 1701, 1702

Create the following users that will be used in this task:

- "**jtapi**" to be used for the JTAPI Subsystem.
- "**rmjtapi**" to be used for the ICD Subsystem.
- "**telecaster**" to be used for the ICD Subsystem and enterprise data.
- "**crsadmin**" which must be the designated administrator for IPCC Express.
- **agent1** [assigned device HQ Phone 3 with ICD ext="1003"].
- **agent2** [assigned device BR Phone 2 with ICD ext="2003"]

[all passwords must be 'cisco' and PIN numbers set to '12345' except of course 'telecaster']

For the ICD application you must use skills based routing with the following information:

- CSQ: "GeneralQ"
- Skills: "sales" & "support"
- 'agent1' shall have the skill of 'support' at a proficiency level of 9 and the skill of 'sales' at a proficiency level of 10

- 'agent2' shall have the skill of 'support' at a proficiency level of 10 and the skill of 'sales' at a proficiency level of 9
- The CSQ 'GeneralQ' should have both skills assigned to it with a proficiency level of at least 5 or better for each
- With this stated, the engine should always choose agent1 over agent2 if agent1 is available (you may use whatever method you wish to accomplish this in the engine)
- The engine should also send every agent into a automatic state of 'Work' for 30 seconds before then automatically returning them to a state of 'Ready' (this should happen regardless of whether the call is routed to a specific agent or through the GeneralQ)

➔ **This should be self-explanatory from previous examples – See Task 10.1.**

Task 30.47

If a call rings into HQ Phone 3, that user must have the option of sending that call to VM without exhausting the CallFwdNoAn timer.

➔ **This should be self-explanatory from previous examples – See Task 11.7.**

Task 30.48

Configure Attendant Console with Pilot number = '1550'. Add HQ phone 3 and BR1 phone 3 into the huntgroup. Enable Circular Hunting within the AC huntgroup. Also ensure that if there are up to 20 callers simultaneously calling 1550, and both IP Phones are presently taking calls, that callers will not be dropped but any number greater that 20 callers will be dropped and not sent to VM. Also, a call should not be dropped no matter how long it remains waiting.

➔ **This should be self-explanatory from previous examples – See Tasks 11.1 and 3.**

Task 30.49

Configure CallManager such that HQ Phones 1 and 2 and BR1 Phones 1 and 2, will encrypt their signaling and media streams using AES128 with any device that will allow such to occur. Configure CCM to install a 1028 bit LSC on each phone. Configure the phones so that when a LSC is to be installed on the phone – that **no** user interaction is required on the IP Phone.

➔ **This should be self-explanatory from previous examples – See Task 17.2.**

Task 30.50

Create a DN of 1005 for Tech Support. Make HQ phone 3 and BR1 Phone 3 ring simultaneously when this DN is called. You may not use a shared line to accomplish this task. DN 1005 should forward directly to VM anytime outside of normal business hours with no user intervention needed. Check **Table 11** for a time schedule. Also, all members of this HuntGroup should get the message in their VM box and see their MWI for any message left for 1005. Finally Create a new DN of 1010. When this DN is called, all calls should be directed to the DN of 1005. The call should ring this DN for approximately 2 rings. If for any reason this DN does not answer, the call should then be forwarded to VM if the call originated from an internal number, however if the call originated from an external number, the call should then be forwarded to the PSTN phone at '221-1111'.

➔ **This should be self-explanatory from previous examples – See Task 29.40.**

Task 30.51

Create an Auto-Attendant application using CUE. The incoming DN will be 3313213000 or 3000 and the AA should give the option to dial-by-name by pressing 1, dial-by-extension at any time during the prompt, and be transferred into a B-ACD TCL Queue at DN 3500 by pressing 2 and be connected to the Support Hunt Group with Queueing and Statistics.

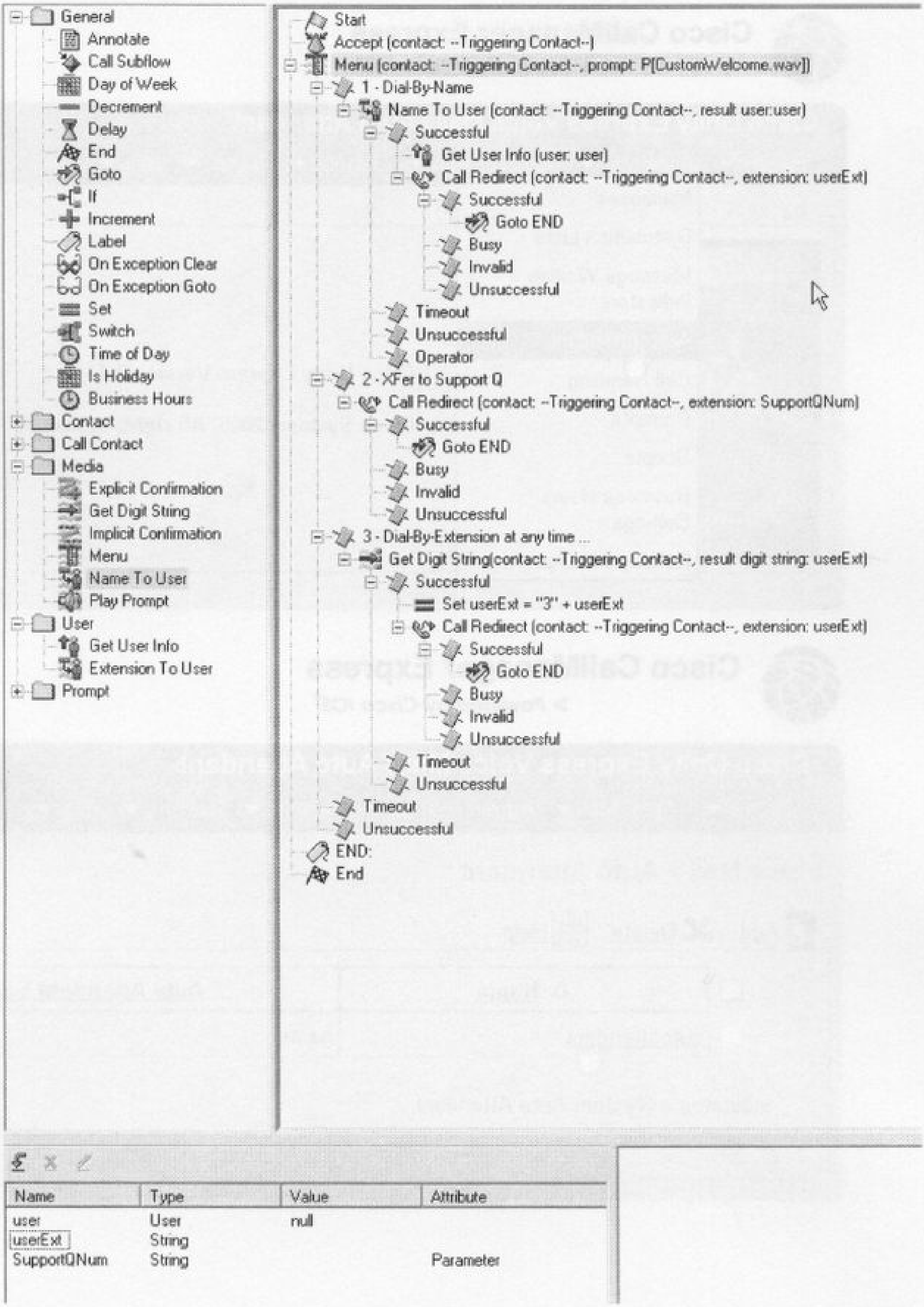
→ **On BR2**

```
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 supplementary-service h450.12 advertise-only
!
voice translation-rule 1
 rule 1 /^331321\(3...\)/ /\1/
!
voice translation-profile VM
 translate calling 1
 translate called 1
 translate redirect-called 1
!
interface Loopback0
 ip address 172.1.102.1 255.255.255.255
!
dial-peer voice 1 pots                       ← Call comes inbound CME from POTs on this Dial-Peer
 incoming called-number .
 direct-inward-dial
!
dial-peer voice 3601 voip
 translation-profile outgoing VM
 destination-pattern                         ← Call goes outbound to CUE on this Dial-Peer
3313213[126]00                               ← When script transfers call – call comes back inbound to
 incoming called-number .                      router from CUE on this Dial-Peer
 session protocol sipv2
 session target ipv4:10.1.202.2
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 3500 voip                    ← Call then routes outbound via this Dial-Peer to DN 3500
 destination-pattern 3500                    – only this dial-peer points to our own Loopback so .......
 session target ipv4:172.1.102.1
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
!
```

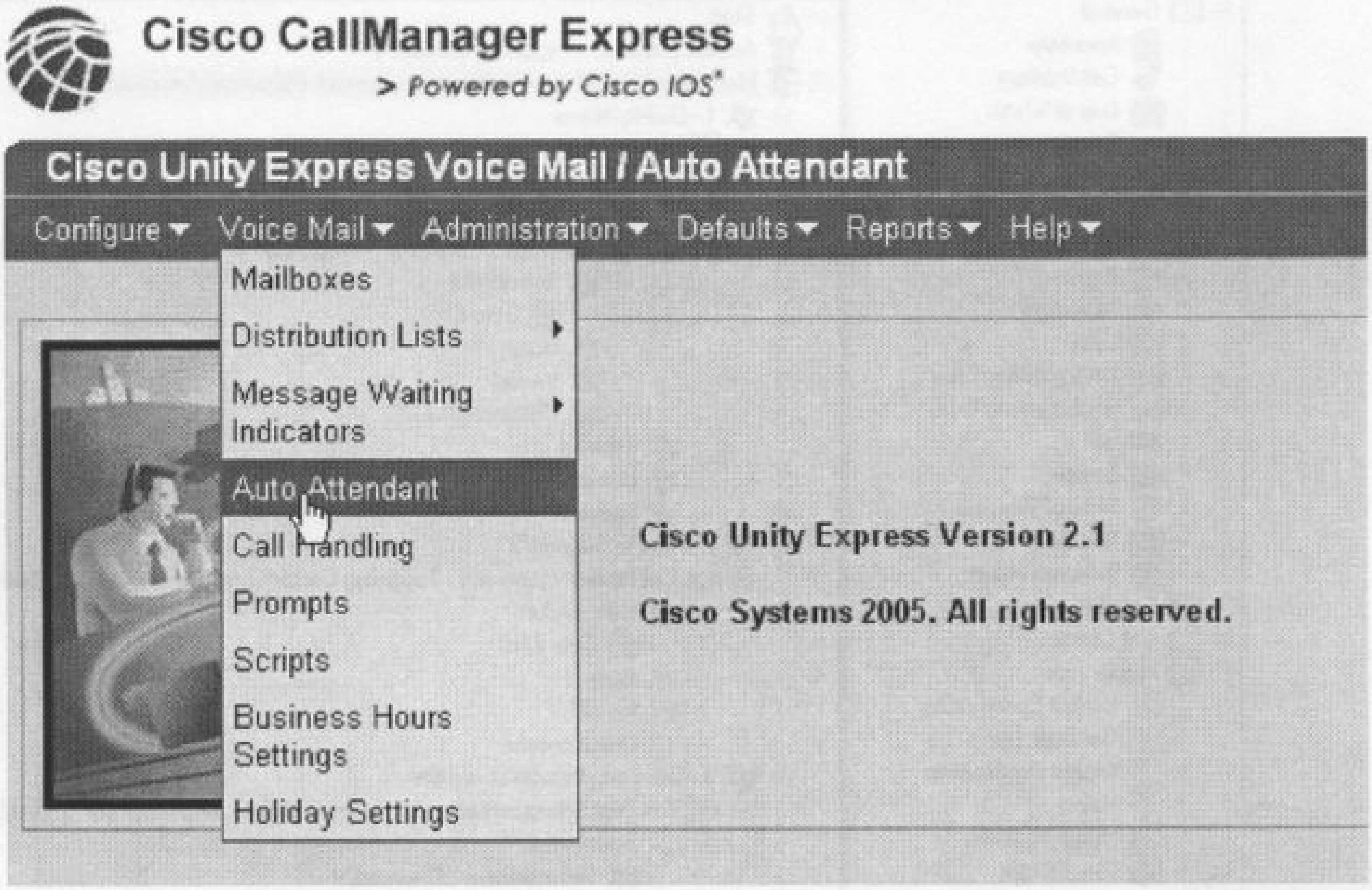
```
dial-peer voice 3501 voip
 service aa
 incoming called-number 3500
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
!
!
application
 service queue flash:app-b-acd-2.1.0.0.tcl
  param queue-len 20
  param queue-manager-debugs 1
  param aa-hunt2 3210
  param number-of-hunt-grps 1
 !
 service aa flash:app-b-acd-aa-2.1.0.0.tcl
  paramspace english index 1
  param number-of-hunt-grps 1
  param handoff-string aa
  param dial-by-extension-option 3
  param operator 3001
  paramspace english language en
  param max-time-vm-retry 2
  param aa-pilot 3500
  param max-extension-length 4
  paramspace english location flash:
  param second-greeting-time 30
  param welcome-prompt en_bacd_welcome.au
  param call-retry-timer 15
  paramspace english prefix en
  param max-time-call-retry 45
  param voice-mail 3215
  param service-name queue
 !
!
ephone-hunt 1 peer
 pilot 3210
 list 3001, 3003
 timeout 12
 statistics collect
```

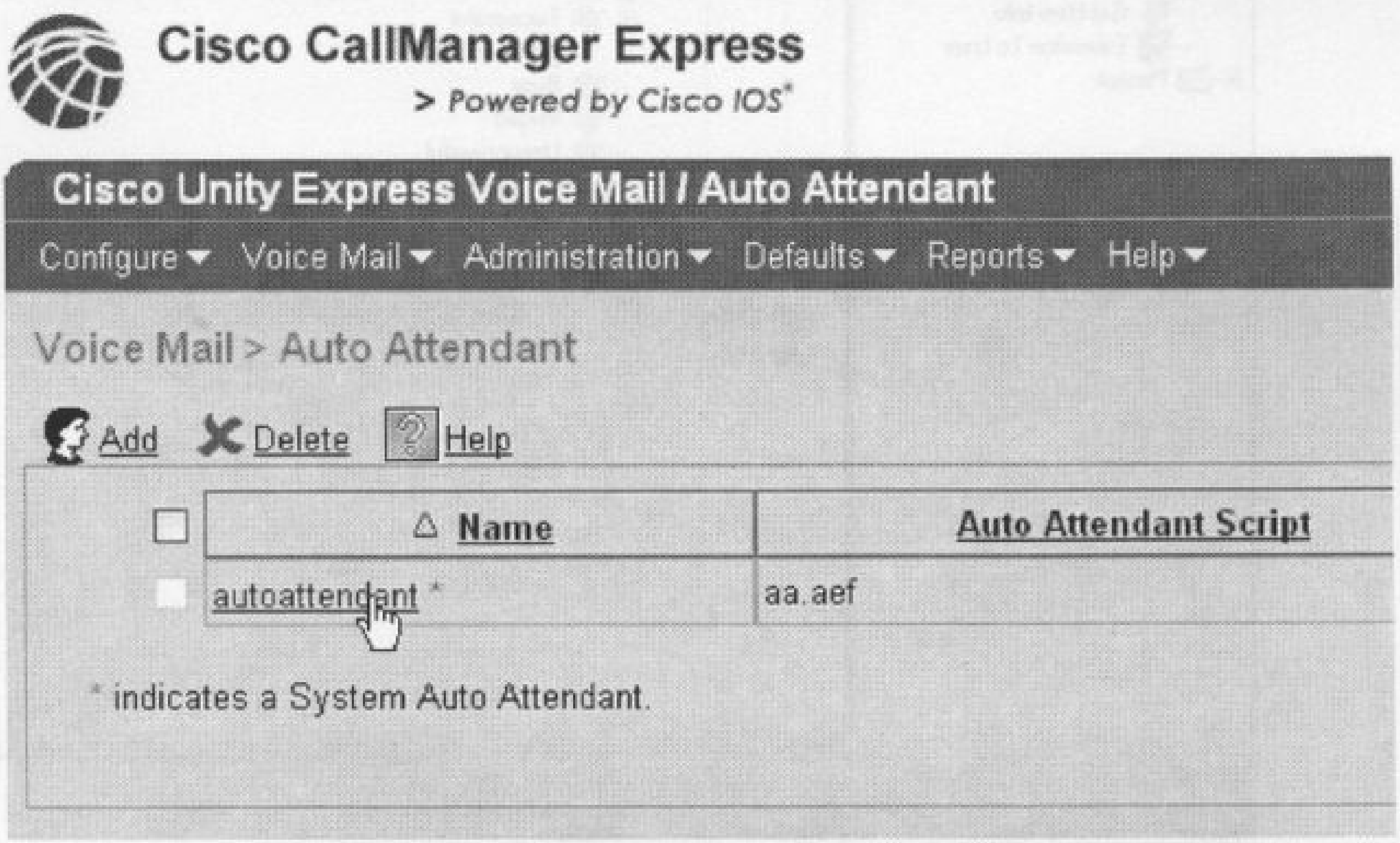
← Finally call comes back into router via its own loopback (even though it never really left the router) and is finally handed off to the AA service application

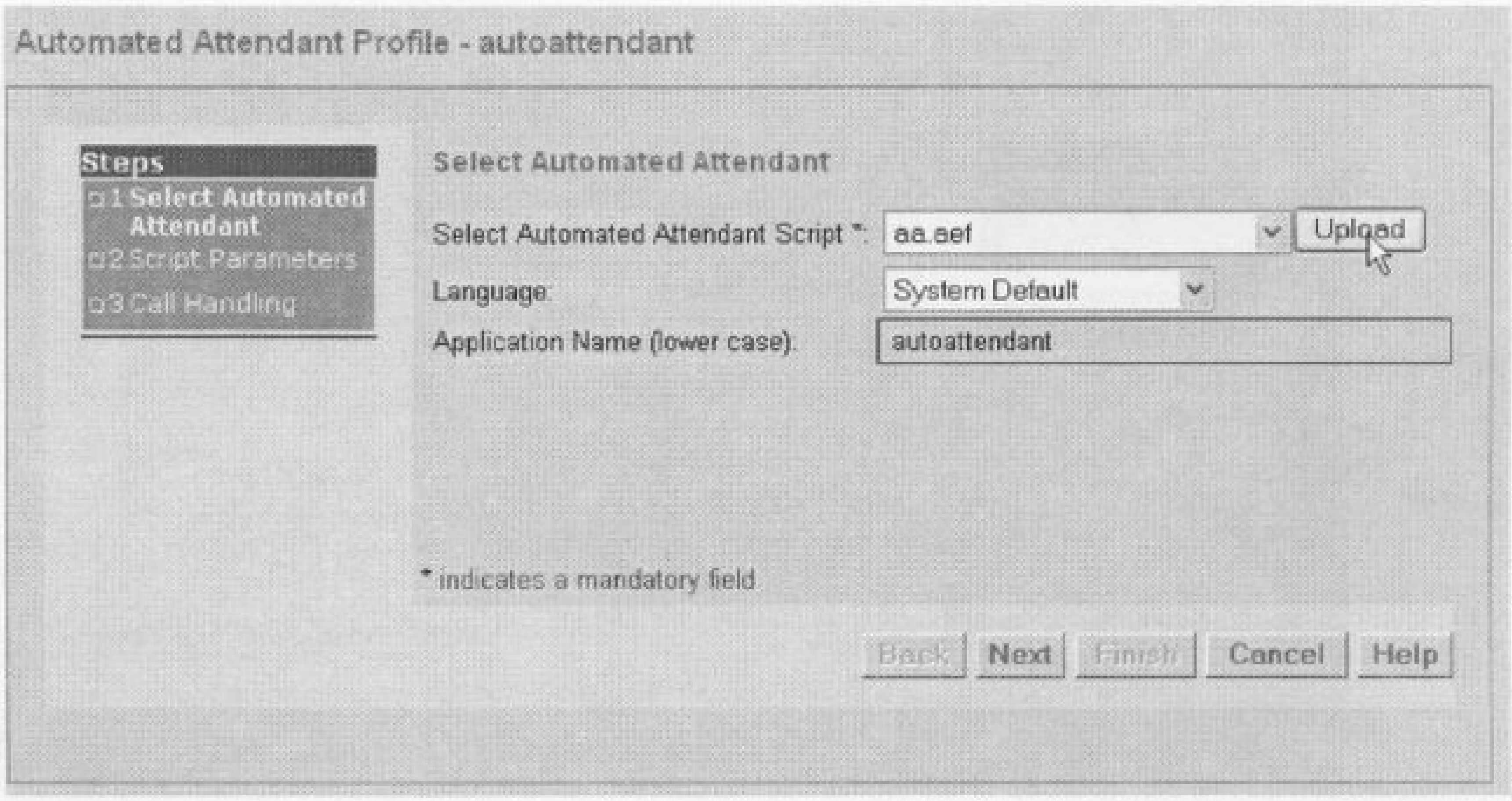
➔ **Using the CUE Editor:**

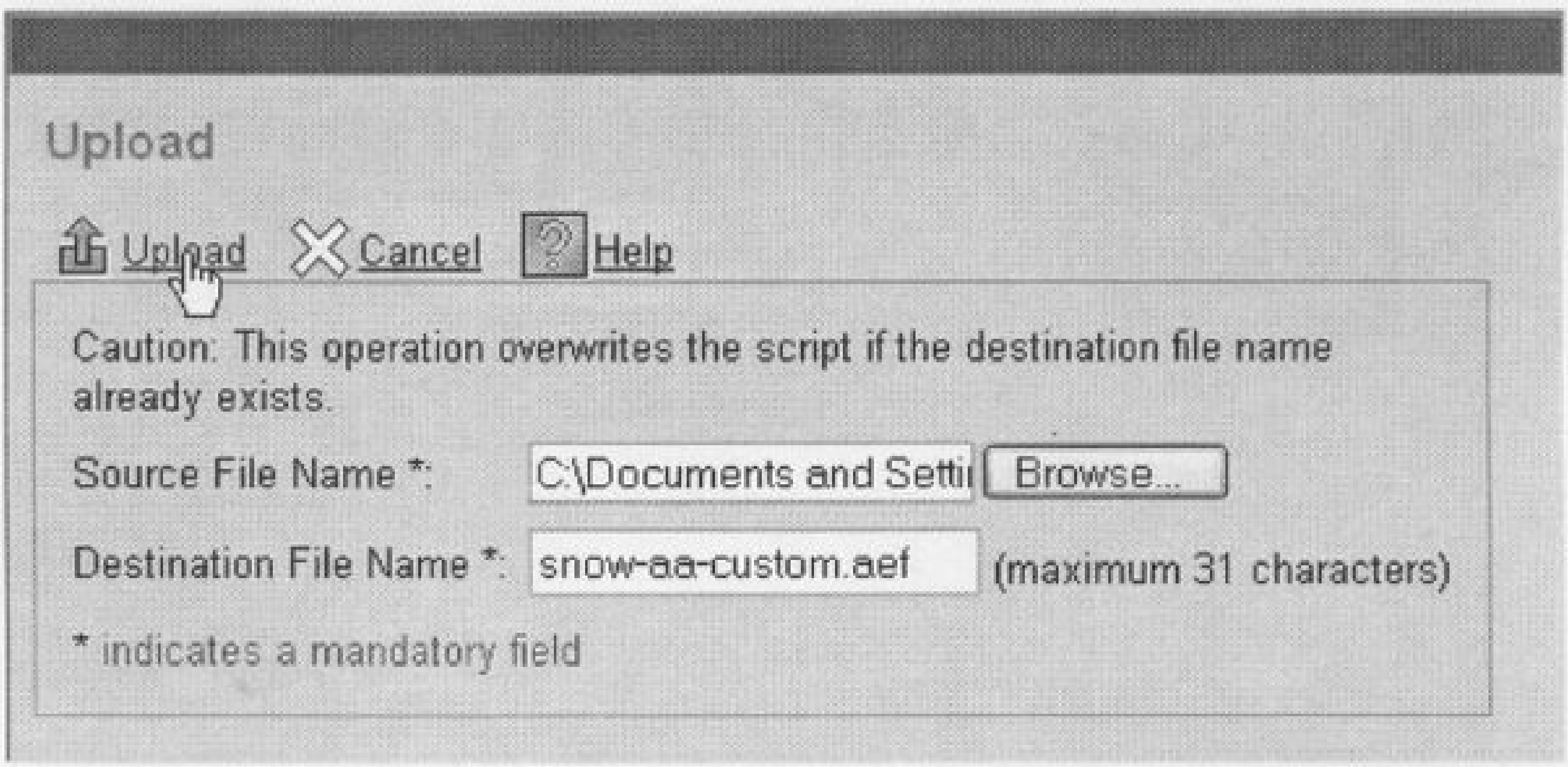


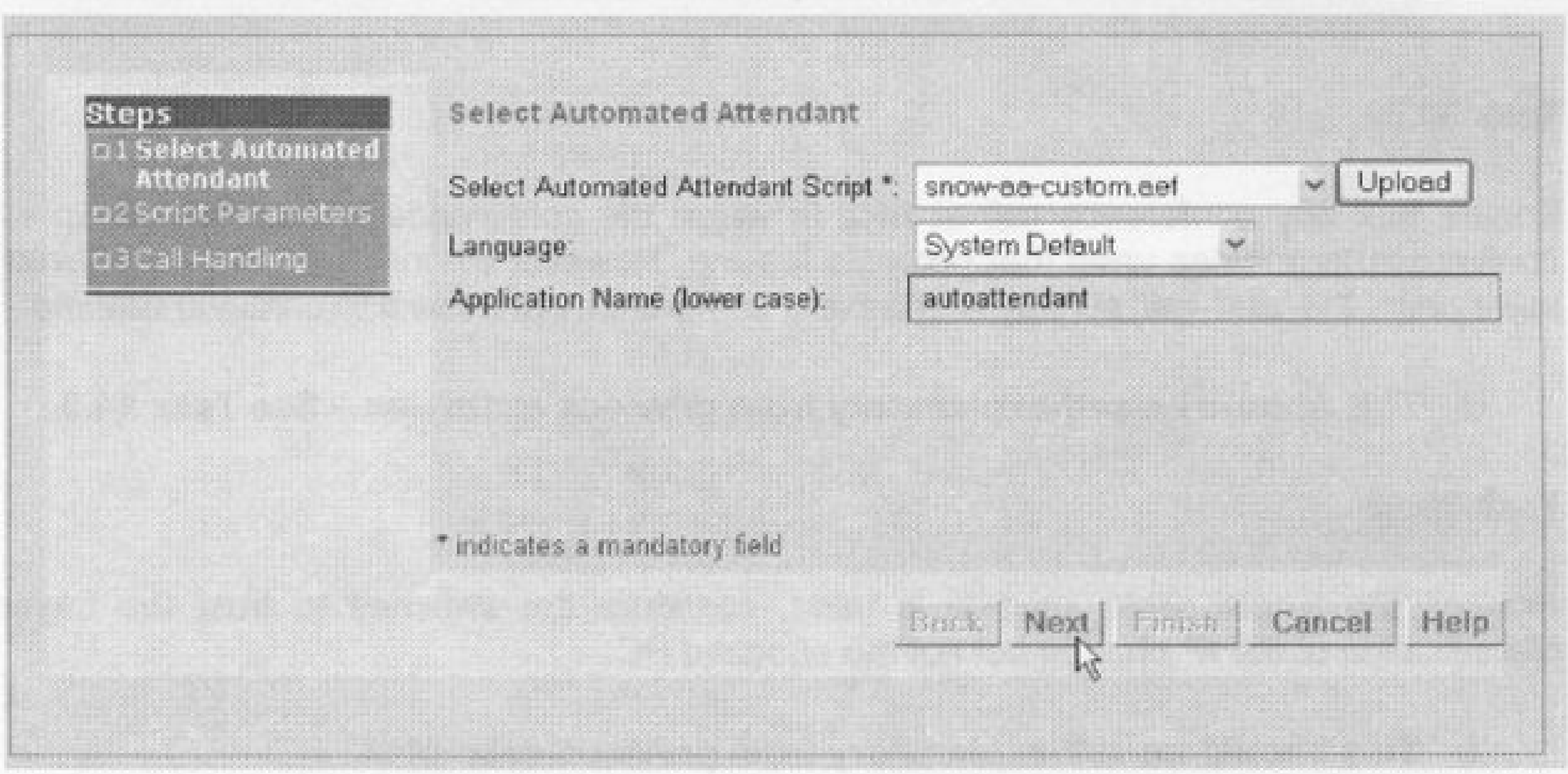
➔ **From Internet Explorer browse to http://10.1.202.2/Web.**

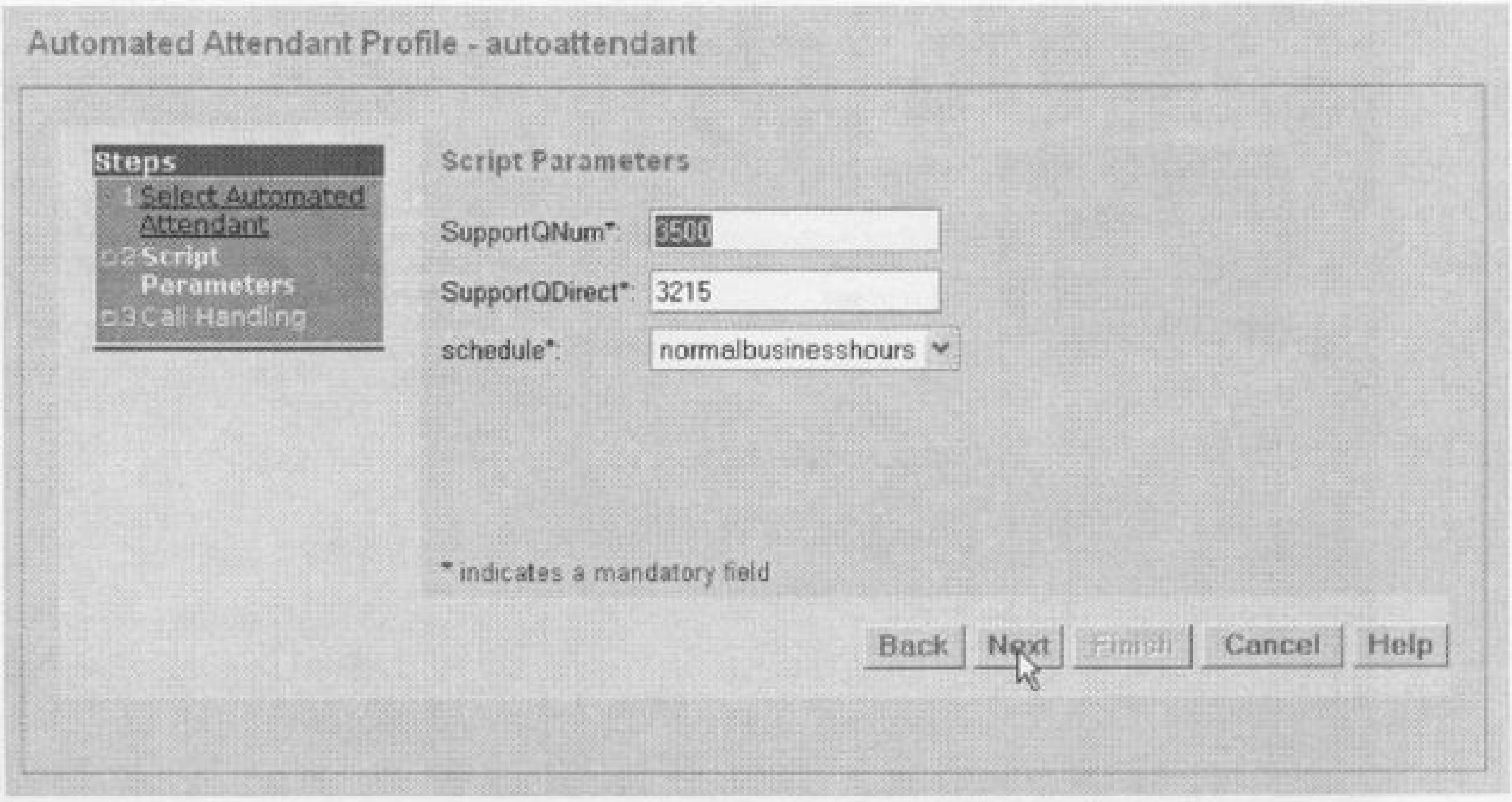


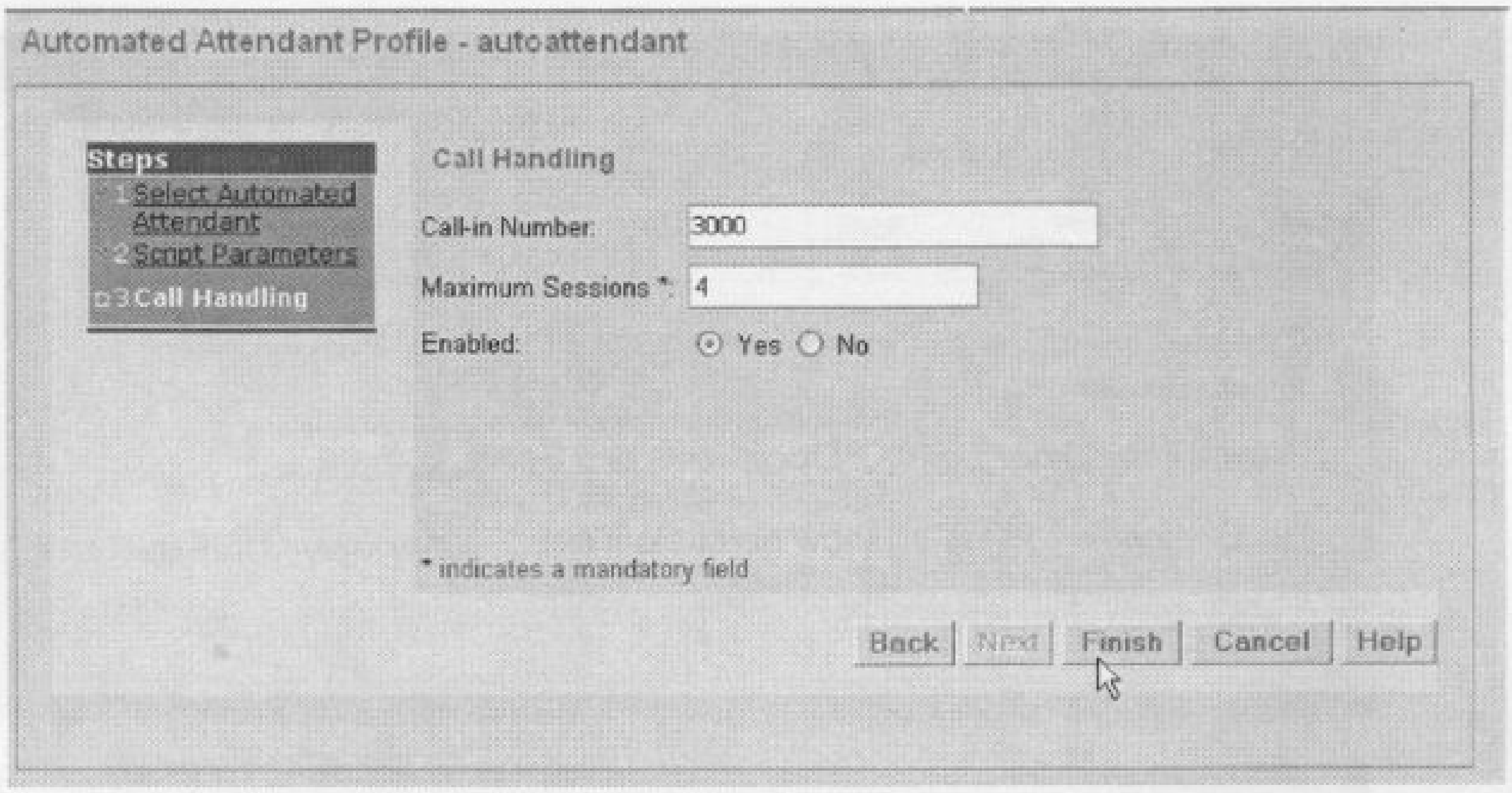



Automated Attendant Profile - autoattendant
Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Select Automated Attendant
Select Automated Attendant Script *: aa.aef
Upload
Language: System Default
Application Name (lower case): autoattendant
* indicates a mandatory field
Back
Next
Finish
Cancel
Help


Upload
Upload
Cancel
Help
Caution: This operation overwrites the script if the destination file name already exists.
Source File Name *: C:\Documents and Setti
Browse...
Destination File Name *: snow-aa-custom.aef
(maximum 31 characters)
* indicates a mandatory field


Steps
1 Select Automated Attendant
2 Script Parameters
3 Call Handling
Select Automated Attendant
Select Automated Attendant Script *: snow-aa-custom.aef
Upload
Language: System Default
Application Name (lower case): autoattendant
* indicates a mandatory field
Back
Next
Finish
Cancel
Help





Task 30.52

Ensure that any conference call at BR2 in which the conference initiator hangs up – that the conference terminates upon that person's leaving. However Phone 3 should be allowed to hang up or press the 'end-call' softkey and leave a conference but allow it to continue running.

➔ **This should be self-explanatory from previous examples – See Task 14.6.**

Task 30.53

Assume the single cable solution is used, configure the switches to trust the Layer 2 QoS classification of the IP phones but not the attached PC.

➔ **This should be self-explanatory from previous examples.**

Task 30.54

Assume that ATA does not mark voice RTP packets correctly to CoS of 5. Configure the switch port connected to ATA to correct this problem.

➔ **This should be self-explanatory from previous examples.**

Task 30.55

Assume that CUE does not mark any of its traffic with correct DSCP bits. Ensure that in the router, this traffic is marked correctly as soon as it comes from CUE and ensure that it follows the same standards of marking set from CCM regarding voice and call control.

➔ **This should be self-explanatory from previous examples – See Task 15.5.**

Task 30.56

Configure the Catalyst 6500 to move VOIP control traffic to the 2nd queue and 1st threshold.

➔ **This should be self-explanatory from previous examples.**

Task 30.57

Configure the Catalyst 6500 and 3550 to map the CoS to DSCP value.

➔ **This should be self-explanatory from previous examples.**

Task 30.58

Configure the HQ router to set the CoS of voice RTP to 5 and CoS of voice control traffic to 3 on traffic sent to Catalyst 6500 in voice VLAN.

➔ **This should be self-explanatory from previous examples.**

Task 30.59

Configure MLPPP between HQ Site and Branch 2.

➔ **This should be self-explanatory from previous examples – assume the PVC speed of BR2 is 768Kbps and BR1 is 1544Kbps.**

Task 30.60

From HQ Site to Branch 2, reserve 128 kbps for voice RTP traffic on a priority queue and reserve minimum guaranteed bandwidth of 8kbps for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queuing.

➔ **This should be self-explanatory from previous examples.**

Task 30.61

From Branch 2 to HQ Site, reserve 128 kbps for voice RTP traffic on a priority queue and reserve minimum guaranteed bandwidth of 8kbps for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queuing.

➔ **This should be self-explanatory from previous examples.**

Task 30.62

From the HQ site to the Branch 1 site, reserve 33% of bandwidth for voice RTP traffic on a high priority queue and 5 % of bandwidth for voice control traffic. The remainder of the traffic should be applied to weighted-fair-queuing.

➔ **This should be self-explanatory from previous examples – assume the PVC speed of BR2 is 768Kbps and BR1 is 1544Kbps.**

Task 30.63

Configure Fax Passthru throughout the network.

➔ **This should be self-explanatory from previous examples.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com

Section 31: Multiprotocol Challenge N

Estimated Time to Complete: 10 hours

NOTE:

Please reference your Voice Workbook for all diagrams and tables.

Section 31 Multiprotocol Challenge N

This lab is intended to use with the on-line rack access that is provided by Proctor Labs. Connect to the Terminal Server for the on-line rack and complete tasks that are detailed below. Any of the normal Telnet Applications will work but it might be useful to become familiar with SecureCRT as this is used in the real lab.

This lab has no pre-requisites and should be attempted after completing all of the previous labs.

Section 31 Configuration Tasks

Task 31.1

Ensure that the link between the HQ/BR1/BR2 routers and appropriate switches are configured as DOT1Q trunks. Give the voice sub-interface the appropriate ip address from Table 1. Check connectivity between all sites and to Call Manager/Unity.

➔ **This should be self-explanatory from previous examples.**

Task 31.2

Configure Voice and Data VLAN for all IP Phones including ATA and VG248. VLAN IDs are defined in Table 2. Use Table 3 for HQ site 6500 port assignment. For BR1 and BR2 port allocation you are required to find out port allocation by your own methods.

➔ **This should be self-explanatory from previous examples.**

Task 31.3

Set the clock on the BR2 router to the correct time.

➔ **This should be self-explanatory from previous examples.**

Task 31.4

For Headquarter and Branch 1, use Microsoft DHCP server to allocate IP address for all Devices. For Branch 2, use IOS DHCP to allocate IP address for the IP phones. For each voice subnet, allocate the IP address from .50 to .69.

➔ **This should be self-explanatory from previous examples.**

Task 31.5

Configure Call Manager to allow devices to register manually. Assign directory number to devices based on Tables 5 and 6.

➔ **This should be self-explanatory from previous examples.**

Task 31.6

Configure CallManager with bandwidth values such that Audio calls within the HQ and BR1 sites are allowed to use any of the following codecs: G711, G722, G729, or G728. Audio calls between the two sites must only be allowed to use G729 or G728 codecs. Configure CallManager with values such that Video calls within each site be allowed to use 1 call at the Maximum bandwidth supported by a Cisco VTA camera in wideband mode and between each site with values such that Video calls be allowed to use 1 call at the Minimum bandwidth supported by a Cisco VTA camera in H263 mode. Assign these newly created entities to a corresponding Device Pool.

➔ **This should be self-explanatory from previous examples – See Task 2.1.**

Task 31.7

Use CallManager's only CAC mechanism to limit the number of calls over the WAN between the HQ and BR1 to one audio call and one video call using the minimum bandwidth allowable by a VTA camera in H263 mode. Configure CallManager so that this CAC mechanism is set such that the trace files reflect the bandwidth changes.

➔ **This should be self-explanatory from previous examples – See Task 2.2.**

Task 31.8

Configure CallManager such that HQ Phones 1 and 2 and BR1 Phones 1 and 2, will encrypt their signaling and media streams using AES128 with any device that will allow such to occur. Configure CCM to install a 1028 bit LSC on each phone. Configure the phones so that when a LSC is to be installed on the phone – that **no** user interaction is required on the IP Phone.

➔ **This should be self-explanatory from previous examples – See Task 17.2.**

Task 31.9

Configure Calling Restriction.

➔ **This should be self-explanatory from previous examples.**

Task 31.10

Set the phones that reside in the POD (all 79XX not physically accessible to you) to auto-answer. Phones must only auto-answer after 5 seconds.

➔ **This should be self-explanatory from previous examples.**

Task 31.11

Register phones at BR2 based on Table 7.

➔ **This should be self-explanatory from previous examples.**

Task 31.12

BR2 should use the same class of restriction as the other sites.

➔ **This should be self-explanatory from previous examples.**

Task 31.13

Configure a Call Block rule for all CME phones. Block all 900 and 976 calls. Create a user "IPExpert" and allow that user to override the block using Toll Bar Override. Deactivate the users login after 25 minutes when the phone becomes idle.

```
telephony-service
 load 7910 P00403020214
 load 7960-7940 P00306000300
 max-ephones 10
 max-dn 15
 ip source-address 10.1.200.21 port 2000
 max-conferences 8
 after-hours block pattern 1 91900
 after-hours block pattern 2 91976
 after-hours day Sun 12:00 11:59
 after-hours day Mon 12:00 11:59
 after-hours day Tue 12:00 11:59
 after-hours day Wed 12:00 11:59
 after-hours day Thu 12:00 11:59
 after-hours day Fri 12:00 11:59
 after-hours day Sat 12:00 11:59
login timeout 25
!
ephone 1
 pin 12345
!
ephone 2
 pin 12345
```

Task 31.14

Change Phone 2 at BR2 so that the user may not utilize the CallBack feature.

➔ **This should be self-explanatory from previous examples – See Task 14.2.**

Task 31.15

Send all IP Phone requests at BR2 for IP XML Services to the CallManager main Services URL.

➔ **This should be self-explanatory from previous examples – See Task 14.8.**

Task 31.16

Configure the HQ 6608 T1 PRI gateway based on Table 8. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Calling Number (10 digits) and Calling Name should be displayed. For Site Numbering plan use Table 12, for 6608 Port Assignment use Table 13.

➔ **This should be self-explanatory from previous examples.**

Task 31.17

Configure BR1 as an MGCP gateway, based on information in **Table 8**. The Telco is selecting B channels using the 'ascending' algorithm. You must configure the T1 PRI to minimize the chances of glare. Only the top 3 B channels are 'lit'. Make sure both media and signaling packets are sourced from the Voice sub-interface. Calling Number (10 digits) and Calling Name should be displayed. Ensure that RTP traffic between the any capable IP Phone and the BR1 MGCP gateway is encrypted with AES128. Also ensure that all MGCP signaling between CallManager and BR1 gateway is encrypted with 3DES 168bit encryption using a SHA hashing algorithm.

➔ **This should be self-explanatory from previous examples – for security setup see task 17.4 – 5.**

Task 31.18

Configure BR2 as an H323 gateway based on the information in Table 8.

➔ **This should be self-explanatory from previous examples.**

Task 31.19

Configure gatekeeper on HQ-RTR with the following information:

Local zone= CCM-GK
domain name = ipexpert.com
[use loopback interface for local zone]
Register CallManager to this zone.

Local zone= BR2-GK
domain name = ipexpert.com
Register the BR2 CME to this zone.

Local zone= VGK
domain name = ipexpert.com
Register the IPIPGW to this zone

You may not use any tech prefix to accomplish this task.

➔ **On HQ-RTR:**

```
gatekeeper
 zone local VGK ipexpert.com 172.1.100.1
 zone local BR2-GK ipexpert.com invia VGK outvia VGK enable-intrazone
 zone local CCM-GK ipexpert.com
 zone prefix BR2-GK 3...
 no shutdown
```

➔ **On CCM – Create a GK Reference to 172.1.100.1.**

➔ **Create a H323 GK-controlled Trunk pointing to the GK Reference you just created and register it with zone 'CCM-GK'.**

➔ **On CCME:**

```
interface Loopback0
 ip address 172.1.102.1 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id BR2-GK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id CME
 h323-gateway voip bind srcaddr 172.1.102.1
```

Task 31.20

Configure CAC such that one G729 call is allowed through the gatekeeper to the remote zone.

```
gatekeeper
 bandwidth remote 128
```

Task 31.21

Enable security on the local gatekeeper such that only devices that need to register CAN register (e.g. Call Manager) – other rogue devices should be prevented from registering.

➔ **This should be self-explanatory from previous examples.**

Task 31.22

For both the HQ and BR1 sites ensure that calls to emergency services are routed to the appropriate local gateway only. All Local, Long Distance and International calls from the HQ site should be routed out of the local gateway with the BR1 gateway acting as backup. All Local, Long Distance and International calls from the BR1 site should be routed out of the BR1 gateway with the HQ gateway acting as backup.

➔ **This should be self-explanatory from previous examples.**

Task 31.23

Calls from the HQ site to BR1 PSTN numbers should be routed out of the BR1 gateway (toll bypass). The HQ gateway should act as the backup gateway. Calls from the BR1 site to HQ PSTN numbers should be routed out of the HQ gateway (toll bypass) with the BR1 gateway acting as backup.

➔ **This should be self-explanatory from previous examples.**

Task 31.24

Calls originating from both the HQ and BR1 sites destined for the BR2 site should be routed out of the HQ-RTR gatekeeper while terminating their RTP streams at the IPIPGW on the HQ-RTR, with the appropriate local gateway acting as backup. Users must be able to dial the BR2 site using access-code of 7 and the users' 4 digit extensions. Seeing as we are using a Gatekeeper for our primary route, calls use H323 signaling end-to-end. Calls will leave using codec G711ulaw but arrive at BR2 CME as G729.

➔ **The following Route Groups should be created:**

Route Group	Gateway	Order
RG-GK	GK-TRUNK	1
RG-IPIPGW-ICT	H323 (non-GK controlled) InterClusterTrunk	1
RG-HQ	HQ-6608	1
RG-BR1	IOS-MGCP	1

➔ **The following Route Lists should be created:**

Route List	Route Group	Digit Manipulation
RL-HQ	RG-HQ	PREDOT
RL-BR1	RG-BR1	PREDOT
RL-HQ-BR1	RG-HQ	PREDOT
	RG-BR1	PREDOT
RL-BR1-HQ	RG-BR1	PREDOT
	RG-HQ	PREDOT
RL-TOLLBY-2-HQ	RG-HQ	PREDOT
	RG-BR1	PREDOT + PREFIX 1212
RL-GK-HQ	RG-GK	PREDOT
	RG-HQ	PREDOT + PREFIX 01133132X
RL-GK-BR1	RG-GK	PREDOT
	RG-BR1	PREDOT + PREFIX 01133132X

➔ **The following Route Patterns should be created:**

Route Pattern	Partition	Route List
911 9.911	PT-HQ-911	RL-HQ
911 9.911	PT-BR1-911	RL-BR1
9.[2-9]xxxxxx	PT-HQ-LOC	RL-HQ
9.[2-9]xxxxxx	PT-BR1-LOC	RL-BR1-HQ
9.1[2-9]xx[2-9]xxxxxx	PT-HQ-LD	RL-HQ
9.1[2-9]xx[2-9]xxxxxx	PT-BR1-LD	RL-BR1
91212.xxxxxxx	PT-BR1-LD	RL-TOLLBY-2-HQ
9.011! 9.011!#	PT-HQ-INTERNATIONAL	RL-HQ
9.011! 9.011!#	PT-BR1-INTERNATIONAL	RL-HQ-BR1
7.3xxx	PT-HQ-911	RL-GK-HQ
7.3xxx	PT-BR1-911	RL-GK-BR1

➔ **On HQ-RTR:**

```
voice-card 2
 no dspfarm
 dsp services dspfarm
!
sccp local vlan210
sccp ccm 10.1.201.1 identifier 1
sccp ip precedence 3
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCODER
 keepalive retries 5
 switchover method immediate
 switchback interval 15
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g729r8
 maximum sessions 2
 associate application SCCP
 no shutdown
!
call-manager-fallback
 ip source-address 10.1.201.1 port 2000
 max-ephones 1
 max-dn 1
```

```
sdspfarm units 1
 sdspfarm transcode sessions 2
!
voice service voip
 allow-connections h323 to h323
!
interface Loopback0
 ip address 172.1.100.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id VGK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip bind srcaddr 172.1.100.1
!
!
!
!
dial-peer voice 10 voip
 destination-pattern [12]...
 codec g711ulaw
 session target ras
!
dial-peer voice 11 voip
 destination-pattern 3...
 session target ras
!
gateway
!
gatekeeper
 zone local VGK ipexpert.com 172.1.100.1
 zone local BR2-GK ipexpert.com invia VGK outvia VGK enable-intrazone
 zone local CCM-GK ipexpert.com
 zone prefix BR2-GK 3...
 no shutdown
```


➔ **On BR2 (register ephone-DNs with GK by simply omitting the 'no-reg' command):**

```
interface Loopback0
 ip address 172.1.102.1 255.255.255.0
 ip ospf network point-to-point
 h323-gateway voip interface
 h323-gateway voip id BR2-GK ipaddr 172.1.100.1 1719
 h323-gateway voip h323-id CME
 h323-gateway voip bind srcaddr 172.1.102.1
!
gateway
!
dial-peer voice 10 voip
 incoming called-number [12]...
```

➔ **Place the call and Verify on HQ-RTR:**

```
P1-HQ-RTR#debug gatek main 10
P1-HQ-RTR#
May 22 19:43:38.608: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.320: gk_process: got a TIMER event

May 22 19:43:39.320: gk_handle_timers

May 22 19:43:39.320: gk_handle_timers: managed timer expired 0x45AAE620

P1-HQ-RTR#
May 22 19:43:39.880: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.880: gk_rassrv_arq: arqp=0x45EEBE7C, crv=0x4, answerCall=0
May 22 19:43:39.880: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:39.880: gk_dns_query: No Name servers
May 22 19:43:39.880: rassrv_get_addrinfo: (3004) Tech-prefix match failed.
May 22 19:43:39.880: rassrv_get_addrinfo: (3004) Matched zone prefix 3 and remainder 004
May 22 19:43:39.880: gk_rassrv_get_ingress_network: returning default ingress network = 1
May 22 19:43:39.880: rassrv_arq_select_viazone: about to check the source side,
src_zonep=0x476A44B0
May 22 19:43:39.880: rassrv_arq_select_viazone: matched zone is CCM-GK, and
z_invianamelen=0
May 22 19:43:39.880: rassrv_arq_select_viazone: about to check the destination side,
dst_zonep=0x45E91474
May 22 19:43:39.880: rassrv_arq_select_viazone: matched zone is BR2-GK, and
z_outvianamelen=3
May 22 19:43:39.880: rassrv_arq_select_viazone     and z_outvianamep=VGK
May 22 1
P1-HQ-RTR#9:43:39.880: rassrv_arq_select_viazone: Received ARQ for a zone (BR2-GK)
that has an outviazone (VGK) specified.  Pick an IP-IP gateway in that viazone.
May 22 19:43:39.880: gk_gw_select_ipipgw: zonep: 0x4724ED54, tpp: 0x0, current_endpt: 1
May 22 19:43:39.880: gk_gw_select_ipipgw: Selecting any IPIPGW. qelemp.head=0x472C0BB0,
use_count=1, current_endpt=1
May 22 19:43:39.880: gk_gw_select_ipipgw: Gateway selection will start at the top of the linked
list. use_count=1, current_endpt=0
May 22 19:43:39.880: gk_gw_select_ipipgw: qelemp=0x472C0BB0, loop_count=0
```

May 22 19:43:39.880: gk_gw_select_ipipgw: Examining tgwp 0x472B0E60, g_supp_prots: 0x50 qelemp: 0x472C0BB0, loop_count: 1
May 22 19:43:39.880: gk_gw_select_ipipgw: Found an IPIPGW. tgwp: 0x472B0E60, endptsigIP: 172.1.100.1, endptrasIP: 172.1.100.1, zone: VGK
May 22 19:43:39.884: gk_gw_select_ipipgw: Selected an IPIPGW.
May 22 19:43:39.884: rassrv_get_addrinfo: (3004) successfully resolved IPIPGW and returning with return code 0
May 22 19:43:39.904: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.904: gk_rassrv_arq: arqp=0x45EAD3AC, crv=0x33, answerCall=1
May 22 19:43:39.904: gk_rassrv_dep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:39.920: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.920: gk_rassrv_arq: arqp=0x45E9B960, crv=0x34, answerCall=0
May 22 19:43:39.920: gk_rassrv_sep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:39.920: gk_dns_query: No Name servers
May 22 19:43:39.920: rassrv_get_addrinfo: (3004) Tech-prefix match failed.
May 22 19:43:39.920: rassrv_get_addrinfo: (3004) Matched zone prefix 3 and remainder 004
May 22 19:43:39.920: gk_rassrv_get_ingress_network: ARQ non-std ingress network = 2
May 22 19:43:39.920: rassrv_arq_select_viazone: about to check the destination side, dst_zonep=0x45E91474
May 22 19:43:39.924: rassrv_arq_select_viazone: matched zone is BR2-GK, and z_outvianamelen=3
May 22 19:43:39.924: rassrv_arq_select_viazone and z_outvianamep=VGK
May 22 19:43:39.924: rassrv_arq_select_viazone: Received ARQ for a zone (BR2-GK) that has an outviazone (VGK) specified, but I am that viazone. Continue normal ARQ processing
May 22 19:43:39.924: gk_zone_get_proxy_usage: local zone= BR2-GK, remote zone= VGK, call direction= 0, eptype= 2050 be_entry= 0
May 22 19:43:39.924: gk_zone_get_proxy_usage: returns proxied = 0
May 22 19:43:39.924: gk_gw_select_px: Source and destination endpoints in different local zones
May 22 19:43:39.924: gk_zone_get_proxy_usage: local zone= VGK, remote zone= BR2-GK, call direction= 1, eptype= 2114 be_entry= 0
May 22 19:43:39.924: gk_zone_get_proxy_usage: returns proxied = 0
May 22 19:43:39.924: rassrv_get_addrinfo: (3004) successfully resolved the alias locally and returning with 0x0
May 22 19:43:39.924: rassrv_get_addrinfo: We know this alias

May 22 19:43:39.952: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:39.952: gk_rassrv_arq: arqp=0x45E9B960, crv=0x3A, answerCall=1
May 22 19:43:39.952: gk_rassrv_dep_arq: ARQ Didn't use GK_AAA_PROC
May 22 19:43:41.264: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:41.268: gk_rassrv_irr: irrp=0x45E9B960, from 172.1.102.1:58652
May 22 19:43:41.404: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:41.404: gk_rassrv_irr: irrp=0x45EA1C30, from 172.1.100.1:53849
May 22 19:43:41.412: gk_process: QUEUE_EVENT (minor 0) wakeup
May 22 19:43:41.412: gk_rassrv_irr: irrp=0x45EA1C30, from 172.1.100.1:53849

```
P1-HQ-RTR#sh voip rtp connections
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP       RemoteIP
1   72      73         18336    24618  172.1.100.1   10.1.200.21
2   73      72         19556    17460  172.1.100.1   172.1.102.1
3   74      75         17516    2000   10.1.200.3    10.1.200.3
4   76      75         18502    2000   10.1.200.3    10.1.200.3
Found 4 active RTP connections
```



```
P1-HQ-RTR#sh sdspfarm sessions sum

 max-mtps:1, max-streams:4, alloc-streams:4, act-streams:2
  ID  MTP  State     CallID confID Usage              Codec/Duration
 ==== ===== ====== ======= ====== ================== ==============
 ===========
 1   1    IDLE  -1       0                      G711Ulaw64k /20ms
 2   1    IDLE  -1       0                      G711Ulaw64k /20ms
 3   1    START  73      3     Ip-Ip             G729 /20ms
 4   1    START  72      3     Ip-Ip             G711Ulaw64k /20ms
```

Task 31.25

In the Branch 2 site, use an access-code of 7 and the users' 4 digit extensions to call other sites (HQ and BR1). Primary route must be via an IPIPGW on the BR1 router inbound as a SIP call, outbound to CCM as H323. If the IPIPGW were to fail for some reason, try a direct call to both CallManagers using H323. Finally if this method were to fail then you must send the calls out the local PSTN trunk. Accomplish this with the **minimum** number of dial-peers. Use the local gateway for all other PSTN calls

➔ **On BR1 Router**

```
voice service voip
 allow-connections sip to h323
!
voice-card 2
 no dspfarm
 dsp services dspfarm
!
sccp local vlan210
sccp ccm 10.1.201.1 identifier 1
sccp ip precedence 3
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCODER
 keepalive retries 5
 switchover method immediate
 switchback interval 15
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g729r8
 maximum sessions 2
 associate application SCCP
 no shutdown
!
call-manager-fallback
```

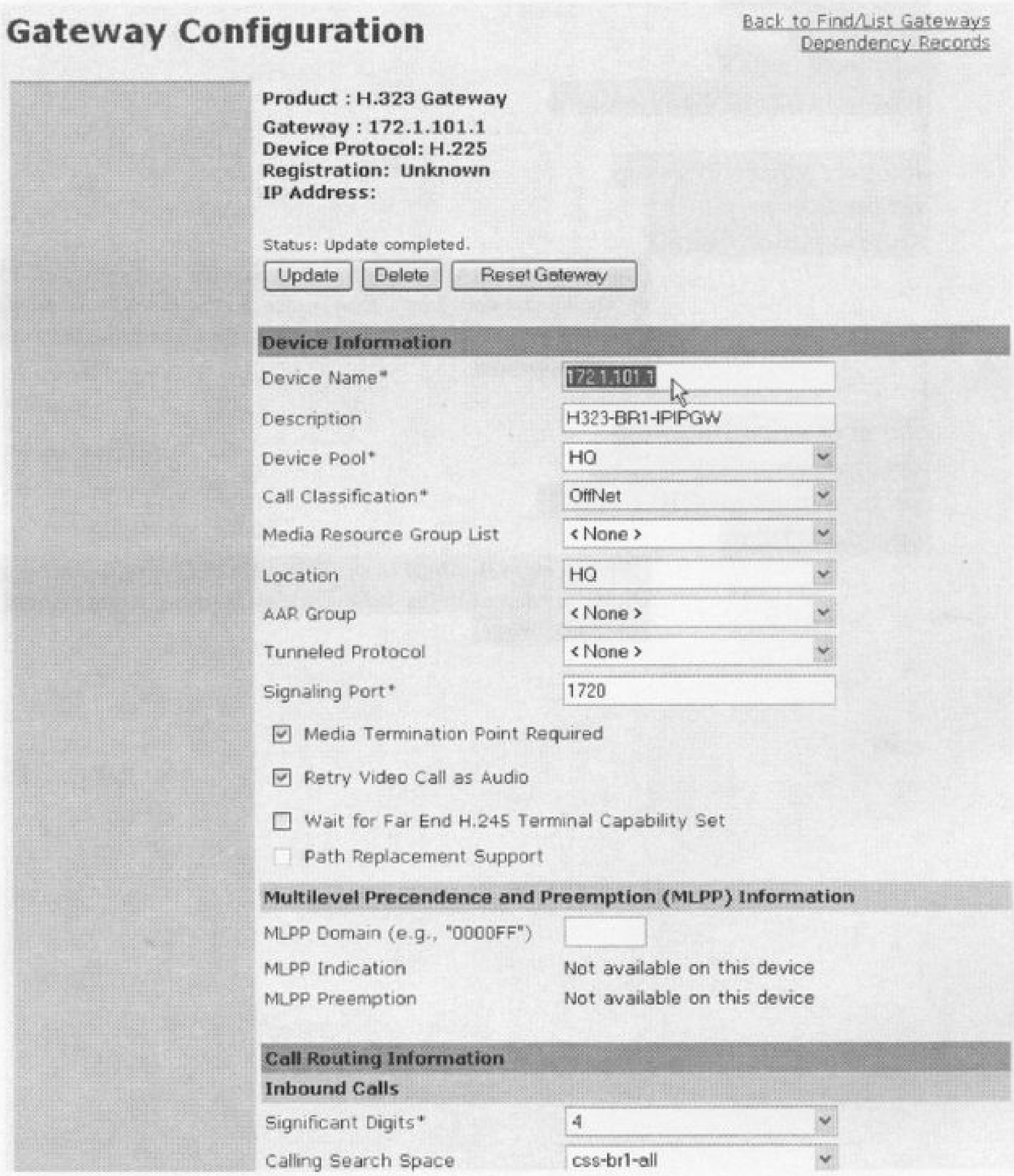
```
ip source-address 10.1.201.1 port 2000
max-ephones 10
max-dn 10
sdspfarm units 1
sdspfarm transcode sessions 2
!
dial-peer voice 1001 voip
 destination-pattern 3...
 session protocol sipv2
```

(Remember that while destination-pattern cmd matches DNIS on an Outbound Call Leg – that it also matches ANI on an Inbound Call Leg – so on an IPIPGW config – we can minimize our dial-peers with such)

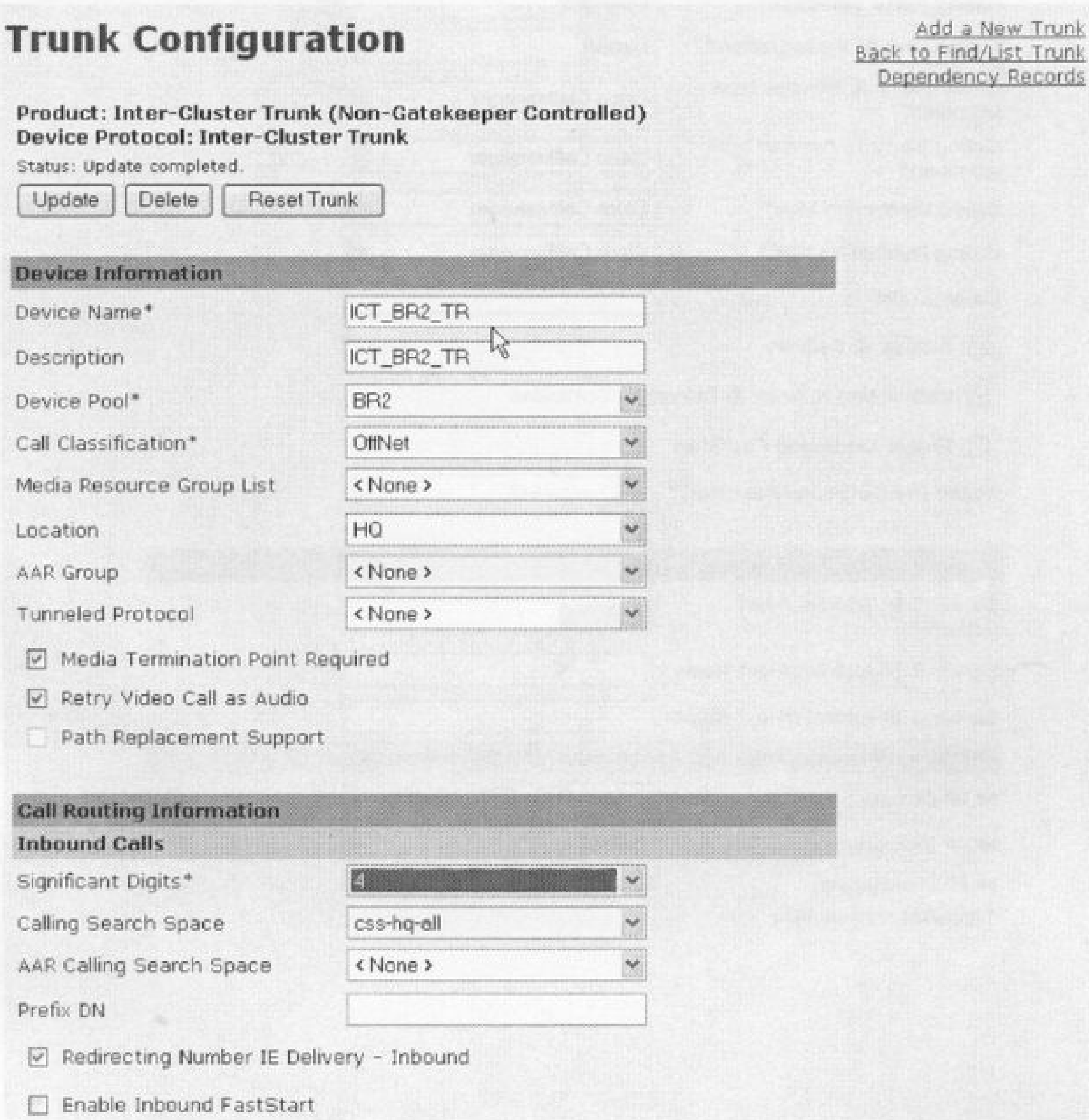
```
!
dial-peer voice 1002 voip
 destination-pattern 7[12]...
 session target ipv4:10.1.200.21
 codec g711ulaw
```

(We will strip the 7 off in the CCM H323 GW with the Significant Digits command in the Inbound Call Routing Rules section of the H323 GW Page)

➔ **Add the BR1 IPIPGW as a H323 GW in CCM for the first inbound route.**



➔ **Add CME as a H323-nonGKcontrolled-ICT in CCM as the second inbound route.**



Trunk Configuration

Add a New Trunk
Back to Find/List Trunk
Dependency Records

Product: Inter-Cluster Trunk (Non-Gatekeeper Controlled)
Device Protocol: Inter-Cluster Trunk

Status: Update completed.

Update | Delete | Reset Trunk

Device Information

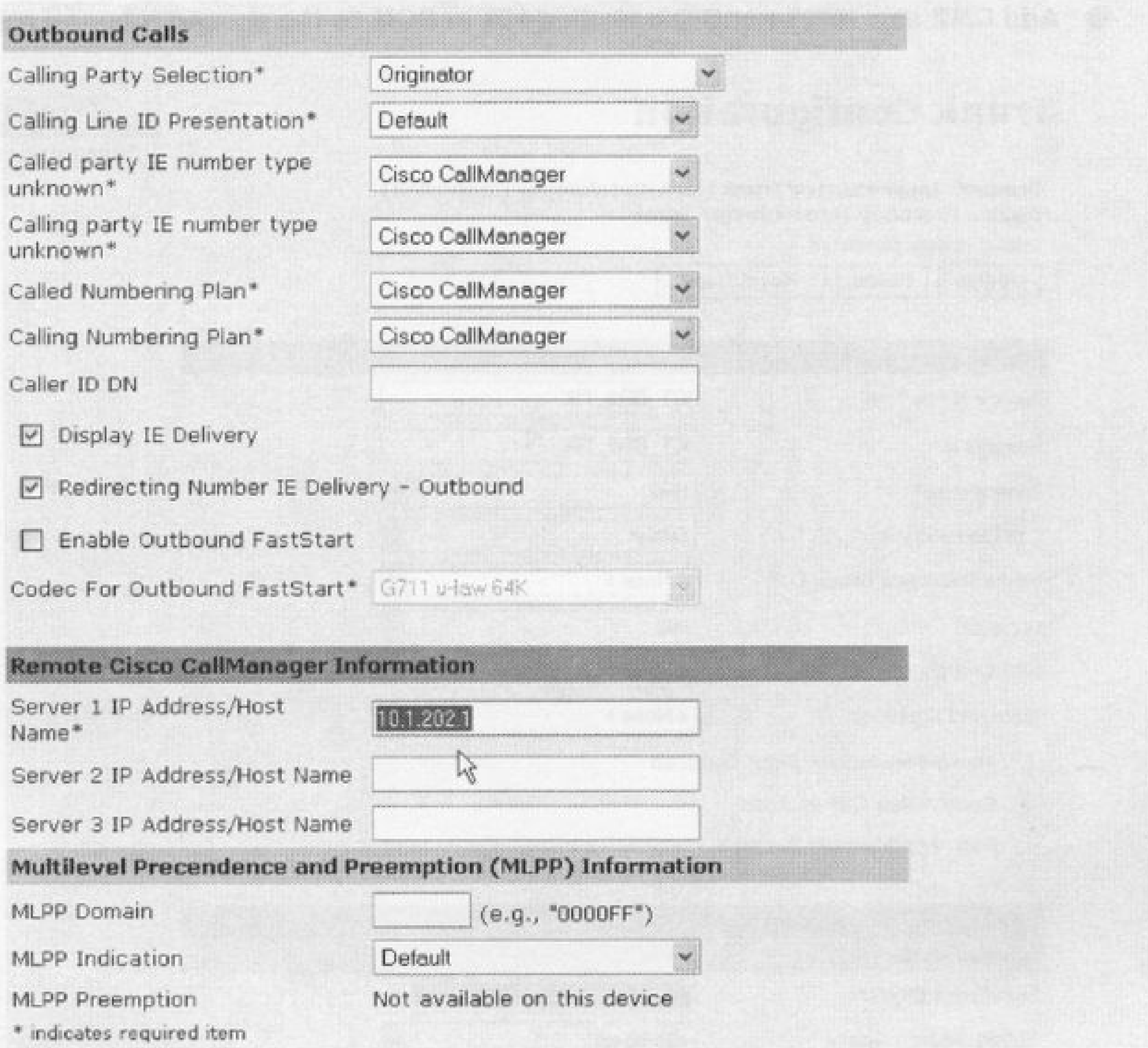
Device Name*	ICT_BR2_TR
Description	ICT_BR2_TR
Device Pool*	BR2
Call Classification*	OffNet
Media Resource Group List	< None >
Location	HQ
AAR Group	< None >
Tunneled Protocol	< None >

☑ Media Termination Point Required
☑ Retry Video Call as Audio
☐ Path Replacement Support

Call Routing Information
Inbound Calls

Significant Digits*	4
Calling Search Space	css-hq-all
AAR Calling Search Space	< None >
Prefix DN	

☑ Redirecting Number IE Delivery - Inbound
☐ Enable Inbound FastStart



Outbound Calls

Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Caller ID DN	

☑ Display IE Delivery

☑ Redirecting Number IE Delivery - Outbound

☐ Enable Outbound FastStart

Codec For Outbound FastStart*	G711 u-law 64K

Remote Cisco CallManager Information

Server 1 IP Address/Host Name*	10.1.202.1
Server 2 IP Address/Host Name	
Server 3 IP Address/Host Name	

Multilevel Precendence and Preemption (MLPP) Information

MLPP Domain	(e.g., "0000FF")
MLPP Indication	Default
MLPP Preemption	Not available on this device

* indicates required item

➔ **On BR2 Router – Add the following dial-peers:**

```
dial-peer voice 1000 voip
 destination-pattern 7[12]...
 session target ipv4:172.1.101.1
 session protocol sipv2
 no huntstop
!
dial-peer voice 1001 voip
 destination-pattern 7[12]...
 session target ipv4:10.1.200.21
 dtmf-relay h245-alphanumeric
 preference 1
 no huntstop
!
dial-peer voice 1001 voip
 destination-pattern 7[12]...
 session target ipv4:10.1.200.20
 dtmf-relay h245-alphanumeric
 preference 2
 no huntstop
!
translation-rule 1
 Rule 1 71... 12122211
 Rule 2 72... 16175212
!
dial-peer voice 1002 pots
 destination-pattern 7[12]...
 preference 3
 port 0/0/0:0
 translate-outgoing called 1
```

Task 31.26

All PSTN calls originating from BR2 should be sent out of the local PSTN gateway.

➔ **This has been covered in Task 31.19.**

Task 31.27

Enable DID for PSTN users dialing into the CM/CME (i.e. 2-stage dialing must not be used). **NOTE**: For all sites the Telco is sending 10 digits.

➔ **This should be self-explanatory from previous examples.**

Task 31.28

Configure your assigned 6608 port as a conference bridge. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 31.29

Configure your assign 6608 port as a transcoder. Use Table 13 for 6608 port assignment.

➔ **This should be self-explanatory from previous examples.**

Task 31.30

Configure conference bridge on BR1 router. Use a maximum of 1 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 31.31

Configure transcoder on BR1 router. Use a maximum of 2 sessions.

➔ **This should be self-explanatory from previous examples.**

Task 31.32

HQ should use 6608 resources and BR1 IOS resources as backup. BR1 should use the IOS resources first and then 6608 resources.

➔ **This should be self-explanatory from previous examples.**

Task 31.33

Configure a Music on Hold server on the Publisher Call Manager. Add another music source which can be found on the C: drive of your Call Manager. Ensure that the default (Sample) audio source is used when a User presses the 'Hold' button on his/her phone. For all other events that require music to be played use the newly added music source. You may not configure music sources on line, device or device pool to accomplish this task.

➔ **This should be self-explanatory from previous examples.**

Task 31.34

All sites must receive music using the G711 codec.

➔ **This should be self-explanatory from previous examples.**

Task 31.35

Ensure that the HQ and BR1 phones receive multicast music on hold.

➔ **This should be self-explanatory from previous examples.**

Task 31.36

Configure music on hold on the BR2 CME.

➔ **This should be self-explanatory from previous examples.**

Task 31.37

Create a meet-me conference with DN=1900. Nobody should be able to dial this number directly other than HQ Phone 1. The maximum number of participants of a single Meet-me conference should be 6 conferencees.

➔ **This should be self-explanatory from previous examples – see Task 7.10.**

Task 31.38

Configure AAR such that calls between HQ and BR1 will be rerouted over the PSTN when there is not enough bandwidth over the WAN. You must preserve 10 digit Calling Number display.

➔ **This should be self-explanatory from previous examples – you can use External Number Mask if you want, otherwise put full E164 number prefix in AAR Group and Prefix Calling Party DN in the Route Patterns.**

Task 31.39

Configure SRST at BR1 so that in the event of a WAN failure users can still make/receive calls from the PSTN. Use the voice sub-interface as the source address.

➔ **This should be self-explanatory from previous examples.**

Task 31.40

Configure the SCCP heartbeat timer to 20 seconds and ensure the clock displayed on the phone is using the 12 hour display. Also ensure that the inter-digit timeout is 7 seconds.

➔ **This should be self-explanatory from previous examples.**

Task 31.41

Configure SRST such that one 3-party conference is allowed.

➔ **This should be self-explanatory from previous examples.**

Task 31.42

Configure Music on Hold for all phones in SRST fallback.

➔ **This should be self-explanatory from previous examples.**

Task 31.43

Configure SRST such that the phones will only re-register back to Call Manager after normal service has been resumed for 2 minutes. (normal service is defined as the WAN is operational and Call Manager is running).

➔ **This should be self-explanatory from previous examples – see Task 8.6.**

Task 31.44

Ensure that if BR1 gateway goes into fallback mode, that it has already created its own certificate, forwarded that certificate to CallManager and that CallManager in turn has installed that certificate into the IP Phones at BR1, so that signaling and media continue to be encrypted during any fallback occurrence.

➔ **This should be self-explanatory from previous examples – see Task 17.3.**

Task 31.45

Ensure that the same Class of restriction is preserved when phones are in SRST fallback.

➔ **This should be self-explanatory from previous examples.**

Task 31.46

Integrate Call Manager with Unity with the following information:

- Voice Mail Pilot = 1600
- Voice Mail Ports = 1601-1604
- MWI On/Off = 1999/1998

➔ **This should be self-explanatory from previous examples.**

Task 31.47

Configure the BR2 router to support the CUE module using information from Table 16. Setup the basic information needed to work the CUE module including what is needed to access the web-based GUI to manipulate user's extensions and mailboxes:

- Voice Mail Pilot = 3600
- MWI On/Off = 3999/3998
- AA DN = 3100
- TUI = 3200

➔ **This should be self-explanatory from previous examples – see Task 15.1.**

Task 31.48

Configure Unity so that if a IP Phone caller conferences in Ext 1650, that Unity will record the conversation and forward that recording to the mailbox of the IP Phone that initiated the conference.

➔ **This should be self-explanatory from previous examples – see Task 9.8.**

Task 31.49

A call from another site supporting only G729 may ring into a BR2 site CME ph**one, and that phone may be busy and have set to forward busy calls into CUE VM. If this is the** case, ensure that G729 call into CUE will not fail.

➔ **This should be self-explanatory from previous examples – see Task 3.8.**

Task 31.50

Add subscriber accounts for phone 3 at each location using descriptive names. Ensure MWI is working.

➔ **This should be self-explanatory from previous examples.**

Task 31.51

Network CUE with Unity. Allow messages to be seamlessly forwarded back and forth.

➔ **This should be self-explanatory from previous examples – see Task 16.5.**

Task 31.52

Configure Unity VM Ports to use AES128 encryption for media traversal between themselves and IP Phones or Gateways that support such.

➔ **This should be self-explanatory from previous examples – see Task 17.6.**

Task 31.53

When the BR1 site is in SRST voicemail must work in exactly the same way as when the phones are in normal service (apart from MWI). The subscriber greeting must be heard for BR1 phone 1 on Call Forward No Answer (CFNA) and Call Forward Busy when the caller is both internal or external. The CFNA timer must be the same length as when the phones are registered to Call Manager.

➔ **On CME:**

```
call-manager-fallback
 max-ephones 24
 max-dn 48
 max-conferences 1
 timeouts interdigit 7
 ip source-address 10.2.201.1 port 2000
```



```
dialplan-pattern 1 6175222 extension-length 4
voicemail 1600
call-forward busy 1600
call-forward noan 1600 timeout 8

dial-peer voice 1001 pots
 destination-pattern 1...
 port 2/0/0:23
!
num-exp 1... 12122221...
```

➔ **On Unity:**

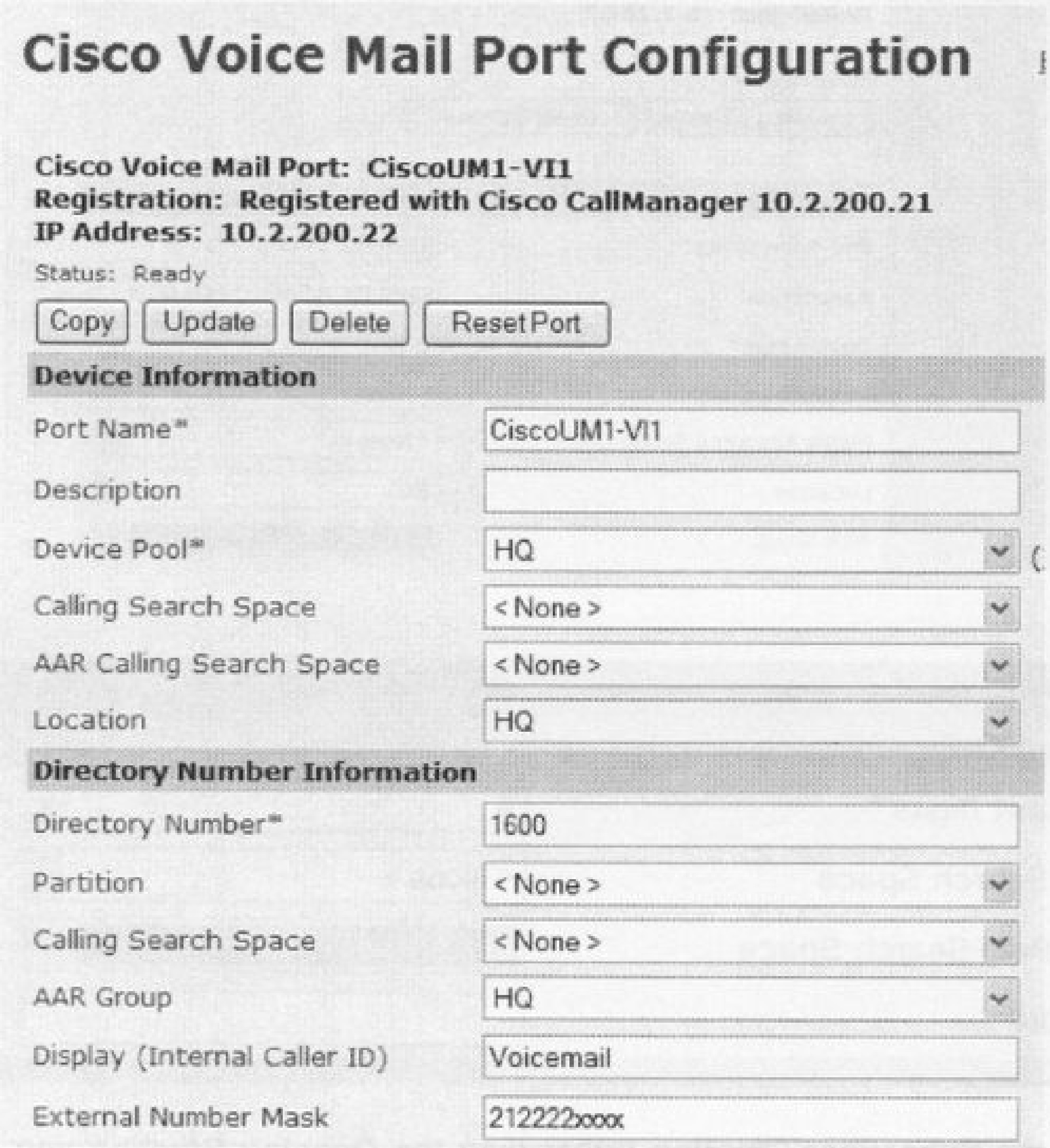
➔ **Create Alternate Extension 617522200X for each subscriber to hear opening greeting.**

➔ **The dialplan-pattern command, as well as stripping the called number for inbound calls FROM the PSTN, will work the reverse on Calling Number for outbound calls TO the PSTN. So the ANI for all outbound calls will be 10 digit.**

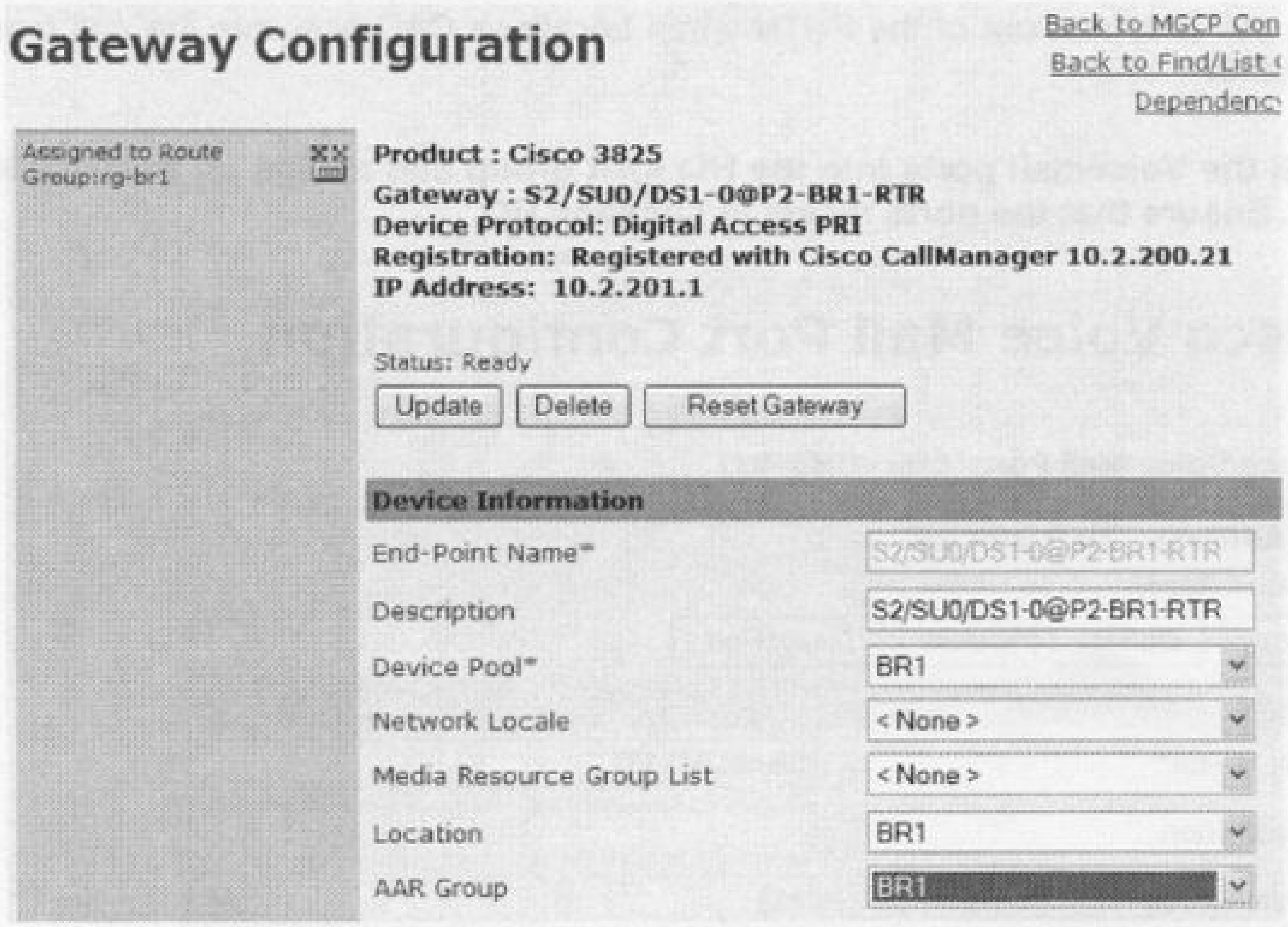
Task 31.54

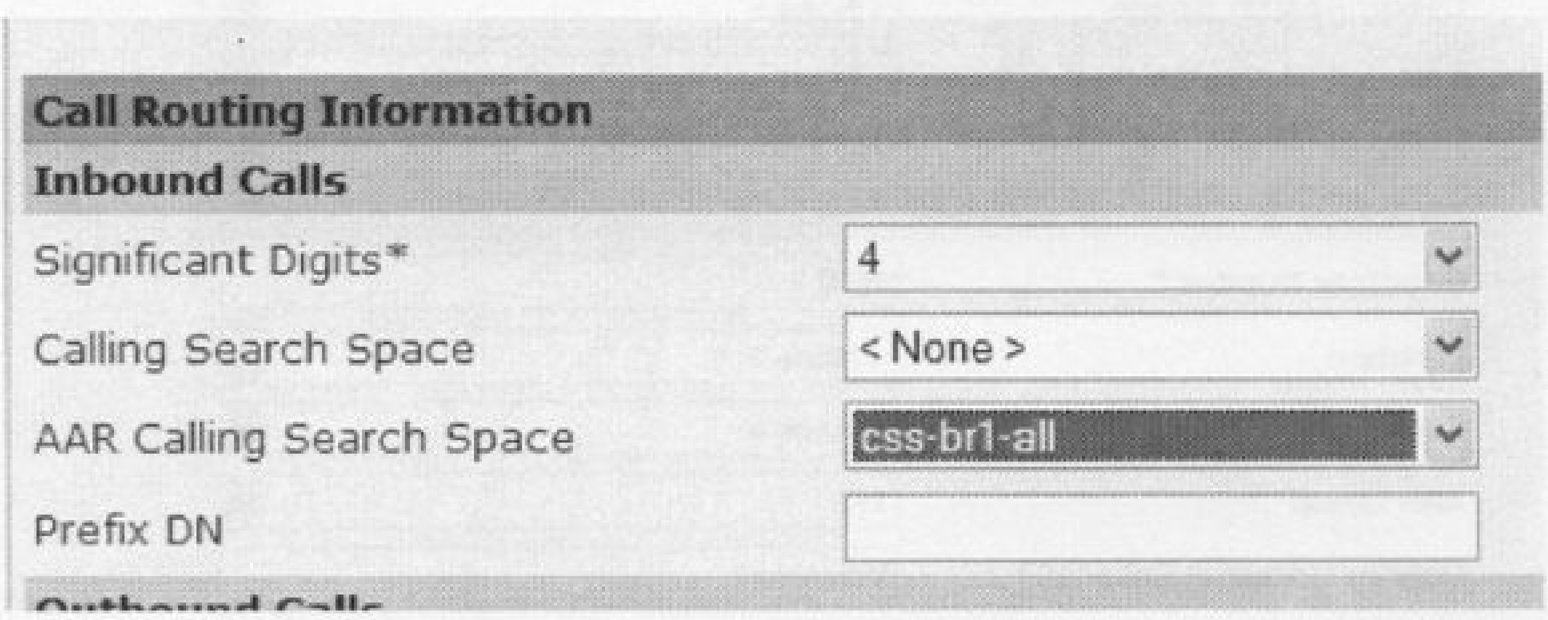
Configure Call Manager such that when a call comes into the BR1 phones and is redirected to voicemail, the call is routed out of the PSTN when Locations CAC prevents the call from being sent over the WAN.

➔ **Put all the Voicemail ports into the HQ AAR group and assign an External Number Mask. Ensure that the ports reside in Location HQ.**

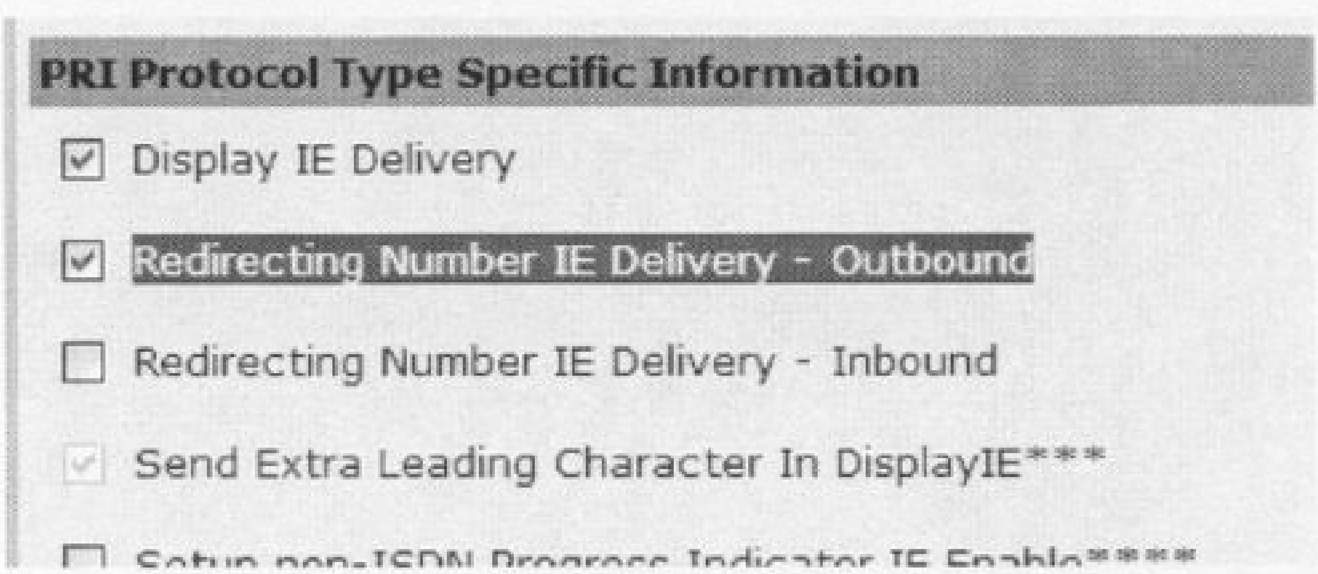


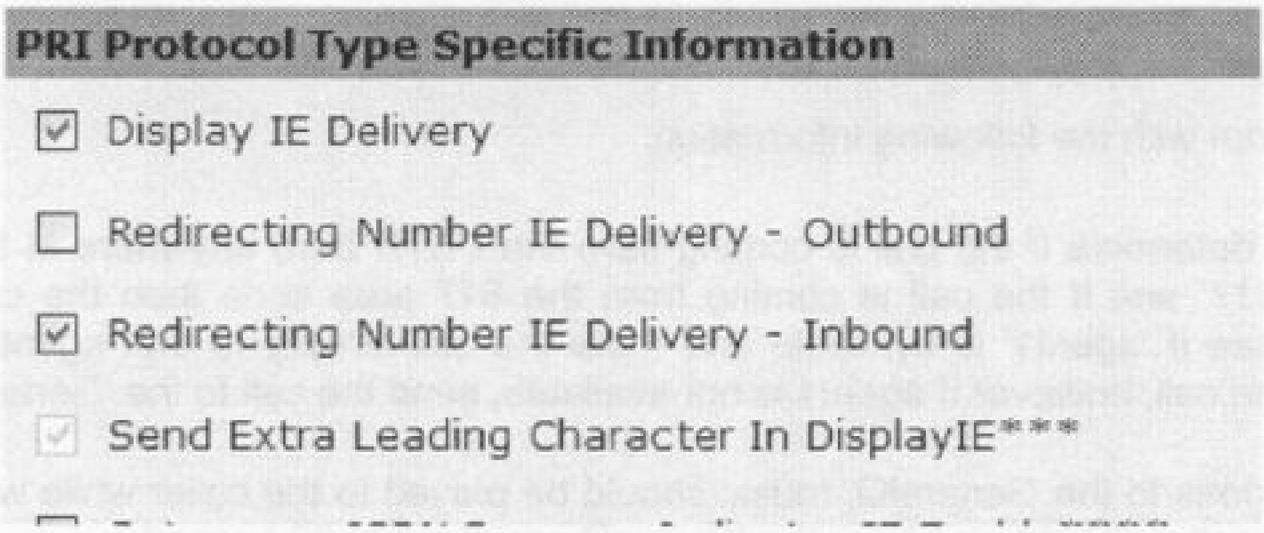
➔ **Put the BR1 IOS MGCP gateway into the BR1 AAR Group and assign an AAR CSS. Ensure that the GW resides in Location BR1.**





➔ **To hear the Subscriber Greeting rather than the Opening Greeting you must set "Redirecting Number IE Delivery Outbound" on the BR1 gateway and Redirecting Number IE Delivery Inbound" on the HQ gateway.**





Task 31.55

Configure Auto-attendant and ICD with the following information:

- AA Route Point = 1710
- Script = aa.aef
- CTI Ports = 1711, 1712

- ICD Route Point = 1700
- Script = icd.aef
- CTI Ports = 1701, 1702

Create the following users that will be used in this task:

- "**jtapi**" to be used for the JTAPI Subsystem.
- "**rmjtapi**" to be used for the ICD Subsystem.
- "**telecaster**" to be used for the ICD Subsystem and enterprise data.
- "**crsadmin**" which must be the designated administrator for IPCC Express.
- **agent1** [assigned device HQ Phone 3 with ICD ext="1003"].
- **agent2** [assigned device BR Phone 2 with ICD ext="2003"]

[all passwords must be 'cisco' and PIN numbers set to '12345' except of course 'telecaster']

For the ICD application you must use skills based routing with the following information:

- CSQ: "GeneralQ"
- Skills: "sales" & "support"
- 'agent1' shall have the skill of 'support' at a proficiency level of 9 and the skill of 'sales' at a proficiency level of 10
- 'agent2' shall have the skill of 'support' at a proficiency level of 10 and the skill of 'sales' at a proficiency level of 9
- The CSQ 'GeneralQ' should have both skills assigned to it with a proficiency level of at least 5 or better for each
- With this stated, the engine should always choose agent1 over agent2 if agent1 is available (you may use whatever method you wish to accomplish this in the engine)
- The engine should also send every agent into a automatic state of 'Work' for 30 seconds before then automatically returning them to a state of 'Ready' (this should happen regardless of whether the call is routed to a specific agent or through the GeneralQ)

➔ **This should be self-explanatory from previous examples – See Task 10.1.**

Task 31.56

Modify the "icd.aef" script with the following information:

- You must determine if the call is coming from the PSTN from anywhere in the area code of '617' and if the call is coming from the 617 area code then the call must check to see if 'agent1' is available and route the call directly to that agent without queuing the call, however if agent1 is not available, send the call to the 'GeneralQ'
- If the call goes to the GeneralQ, music should be played to the caller while waiting in Q and the caller should also hear the 'QueuePrompt' every 30 seconds
- Regardless of whether the call is routed to a specififc agent or through the GeneralQ, the agent receiving the call should be presented with Enterprise Data showing both the ANI of the call and a disposition of how the call was routed (a string showing 'Agent' or 'Queue')

➔ **This should be self-explanatory from previous examples – See Task 10.2.**

Task 31.57

Configure IPCC Phone Agent for both phones and also ensure that they only have to press the services button once (i.e. that they don't have to provide User/Ext/Pin information on the phone when logging in).

➔ **This should be self-explanatory from previous examples – See Task 10.3.**

Task 31.58

Restrict internal callers from BR1 only, so that they may not see CNAM information only regarding who they are calling or who is calling them, however ensure that BR1 Phone 3 **can** see all CNAM information.

➔ **This should be self-explanatory from previous examples – See Task 11.14.**

Task 31.59

Configure calls such that a HQ user must enter a forced auth code with a level of at least 20 or better in order to be allowed to dial an LD number and one of 30 or better in order to be allowed to dial an International number. See **Table 20** for Auth Codes.

➔ **This should be self-explanatory from previous examples – See Task 11.15.**

Task 31.60

Create a circular hunt group for Support with a DN of 3210 at BR2 between phones 1 and 3, and ensure that those phones can login-to and out-of the hunt group in order to receive calls. Allow the call to ring at around 3 times before searching for the next member.

➔ **This should be self-explanatory from previous examples – See Task 14.7.**

Task 31.61

Create an incoming AutoAttendant at the DN of 3000. Also Create a Basic ACD using the support team hunt group you just created (The necessary TCL scripts are already loaded in BR2 router's flash memory). Have the AA script automatically hand-off the callers into the support ACD hunt group when a user presses 2. Allow no more than 20 callers in the Q at any one point. Play a prompt for the user every 30 seconds to let them know that all agents are busy. Allow the users to dial-by-extension by pressing 4. Ensure that the Q is collecting statistics and view them as part of your troubleshooting.

➔ **This should be self-explanatory from previous examples – See Task 4.9.**

Task 31.62

Configure the Catalyst 6500 to move VOIP control traffic to the 2nd queue and 1st threshold.

➔ **This should be self-explanatory from previous examples.**

Task 31.63

Configure the Catalyst 6500 and 3550 to map the CoS to DSCP value.

➔ **This should be self-explanatory from previous examples.**

Task 31.64

The speed of the PVC between the HQ and Branch 2 is 128 kbps. Configure the recommended tx-ring value to reduce latency.

➔ **This should be self-explanatory from previous examples.**

Task 31.65

Configure LFI between the HQ and Branch 2. Configure such that the serialization delay is appropriate for the link speed. You may not use FRF.12 for this task.

➔ **This should be self-explanatory from previous examples – See Task 12.11.**

Task 31.66

Configure Low Latency Queuing (LLQ) for the HQ and Branch 2. Allocate enough bandwidth for 4 G729 calls over the WAN to Media and use the recommended values for control traffic.

➔ **RTP will require 96Kps and Signaling will requite 2Kbps.**

Task 31.67

Configure LLQ between the HQ and Branch 1 sites. Allocate 256Kbps for media and 8Kbps for signaling. Assume the speed of the PVC between HQ and Branch 1 is 800 Kbps.

➔ **This should be self-explanatory from previous examples.**

Task 31.68

Police all SCCP traffic on the 6500 and 3550 to 32 Kbps – the exceed action should be to remark control traffic to DSCP 10.

➔ **Inside the ACL created in Task 31.61 replace the line marking SCCP traffic to DSCP 26**

➔ **Remove:**

```
set qos acl ip SCCPPHONE dscp 26 tcp any range 2000 2002 any
!
set qos policed-dscp-map 26:10
set qos policer microflow SCCPPOLICER rate 32 burst 8 policed-dscp
!
set qos acl ip SCCPPHONE dscp 26 microflow SCCPPOLICER tcp any range
2000 2002 any
commit qos acl all
```

Task 31.69

Configure Fax Passthru throughout the network.

➔ **This should be self-explanatory from previous examples.**

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: http://www.ipexpert.com/configs

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): http://www.ipexpert.com
- Mailing List: http://www.OnlineStudyList.com
- Online Forum: http://www.CertificationTalk.com