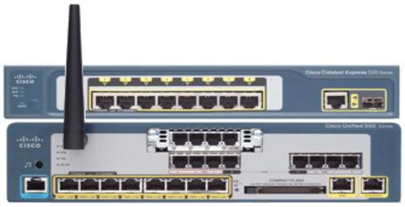
Smart Business Communications System

Unified Communications 500



SBCS/UC500 – 'First Look'

Technical Training Lab Guide

Labs by
Channels Unified Communications Field Training Team

Lab Objective: To gain experience configuring the Cisco UC500, configuring call processing, Key System, PBX, Voicemail, Auto Attendant, hunt groups, and additional features of the Cisco UC520.

Please note: Due to the labs being hosted on remote equipment not all components configured within the lab environment can be tested.

Browser Requirements: The recommended browser for this lab is Microsoft Internet Explorer 6. If you are accessing Gold Labs (LabOps) with IE7 please drop the security level of the browser, add the student URL into the list of trusted sites, ensure that pop ups are not being blocked, run the Active X control when requested, and run the Telnet Fix offered on the Topology page. Restart IE7 after making these changes. The labs cannot be accessed via Firefox/Mozilla.

Table of Contents

LAB TOPOLOGY 3

LAB OVERVIEW: 4

SBCS – Initial Lab Access.. 5

Installing CCA 2.0 8

LAB SETUP.. 9

Exercise-1: KEY SYSTEM w/ VOICEMAIL.. 15

Exercise-2: PBX, VOICEMAIL/AUTO ATTENDANT 22

Exercise-3: Business Schedule and Auto Attendant 39

Exercise-4: ADVANCED FEATURE EXERCISE.. 51

Exercise 5- SECURITY & WIRELESS.. 60

APPENDIX A: Reset to factory default.. 67

APPENDIX B: Verifying VoiceView Express & IMAP 69

APPENDIX C: Configuring Security on the Cisco UC500 and SR500 73

APPENDIX D: Prompt Management 103

APPENDIX E: PPPoE on the WAN 108

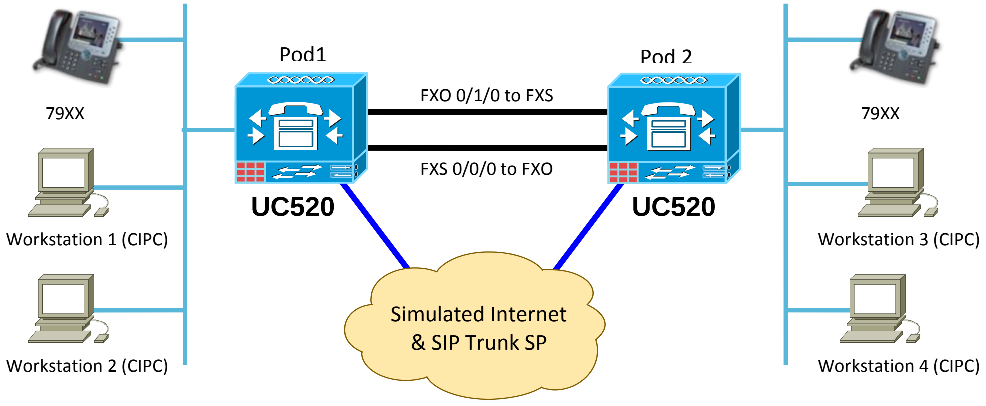
APPENDIX F: Configuring IPSEC VPNs between sites on the UC520 110

APPENDIX G: IOS Dial-Peer Configuration...111

APPENDIX H: Designing for a Scenario 118

APPENDIX I: Device Manager Cross Launch 119

LAB TOPOLOGY



Addressing and Directory Number Assignments

WAN IP Addressing	
WAN IP Address	1.1.100.xx
WAN Subnet Mask	255.255.255.0
WAN Default Router	1.1.100.254

Inbound SIP Trunk DID (PSTN Call in) Numbers (Use PSTN phone to test)	
Auto attendant	4085xx1200
Extension 1 (201)	4085xx1201
Extension 2 (202)	4085xx1202
VoiceMail	4085xx1209

Outbound Numbers to Call (From IP Phones on UC520 to PSTN Phone)

Emergency Number	9911
Local Call	9 777 1000
Long Distance	9 1 650 7772000
International	9 011 44 1234512345

For example:
The value 'xx' corresponds to your assigned POD number.

Pod 1	**IP Address**	1.1.100.**1**
	Auto Attendant	4085**01**1200
Pod 2	**IP Address**	1.1.100.**2**
	Auto Attendant	4085**02**1200

LAB OVERVIEW:

Several of the exercises will require partnering with another pod to demonstrate certain features of the system. To complete this, the hardware is pre-wired to your 'buddy' pod. This will emulate a PSTN connection for the lab environment. Normally, trunks from the PSTN are connected into the FXO ports and analog devices (such as a fax machines) are connected into the FXS ports. Please coordinate with the team seated at your 'buddy' pod to ensure that progress of the lab is simultaneously made thereby making it easier to complete the verification steps successfully.

All of the software needed to complete the exercises has been installed on the virtual workstations. This software includes the Cisco Configuration Assistant (CCA), Cisco IP Communicator (CIPC), and the new auto attendant (AA) script.

It will be necessary, *unless otherwise noted*, to restore the UC500 to factory defaults after each exercise. Instructions on how to do this are included in Appendix A.

Please pay close attention to items highlighted in **RED**.

⚠ This symbol will indicate that the UC520 needs to be reset to factory defaults.

Note: A UC520 system set up as a Key System must be reset to factory defaults before being configured as a PBX system and visa versa.

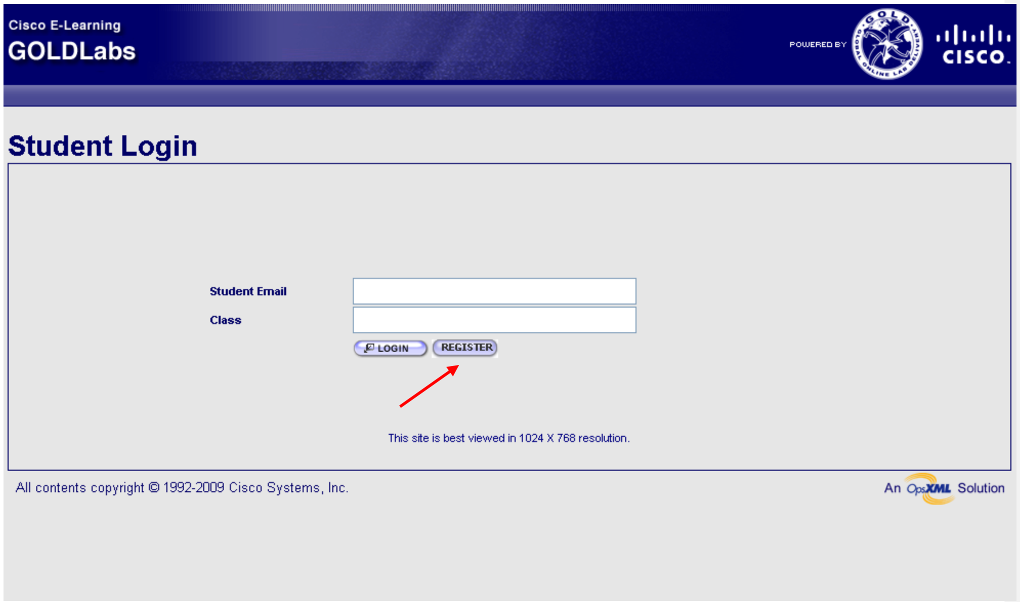
SBCS – Initial Lab Access

Log into the LabOps lab portal and access the Windows XP Workstation 1 or Workstation 3. Class Name information for logging into LabOps is assigned by your instructor.

Step 1: Go to the following URL.

https://labops-out.cisco.com/labops/ilt/default.asp

Step 2: If you have not done so before you will now need to register with Labops before you can use the lab equipment.



Student Login

Student Email

Class

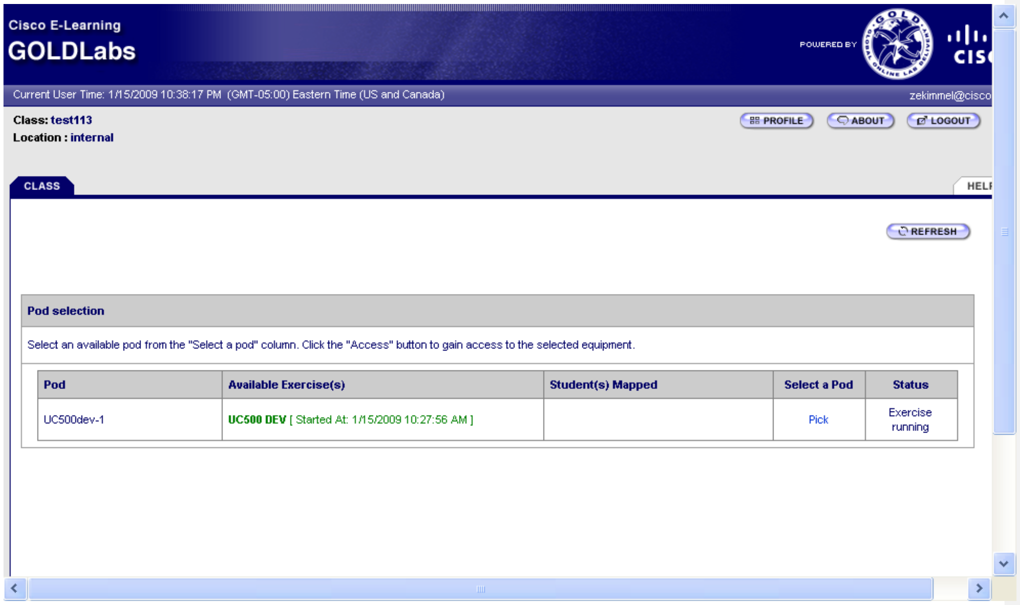
This site is best viewed in 1024 X 768 resolution.

All contents copyright © 1992-2009 Cisco Systems, Inc.

An OpsXML Solution

Registration includes providing your name and email address to Gold Labs and then clicking save. You will get a window saying you have successfully registered. Then you will be able to go in and log in using your registered email address and the class name provided by the instructor.

Step 3: "Pick" a pod. Students should choose the pod assigned to them by the instructor. If you pick the same pod as someone else you will be sharing that set of equipment with them.



Current User Time: 1/15/2009 10:38:17 PM (GMT-05:00) Eastern Time (US and Canada) zekimmel@cisco

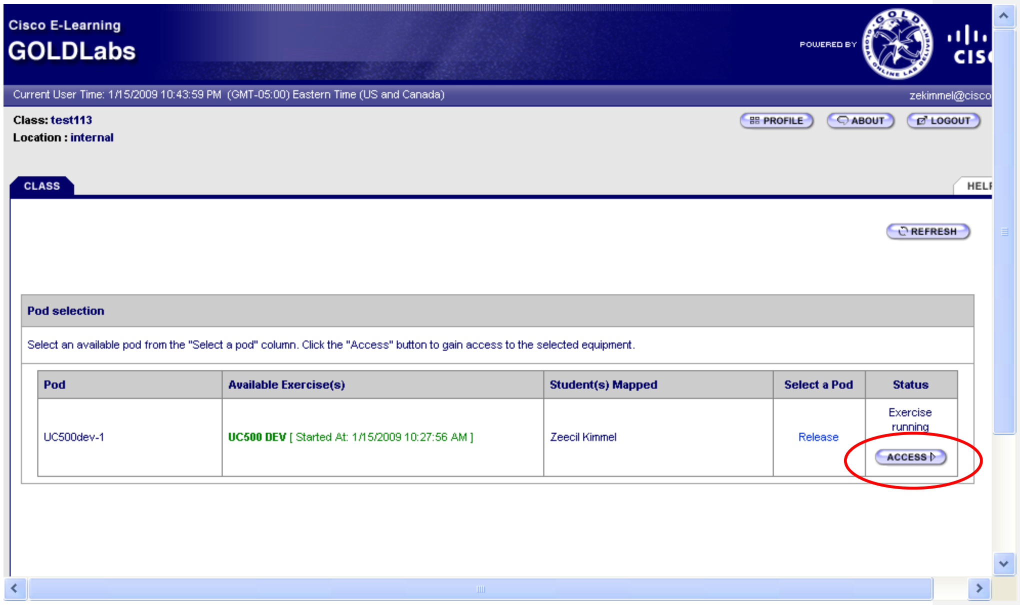
Class: test113
Location : internal

Pod selection

Select an available pod from the "Select a pod" column. Click the "Access" button to gain access to the selected equipment.

Pod	Available Exercise(s)	Student(s) Mapped	Select a Pod	Status
UC500dev-1	UC500 DEV [Started At: 1/15/2009 10:27:56 AM]		Pick	Exercise running

Step 4: You can access your equipment by clicking the "Access" button.



Current User Time: 1/15/2009 10:43:59 PM (GMT-05:00) Eastern Time (US and Canada) zekimmel@cisco

Class: test113
Location : internal

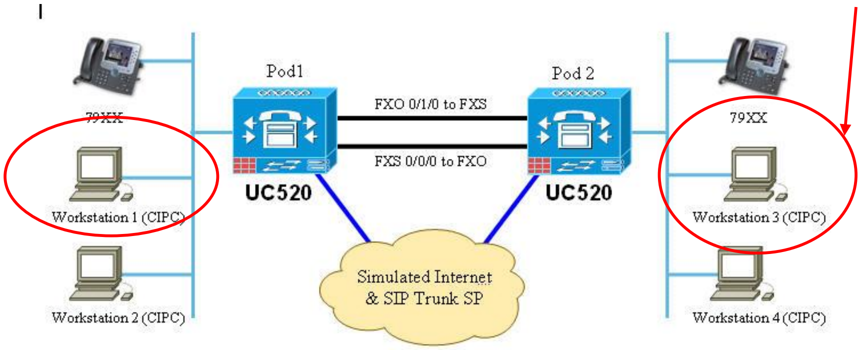
Pod selection

Select an available pod from the "Select a pod" column. Click the "Access" button to gain access to the selected equipment.

Pod	Available Exercise(s)	Student(s) Mapped	Select a Pod	Status
UC500dev-1	UC500 DEV [Started At: 1/15/2009 10:27:56 AM]	Zeecil Kimmel	Release	Exercise running ACCESS

Step 5: A new browser window will open displaying the lab network diagram. This is an interactive portal giving access to each of the Workstations. You can telnet or RDP to your devices by scrolling

over the topology and clicking a device. Please access the workstations when instructed to do so in the lab guide. Click in the center of Workstation 1's screen. Click in the center of Workstation 3's screen if working on Pod 2.

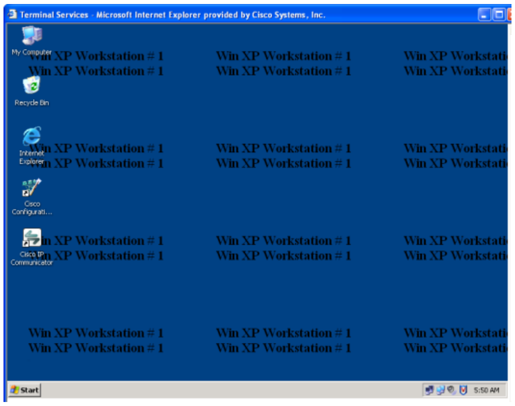


Note:
Onsite Live Class - you may have up to 3 lab partners. Your instructor will assign you to either POD 1 or POD 2 within the lab. Please only access your assigned workstations within the POD. Each POD is configured to reside on it's own VLan and as such does not see the other UC520.

Only one terminal service session may be active per desktop. If you have a lab partner, you will find it easier for one person to access the workstations while the other person displays the lab guide on their laptop. After one or two exercises, you may want to switch roles to allow the other person hands on experience.

Online Class – you will not have a lab partner. You will be configuring POD 1 and POD 2 within your exercise. For example, when you have complete Exercise-2 in POD 1, you must then complete Exercise-2 in POD 2. Look for online specific instructions at the beginning and end of each individual exercise.

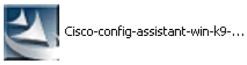
Step 6: Click on the Terminal Services bar to initiate a remote desktop session to the Windows XP Workstation 1 or Workstation 3.



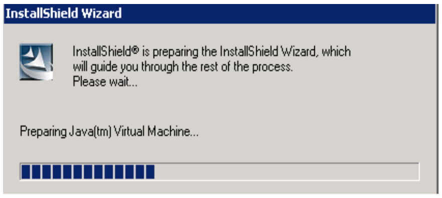
Installing CCA 2.0

Step 1: Open the my computer icon on the desktop. Click on the NEW(D:) icon in the removable storage section and open the folder. (Make sure this is upgraded for one workstation on each side of the pods A and B)

Step 2: Click on the Cisco-config-assistant executable.



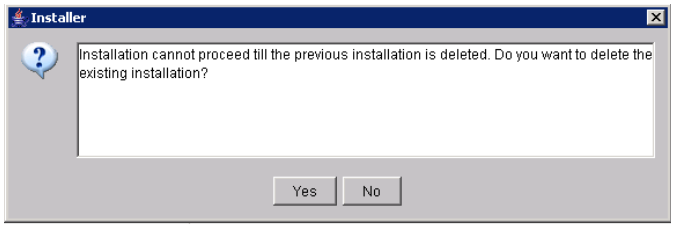
Step 3: The install wizard will appear to guide you through the rest of the process.



InstallShield® is preparing the InstallShield Wizard, which will guide you through the rest of the process.
Please wait...

Preparing Java(tm) Virtual Machine...

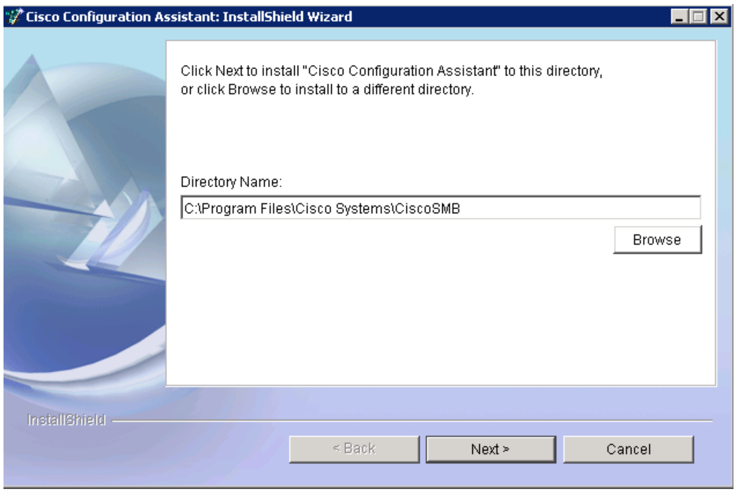
Step 4: The message "install cannot complete until the previous version is deleted" will appear. Click yes to delete the previous version.



Installation cannot proceed till the previous installation is deleted. Do you want to delete the existing installation?

Step 5: Click yes to accept the licensing agreement.

tep 6: Click next to accept the default directory for CCA.



Click Next to install "Cisco Configuration Assistant" to this directory, or click Browse to install to a different directory.

Directory Name:

C:\Program Files\Cisco Systems\CiscoSMB

Step 7: Click finish to exit the wizard once the installation has completed.

Step 8: Close the CCA 2.0 folder.

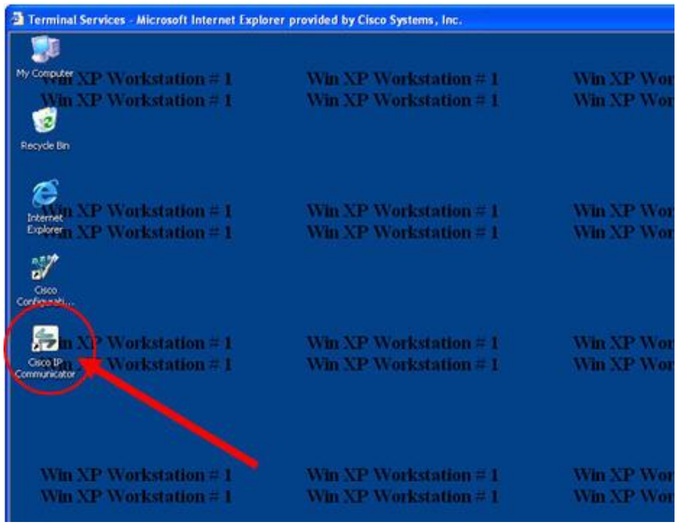
LAB SETUP

Setup steps:

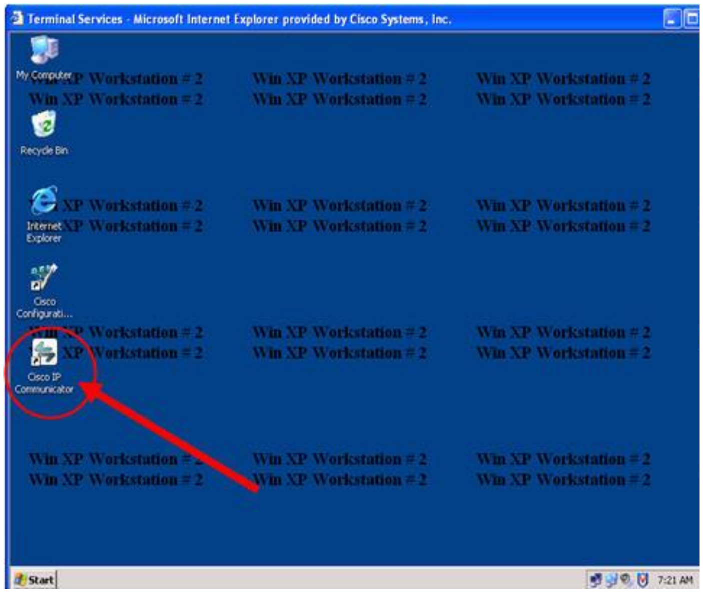
⚠ **Step 1:** Using Appendix A – Reset each UC520 to its default factory configuration using the **Command Line Interface (CLI)** instructions. (Page 68, do not reset CUE.)

Step 2: Access Workstation 1 and Workstation 2 in your POD. If working on POD 2 access Workstation 3 and Workstation 4.

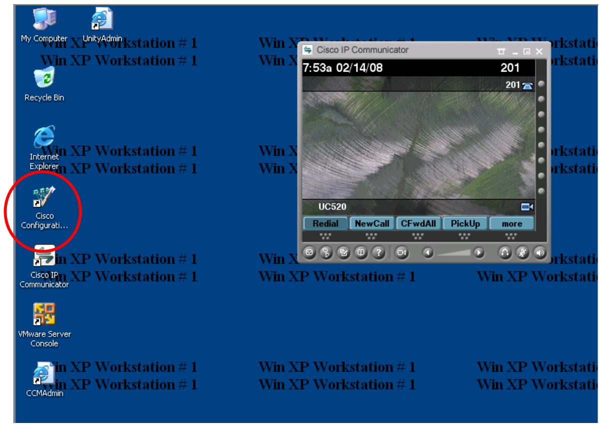
Step 3: Start IP Communicator on Workstation 1 or Workstation 3. (Online classes start on all workstations)



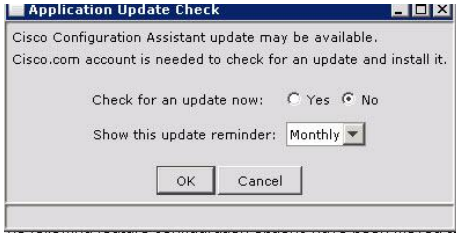
Step 4: Start IP Communicator on Workstation 2 or Workstation 4. (Online classes start on all workstations)



Step 5: Once your CIPC's have registered (show and extension and the System Message) open the Configuration Assistant by clicking on either of the Cisco Configuration Icons on the desktop.



Step 6: The Cisco music will play and a prompt may appear asking to check for updates to the application appear. Leave the default of 'no' and do not have the system check for updates. Click OK.



Application Update Check

Cisco Configuration Assistant update may be available.
Cisco.com account is needed to check for an update and install it.

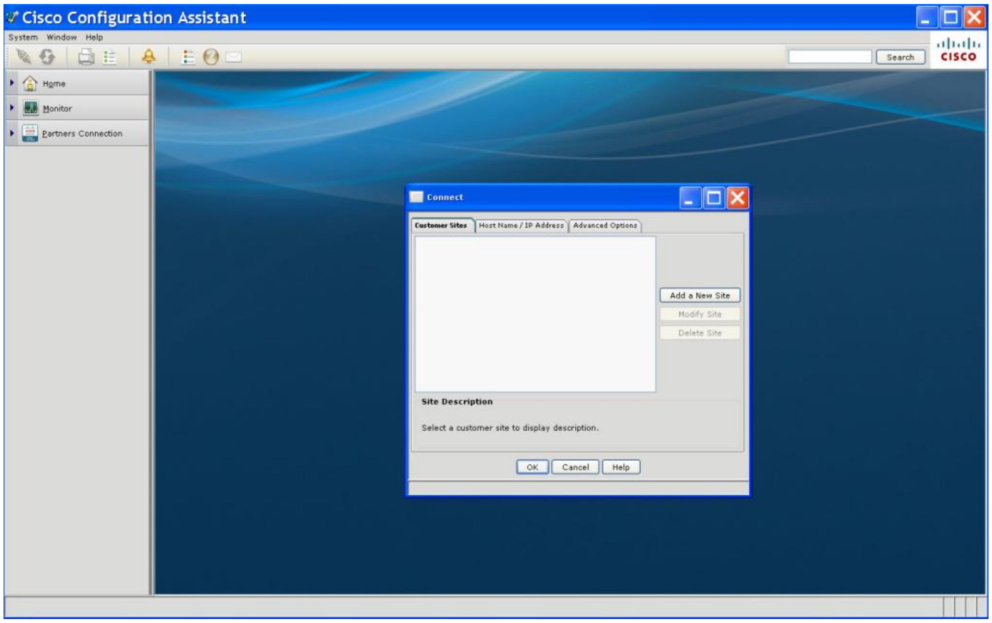
Check for an update now: ○ Yes ● No

Show this update reminder: Monthly

OK Cancel

Step 7: CCA will open with a window to Connect to a UC520 via IP address. This can be a local UC520 or a remote customer network.

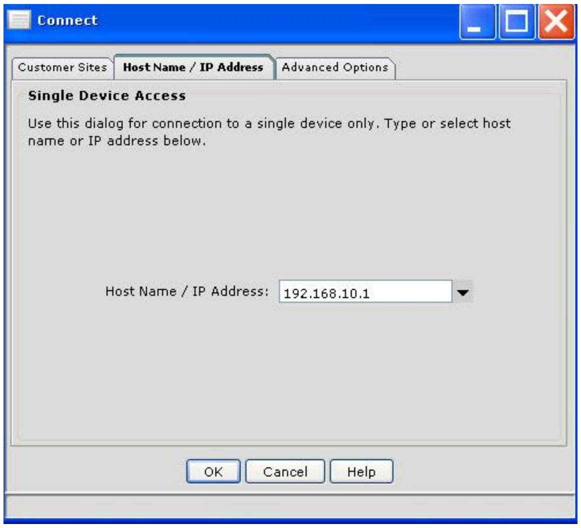
NOTE: It is possible to create Customer Sites for monitoring customer networks. Configurations can be stored in CCA on any workstation.



Site Description

Select a customer site to display description.

Step 8: Select the Host Name/IP Address tab.



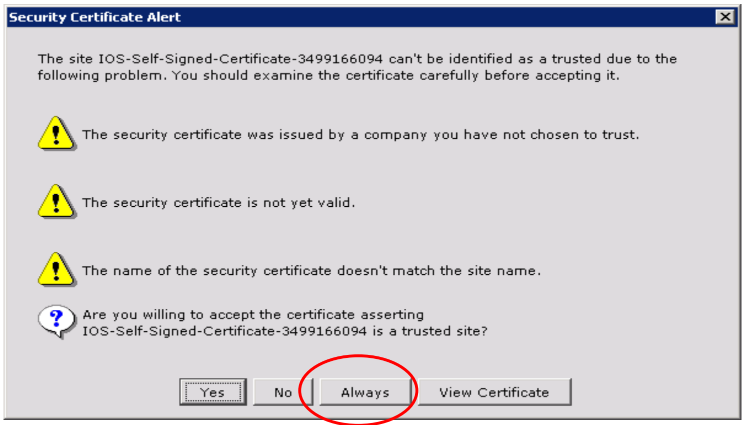
Single Device Access

Use this dialog for connection to a single device only. Type or select host name or IP address below.

Host Name / IP Address: 192.168.10.1

Step 9: Enter in the IP address 192.168.10.1. (The UC520's do not see each other and as such use this IP address on both Pod 1 and Pod 2.) **This is the default IP Address of the UC520.**

(Step 9a: If the Security Certificate Alert appears, click always to accept the Security Certificate.)



Security Certificate Alert

The site IOS-Self-Signed-Certificate-3499166094 can't be identified as a trusted due to the following problem. You should examine the certificate carefully before accepting it.

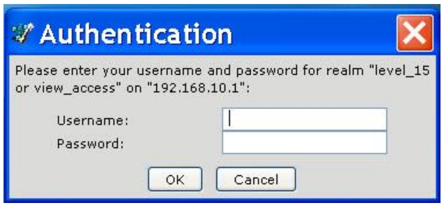
The security certificate was issued by a company you have not chosen to trust.

The security certificate is not yet valid.

The name of the security certificate doesn't match the site name.

Are you willing to accept the certificate asserting IOS-Self-Signed-Certificate-3499166094 is a trusted site?

Step 10: Enter cisco, cisco for the Username and password.



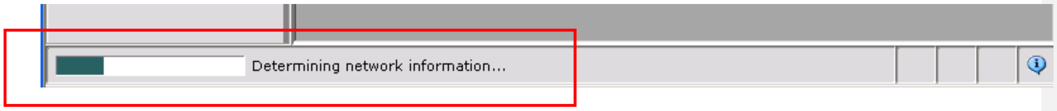
Authentication

Please enter your username and password for realm "level_15 or view_access" on "192.168.10.1":

Username:

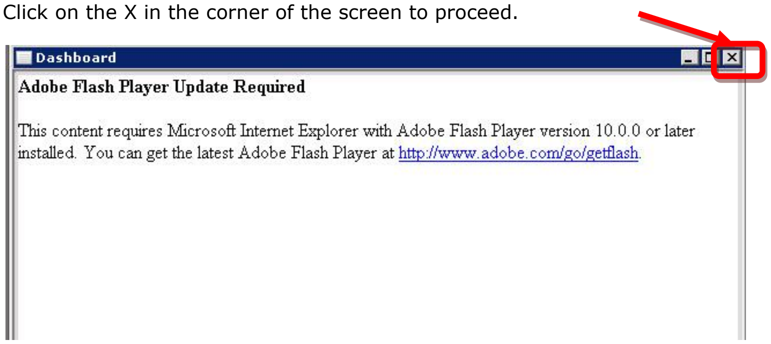
Password:

Note: The dialog box from step 7 will appear. The progress for discovery can be seen at the bottom left corner of the screen.



Determining network information...

Step 11: The CCA will attempt to open a Dashboard view of the system information for the UC520. In this lab it will cause an error message because the Java on the workstations are not updates. Click on the X in the corner of the screen to proceed.

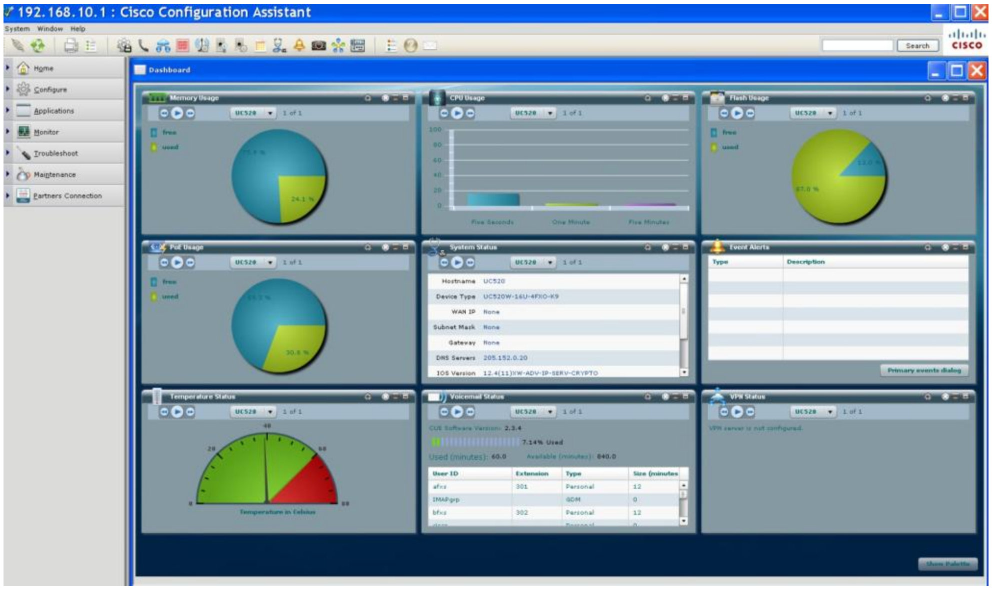


Dashboard

Adobe Flash Player Update Required

This content requires Microsoft Internet Explorer with Adobe Flash Player version 10.0.0 or later installed. You can get the latest Adobe Flash Player at http://www.adobe.com/go/getflash.

Note: Sample Dashboard Screen:



192.168.10.1 : Cisco Configuration Assistant

Dashboard

System Status

Hostname	UC520
Device Type	UC520W-16U-4FXO-K9
WAN IP	None
Subnet Mask	None
Gateway	None
DNS Servers	205.152.0.20
IOS Version	12.4(11)XW-ADV-IP-SERV-CRYPTO

Voicemail Status

CUE Software Version: 2.3.4

7.14% Used

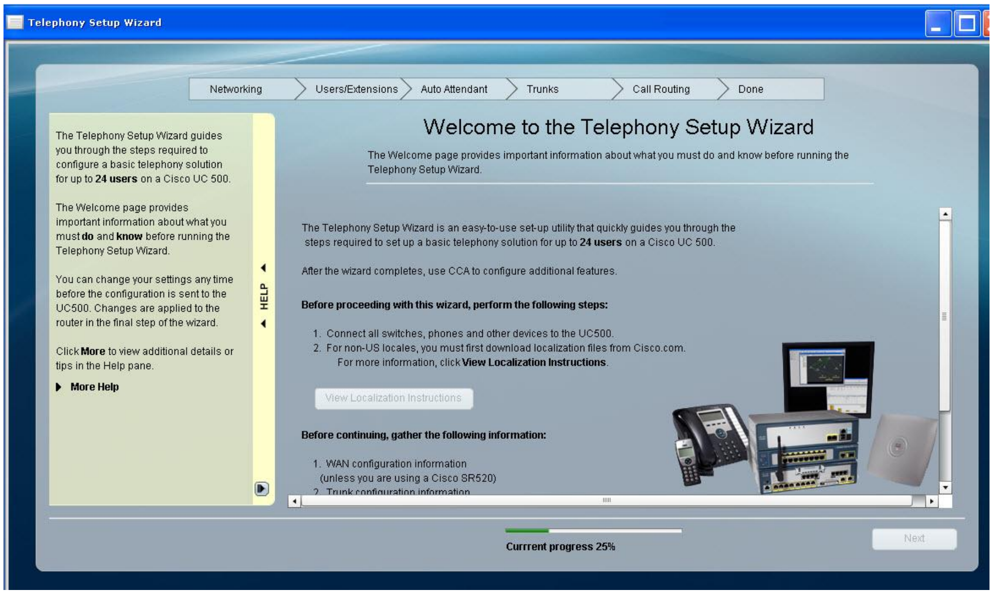
Used (minutes): 60.0 Available (minutes): 840.0

User ID	Extension	Type	Size (minutes
afxs	301	Personal	12
IMAPgrp		GDM	0
bfxs	302	Personal	12

VPN Status

VPN server is not configured.

Step 12: When the screen updates the telephony setup wizard will be available. Close the telephony wizard window, in this lab environment the wizard will not be used.



Telephony Setup Wizard

The Telephony Setup Wizard guides you through the steps required to configure a basic telephony solution for up to **24 users** on a Cisco UC 500.

The Welcome page provides important information about what you must **do** and **know** before running the Telephony Setup Wizard.

You can change your settings any time before the configuration is sent to the UC500. Changes are applied to the router in the final step of the wizard.

Click **More** to view additional details or tips in the Help pane.

▶ **More Help**

Welcome to the Telephony Setup Wizard

The Welcome page provides important information about what you must do and know before running the Telephony Setup Wizard.

The Telephony Setup Wizard is an easy-to-use set-up utility that quickly guides you through the steps required to set up a basic telephony solution for up to **24 users** on a Cisco UC 500.

After the wizard completes, use CCA to configure additional features.

Before proceeding with this wizard, perform the following steps:

1. Connect all switches, phones and other devices to the UC500.
2. For non-US locales, you must first download localization files from Cisco.com. For more information, click **View Localization Instructions**.

View Localization Instructions

Before continuing, gather the following information:

1. WAN configuration information (unless you are using a Cisco SR520)
2. Trunk configuration information

Current progress 25%

Next

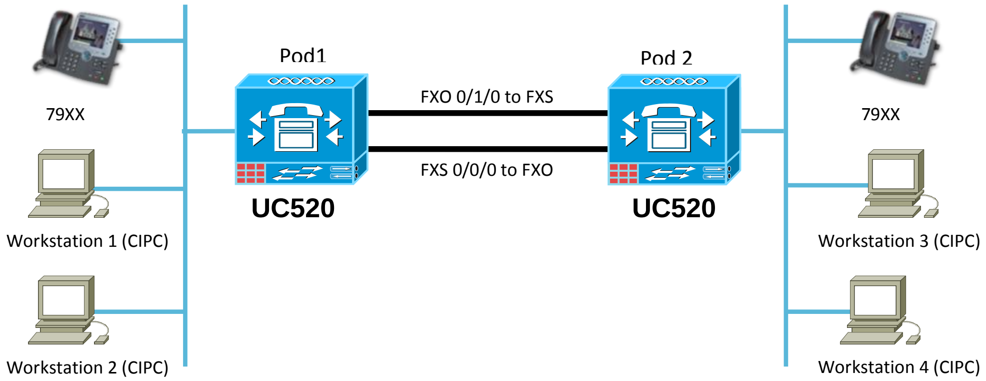
Exercise-1: KEY SYSTEM w/ VOICEMAIL

Introduction:
The UC520 supports two voice system configuration types – PBX type and Key system type. This exercise focuses on the Key System configuration. A typical Key Systems consist of one or more lines coming from the PSTN (e.g. Analog FXO trunks) that rings a group of selected phones. To make outbound calls, IP Phone users select one of the buttons on their IP Phones that correspond to the lines from the PSTN. In addition to the PSTN lines, users have internal extensions with voicemail.

Objective:
The main objective of this exercise is to configure the basic Key System with voicemail features. This is configured using the Cisco Configuration Assistant (CCA). At the completion of this exercise, the system will be configured as a Key System including extensions for all users, voicemail boxes, intercom, paging and power failover.

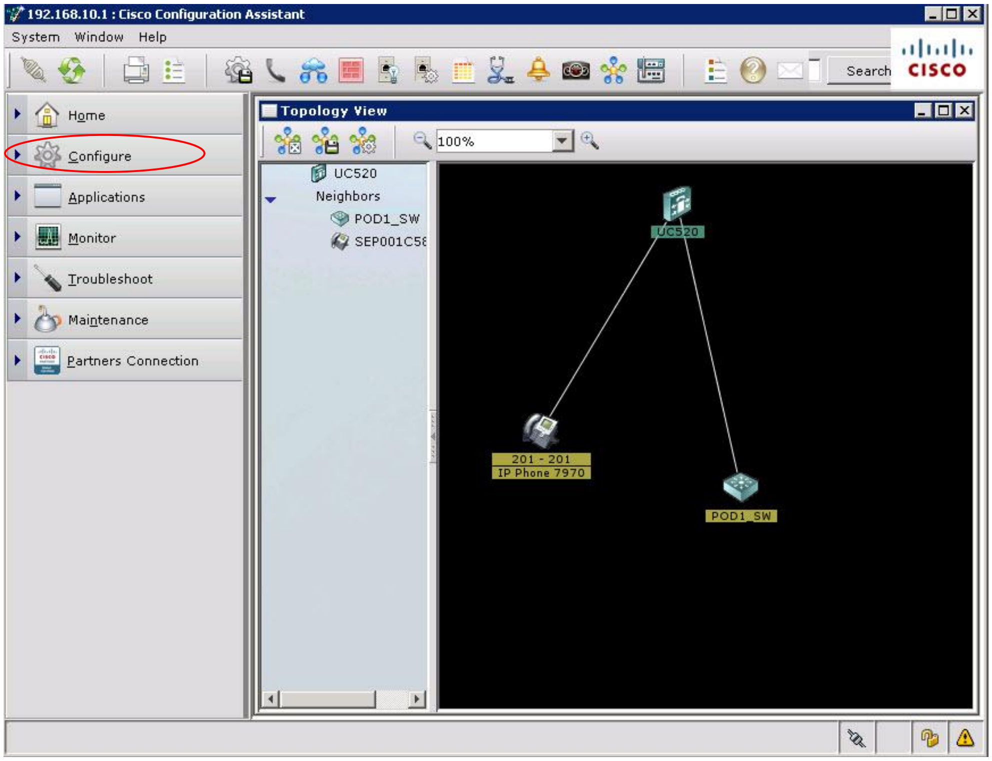
Reference:
Video Demo for CCA: http://tools.cisco.com/cmn/jsp/index.jsp?id=61293

Topology:



NOTE: Before making any changes in CCA, ensure that the 'Refresh' button at the bottom of the screen is active. It is grayed out while CCA reads the configuration from the UC520.

Step 1: Close the Telephony wizard that opened automatically with CCA. Note the menu options available with this version from the left menu pain.

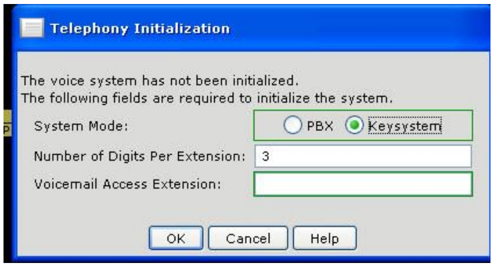


NOTE: Each Pod's topology should be similar to the screen shot in Exercise1 step 1 (above). The CIPC device will not show in the topology view. (Where the virtual device is plugged in, such as behind an IP Phone or not, the device will or will not be shown in the topology view.)

The Switch shown is the lab Switch being used to simulate the Internet. The IP phones will appear in the Telephony configuration menu further in the lab.

Step 2: Select Configure → Telephony → Region from the menus on the left side.

Step 3: A message will appear asking for the initialization of the system. For this lab choose Key System for the system type.



The voice system has not been initialized.
The following fields are required to initialize the system.

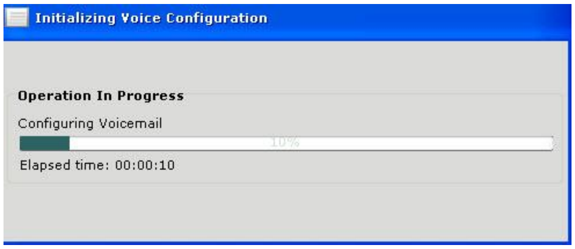
System Mode: ○ PBX ● Keysystem

Number of Digits Per Extension: 3

Voicemail Access Extension:

Step 4: Leave the default of 3 for the Digits per Extension. Enter 298 for the Voicemail Access Extension. Click OK

Step 5: An Initialization box will appear.



Initializing Voice Configuration

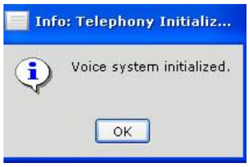
Operation In Progress

Configuring Voicemail

10%

Elapsed time: 00:00:10

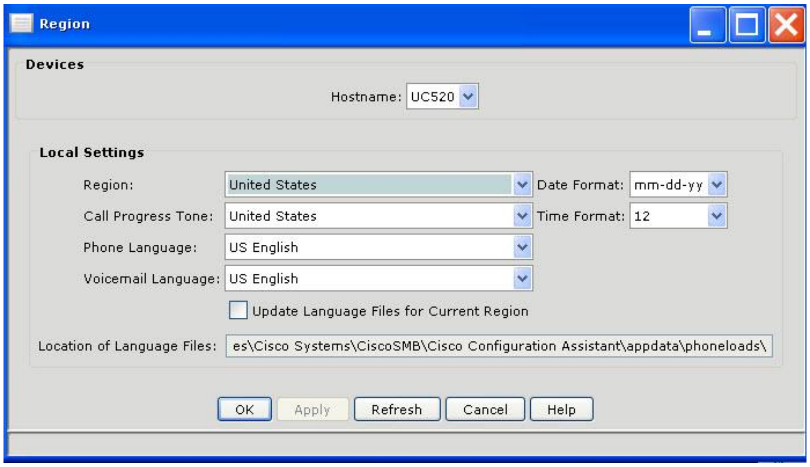
Step 6: When the system is ready a pop-up box will appear stating the voice system is initialized. Click OK.



Info: Telephony Initializ...

Voice system initialized.

Step 7: Set the regional information for the UC520 according to the correct switch location. For US leave the default information as configured. Click OK.



Region

Devices

Hostname: UC520

Local Settings

Region: United States

Date Format: mm-dd-yy

Call Progress Tone: United States

Time Format: 12

Phone Language: US English

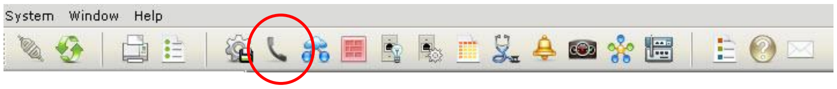
Voicemail Language: US English

□ Update Language Files for Current Region

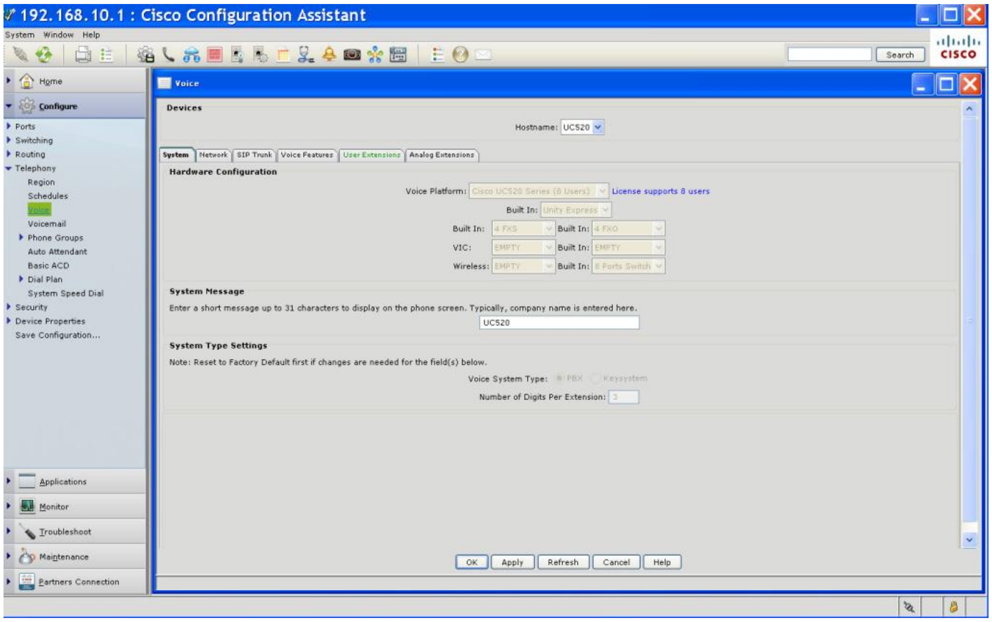
Location of Language Files: es\Cisco Systems\CiscoSMB\Cisco Configuration Assistant\appdata\phoneloads\

NOTE: Do NOT continue until the Refresh button is available. If it is grayed out, CCA is updating information on the UC520.

Step 8: Select Configure → Telephony → Voice from the menus on the left or alternatively click the Phone icon on the top menu bar.



Step 9: In the initial System Tab note the hardware that is in the UC520 in the lab. Also note that the System settings that were configured initially are stored here. All those options are grayed out as they cannot be changed. (To change from Keysystem to PBX requires a reset to factory default.)



Devices

Hostname: UC520

Hardware Configuration

Voice Platform: Cisco UC520 Series (8 Users) License supports 8 users

Built In: Unity Express

Built In: 4 FXS Built In: 4 FXO

VIC: EMPTY Built In: EMPTY

Wireless: EMPTY Built In: 8 Ports Switch

System Message

Enter a short message up to 31 characters to display on the phone screen. Typically, company name is entered here.

UC520

System Type Settings

Note: Reset to Factory Default first if changes are needed for the field(s) below.

Voice System Type: ● PBX ○ Keysystem

Number of Digits Per Extension: 3

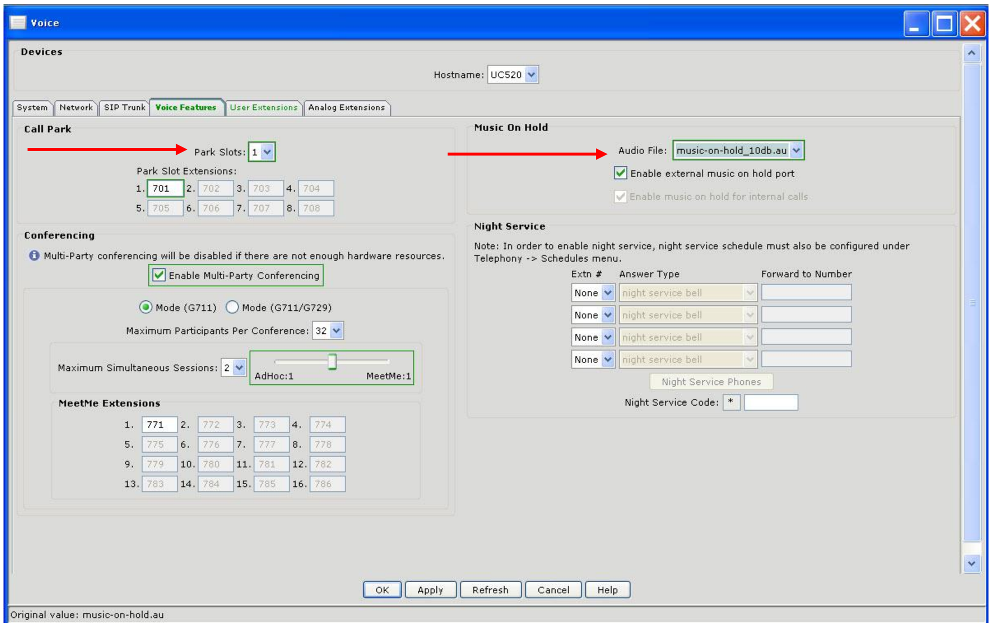
Step 10: Change the System Message to 'UC520-PODxx'. (Where XX is your assigned pod number.)

NOTE: Do NOT continue until the Apply and Refresh buttons are available. If they are grayed out, CCA is updating information on the UC520.

DO NOT CLICK OK or Apply until steps 11 – 15 are completed.

Note: As system configuration is done color highlighting is used both on the tab label and throughout the tab pages. To indicate if steps were completed correctly (green) highlighting is used. If additional configuration is required or if the configuration is incorrect (red) highlighting is used. The configuration cannot be saved until all items that are critical to the system are configured. Once all configuration is correct it can be saved to memory.

Step 11: Choose the Voice Features tab. Change the Audio file to the music-on-hold-10db.au



Hostname: UC520

Park Slots: 1

Park Slot Extensions: 1. 701 2. 702 3. 703 4. 704 5. 705 6. 706 7. 707 8. 708

Audio File: music-on-hold_10db.au

☑ Enable external music on hold port

☑ Enable music on hold for internal calls

Multi-Party conferencing will be disabled if there are not enough hardware resources.

☑ Enable Multi-Party Conferencing

● Mode (G711) ○ Mode (G711/G729)

Maximum Participants Per Conference: 32

Maximum Simultaneous Sessions: 2 AdHoc:1 MeetMe:1

MeetMe Extensions: 1. 771 2. 772 3. 773 4. 774 5. 775 6. 776 7. 777 8. 778 9. 779 10. 780 11. 781 12. 782 13. 783 14. 784 15. 785 16. 786

Note: In order to enable night service, night service schedule must also be configured under Telephony -> Schedules menu.

Extn #	Answer Type	Forward to Number
None	night service bell	
None	night service bell	
None	night service bell	
None	night service bell	

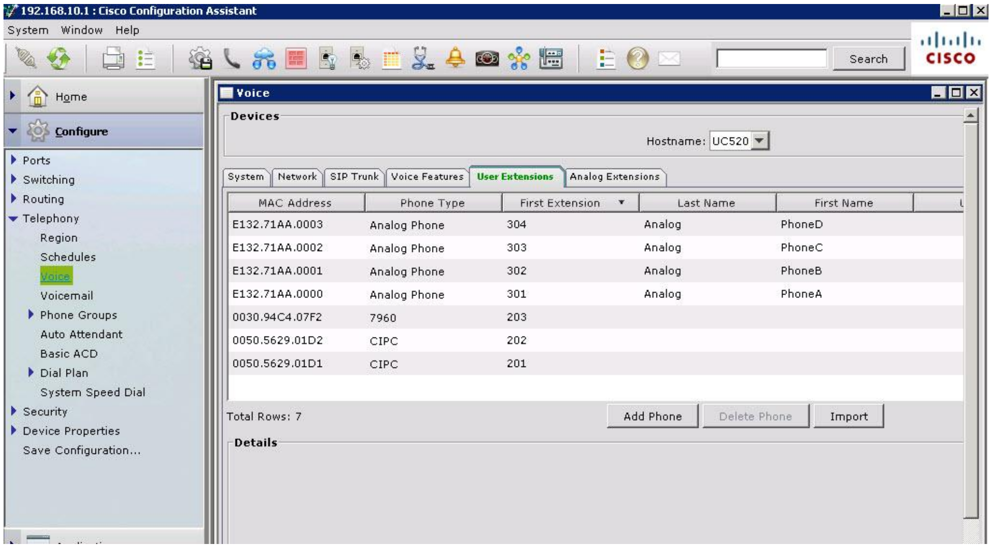
Night Service Code: *

Original value: music-on-hold.au

Step 12: Set the number of Park Slots to 1. (Park slots allow phone calls to be placed on hold in a location for other users to pick up.)

Step 13: Multi-party conferencing can also be enabled here. More attention to this feature will be given in the Advanced SBCS lab.

Step 14: Select the Users Extensions tab:



Hostname: UC520

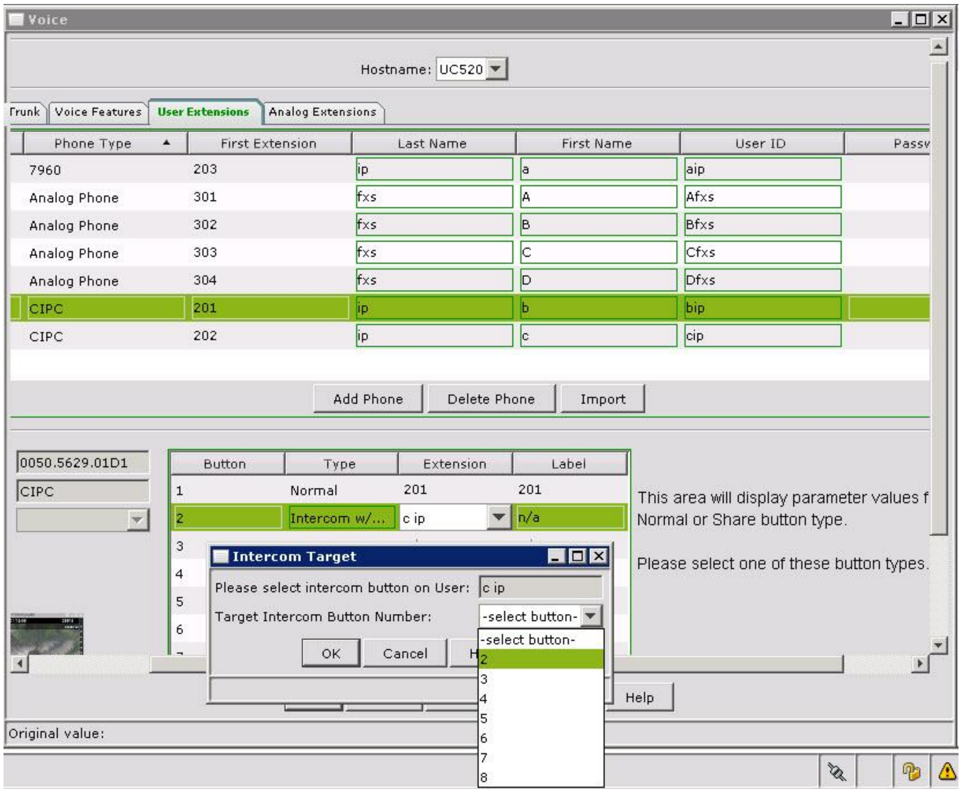
MAC Address	Phone Type	First Extension	Last Name	First Name
E132.71AA.0003	Analog Phone	304	Analog	PhoneD
E132.71AA.0002	Analog Phone	303	Analog	PhoneC
E132.71AA.0001	Analog Phone	302	Analog	PhoneB
E132.71AA.0000	Analog Phone	301	Analog	PhoneA
0030.94C4.07F2	7960	203		
0050.5629.01D2	CIPC	202		
0050.5629.01D1	CIPC	201		

Total Rows: 7

a. For all the Analog Phones (none connected but configured by default on the UC520):
   - **i.** Configure the LastName for all Analog phones as fxs
   - **ii.** Configure the FirstName as a, b, c, d.
   - **iii.** Configure the userid as afxs, bfxs, cfxs, dfxs.
   - **iv.** Set the passwords to 1234.

b. For the 7960:
   - **i.** Configure the LastName for the phone as ip
   - **ii.** Configure the FirstName as 'c'
   - **iii.** Configure the userid as cip.
   - **iv.** Set the passwords to 1234.

c. For the two CIPC Phones:
   - **i.** Configure the LastName for the CIPC phones as 'cipc'
   - **ii.** Configure the FirstName as 'a' or 'b'.
   - **iii.** Configure the userid as aip for one and bip for the other.
   - **iv.** Set the passwords to 1234.
   - **v.** Setup Intercom for phone button 2 on AIPC select Intercom to IP phone BIPC from the pull down menu.
   - **vi.** Choose button 2 for the intercom location of BIPC.



Voice

Hostname: UC520

Trunk | Voice Features | User Extensions | Analog Extensions

Phone Type	First Extension	Last Name	First Name	User ID	Passw
7960	203	ip	a	aip	
Analog Phone	301	fxs	A	Afxs	
Analog Phone	302	fxs	B	Bfxs	
Analog Phone	303	fxs	C	Cfxs	
Analog Phone	304	fxs	D	Dfxs	
CIPC	201	ip	b	bip	
CIPC	202	ip	c	cip	

Add Phone | Delete Phone | Import

0050.5629.01D1

CIPC

Button	Type	Extension	Label
1	Normal	201	201
2	Intercom w/...	c ip	n/a
3			
4			
5			
6			

This area will display parameter values f Normal or Share button type.

Please select one of these button types.

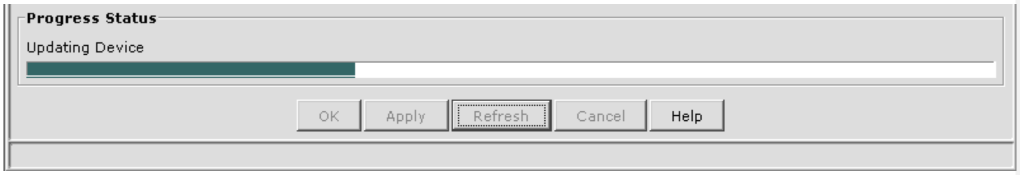
Intercom Target

Please select intercom button on User: c ip

Target Intercom Button Number: -select button-

Original value:

Step 15: Click on the 'Apply' button at the bottom of the screen and observe the progress bar.



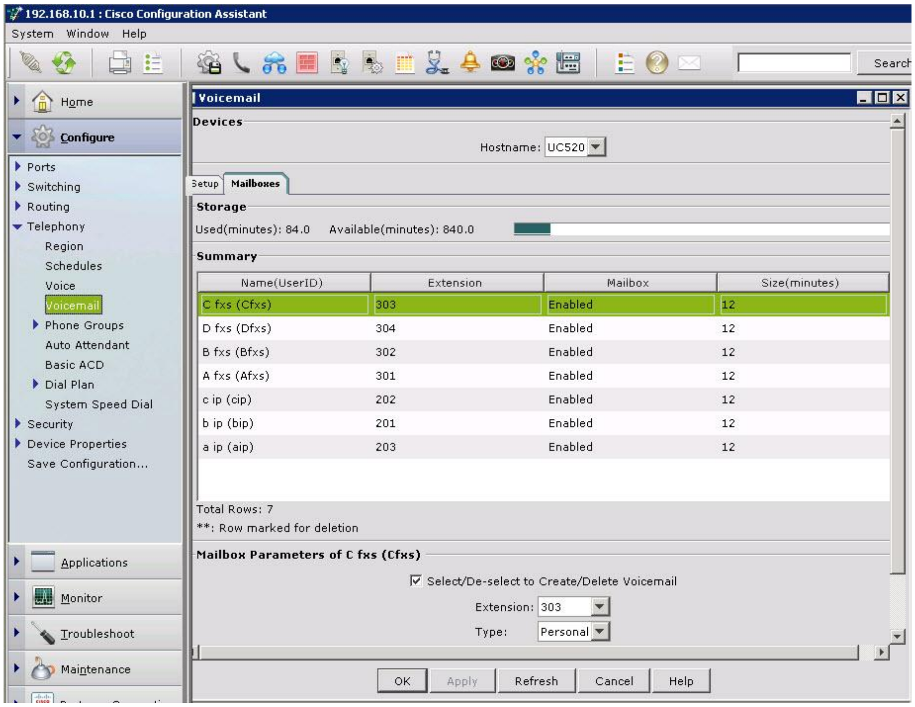
Progress Status

Updating Device

Note: If you want to save the CCA configuration you can by clicking on the 'Save' icon at the top of CCA. Select All Devices if requested to specify which devices to save.

Verification Steps:

Step 1: Check the FirstName and LastName on the IP Phones. Place a call from ACIPC to BCIPC, do not answer the call and ensure that call rolls over to VM.
Step 2: Press the 'Messages' button on BCIPC and enroll the user in voicemail. Use '789' as a password. If pressing the voicemail button results in a fast busy go to the Configure → Telephony → Voicemail → Mailbox tab and make sure that all the extensions have voicemail enabled.



Devices

Hostname: UC520

Storage

Used(minutes): 84.0 Available(minutes): 840.0

Summary

Name(UserID)	Extension	Mailbox	Size(minutes)
C fxs (Cfxs)	303	Enabled	12
D fxs (Dfxs)	304	Enabled	12
B fxs (Bfxs)	302	Enabled	12
A fxs (Afxs)	301	Enabled	12
c ip (cip)	202	Enabled	12
b ip (bip)	201	Enabled	12
a ip (aip)	203	Enabled	12

Total Rows: 7

**: Row marked for deletion

Mailbox Parameters of C fxs (Cfxs)

☑ Select/De-select to Create/Delete Voicemail

Extension: 303

Type: Personal

Step 3: Test Intercom by pressing the intercom button on ACIPC

Step 4: For the next two steps you need to work with your 'partner' POD. **(This has already been done for you:** Connect an analog cable from FXO port 0/1/0 (on your POD), to the FXS port 0/0/3 (on the partner's POD). Configure the CFNA timer on the analog FXS ports to 20 seconds. Run the test below and then reverse the ports between the two PODs.

a. From the partner's POD call x304– this should ring x201 on your POD.

⚠ **POD CLEAN UP**

Once this exercise is completed and testing done with the buddy pod, please close all instances of CIPC and reset the UC520 and CUE to factory default settings using the CLI procedure in Appendix A.

Exercise-2: PBX, VOICEMAIL/AUTO ATTENDANT

Introduction:

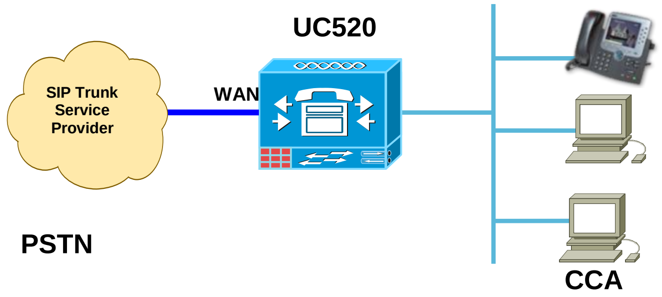
The UC520 supports two voice system configuration types – PBX and Key System. This exercise focuses on the PBX system configuration. A typical PBX system involves an Auto Attendant that handles incoming calls from a PSTN line (e.g. Analog FXO trunks) and transfers the caller to one of the internal extensions. Outbound Local, Long Distance, and International calls are routed out through a PSTN line. In addition, local extensions have voicemail boxes messages can be left.

Objective:

The main objective of this exercise is to configure the basic PBX system, voicemail and Auto Attendant features. These features will be configured using the Cisco Configuration Assistant (CCA). After completion of this exercise, you will be able to setup the SBCS system as a PBX, place calls between extensions, and configure a SIP Trunk on the UC520 to a Service Provider (Lab Simulation), and place calls in & out to the PSTN via the SIP trunk.

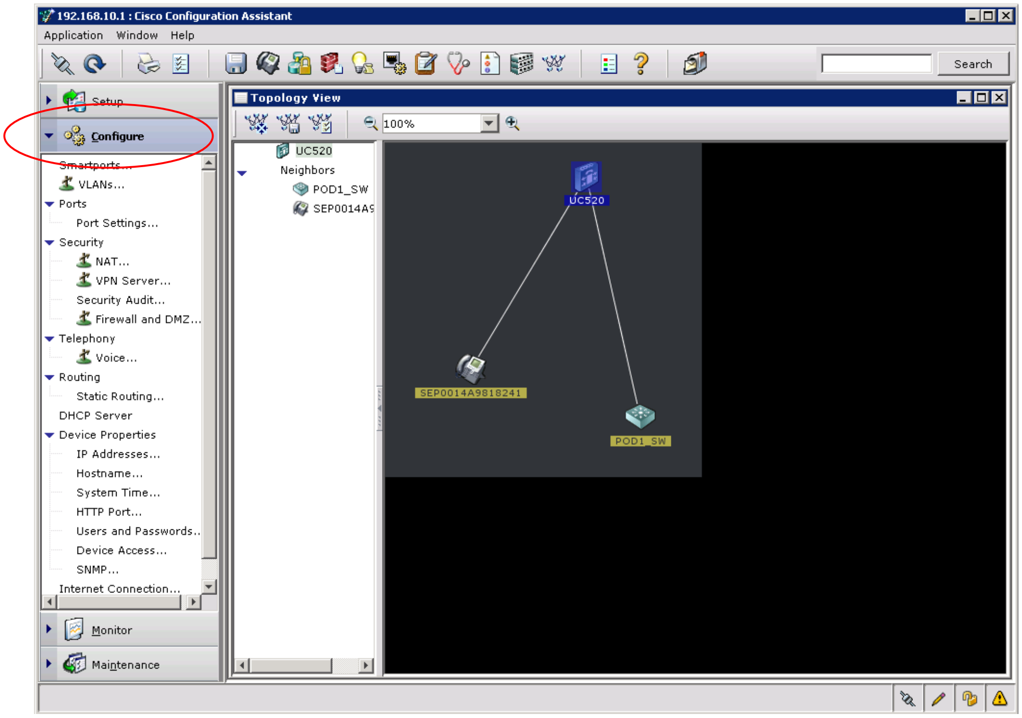
Note: Due to the virtual nature of this exercise, although you will configure the SIP trunk, you will not be able to test the SIP functionality.

Topology:



Setup steps:
Launch CIPC on both workstations and use the CIPC that displays extension 203 for the remainder of this exercise.
Launch Cisco Configuration Assistant, connect to the created community and enter the username and password (cisco/cisco), let it discover the network and connected devices.

Step 1: Close the error message that is received in this lab re: Adobe flash player. If the Telephony Wizard appears, close that as well. Take a moment to identify objects in the Topology view and also note the menu options available with this version from the left menu pain.



NOTE: Each Pod's topology should be similar to the screen shot in Exercise2 step 18 (above). The CIPC device will not show in the topology view. (Where the virtual device is plugged in, such as behind an IP Phone or not, the device will or will not be shown in the topology view.)

The Switch shown is the lab Switch being used to simulate the Internet. The IP phones will appear in the Telephony configuration menu further in the lab.

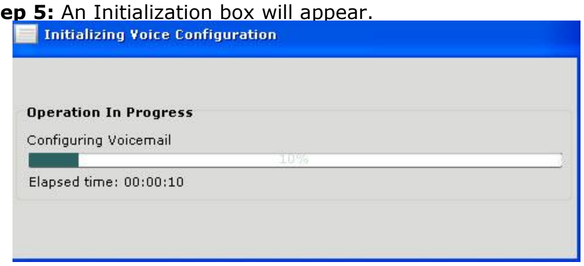
Step 2: Select Configure → Telephony → Region from the menus on the left side.

Step 3: A message will appear asking for the initialization of the system. For this lab choose PBX for the System Mode.

Step 4: Leave the default of 3 for the Digits per Extension. Enter 401 for the Voicemail Access Extension. Click OK.

Note: Voicemail can be configured in the Telephony → Voicemail tab as well.

Step 5: An Initialization box will appear.



Initializing Voice Configuration

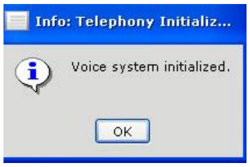
Operation In Progress

Configuring Voicemail

10%

Elapsed time: 00:00:10

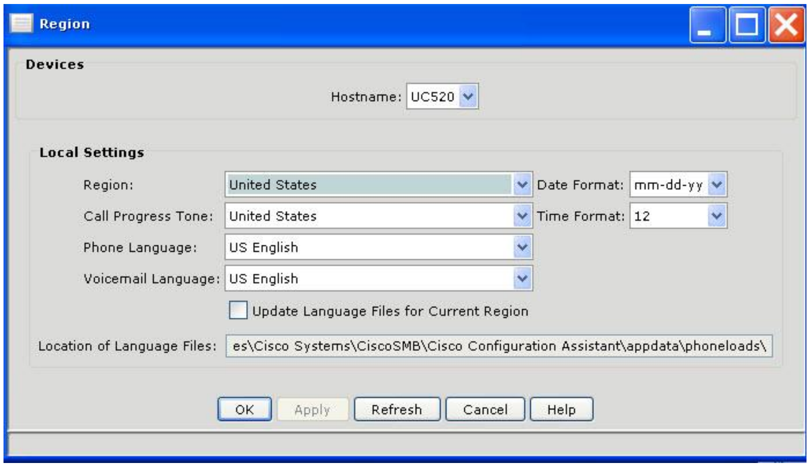
Step 6: When the system is ready a pop-up box will appear stating the voice system is initialized. Click OK.



Info: Telephony Initializ...

Voice system initialized.

Step 7: Set the regional information for the UC520 according to the correct switch location. For US leave the default information as configured. Click OK.



Region

Devices

Hostname: UC520

Local Settings

Region: United States

Date Format: mm-dd-yy

Call Progress Tone: United States

Time Format: 12

Phone Language: US English

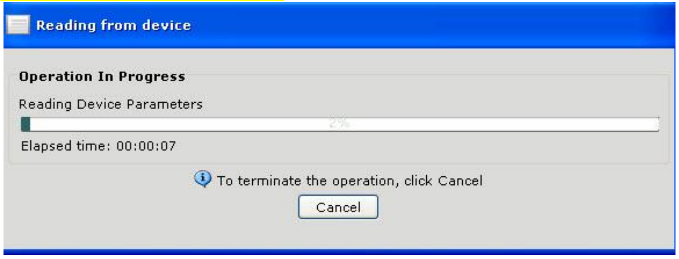
Voicemail Language: US English

□ Update Language Files for Current Region

Location of Language Files: es\Cisco Systems\CiscoSMB\Cisco Configuration Assistant\appdata\phoneloads\

NOTE: Do NOT continue until the Apply and Refresh buttons are available. If they are grayed out, CCA is updating information on the UC520.

Step 8: A window will pop up that the system is updating the UC520 configuration. Wait until the system is ready to configure.


Reading from device

Operation In Progress

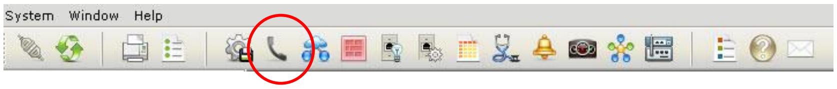
Reading Device Parameters

2%

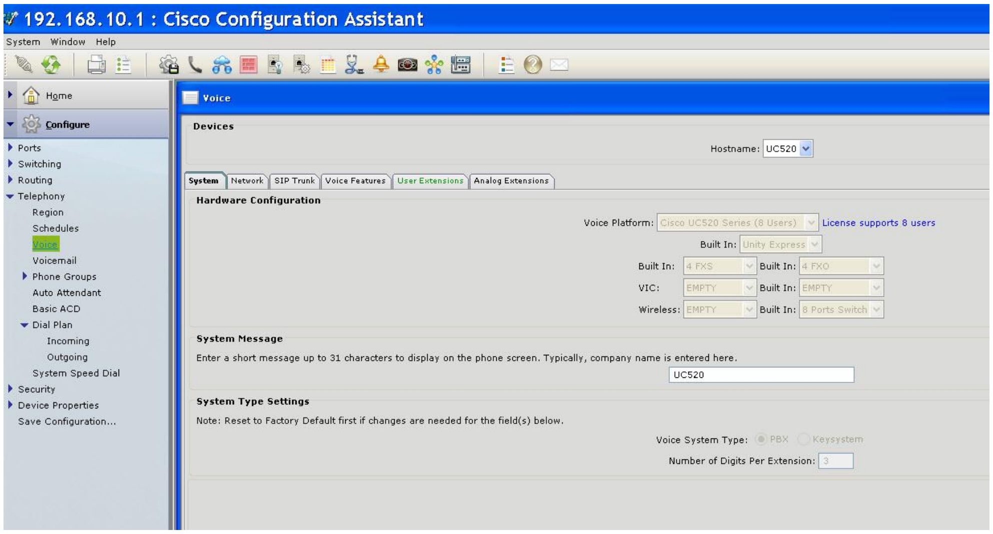
Elapsed time: 00:00:07

To terminate the operation, click Cancel

Step 9: Select Configure → Telephony → Voice from the menus on the left or alternatively click the Phone icon on the top menu bar.



Step 10: In the initial System Tab note the hardware that is in the UC520 in the lab. Also note that the System settings that were configured initially are stored here. All those options are grayed out as they cannot be changed. (To change from PBX to Keysystem requires a reset to factory default.)


192.168.10.1 : Cisco Configuration Assistant

Voice

Devices

Hostname: UC520

Hardware Configuration

Voice Platform: Cisco UC520 Series (8 Users) License supports 8 users

Built In: Unity Express

Built In: 4 FXS Built In: 4 FXO

VIC: EMPTY Built In: EMPTY

Wireless: EMPTY Built In: 8 Ports Switch

System Message

Enter a short message up to 31 characters to display on the phone screen. Typically, company name is entered here.

UC520

System Type Settings

Note: Reset to Factory Default first if changes are needed for the field(s) below.

Voice System Type: ● PBX ○ Keysystem

Number of Digits Per Extension: 3

Step 11: Change the System Message to *UC520-PODxx* (replace 'xx' with your pod number). The System Message is displayed on all phones and can be the business name or any other message.

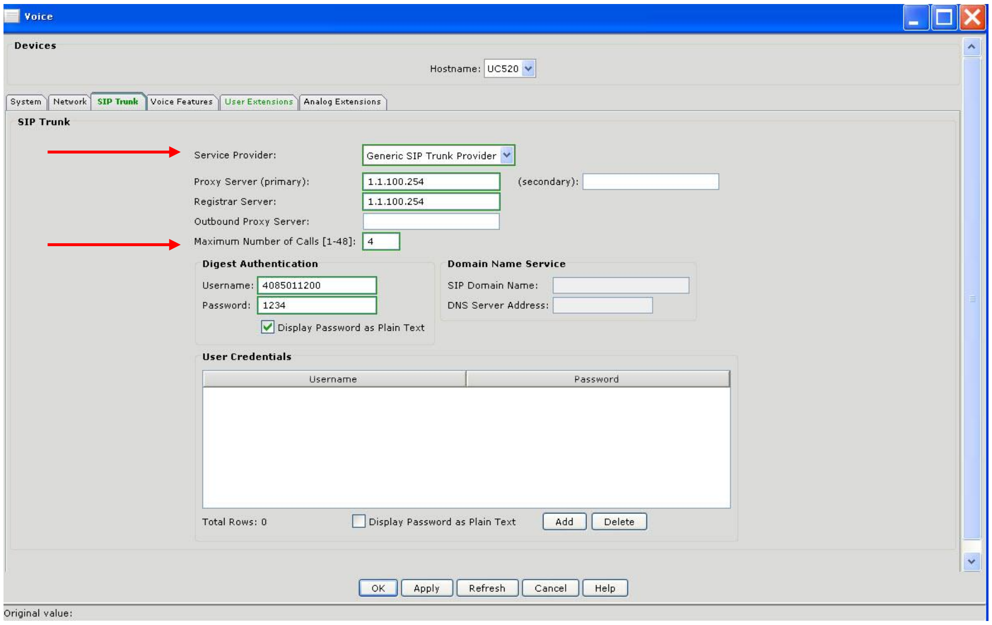
Note: Don't click on 'OK' or 'Apply' until all required tabs are configured.

Step 12: Click on the SIP Trunk tab to configure the UC520 for SIP trunking to a Service Provider for PSTN access.
Step 13: Select Generic SIP Trunk Provider from the Service Provider pull down menu.

Step 14: Set the Registrar Server and Proxy server fields with: 1.1.100.254. This is the SIP PSTN network setup in this exercise.

Step 15: Under Digest Authentication set the username to 4085xx1200 and the password to 1234. (Where XX is your pod number.)

Step 16: Set Maximum Number of Calls to 4. This parameter controls the number of concurrent calls supported across the SIP trunk. If the maximum is exceeded, depending on the dial plan configuration, the outbound call may be blocked or may rollover to a secondary PSTN trunk.



Hostname: UC520

SIP Trunk

Service Provider: Generic SIP Trunk Provider

Proxy Server (primary): 1.1.100.254 (secondary):

Registrar Server: 1.1.100.254

Outbound Proxy Server:

Maximum Number of Calls [1-48]: 4

Digest Authentication

Username: 4085011200

Password: 1234

☑ Display Password as Plain Text

Domain Name Service

SIP Domain Name:

DNS Server Address:

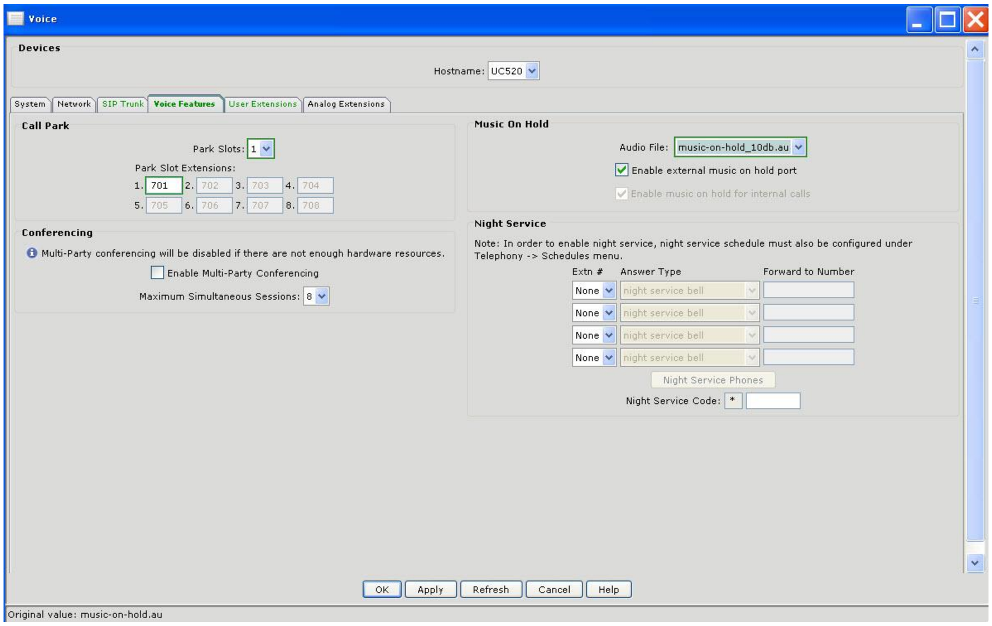
User Credentials

Username	Password

Total Rows: 0 □ Display Password as Plain Text Add Delete

Original value:

Step 17: Select the Voice Features tab. Choose a different Music on Hold audio file from the drop-down menu. The UC500 7.0.3 software pack ships with two different music-on-hold files at different volume levels.



Devices

Hostname: UC520

Call Park

Park Slots: 1

Park Slot Extensions:

1. 701 2. 702 3. 703 4. 704

5. 705 6. 706 7. 707 8. 708

Conferencing

Multi-Party conferencing will be disabled if there are not enough hardware resources.

☐ Enable Multi-Party Conferencing

Maximum Simultaneous Sessions: 8

Music On Hold

Audio File: music-on-hold_10db.au

☑ Enable external music on hold port

☑ Enable music on hold for internal calls

Night Service

Note: In order to enable night service, night service schedule must also be configured under Telephony -> Schedules menu.

Extn #	Answer Type	Forward to Number
None	night service bell	
None	night service bell	
None	night service bell	
None	night service bell	

Night Service Code: *

Original value: music-on-hold.au

Step 18: Select 1 for number of Park Slots. The first Park Slot Extension is 701.

Note: Multi-Party (Ad-hoc and Meet me) Conferencing can be configured. This will be explored in more detail in the Advanced Lab.

Step 19: Click on the User Extensions tab. Configure the users as outlined below.

a. For all the Analog Phones (none connected but configured by default on the UC520):

i. Configure the userid as afxs, bfxs, cfxs, dfxs.

ii. Set the passwords to 1234.

b. For all the CIPC Phones:

i. Configure the LastName for all CIPC phones as cipc.

ii. Configure the FirstName as a, or b.

iii. Configure the userid as aip, bip.

iv. Set the passwords to 1234.

v. Note Call Forward No Answer and Call Forward Busy are set to forward calls to 401 the configured Voicemail extension.

vi. Set Permissions to National. Make sure Block restricted number is checked.

vii. On Button number 2 set the Intercom with mute to user bipc. Set the target intercom button number as 2 and click OK.

c. For the 7960 phone:

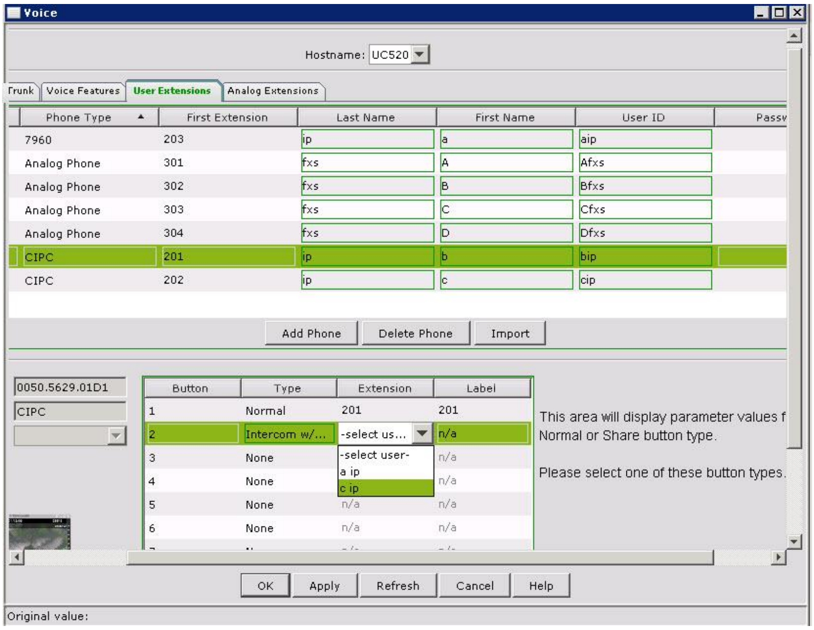
i. Configure the LastName for all the phones as ip.

ii. Configure the FirstName as c.

iii. Configure the userid as cip.

iv. Set the passwords to 1234.

i. Set Permissions to International. Ensure Block restricted number is checked.



Hostname: UC520

Phone Type	First Extension	Last Name	First Name	User ID	Passw
7960	203	ip	a	aip	
Analog Phone	301	fxs	A	Afxs	
Analog Phone	302	fxs	B	Bfxs	
Analog Phone	303	fxs	C	Cfxs	
Analog Phone	304	fxs	D	Dfxs	
CIPC	201	ip	b	bip	
CIPC	202	ip	c	cip	

0050.5629.01D1

CIPC

Button	Type	Extension	Label
1	Normal	201	201
2	Intercom w/...	-select us...	n/a
3	None	-select user-	n/a
4	None	a ip	n/a
5	None	c ip n/a	n/a
6	None	n/a	n/a

This area will display parameter values f Normal or Share button type.

Please select one of these button types.

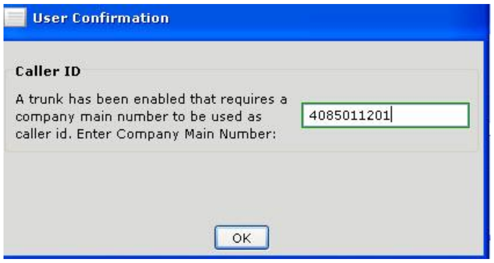
Original value:

d. For the BCIPC phone

i. Set Permissions to National. Do not check Block restricted number.

ii. Verify intercom is configured on button 2 to connect with user aipc.

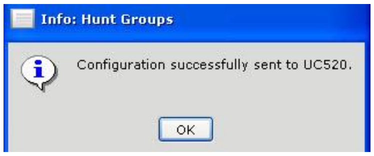
Step 20: Click OK at the bottom of the screen. A message will pop up prompting for the company main number. Enter 4085XX1201 (where XX is your pod number.) Click OK.



Caller ID

A trunk has been enabled that requires a company main number to be used as caller id. Enter Company Main Number: 4085011201

Step 21: Click OK when the ‘Configuration successfully sent to UC520’ message box pops up.



Info: Hunt Groups

Configuration successfully sent to UC520.

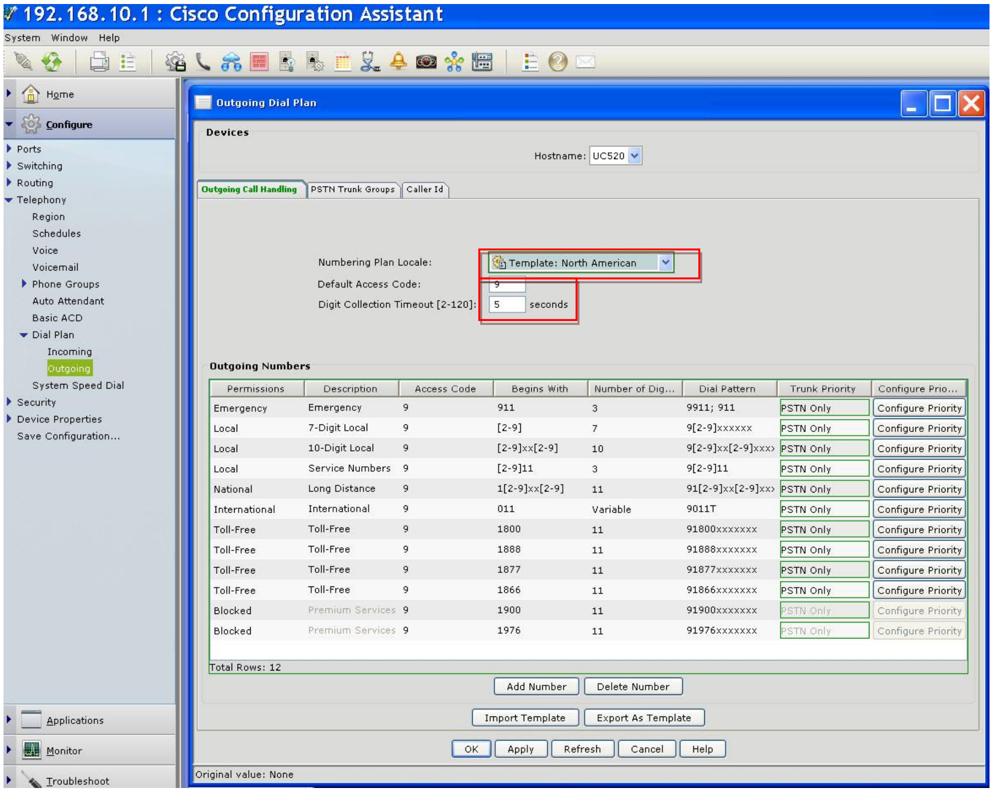
Note: If you want to save the CCA configuration you can by clicking on the 'Save' icon at the top of CCA. Select All Devices if requested to specify which devices to save.

System Feature Outbound Call Handling:

Step 22: Select the Configure → Telephony → Dial Plan → Outgoing menu. Choose the Outgoing Call Handling Tab. This will show the entire dial plan for the selected template. Set the numbering plan locale to the destination region for the UC520.

The following are the defaults for North American dialing:

Numbering Plan Locale	Template: North American
Default Access Code	9
Digit Collection Timeout	5



192.168.10.1 : Cisco Configuration Assistant

Hostname: UC520

Numbering Plan Locale: Template: North American

Default Access Code: 9

Digit Collection Timeout [2-120]: 5 seconds

Outgoing Numbers

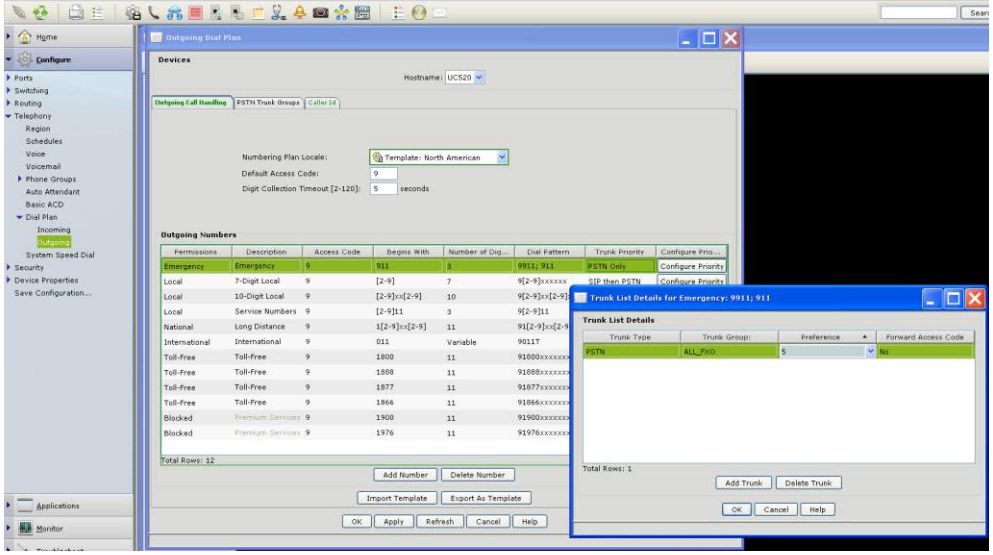
Permissions	Description	Access Code	Begins With	Number of Dig...	Dial Pattern	Trunk Priority	Configure Prio...
Emergency	Emergency	9	911	3	9911; 911	PSTN Only	Configure Priority
Local	7-Digit Local	9	[2-9]	7	9[2-9]xxxxxx	PSTN Only	Configure Priority
Local	10-Digit Local	9	[2-9]xx[2-9]	10	9[2-9]xx[2-9]xxx›	PSTN Only	Configure Priority
Local	Service Numbers	9	[2-9]11	3	9[2-9]11	PSTN Only	Configure Priority
National	Long Distance	9	1[2-9]xx[2-9]	11	91[2-9]xx[2-9]xx›	PSTN Only	Configure Priority
International	International	9	011	Variable	9011T	PSTN Only	Configure Priority
Toll-Free	Toll-Free	9	1800	11	91800xxxxxxx	PSTN Only	Configure Priority
Toll-Free	Toll-Free	9	1888	11	91888xxxxxxx	PSTN Only	Configure Priority
Toll-Free	Toll-Free	9	1877	11	91877xxxxxxx	PSTN Only	Configure Priority
Toll-Free	Toll-Free	9	1866	11	91866xxxxxxx	PSTN Only	Configure Priority
Blocked	Premium Services	9	1900	11	91900xxxxxxx	PSTN Only	Configure Priority
Blocked	Premium Services	9	1976	11	91976xxxxxxx	PSTN Only	Configure Priority

Total Rows: 12

Original value: None

Step 23: Modify the emergency numbers to route to the PSTN only. Select the emergency number 911, under the trunk priority select PSTN only and click OK. Configure Preference to 1 (the highest.)

NOTE: By default, if a SIP trunk is configured all outbound calls will be routed to SIP trunk first, followed by the PSTN.



Hostname: UC520

Numbering Plan Locale: Template: North American

Default Access Code: 9

Digit Collection Timeout [2-120]: 5 seconds

Outgoing Numbers

Permissions	Description	Access Code	Begins With	Number of Dig...	Dial Pattern	Trunk Priority	Configure Prio...
Emergency	Emergency	9	911	3	9911; 911	PSTN Only	Configure Priority
Local	7-Digit Local	9	[2-9]	7	9[2-9]xxxxxx	SIP then PSTN	Configure Priority
Local	10-Digit Local	9	[2-9]xx[2-9]	10	9[2-9]xx[2-9]		
Local	Service Numbers	9	[2-9]11	3	9[2-9]11		
National	Long Distance	9	1[2-9]xx[2-9]	11	91[2-9]xx[2-9		
International	International	9	011	Variable	9011T		
Toll-Free	Toll-Free	9	1800	11	91800xxxxxxx		
Toll-Free	Toll-Free	9	1888	11	91888xxxxxxx		
Toll-Free	Toll-Free	9	1877	11	91877xxxxxxx		
Toll-Free	Toll-Free	9	1866	11	91866xxxxxxx		
Blocked	Premium Services	9	1900	11	91900xxxxxxx		
Blocked	Premium Services	9	1976	11	91976xxxxxxx		

Total Rows: 12

Trunk List Details for Emergency: 9911; 911

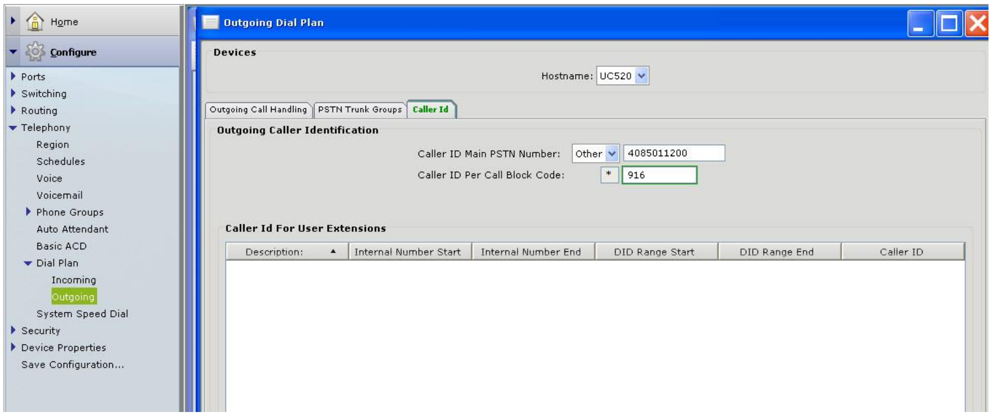
Trunk List Details

Trunk Type	Trunk Group:	Preference	Forward Access Code
PSTN	ALL_FXO	5	No

Total Rows: 1

NOTE: This option allows specifying of the caller ID for outbound calls from the SIP, ISDN, BRI and PRI trunks. Note that the caller ID for the FXO trunks is determined by the telco service provider and cannot be modified from CCA or the UC500.

Step 25: For the Caller ID block code use the 916 and click OK.



Hostname: UC520

Outgoing Caller Identification

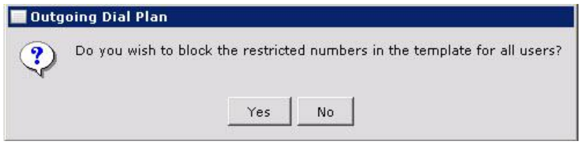
Caller ID Main PSTN Number: Other 4085011200

Caller ID Per Call Block Code: * 916

Caller Id For User Extensions

Description:	Internal Number Start	Internal Number End	DID Range Start	DID Range End	Caller ID

Step 26: A message will come up asking to block the restricted number for all users. Click yes.



Outgoing Dial Plan

Do you wish to block the restricted numbers in the template for all users?

Step 27: A message will be received that configuration was saved to the UC520.

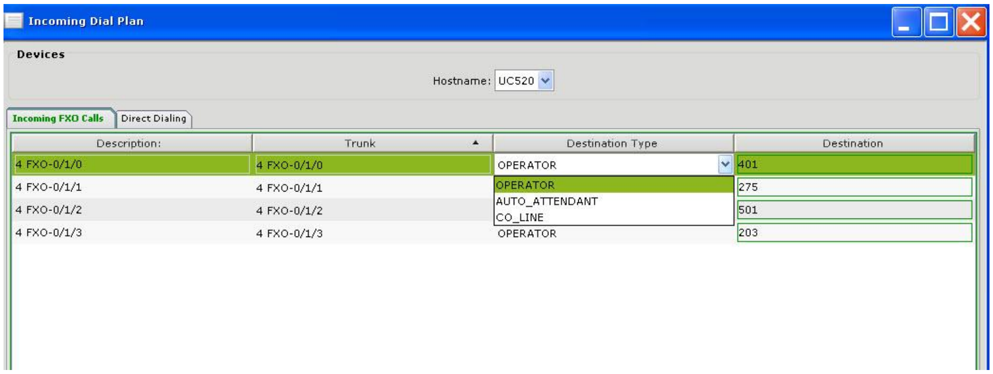
Systems feature – Incoming call handling

CCA can configure the desired call flow for incoming calls. Using this feature incoming calls can be directed to a hunt-group, shared line, auto attendant, or any other desired destination.

Step 28: Click on the Configure button for Incoming Numbers. Select Configure → Telephony → Dial Plan → Incoming.

Step 29: Incoming Call Handling → FXO Trunk Destination is set to Operator. The FXO destination can also be set to Auto Attendant pilot once it has been configured. Configure the FXO ports as follows:

FXO port 0/1/0: 401
FXO port 0/1/1: 275
FXO port 0/1/2: 501
FXO port 0/1/3: 203



Incoming Dial Plan

Devices

Hostname: UC520

Description:	Trunk	Destination Type	Destination
4 FXO-0/1/0	4 FXO-0/1/0	OPERATOR	401
4 FXO-0/1/1	4 FXO-0/1/1		275
4 FXO-0/1/2	4 FXO-0/1/2		501
4 FXO-0/1/3	4 FXO-0/1/3	OPERATOR	203

Step 30: Click OK on the FXO port configuration window. A pop-up window verifying that configuration has been sent to the UC500 will appear.

This step is greyed out as it cannot be performed in the lab.
Step 31: Verify the functionality. Use an analog cable to connect the FXO port on the UC500 to the FXS port on the next pod's UC500 (Increase the CFNA timer on the FXS ports using CCA).

– Calls to the port 0/1/0 should be directed to the Auto Attendant
– Calls to the port 0/1/1 should be directed to the IP Phones that have shared line 275
– Calls to the port 0/1/2 should be directed to the 501 hunt-group, unanswered calls are forwarded to AA
– Calls to the port 0/1/3 should be directed to the operator at extension 203

Step 32: Click on the Dial Plan → Incoming → Direct Dialing Tab. This feature will be used to add the PSTN DID numbers to two of the IP phone users. It may be helpful to maximize this window so additional headings are displayed.

Step 33: Click on Add in the Direct Dial to User Extension area.

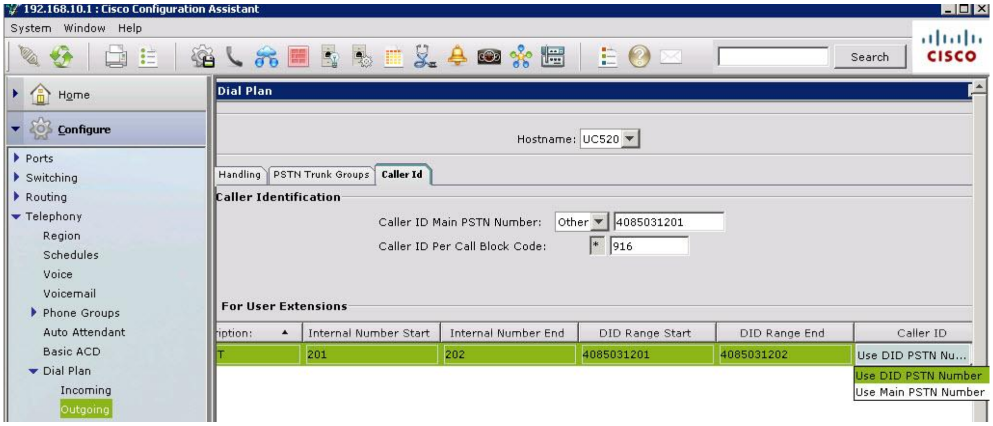
Step 34: Click in the Description text box and enter SIPPSTN.

Step 35: Enter the starting DID range as 4085xx1201 and ending as 4085xx1202.

Step 36: Enter the starting Internal Extension range as 201 and ending as 202.

Step 37: Verify that SIP Trunk is selected. Click OK to save the changes.

Step 38: Go back to the Dial Plan → Outbound → Caller ID tab and select 'Use DID PSTN Number' for the SIPPSTN trunk for Caller ID and then click OK.



Hostname: UC520

Caller Identification

Caller ID Main PSTN Number: Other 4085031201

Caller ID Per Call Block Code: * 916

For User Extensions

ription: ▲	Internal Number Start	Internal Number End	DID Range Start	DID Range End	Caller ID
T	201	202	4085031201	4085031202	Use DID PSTN Nu...

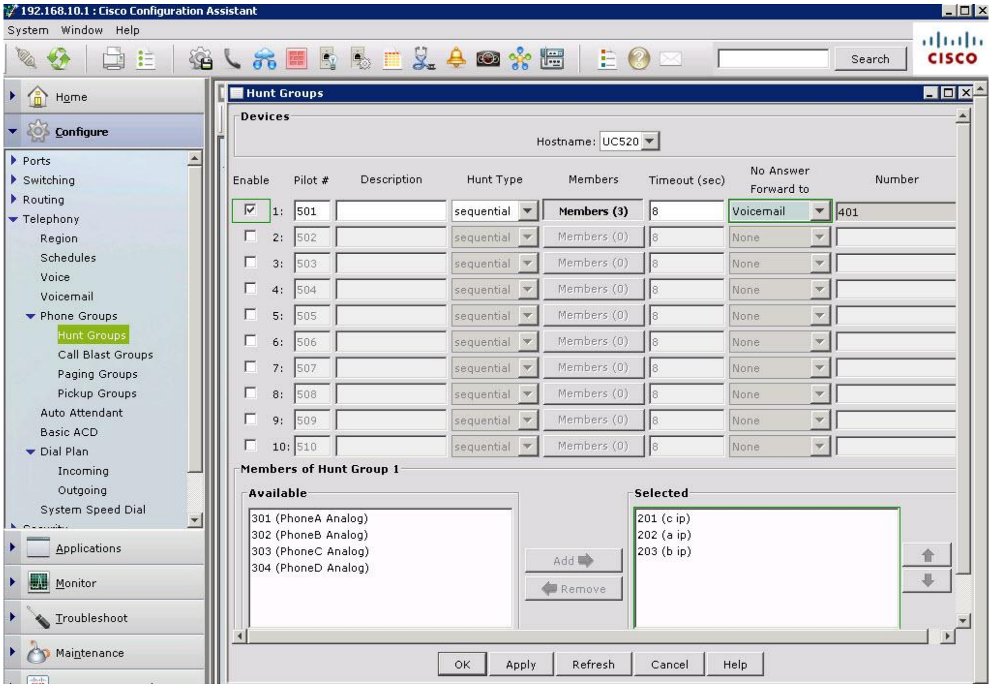
Use DID PSTN Number
Use Main PSTN Number

By selecting this option, outbound calls from extension 201 will show called ID of 4085xx1201 and calls from 202 will show 4085xx1202. Calls from all other extensions will show the main PSTN caller ID, configured in step 10. If you select "Use Main PSTN number" for Caller ID, all outbound calls on SIP or BRI/PRI trunks will show the main PSTN number as the caller ID

Hunt group Configuration:

Hunt groups create a shared line appearance on specified phones that hunts for members of the hunt group based on configured parameters. Phones in a hunt group can ring based on a configured sequence, based on longest idle time or in a peer fashion. If no member of the hunt group is available to take the call, behaviors can be configured for forwarding the call or sending the caller to voicemail.

Step 39: Open the Telephony → Phone Groups → Hunt Groups menu. Enable the first hunt group (#501). Leave the hunt group type as sequential. Add all three IP phones to the hunt group. Select 'Forward to Voicemail' on no answer. Click OK to save the configuration.



Hostname: UC520

Enable	Pilot #	Description	Hunt Type	Members	Timeout (sec)	No Answer Forward to	Number
☑ 1:	501		sequential	Members (3)	8	Voicemail	401
□ 2:	502		sequential	Members (0)	8	None	
□ 3:	503		sequential	Members (0)	8	None	
□ 4:	504		sequential	Members (0)	8	None	
□ 5:	505		sequential	Members (0)	8	None	
□ 6:	506		sequential	Members (0)	8	None	
□ 7:	507		sequential	Members (0)	8	None	
□ 8:	508		sequential	Members (0)	8	None	
□ 9:	509		sequential	Members (0)	8	None	
□ 10:	510		sequential	Members (0)	8	None	

Members of Hunt Group 1

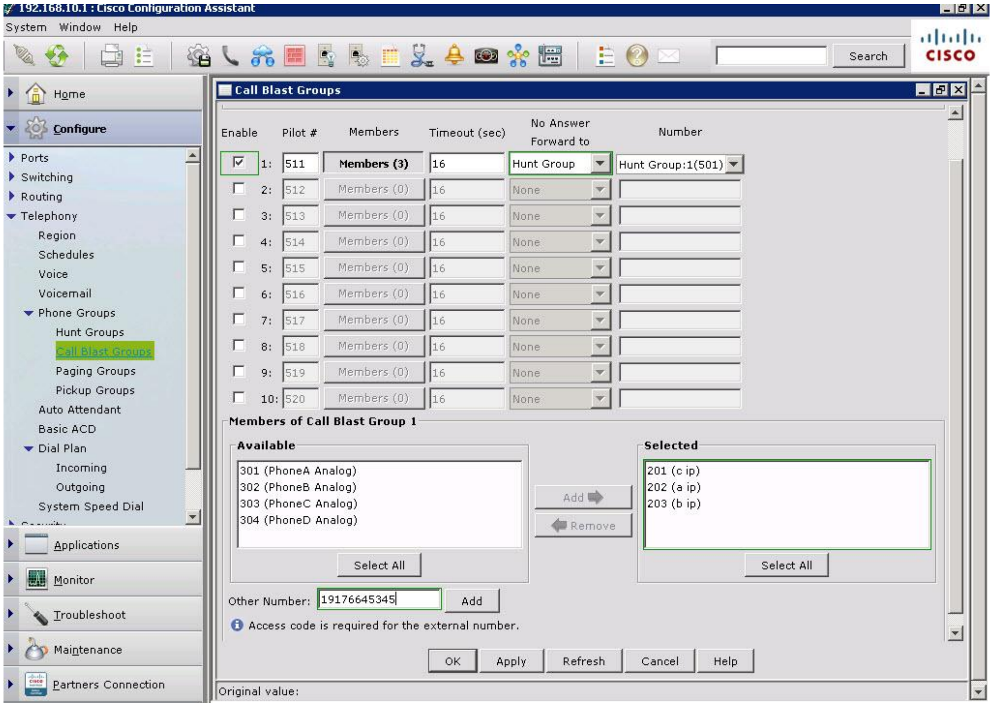
Available	Selected
301 (PhoneA Analog)	201 (c ip)
302 (PhoneB Analog)	202 (a ip)
303 (PhoneC Analog)	203 (b ip)
304 (PhoneD Analog)	

Step 40: Click OK when the 'Configuration successfully sent to UC520' message box pops up.

Call Blast Group Configuration:

Call blast groups are a type of hunt group and as such members of the group share a common line appearance on their phones. When the extension is called ALL members of the blast group will be contacted. If no member of the blast group is available to take the call, behaviors can be configured for forwarding the call or sending the caller to voicemail.

Step 41: Open the Telephony → Phone Groups → Phone Blast Groups menu. Enable the first Blast group (extension 511). Add all IP phones to the Blast group. Enter the number '19176645345' into the other number on the bottom of the screen. Add that number to the members of the blast group. On no answer forward calls to the hunt group 501. Click OK to save the configuration.



Call Blast Groups

Enable		Pilot #	Members	Timeout (sec)	No Answer Forward to	Number
☑	1:	511	Members (3)	16	Hunt Group	Hunt Group:1(501)
□	2:	512	Members (0)	16	None	
□	3:	513	Members (0)	16	None	
□	4:	514	Members (0)	16	None	
□	5:	515	Members (0)	16	None	
□	6:	516	Members (0)	16	None	
□	7:	517	Members (0)	16	None	
□	8:	518	Members (0)	16	None	
□	9:	519	Members (0)	16	None	
□	10:	520	Members (0)	16	None	

Members of Call Blast Group 1

Available:
301 (PhoneA Analog)
302 (PhoneB Analog)
303 (PhoneC Analog)
304 (PhoneD Analog)

Selected:
201 (c ip)
202 (a ip)
203 (b ip)

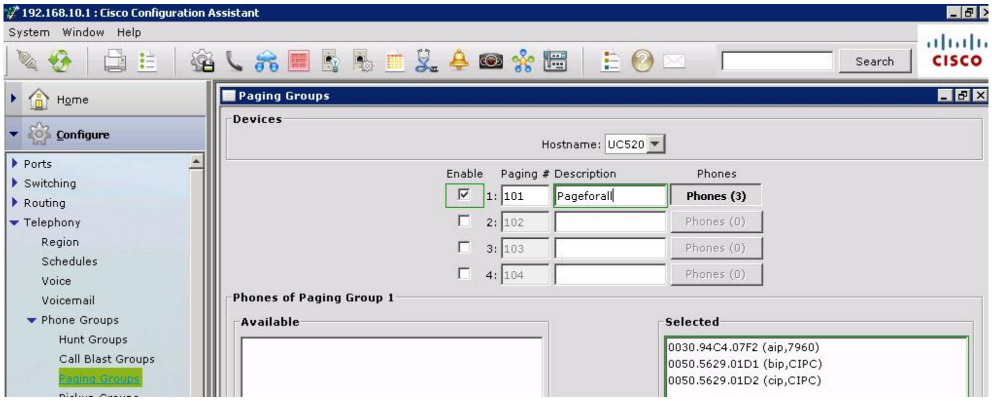
Other Number: 19176645345

Access code is required for the external number.

Original value:

Step 42: Click OK and OK again when the 'Configuration successfully sent to UC520' message box pops up.

Step 43: Open the Telephony → Phone Groups → Paging Groups menu. Enable the first paging group and give it a description. Add all 3 IP phones to the paging group. Click OK.



Paging Groups

Devices

Hostname: UC520

Enable		Paging #	Description	Phones
☑	1:	101	Pageforall	Phones (3)
□	2:	102		Phones (0)
□	3:	103		Phones (0)
□	4:	104		Phones (0)

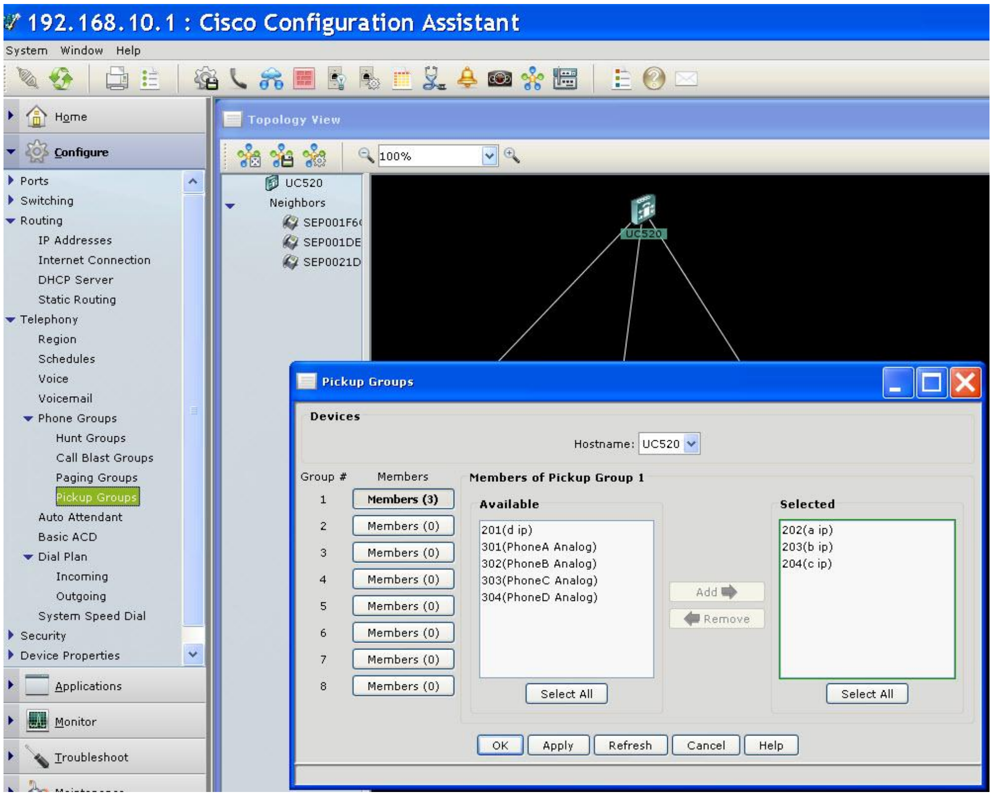
Phones of Paging Group 1

Available:

Selected:
0030.94C4.07F2 (aip,7960)
0050.5629.01D1 (bip,CIPC)
0050.5629.01D2 (cip,CIPC)

Step 44: Click OK when the 'Configuration successfully sent to UC520' message box pops up.

Step 45: Open the Telephony → Phone Groups → Pickup Groups menu. Add the three IP phones as members of the first pickup group. Click OK to save the configuration.



Hostname: UC520

Group #	Members
1	Members (3)
2	Members (0)
3	Members (0)
4	Members (0)
5	Members (0)
6	Members (0)
7	Members (0)
8	Members (0)

Members of Pickup Group 1

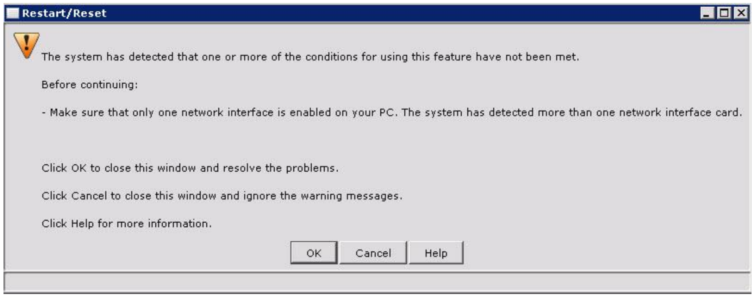
Available:
201(d ip)
301(PhoneA Analog)
302(PhoneB Analog)
303(PhoneC Analog)
304(PhoneD Analog)

Selected:
202(a ip)
203(b ip)
204(c ip)

Step 46: Click OK when the 'Configuration successfully sent to UC520' message box pops up.

Step 47: To configure a system-wide speed dial click on Configure → Telephony → Dial Plan → System Speed Dial.

Step 48: An error message will appear regarding multiple NICs on the PC. **Click Cancel to ignore this message. Do not disable either NICs on the workstation.**



The system has detected that one or more of the conditions for using this feature have not been met.

Before continuing:

- Make sure that only one network interface is enabled on your PC. The system has detected more than one network interface card.

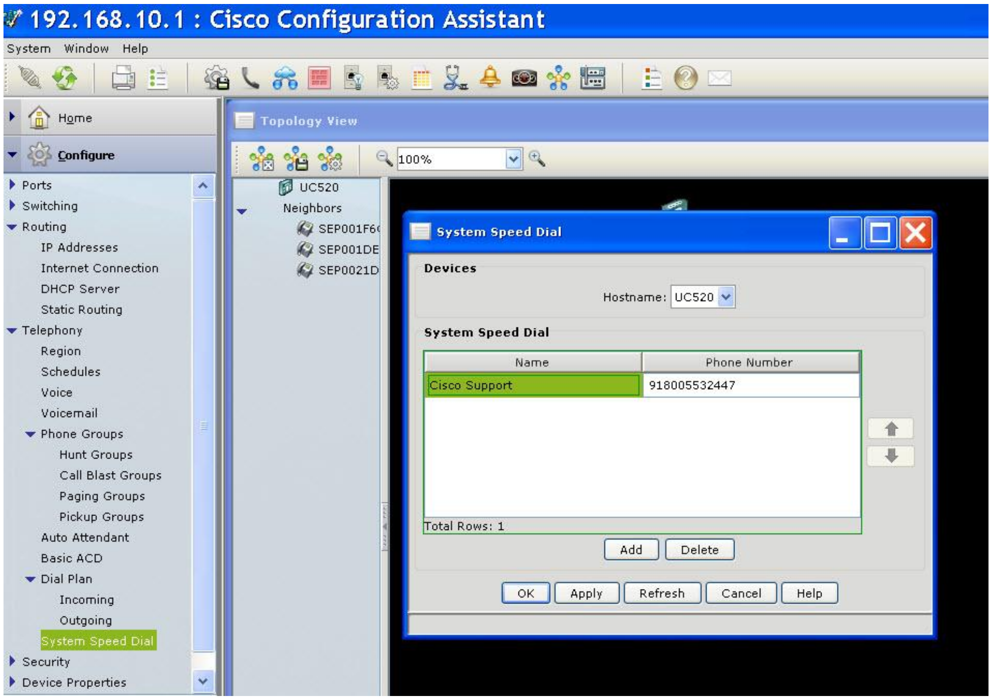
Click OK to close this window and resolve the problems.

Click Cancel to close this window and ignore the warning messages.

Click Help for more information.

NOTE: If this error message appears again in the lab click Cancel every time.

Step 49: Click the "Add" button and configure a name and a corresponding number (eg. Cisco Support, Number: 918005532447). Remember to include the PBX Access code and the long distance prefix for the speed-dial. These parameters are defaulted to 9 and 1 respectively for North American dialing and can be changed in the "Dial Plan" tab. Click OK to apply the configuration.



Hostname: UC520

Name	Phone Number
Cisco Support	918005532447

Total Rows: 1

Configuring WAN Connectivity

Step 1: On the menus on the left under Routing select Internet Connections.

Step 2: In the Internet Connections click on FastEthernet 0/0

Step 3: Click on Modify.

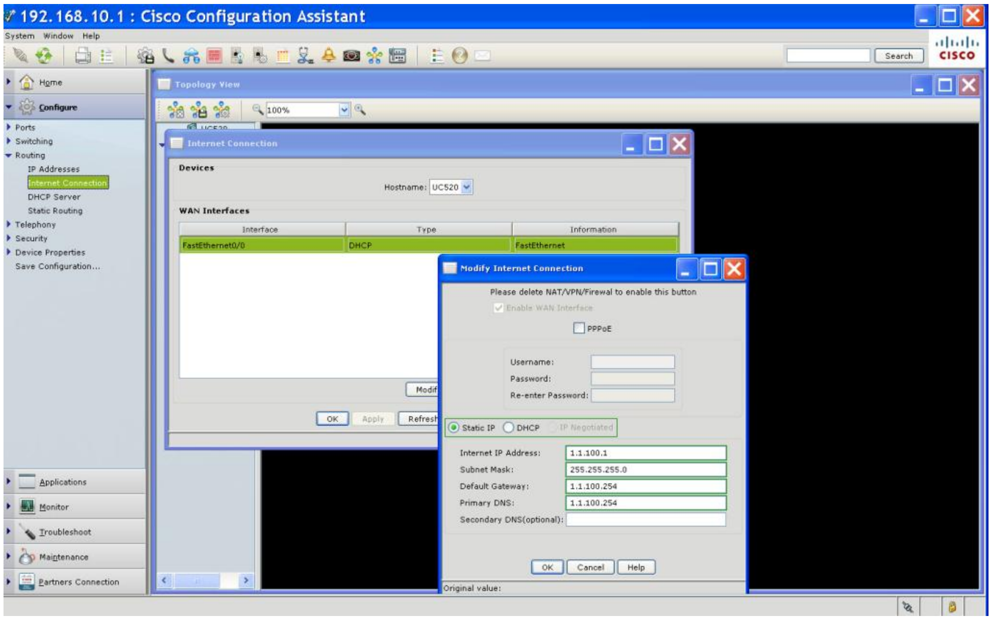
Step 4: In the Modify Internet Connections window select the Static IP radial button.

Step 5: Enter the IP address as 1.1.100.xx ('xx' POD number - drop any leading 0, only enter 1 for POD 01).

Step 6: Enter the Subnet mask as 255.255.255.0.

Step 7: Enter the Default Gateway and Primary DNS as 1.1.100.254.

Step 8: Click OK twice to apply changes.



Internet Connection

Devices

Hostname: UC520

WAN Interfaces

Interface	Type	Information
FastEthernet0/0	DHCP	FastEthernet

Modify | OK | Apply | Refresh

Modify Internet Connection

Please delete NAT/VPN/Firewal to enable this button

☑ Enable WAN Interface

□ PPPoE

Username:
Password:
Re-enter Password:

● Static IP ○ DHCP ○ IP Negotiated

Internet IP Address: 1.1.100.1
Subnet Mask: 255.255.255.0
Default Gateway: 1.1.100.254
Primary DNS: 1.1.100.254
Secondary DNS(optional):

OK | Cancel | Help

Original value:

Verification Steps:

Step 1: On the IP Phones ensure the First Name and the Last Name is visible.

Step 2: Dial the voicemail access number (401) or press the Messages key on each phone and enroll the users. Use 789 as the password.

Note: you will not be able to record a greeting, simply use the default blank greeting.

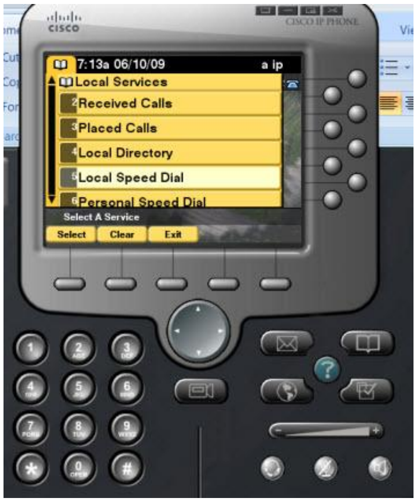
If pressing the voicemail button results in a fast busy go to the Configure → Telephony → Voicemail → Mailbox tab (see figure on page 21) and make sure that all the extensions have voicemail enabled.

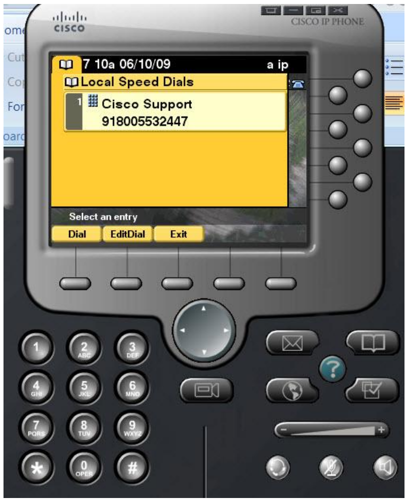
Step 3: Place calls between IP Phones and ensure that calls roll over to VM when not answered.

Step 4: Check that the MWI light turns on when a message is left and check messages. (Messages cannot be left because of the issue with the microphones and drivers.)

Step 5: OPTIONAL: Press "Services" key on the IP Phone and select the "CME Services URL" to launch Voice View Express (VVE). Use the password 789 from step 3 for PIN.
VoiceView Express (VVE) and IMAP exercises are outlined in Appendix B.

Step 6: From any phone, press "*Directory*" key and then select the "*Local Speed Dial*" option (option 5). Verify that the system-wide speed-dial configured in the system tab appears here.





Test the Call Park and Pickup feature

Step 1: Dial extension aipc from extension bipc.

Step 2: Answer the call on extension aipc.

Step 3: Click the More softkey and then click the Park softkey. The call will be placed in the Parked area and music on hold will be audible.

Step 4: Click the Pickup softkey from extension aipc, dial 701 and the call will resume. Ideally the call would be picked up from another extension, however, due to the limited number of phones in this exercise extension 203 is used to test this functionality.

Test the Paging feature

Step 1: From one of the CIPC phones, dial 101.

Step 2: View the other CIPC phone and notice that the IP Communicator is off hook. Initially IP Paging1 will display on the screen.

Test the Intercom feature

Step 1: From ACIPC press the intercom to verify that intercom to line BCIPC works.

Test the hunt-group functionality

Step 1: From any extension dial extension 501 (the hunt-group pilot number).

Step 2: If configured correctly, the call will attempt to call AIP, if no answer, BIP, and then CIP and finally it will go to voicemail.

Test the blast-group functionality

Step 1: From any extension dial 511 (the blast group pilot number).

Step 2: If configured correctly, the call will ring all extensions and if not answered roll-over to 501.

Note: It is NOT necessary to reset the system at the end of this exercise.

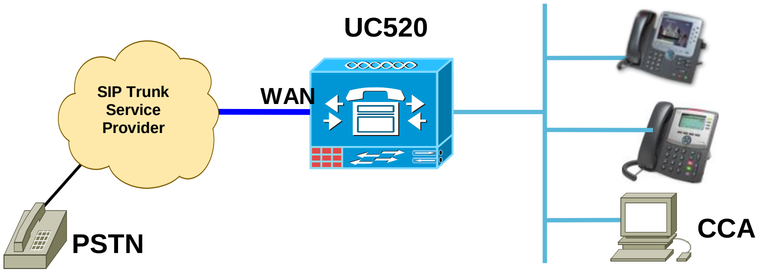
Exercise-3: Business Schedule and Auto Attendant

Introduction:
The UC520 supports Automated Attendant (AA) that can provide flexible call handling. CCA release 1.9 supports an advanced AA system that can meet the need of a typical Small Business. This AA supports a Business Schedule and a Holiday Schedule that enables intelligent time-of-the-day routing. The new enhanced capability includes a multi-menu system and also allows a provision to have multiple Auto Attendant scripts that can be triggered by different incoming DIDs. Finally, the system provides an easy interface for recording AA greetings and helps set up a Greetings Management System that can be used by the end customers to alter the greetings from their IP Phones.

Objective:
The main objective of this lab is to configure a fully functional Auto Attendant system. The lab will focus on a multi-menu AA system which integrates itself with a Business Schedule and a Holiday Schedule. Students will also experience the ease of recording a greeting and the process of setting up a Greetings Management System.

Prerequisite:
This lab requires a basic PBX system to be already in place

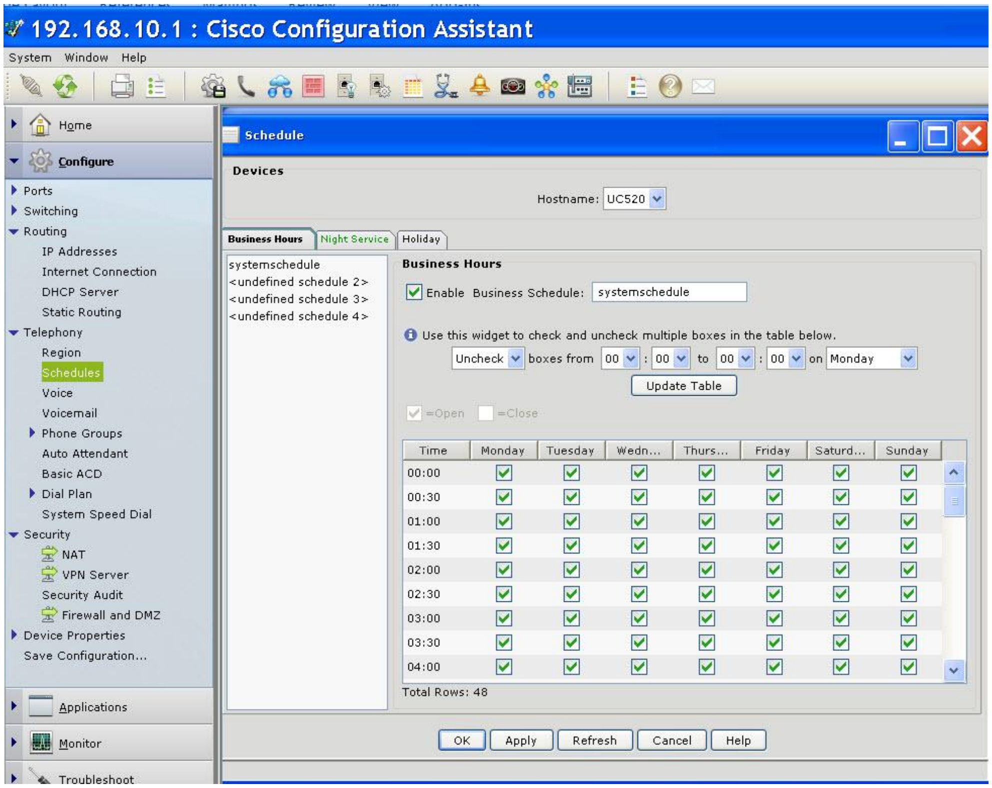
Topology:



Setup steps:

Step 1: Launch Cisco Configuration Assistant (CCA) on your laptop. Please make sure that a basic PBX system is already setup

Step 2: From the left menus, click on Configure > Telephony > Schedules



Hostname: UC520

systemschedule
<undefined schedule 2>
<undefined schedule 3>
<undefined schedule 4>

Business Hours

☑ Enable Business Schedule: systemschedule

Use this widget to check and uncheck multiple boxes in the table below.

Uncheck boxes from 00 : 00 to 00 : 00 on Monday

☑ =Open □ =Close

Time	Monday	Tuesday	Wedn...	Thurs...	Friday	Saturd...	Sunday
00:00	☑	☑	☑	☑	☑	☑	☑
00:30	☑	☑	☑	☑	☑	☑	☑
01:00	☑	☑	☑	☑	☑	☑	☑
01:30	☑	☑	☑	☑	☑	☑	☑
02:00	☑	☑	☑	☑	☑	☑	☑
02:30	☑	☑	☑	☑	☑	☑	☑
03:00	☑	☑	☑	☑	☑	☑	☑
03:30	☑	☑	☑	☑	☑	☑	☑
04:00	☑	☑	☑	☑	☑	☑	☑

Total Rows: 48

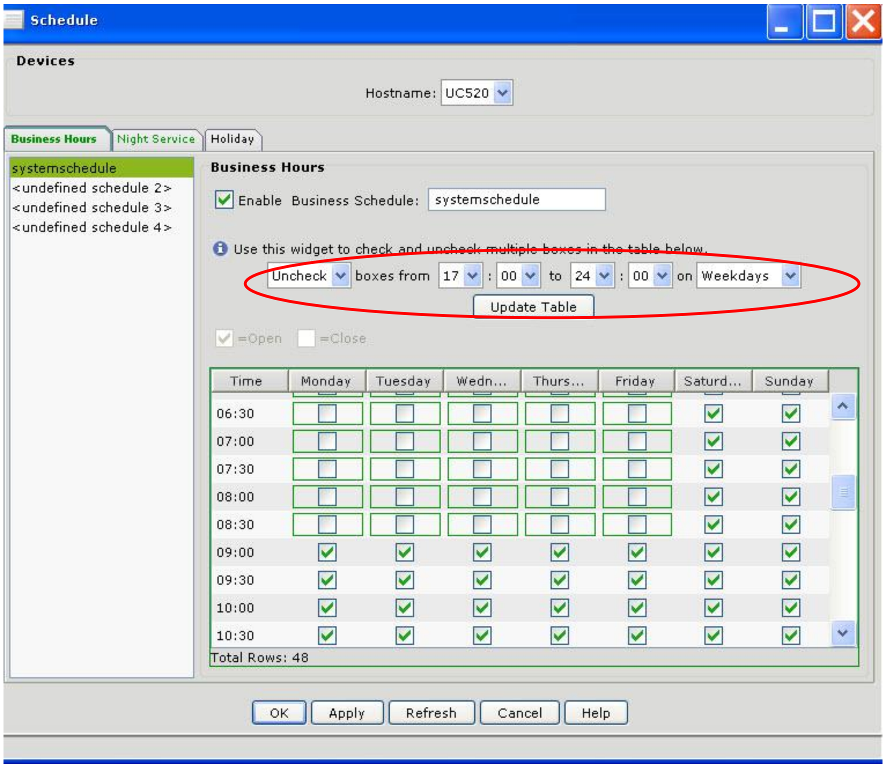
Step 3: Configure the system schedule. Make sure to check the box for Enable Business Schedule.

Step 4: Make sure that you are modifying the systemschedule and from the pull-down select Uncheck boxes from 00:00 to 09:00 for weekdays (this will mark 12am to 9am as closed hours on weekdays). You can also use the widget to uncheck all the boxes for a specific day/time.

Step 5: Click on Update Table. Once, the table is updated, Uncheck boxes from 17:00 to 24:00 for weekdays (this will mark 5pm to 12am as closed hours on weekday).

Step 6: Next, Uncheck boxes from 00:00 to 24:00 for weekends – this will mark the weekends as closed

Step 7: The above steps will set your Business Hours from Monday to Friday 9am to 5pm.



Hostname: UC520

systemschedule
<undefined schedule 2>
<undefined schedule 3>
<undefined schedule 4>

Business Hours

☑ Enable Business Schedule: systemschedule

Use this widget to check and uncheck multiple boxes in the table below.

Uncheck boxes from 17 : 00 to 24 : 00 on Weekdays

Update Table

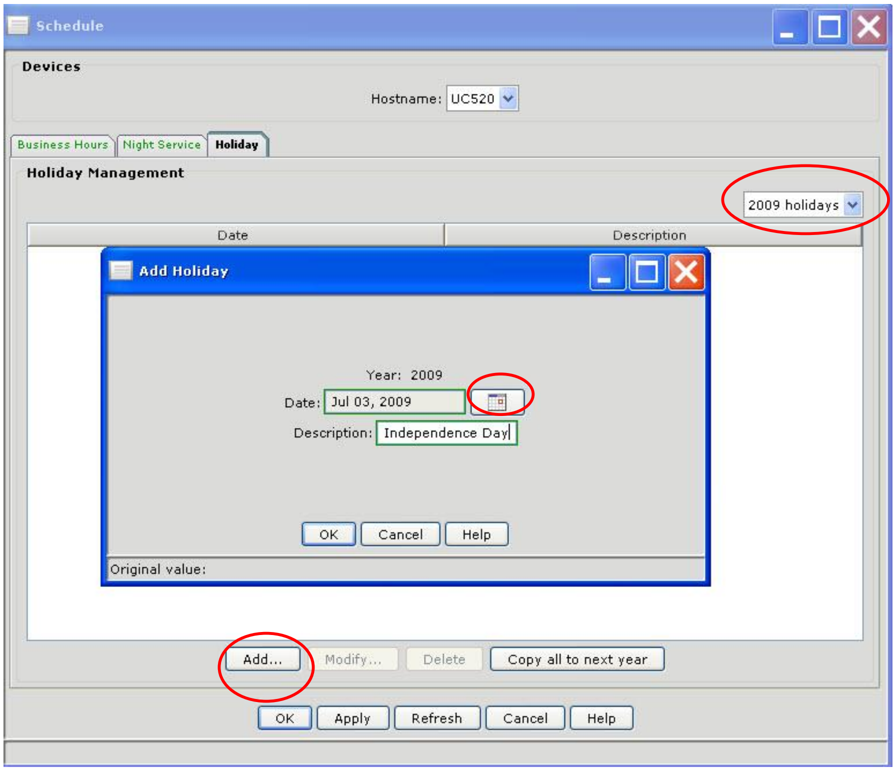
☑ =Open □ =Close

Time	Monday	Tuesday	Wedn...	Thurs...	Friday	Saturd...	Sunday
06:30	□	□	□	□	□	☑	☑
07:00	□	□	□	□	□	☑	☑
07:30	□	□	□	□	□	☑	☑
08:00	□	□	□	□	□	☑	☑
08:30	□	□	□	□	□	☑	☑
09:00	☑	☑	☑	☑	☑	☑	☑
09:30	☑	☑	☑	☑	☑	☑	☑
10:00	☑	☑	☑	☑	☑	☑	☑
10:30	☑	☑	☑	☑	☑	☑	☑

Total Rows: 48

Step 8: Setup the holiday schedule as per the requirement. For this, click on the Holiday tab and on Holiday Management select 2009 holidays.

Step 9: Next, click on the Add button at the bottom of the Holiday Management tab. This will launch as Add Holiday window. In this window, make sure that the year is set to 2009.



Hostname: UC520

2009 holidays

Year: 2009

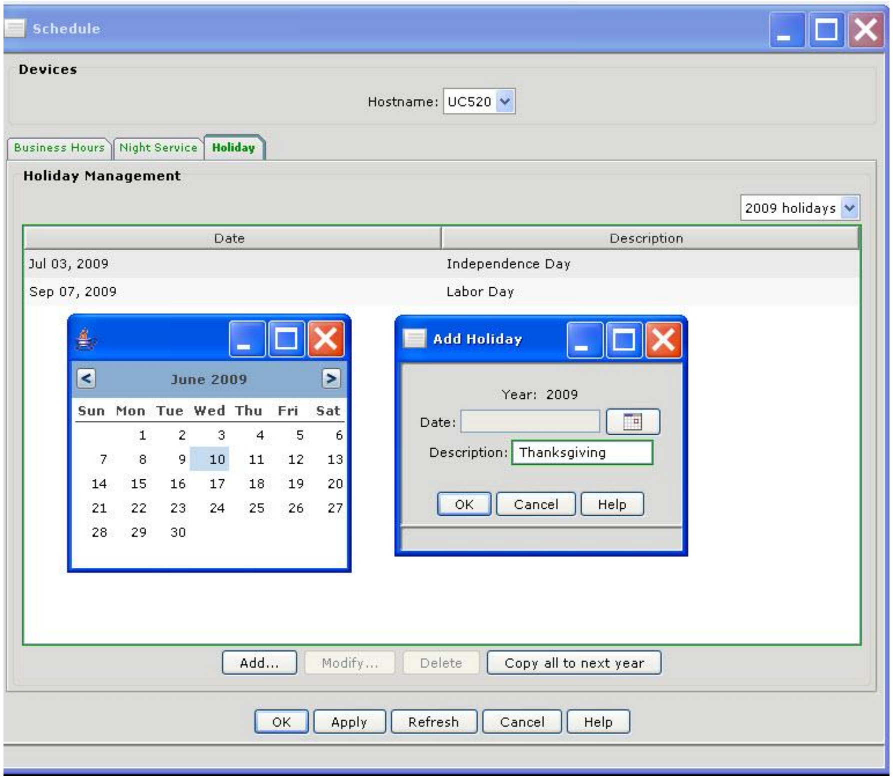
Date: Jul 03, 2009

Description: Independence Day

Original value:

Step 10: Specify ‘Independence Day’ in the description of the holiday that is being added then click on the Date Picker icon. This will Launch a Date Picker window.

Step 11: Set the date to July 3. Using these steps all holidays observed by the company can be added to the schedule. Click on OK to apply the changes. Now the system schedule is set.



Hostname: UC520

Date	Description
Jul 03, 2009	Independence Day
Sep 07, 2009	Labor Day

June 2009

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

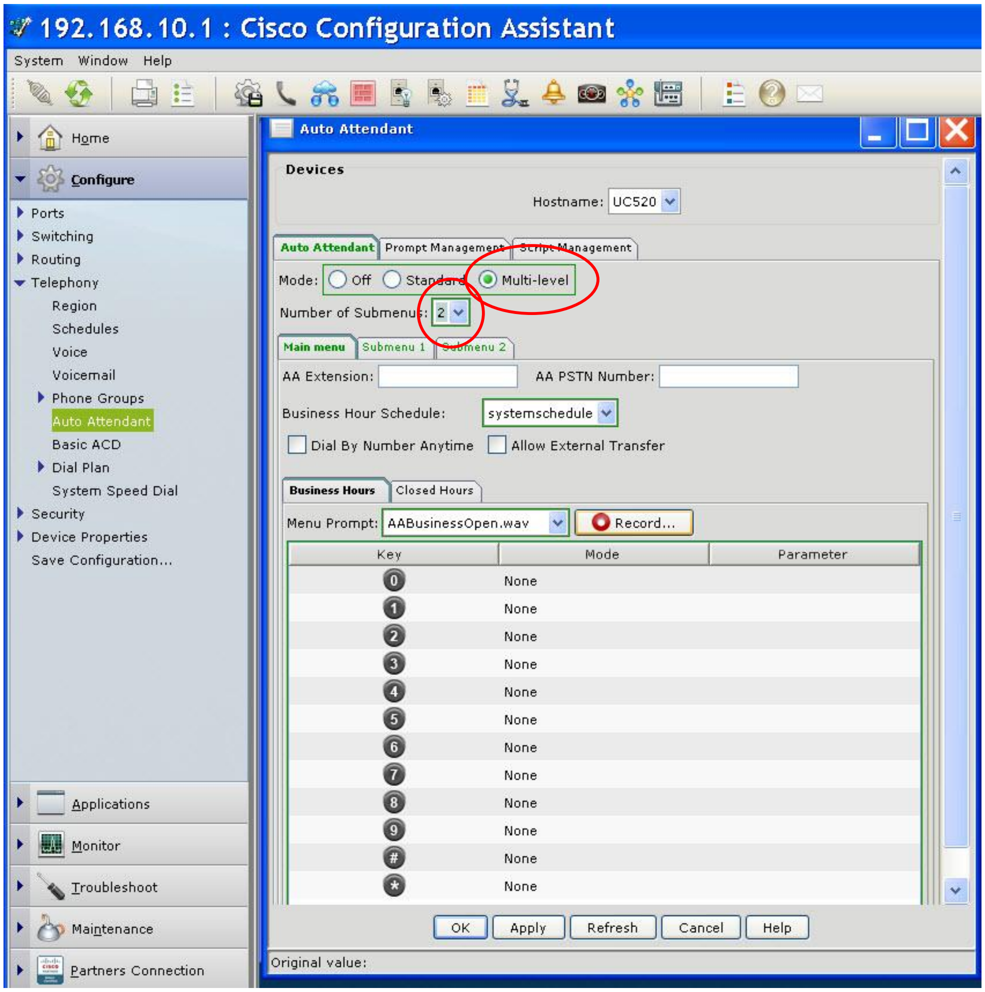
Year: 2009

Date:

Description: Thanksgiving

Step 12: Proceed with the configuration of the Auto Attendant. Click on Configure → Telephony → Auto Attendant. This will launch the AA multilevel node window.

Step 13: Click on the Multi-Level mode.



Devices

Hostname: UC520

Mode: ○ Off ○ Standard ● Multi-level

Number of Submenus: 2

AA Extension: AA PSTN Number:

Business Hour Schedule: systemschedule

□ Dial By Number Anytime □ Allow External Transfer

Menu Prompt: AABusinessOpen.wav

Key	Mode	Parameter
0	None	
1	None	
2	None	
3	None	
4	None	
5	None	
6	None	
7	None	
8	None	
9	None	
#	None	
*	None	

Original value:

Step 14: On the Multi-Level Auto Attendant, select the number of submenus as 2. This will create two additional Submenu tabs.

Step 15: Configure the parameters for the Main menu. Configure the AA Extension to be 400. The AA PSTN number will be 4085xx1200 (where xx is the 2-digit POD #)

Step 16: For the Business Hour Schedule make sure that system schedule is selected from the pull-down menu.

Step 17: Check the Dial by Number Anytime parameter.

Note: Due to VMware restrictions you will not be able to record greetings. The next step is therefore greyed out.

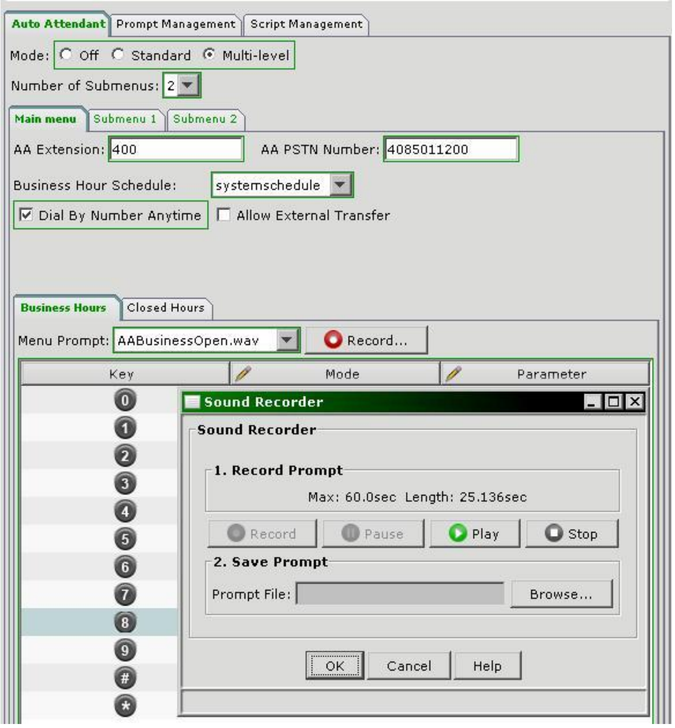
Step 18: Click on the "Record" button and record the following greeting:

i. The main open greetings, which says "Thank you for calling, if you know your party's extension you can enter it at any time. For dial-by-name directory hit 7. If you have a mailbox on this system press 9. For Sales press 1 for Customer Support press2. For directions to our location press 8. To repeat these options press *, or press 0 to reach an operator.

ii. A greetings to record directions to your facility

iii. An opening greetings for Sales department

iv. An opening greetings for the Customer Support department



Mode: ○ Off ○ Standard ● Multi-level

Number of Submenus: 2

AA Extension: 400

AA PSTN Number: 4085011200

Business Hour Schedule: systemschedule

☑ Dial By Number Anytime ☐ Allow External Transfer

Menu Prompt: AABusinessOpen.wav

Sound Recorder

1. Record Prompt

Max: 60.0sec Length: 25.136sec

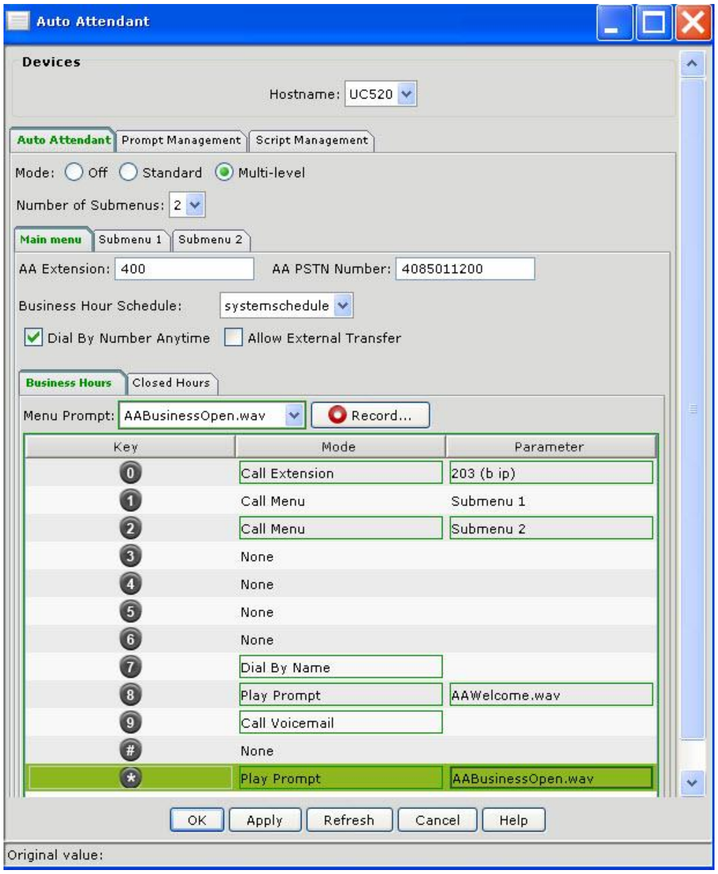
2. Save Prompt

Prompt File:

Step 19: Configure the main menu Business Hours. Select the Menu Prompt as AABusinessOpen.wav.

Step 20: For Keys 0-9,# and *, select the following values corresponding to modes and parameters from the pull-down menus.

0	Call Extension	203 (CIP)
1	Call Menu	Submenu 1
2	Call Menu	Submenu 2
7	Dial By Name	
8	Play Prompt	AAWelome.wav
9	Call Voicemail	
*	Play Prompt	AABusinessOpen.wav



Hostname: UC520

Mode: ○ Off ○ Standard ● Multi-level

Number of Submenus: 2

AA Extension: 400 AA PSTN Number: 4085011200

Business Hour Schedule: systemschedule

☑ Dial By Number Anytime ☐ Allow External Transfer

Menu Prompt: AABusinessOpen.wav

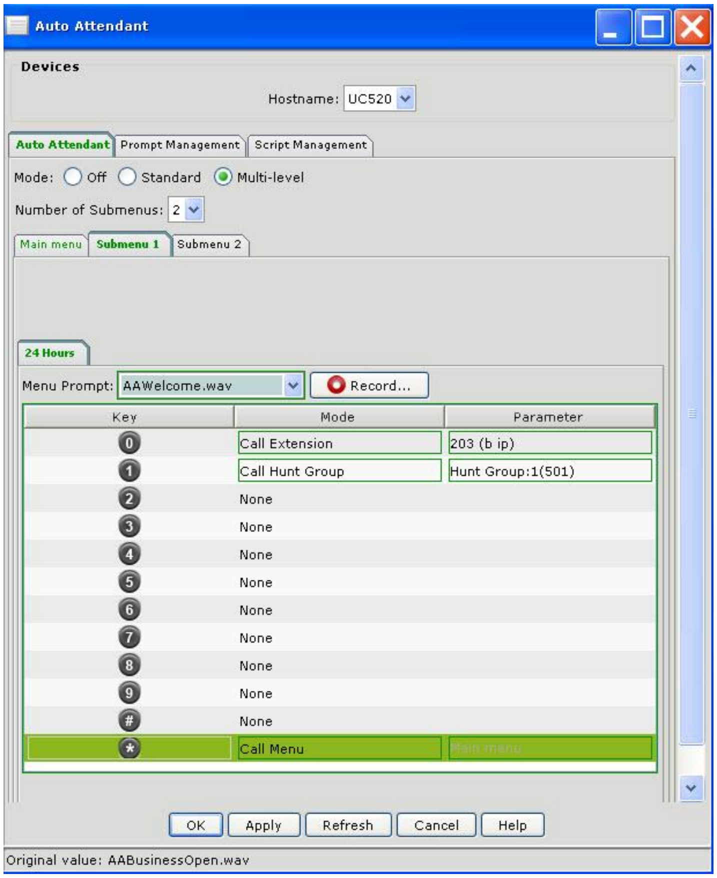
Key	Mode	Parameter
0	Call Extension	203 (b ip)
1	Call Menu	Submenu 1
2	Call Menu	Submenu 2
3	None	
4	None	
5	None	
6	None	
7	Dial By Name	
8	Play Prompt	AAWelcome.wav
9	Call Voicemail	
#	None	
*	Play Prompt	AABusinessOpen.wav

Original value:

Step 21: Click on the Submenu1 sub-tab. For this, from the pull-down menu, select the Prompt AAWelcome.wav.

Step 22: For Keys 0-9,# and *, select the following values corresponding to modes and parameters from the pull-down menus.

0	Call Extension	203 (CIP)
1	Call Hunt Group	Hunt Group:1(501)
*	Call Menu	Main menu (to skip and go back to the main menu)



Hostname: UC520

Mode: ○ Off ○ Standard ● Multi-level

Number of Submenus: 2

Menu Prompt: AAWelcome.wav

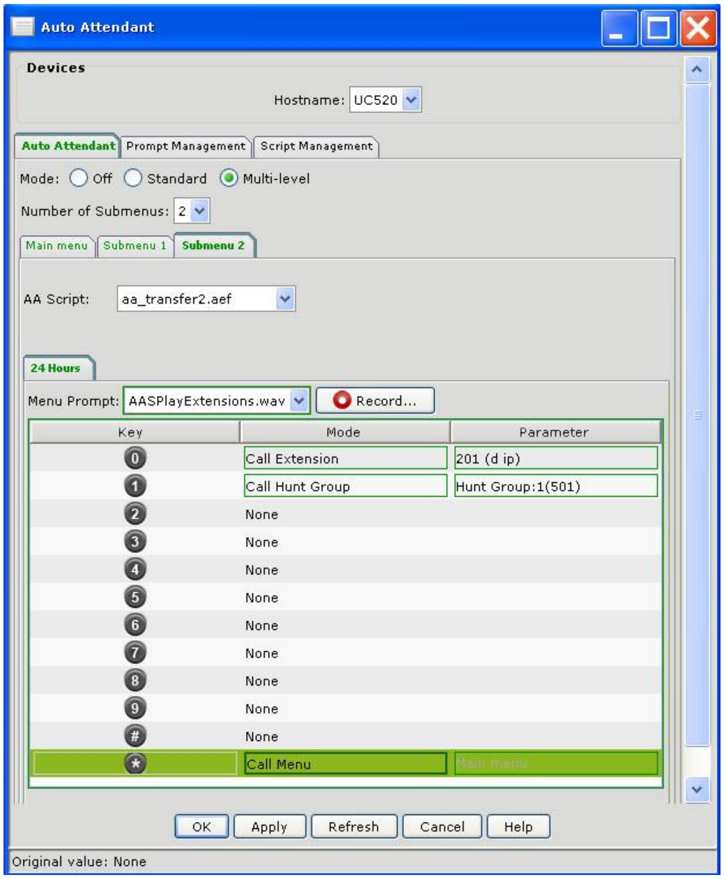
Key	Mode	Parameter
0	Call Extension	203 (b ip)
1	Call Hunt Group	Hunt Group:1(501)
2	None	
3	None	
4	None	
5	None	
6	None	
7	None	
8	None	
9	None	
#	None	
*	Call Menu	Main menu

Original value: AABusinessOpen.wav

Step 23: Next Click on the Submenu2 sub-tab. For this, from the pull-down menu, select the Prompt AASPlayExtensions.wav.

Step 24: For Keys 0-9,# and *, select the following values corresponding to modes and parameters from the pull-down menus.

0	Call Extension	203 (Operator)
1	Call Hunt Group	Hunt Group:1(501)
*	Call Menu	Main menu (to skip and go back to the main menu)



Hostname: UC520

Mode: ○ Off ○ Standard ● Multi-level

Number of Submenus: 2

AA Script: aa_transfer2.aef

Menu Prompt: AASPlayExtensions.wav

Key	Mode	Parameter
0	Call Extension	201 (d ip)
1	Call Hunt Group	Hunt Group:1(501)
2	None	
3	None	
4	None	
5	None	
6	None	
7	None	
8	None	
9	None	
#	None	
*	Call Menu	Main menu

Original value: None

Step 25: Once you have completed this exercise click on the "Apply" button to commit these changes.

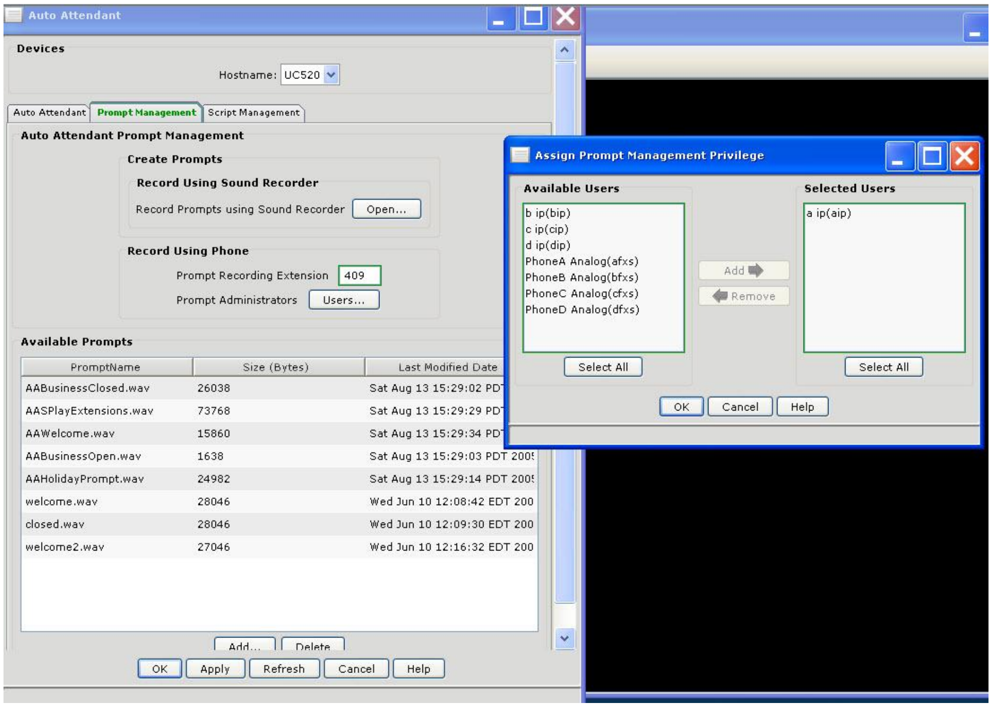
Step 26: To allow end customers to make changes to the recorded greetings, setup a Greetings Management System. Click on the Prompt Management tab.

Step 27: Select an extension (for example 409), that is not in use, that will be dialed to interact with the Greetings Management system.

Step 28: Next assign administrators that are authorized to change the greetings. For this, click on the Prompt Administrators button – this will launch an "Assign Prompt Management Privilege" window.

Step 29: On this window, select user aip as authorized users to alter pre-recorded greetings. Once finished, click on OK button on this window and Apply button on the Prompt Management tab.

Step 30: CCA 1.9 also allows uploading custom auto-attendant scripts.



Devices

Hostname: UC520

Auto Attendant Prompt Management

Create Prompts

Record Using Sound Recorder

Record Prompts using Sound Recorder

Record Using Phone

Prompt Recording Extension: 409

Prompt Administrators

Available Prompts

PromptName	Size (Bytes)	Last Modified Date
AABusinessClosed.wav	26038	Sat Aug 13 15:29:02 PDT
AASPlayExtensions.wav	73768	Sat Aug 13 15:29:29 PDT
AAWelcome.wav	15860	Sat Aug 13 15:29:34 PDT
AABusinessOpen.wav	1638	Sat Aug 13 15:29:03 PDT 200!
AAHolidayPrompt.wav	24982	Sat Aug 13 15:29:14 PDT 200!
welcome.wav	28046	Wed Jun 10 12:08:42 EDT 200
closed.wav	28046	Wed Jun 10 12:09:30 EDT 200
welcome2.wav	27046	Wed Jun 10 12:16:32 EDT 200

Available Users

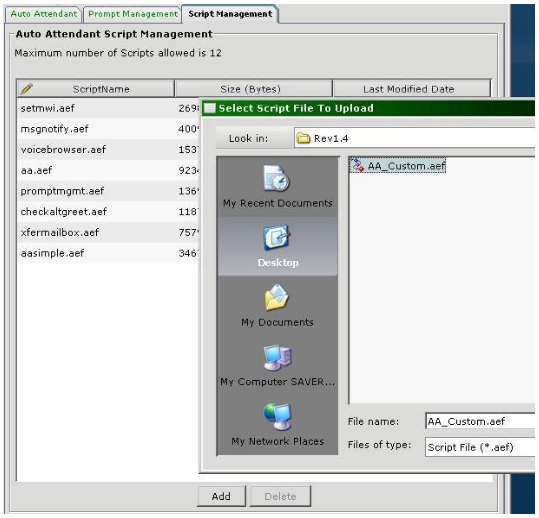
b ip(bip)
c ip(cip)
d ip(dip)
PhoneA Analog(afxs)
PhoneB Analog(bfxs)
PhoneC Analog(cfxs)
PhoneD Analog(dfxs)

Selected Users

a ip(aip)

Note: that this is an advanced exercise for partners that have expertise in creating custom scripts – this is an optional section of the lab for those who need to know how to setup custom scripts using CCA

Step 31: Once you have created a script that meets your customer's needs, save it on your laptop. Click on the Add button and browse to the location of the script. Once added, the script appears along with the other system scripts.



Auto Attendant Script Management

Maximum number of Scripts allowed is 12

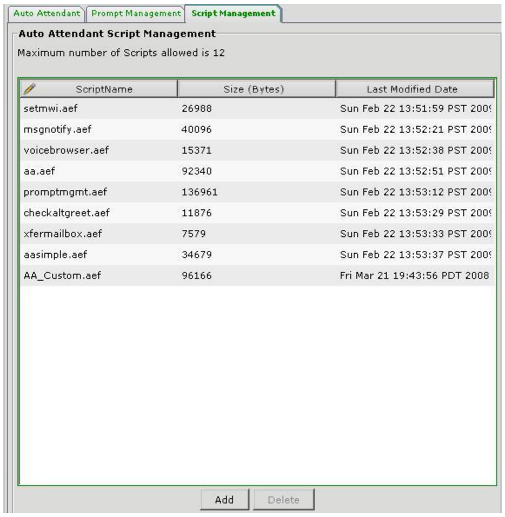
ScriptName	Size (Bytes)	Last Modified Date
setmwi.aef	269	
msgnotify.aef	400	
voicebrowser.aef	153	
aa.aef	923	
promptmgmt.aef	136	
checkaltgreet.aef	118	
xfermailbox.aef	757	
aasimple.aef	346	

Select Script File To Upload

Look in: Rev1.4

File name: AA_Custom.aef

Files of type: Script File (*.aef)



Auto Attendant Script Management

Maximum number of Scripts allowed is 12

ScriptName	Size (Bytes)	Last Modified Date
setmwi.aef	26988	Sun Feb 22 13:51:59 PST 200
msgnotify.aef	40096	Sun Feb 22 13:52:21 PST 200
voicebrowser.aef	15371	Sun Feb 22 13:52:38 PST 200
aa.aef	92340	Sun Feb 22 13:52:51 PST 200
promptmgmt.aef	136961	Sun Feb 22 13:53:12 PST 200
checkaltgreet.aef	11876	Sun Feb 22 13:53:29 PST 200
xfermailbox.aef	7579	Sun Feb 22 13:53:33 PST 200
aasimple.aef	34679	Sun Feb 22 13:53:37 PST 200
AA_Custom.aef	96166	Fri Mar 21 19:43:56 PDT 2008

Verify steps:

Step 1: Call in using SIP trunk to the 4085xx1200 number (where xx is the 2-digit POD #). Make sure that the call is answered by the Auto Attendant

Step 2: There should be silence because there is no ability to record in this lab.

Step 3: Browse through the different options of the Auto Attendant and make sure all menu options are working as expected.

Step 4: Press 0 to reach the operator.

Step 5: Reach the appropriate submenu by dialing option 1 or 2

Step 6: Pressing 9 should transfer to the voicemail. Try to hear the other greeting options (8 and *)

Step 7: Verify the correct greetings from the Sub-menus, get transferred to the appropriate hunt-group, and are able to fallback to the main menu using the * key

Step 8: See if an authorized user is able to access the Greeting Management System.

Exercise-4: ADVANCED FEATURE EXERCISE

This exercise will focus on configuring some advanced features using CCA, CME/CUE GUI, and CLI. Features configured in this exercise include but are not limited to:

Phone features - Monitor buttons, Overlays, Shared DNs, Speed-dial, CFW from a non-primary line.

System features - Local Directory, DNs w/ multiple Hunt-groups, Forwarding from hunt-groups.

Phone features – Monitor buttons

Step 1: Launch the Configure → Telephony → Voice configuration page on CCA.

Step 2: Select the User Extensions tab.

Step 3: Select the phone 'bip'. This user's phone will be treated as operator's phone.

Step 4: On button 3, select the type as Monitor.

Step 5: From the extension pull-down select 201.

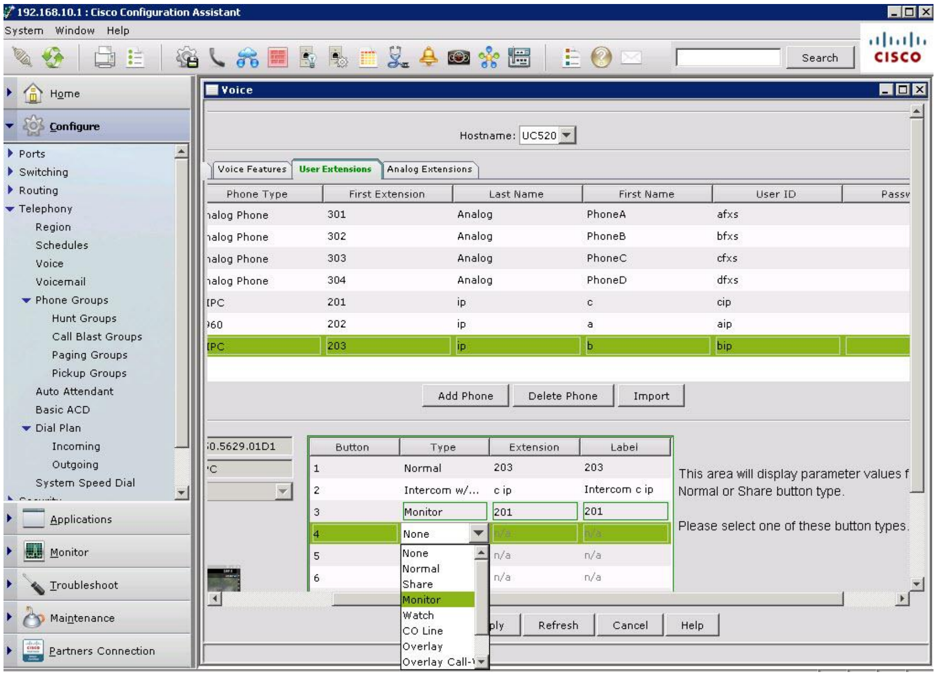
Step 6: On button 4, select the type as Monitor.

Step 7: From the extension pull-down select 203.

Step 8: Click on OK.

Step 9: Click on OK at the bottom of the Voice configuration page and apply the changes.

Step 10: Verify the monitor buttons and functionality. Place 201 or 203 off hook, this should indicate a busy presence status on the respective monitor button.



Hostname: UC520

Phone Type	First Extension	Last Name	First Name	User ID	Passv
ıalog Phone	301	Analog	PhoneA	afxs	
ıalog Phone	302	Analog	PhoneB	bfxs	
ıalog Phone	303	Analog	PhoneC	cfxs	
ıalog Phone	304	Analog	PhoneD	dfxs	
IPC	201	ip	c	cip	
›60	202	ip	a	aip	
IPC	203	ip	b	bip	

;0.5629.01D1

'C

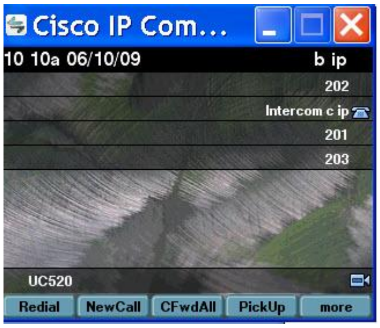
Button	Type	Extension	Label
1	Normal	203	203
2	Intercom w/...	c ip	Intercom c ip
3	Monitor	201	201
4	None	n/a	n/a
5		n/a	n/a
6		n/a	n/a

This area will display parameter values f Normal or Share button type.

Please select one of these button types.

Step 11: Press the monitor button while the monitored line is idle, this should speed dial the extension that it is being monitored.

Step 12: Transfer a call from 201 to 202 by answering the incoming call, pressing the Trnsfer softkey and pressing the third button on the phone. Then press the Trnsfr softkey again.



Phone features – Shared DNs

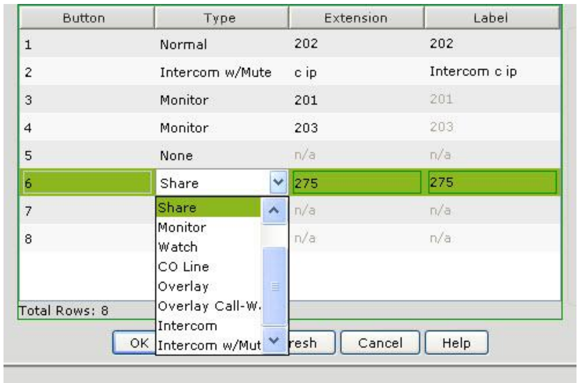
In this section, extension 275 will be configured as a shared line between bip and cip.

Step 1: Launch the Voice configuration page on CCA.

Step 2: Select the Users tab.

Step 3: Click on the more option for bip.

Step 4: On the More Options set the button 6 type as share.



Button	Type	Extension	Label
1	Normal	202	202
2	Intercom w/Mute	c ip	Intercom c ip
3	Monitor	201	201
4	Monitor	203	203
5	None	n/a	n/a
6	Share	275	275
7		n/a	n/a
8		n/a	n/a

Total Rows: 8

Step 5: Select extension 275 in the Extension column.

Step 6: Click OK.

Step 7: Now select cip.

Step 8: Set the button 5 type as share.

Step 9: Select extension 275 in the Extension(s) column.

Step 10: Click OK.

Step 11: Click OK at the bottom of the Voice configuration page.

Step 12: Once the changes are applied, check both IP Phones for ext 275.

Step 13: Verify the functionality by making a call to 275 and ensure that both IP Phones ring.

Step 14: Answer the call on bip. When the shared line is in use by another phone, the LED turns red

Step 15: On the phone labeled bip, place a call. When the shared line is in on hold by another phone, the LED blinks red.

Step 16: On cip, press button 4 (ext 275) to resume the call. When the shared line is picked up, the LED turns solid green.

Phone features – Multi line appearance

The ability to have more than one phone number (or ‘line’) appear on a phone for answering purposes or visual indication of line in use.

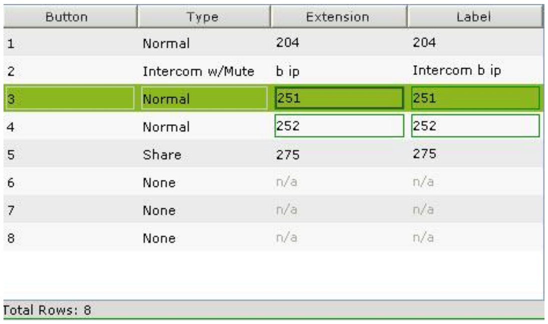
Step 1: Launch the Configure → Telephony → Voice menu in CCA.

Step 2: Select the Users tab.

Step 3: Select the more option for aip.

Step 4: On button 3, select the type as Normal and specify the extension as 251.

Step 5: On button 4, select the type as Normal and specify the extension as 252.



Button	Type	Extension	Label
1	Normal	204	204
2	Intercom w/Mute	b ip	Intercom b ip
3	Normal	251	251
4	Normal	252	252
5	Share	275	275
6	None	n/a	n/a
7	None	n/a	n/a
8	None	n/a	n/a

Total Rows: 8

Step 6: Click on OK.

Step 7: Select the Users tab.

Step 8: Select the more option for cip.

Step 9: On button 3, select the type as Normal and specify the extension as 261.

Step 10: On button 4, select the type as Normal and specify the extension as 262.

Step 11: Click on OK.

Step 12: Click on OK at the bottom of the Voice configuration page.

Step 13: Once the changes are applied, verify the IP Phones display the additional lines. Place calls to ensure the additional lines are functional.

Phone features – Overlay DNs

Overlay DNs are used in scenarios where a single button can be used to answer calls to multiple numbers. This is typically true for lower end phones that have fewer buttons. Follow the steps below to configure the operator's phone with overlay for extensions 261 and 262.

Step 1: Launch the Voice configuration page on CCA.

Step 2: Select the Users tab.

Step 3: Select the more option for bip. This is the operator phone for this exercise.

Step 4: For button 5 select the type as Overlay.

Step 5: Select Overlay under the Extension(s) column.

Step 6: In the next window Overlay - bip, add extensions 261 and 262.

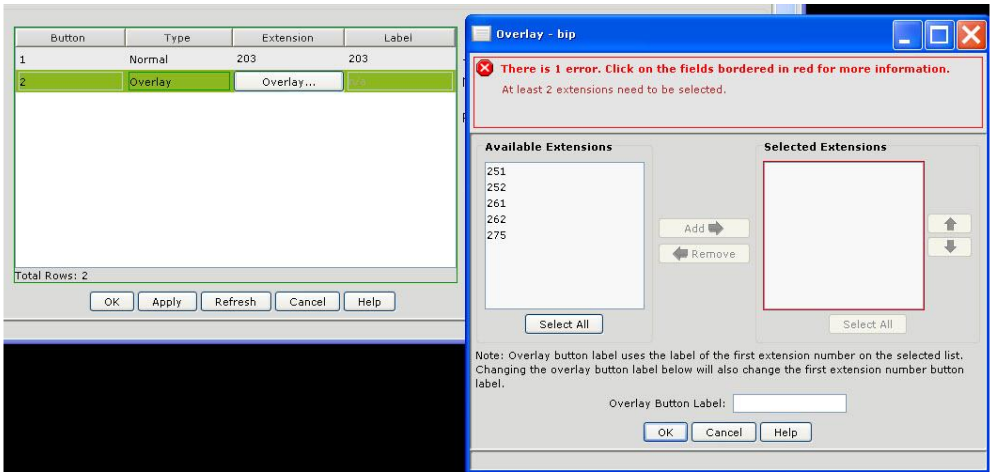
Step 7: Use 261 for the Overlay button label. Click on OK

Step 8: Click OK again on the More Options window.

Step 9: Click on OK at the bottom of the Voice configuration page.

Step 10: Once the changes are applied, check bip's IP Phone and ensure that an overlay button is created. The overlay line label will display the first extension from the overlay group.

Step 11: Verify the overlay functionality by making calls to 261, and 262 and ensure that this overlay line rings.



Button	Type	Extension	Label
1	Normal	203	203
2	Overlay	Overlay...	n/a

Total Rows: 2

Overlay - bip

There is 1 error. Click on the fields bordered in red for more information.

At least 2 extensions need to be selected.

Available Extensions

251
252
261
262
275

Selected Extensions

Note: Overlay button label uses the label of the first extension number on the selected list. Changing the overlay button label below will also change the first extension number button label.

Overlay Button Label:

Phone features – Label for buttons

Labels default to the phone number associated with the button. The Label cannot be changed for Monitored lines all others can be changed. Changing the label on a shared line will change the label for all phones sharing the line.

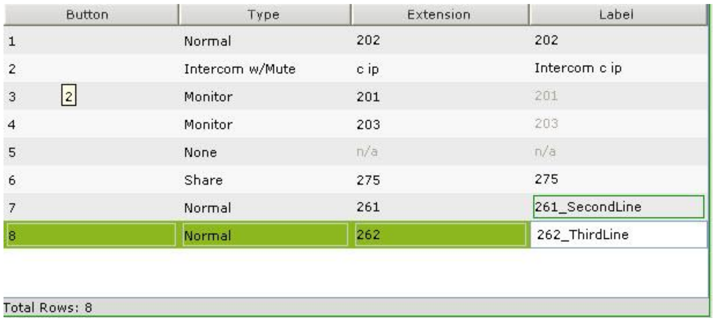
Step 1: Launch the Voice configuration page on CCA.

Step 2: Select the Users tab.

Step 3: Click on the more option for cip.

Step 4: On button 3, extension 261 configure the label as 261_SecondLine.

Step 4: On button 4, extension 262 configure the label as 262_ThirdLine.

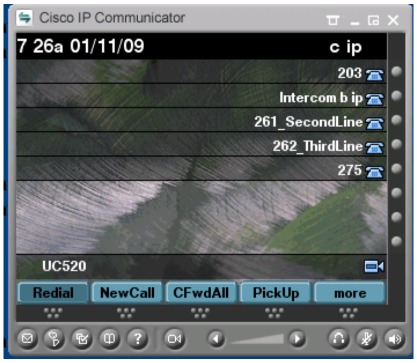


Button	Type	Extension	Label
1	Normal	202	202
2	Intercom w/Mute	c ip	Intercom c ip
3 2	Monitor	201	201
4	Monitor	203	203
5	None	n/a	n/a
6	Share	275	275
7	Normal	261	261_SecondLine
8	Normal	262	262_ThirdLine

Total Rows: 8

Step 5: Click on ok to save the configuration.

Step 6: Verify the functionality – check the IP Communicator for the appropriate display of labels.



Phone features – Speed dials

CCA supports global speed dial configuration. Users can configure personal speed dials by going to the CME user web GUI or they can be configured for the user by the Administrator. (The CUE GUI can also be used to create speed dials on a phone.)

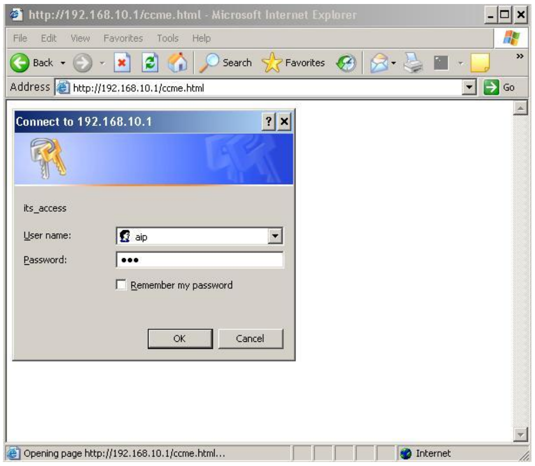
Step 1: Launch a web-browser and browse to the URL http://192.168.10.1/ccme.html.

Step 2: Use the credentials configured in the Users tab. For example, for phone 202, use username/password as bip/1234.

Step 3: Click on Configure → Phone

Step 4: Scroll down to the Speed dial section and configure 97771000 for speedial1.

Step 5: Scroll down to the bottom of the screen and click on Save change.



Address http://192.168.10.1/ccme.html

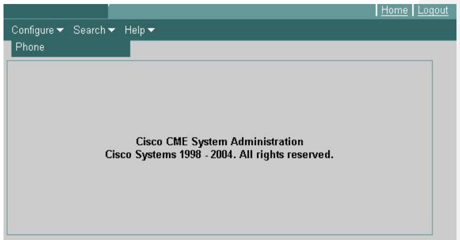
its_access

User name: aip

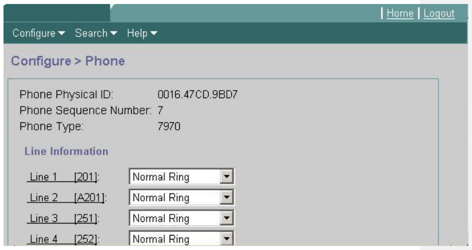
Password: •••

□ Remember my password

Opening page http://192.168.10.1/ccme.html...



Cisco CME System Administration
Cisco Systems 1998 - 2004. All rights reserved.

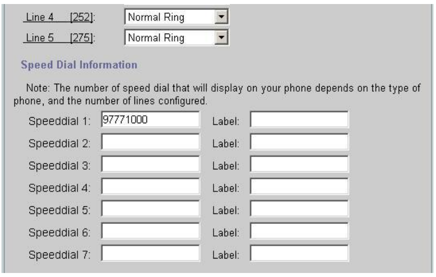


Configure > Phone

Phone Physical ID: 0016.47CD.9BD7
Phone Sequence Number: 7
Phone Type: 7970

Line Information

Line 1 [201]: Normal Ring
Line 2 [A201]: Normal Ring
Line 3 [251]: Normal Ring
Line 4 [252]: Normal Ring



Line 4 [252]: Normal Ring

Line 5 [275]: Normal Ring

Speed Dial Information

Note: The number of speed dial that will display on your phone depends on the type of phone, and the number of lines configured.

Speeddial 1: 97771000 Label:

Speeddial 2: Label:

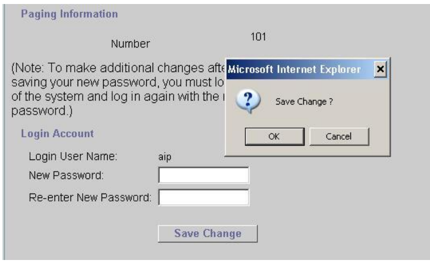
Speeddial 3: Label:

Speeddial 4: Label:

Speeddial 5: Label:

Speeddial 6: Label:

Speeddial 7: Label:



Paging Information

Number 101

(Note: To make additional changes afte saving your new password, you must lo of the system and log in again with the r password.)

Login Account

Login User Name: aip

New Password:

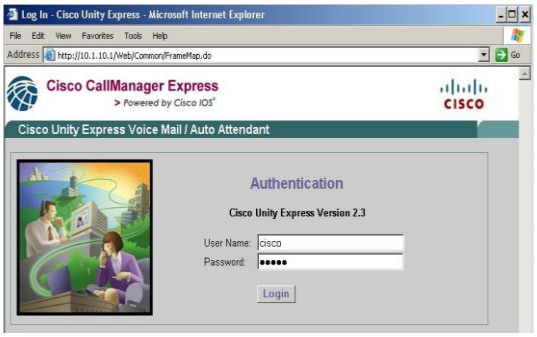
Re-enter New Password:

Phone features: Using the CUE GUI

Follow the steps below to configure this using CME/CUE GUI.

Step 1: From workstation 1 or Workstation 3, access CUE via a web browser using the following URL http://10.1.10.1.

Step 2: The Username is 'cisco' and password is 'cisco'.



Log In - Cisco Unity Express - Microsoft Internet Explorer

Address http://10.1.10.1/Web/Common/FrameMap.do

Cisco CallManager Express

> Powered by Cisco IOS

Cisco Unity Express Voice Mail / Auto Attendant

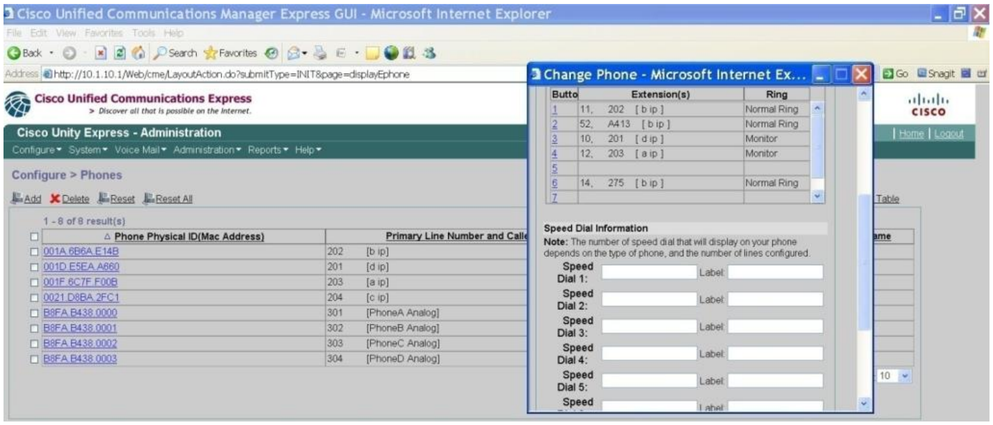
Authentication

Cisco Unity Express Version 2.3

User Name: cisco

Password: •••••

Step 3: Select from the menus Configure → Phones.



Cisco Unified Communications Manager Express GUI - Microsoft Internet Explorer

Address http://10.1.10.1/Web/cme/LayoutAction.do?submitType=INIT&page=displayEphone

Cisco Unified Communications Express

> Discover all that is possible on the Internet.

Cisco Unity Express - Administration

Configure > Phones

1 - 8 of 8 result(s)

□	Phone Physical ID(Mac Address)	Primary Line Number and Calle
□	001A.6B6A.E14B	202 [b ip]
□	001D.E5EA.A660	201 [d ip]
□	001F.6C7F.F00B	203 [a ip]
□	0021.D8BA.2FC1	204 [c ip]
□	B8FA.B438.0000	301 [PhoneA Analog]
□	B8FA.B438.0001	302 [PhoneB Analog]
□	B8FA.B438.0002	303 [PhoneC Analog]
□	B8FA.B438.0003	304 [PhoneD Analog]

Change Phone - Microsoft Internet Ex...

Butto	Extension(s)	Ring
1	11, 202 [b ip]	Normal Ring
2	52, A413 [b ip]	Normal Ring
3	10, 201 [d ip]	Monitor
4	12, 203 [a ip]	Monitor
5		
6	14, 275 [b ip]	Normal Ring
7		

Speed Dial Information

Note: The number of speed dial that will display on your phone depends on the type of phone, and the number of lines configured.

Speed Dial 1: Label:

Speed Dial 2: Label:

Speed Dial 3: Label:

Speed Dial 4: Label:

Speed Dial 5: Label:

Speed Label

Step 4: Speed dials can be configured here as well.

System feature – Local directory

To create directory entries, CLI will be used for the following section.

Step 1: For CLI access open a telnet session to UC520 at 192.168.10.1.

Step 2: Login with the username cisco and password cisco.

Step 3: Enter the enable mode by typing in '***enable'*** at the router prompt. Use the enable password of cisco.

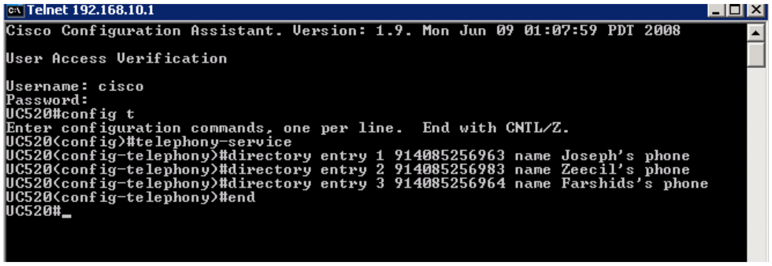
Step 4: To configure the directory entries enter configuration mode by typing in '***config t***' once in the enable mode.

Step 5: Enter the telephony-service mode by typing '***telephony-service***' at the config prompt.

Step 6: Enter the local directory entries for the TME's phones as indicated below.

```
directory entry 1 914085256963 name Joseph's Phone
directory entry 2 914085257827 name Zeecil's Phone
directory entry 3 914085274236 name Farshids's Phone
```

Step 7: Type 'end' once completed to exit out of the configuration mode.

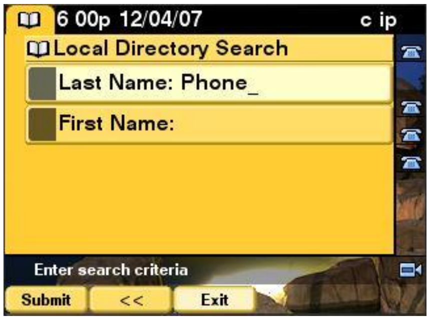


```
Telnet 192.168.10.1
Cisco Configuration Assistant. Version: 1.9. Mon Jun 09 01:07:59 PDT 2008

User Access Verification

Username: cisco
Password:
UC520#config t
Enter configuration commands, one per line.  End with CNTL/Z.
UC520(config)#telephony-service
UC520(config-telephony)#directory entry 1 914085256963 name Joseph's phone
UC520(config-telephony)#directory entry 2 914085256983 name Zeecil's phone
UC520(config-telephony)#directory entry 3 914085256964 name Farshids's phone
UC520(config-telephony)#end
UC520#_
```

Using one of the IP Communicator phones to check the directory entries.
Step 1: Press the 'Directories' button

Step 2: Select option 4 for Local Directory. This can be done by either pressing the 4 on the number key pad or by using the scroll buttons and then pressing the Select softkey button.

Step 3: In the Directory Search, enter 'Phone' for LastName. All three entries that were created above should be displayed in the list.



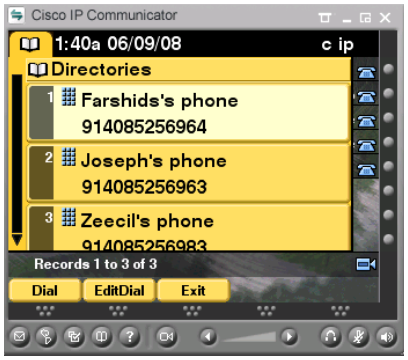
6 00p 12/04/07 c ip

Local Directory Search

Last Name: Phone_

First Name:

Enter search criteria



Cisco IP Communicator

1:40a 06/09/08 c ip

Directories

1 Farshids's phone
914085256964

2 Joseph's phone
914085256963

3 Zeecil's phone
914085256983

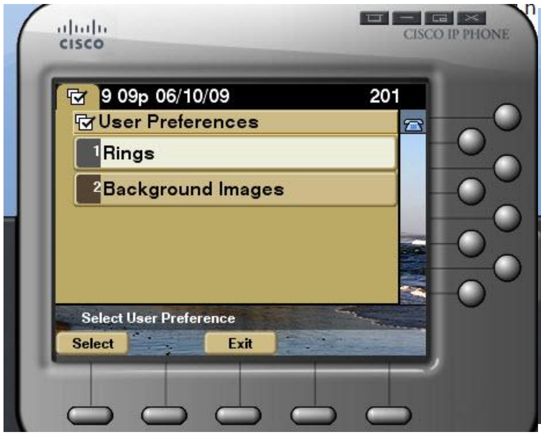
Records 1 to 3 of 3

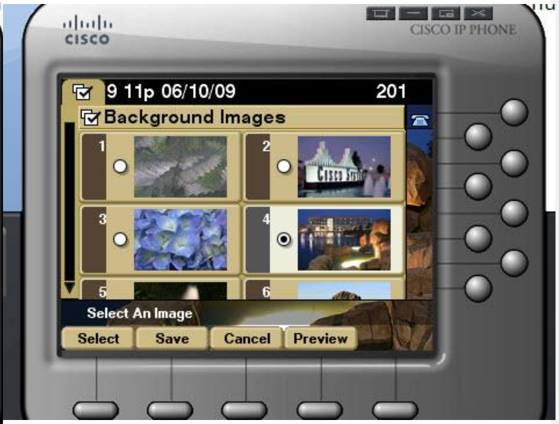
Changing Phone Settings - Ring Tone and Background

Step 1: On the CIPC on workstation 1 press the Settings button. Go to User Settings.

Step 2: Select Ring and change the ring tone. Save.

Step 3: Select Background, choose a new background for the phone and Select. Save the new background.





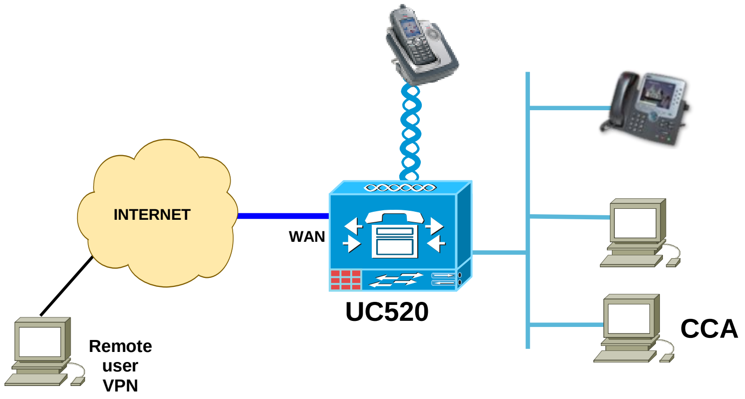
Pod Clean Up
After completing the verification steps above RESTORE the system to factory default using the CLI as shown in Appendix A.

Exercise 5- SECURITY & WIRELESS

Introduction:
The UC520 is a part of the SBCS (Smart Business Communications System) family of products. In addition to its role as an IP phone system, it will also provide Wireless, VPN and Security services.

Objective:
The main objective of this exercise is to configure the basic Wireless and Security features. These features will be configured using Cisco Configuration Assistant (CCA). At the end of this exercise, a user should be able to configure a WiFi IP phone and also configure VPN access for remote teleworkers to access the internet.

Topology:



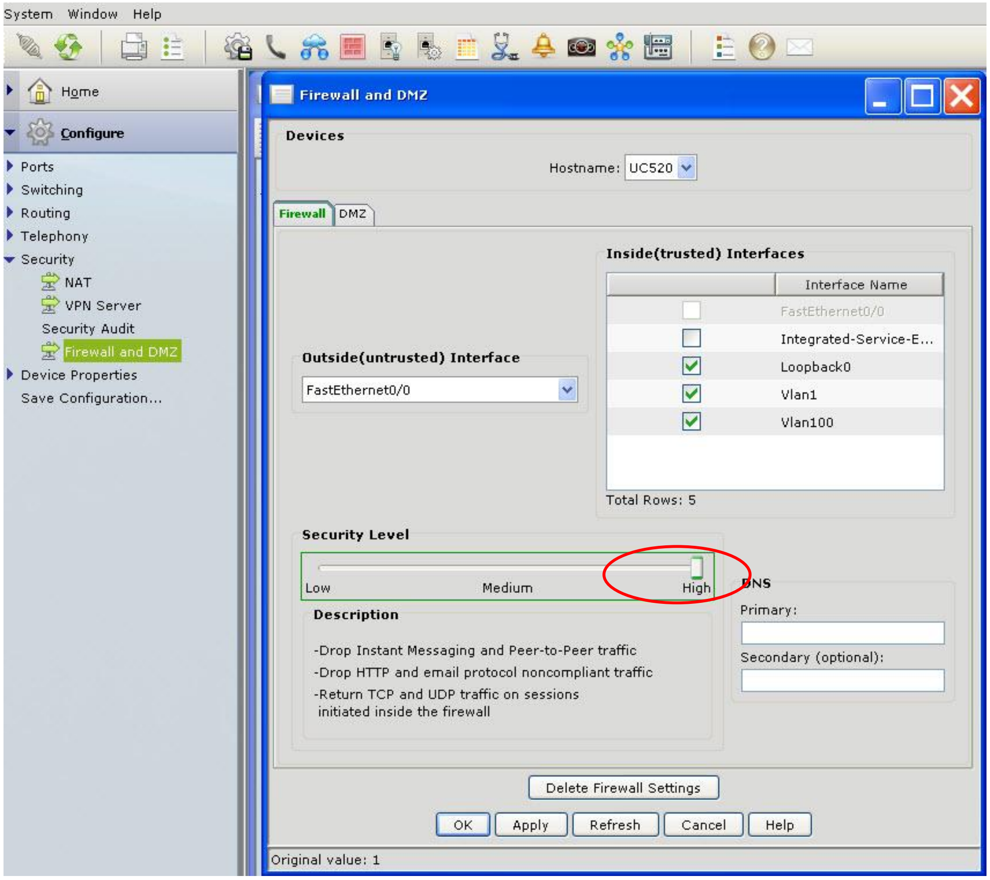
Setup Steps:

Step 1: Open CCA and login.

Step 2: Select from within the Configure Tab on the left side Security → Firewall and DMZ.

Step 3: Change the firewall setting from Low to Medium to High. Notice the description changes as you move the bar. Change the setting back to Low. Leave the remaining settings in their default configuration.

Step 4: Click OK to close the screen.



Devices

Hostname: UC520

Outside(untrusted) Interface

FastEthernet0/0

Inside(trusted) Interfaces

	Interface Name
□	FastEthernet0/0
□	Integrated-Service-E...
☑	Loopback0
☑	Vlan1
☑	Vlan100

Total Rows: 5

Security Level

Description

-Drop Instant Messaging and Peer-to-Peer traffic
-Drop HTTP and email protocol noncompliant traffic
-Return TCP and UDP traffic on sessions
initiated inside the firewall

DNS

Primary:

Secondary (optional):

Original value: 1

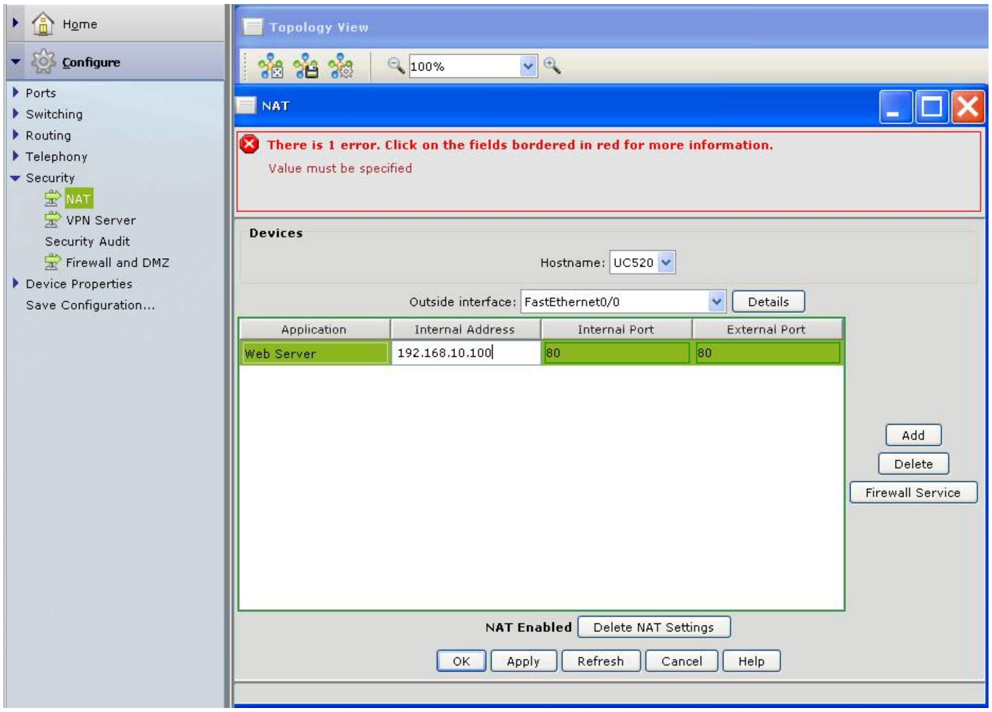
Step 5: From the Security menu on the left select NAT.

Step 6: In the NAT window select Add then in the window choose Web Server as the Type of Service. This sets NAT for HTTP traffic.

Step 7: Set the Private IP Address to 192.168.10.100. (This is a simulated web server address.)

Step 8: Set both the Original Port and Translated port to 80.

Step 9: Click OK.



There is 1 error. Click on the fields bordered in red for more information.

Value must be specified

Hostname: UC520

Outside interface: FastEthernet0/0

Application	Internal Address	Internal Port	External Port
Web Server	192.168.10.100	80	80

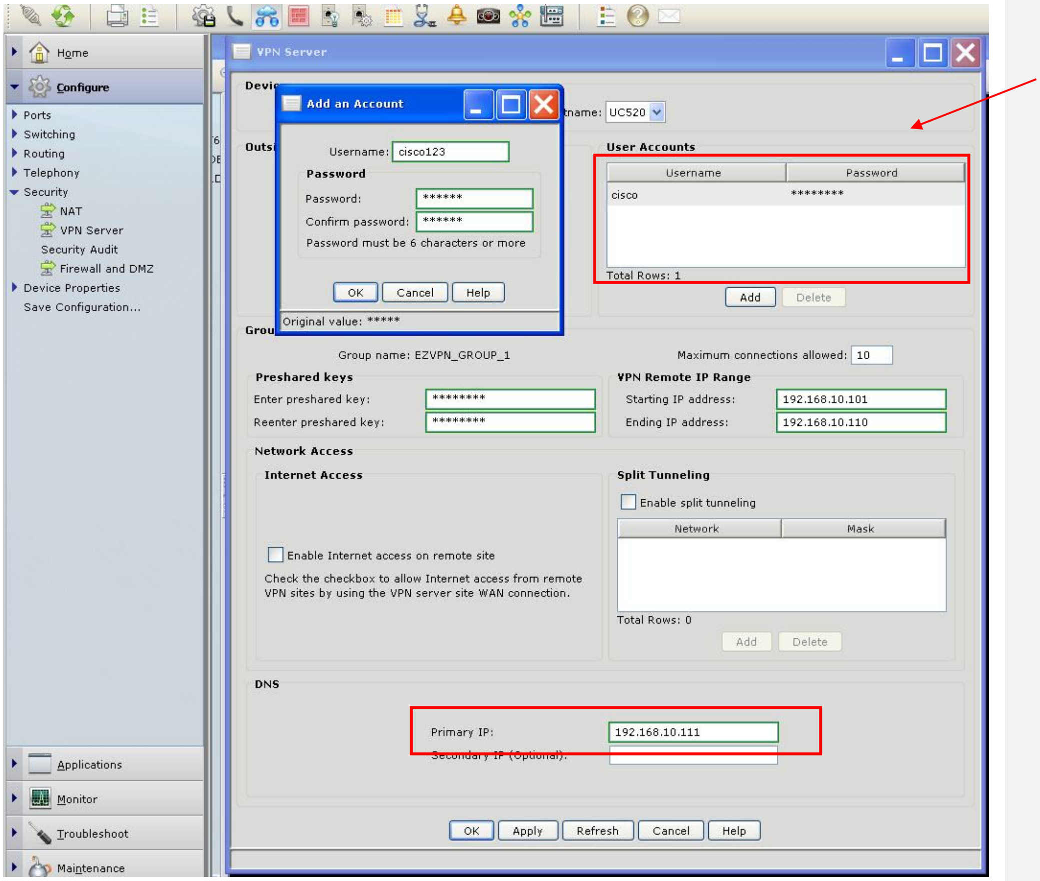
NAT Enabled

Step 10: Again under Security select VPN Server.

Step 11: Create a EZVPN account by clicking on the Add button on the right side of the screen. Use the following criteria for the account.

Username	cisco123
Password	cisco123
Preshared key	cisco123
Starting IP Address	192.168.10.101
Ending IP Address	192.168.10.110
DNS Primary IP	192.168.10.111

Step 12: Click OK.



Add an Account

Username: cisco123

Password

Password: ******

Confirm password: ******

Password must be 6 characters or more

Original value: *****

Hostname: UC520

User Accounts

Username	Password
cisco	********

Total Rows: 1

Group name: EZVPN_GROUP_1

Maximum connections allowed: 10

Preshared keys

Enter preshared key: ********

Reenter preshared key: ********

VPN Remote IP Range

Starting IP address: 192.168.10.101

Ending IP address: 192.168.10.110

Network Access

Internet Access

□ Enable Internet access on remote site

Check the checkbox to allow Internet access from remote VPN sites by using the VPN server site WAN connection.

Split Tunneling

□ Enable split tunneling

Network	Mask

Total Rows: 0

DNS

Primary IP: 192.168.10.111

Secondary IP (Optional):

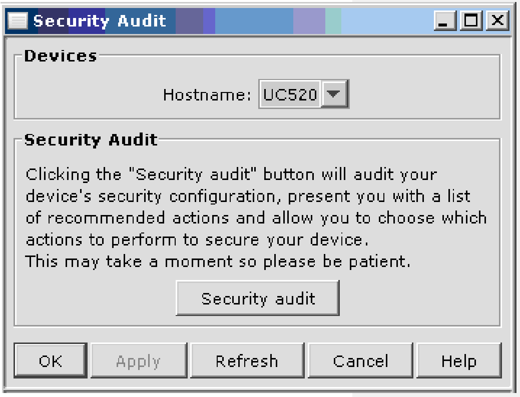
Verification Steps

This section is for reference only. As the equipment resides in a remote location, connecting a laptop to the unit is not possible in this scenario.

Connect a laptop to the available 'broadband internet' connection at your pod. Verify that an IP address in the 1.1.100.1xx range is obtained. Using a VPN client, create a profile for the UC520 and see if you can open a VPN connection to it.
Create a new connection and set the following parameters:
Host 1.1.100.xx (xx is your POD# - drop the leading 0 if any)
Name EZVPN_GROUP_1
Password cisco123
If the connection is successfully established, an IP address in the 192.168.10.x network is obtained.
Launch CCA at this time. This emulates the method that would be used to provide remote support to a customer system.

Running a Security Audit

Running the security audit allows the administrator to quickly determine whether or not changes need to be made to the UC520's configuration to better secure it against possible problems.



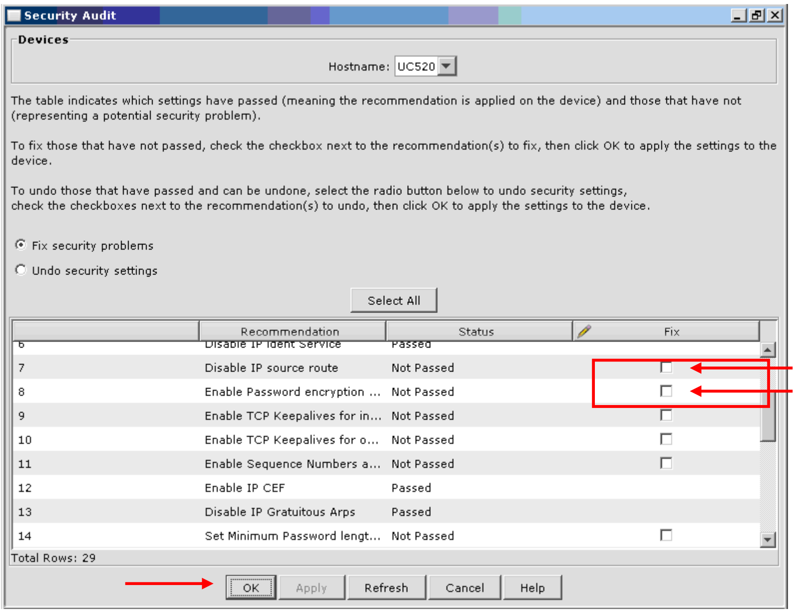
Clicking the "Security audit" button will audit your device's security configuration, present you with a list of recommended actions and allow you to choose which actions to perform to secure your device.
This may take a moment so please be patient.

Step 1: Select from the Security Audit from the security menu.

Step 2: In the Security Audit window click the Security Audit button.

Note that it may take several minutes to get a response from the audit.

When the audit completes, it will display a list of potential security problems that may need attention such as is seen in the following screen shot. To complete any of the recommendations simply click on the check box in the Fix column and click OK at the bottom of the screen. In this scenario two recommendations will be fixed.



The table indicates which settings have passed (meaning the recommendation is applied on the device) and those that have not (representing a potential security problem).

To fix those that have not passed, check the checkbox next to the recommendation(s) to fix, then click OK to apply the settings to the device.

To undo those that have passed and can be undone, select the radio button below to undo security settings, check the checkboxes next to the recommendation(s) to undo, then click OK to apply the settings to the device.

● Fix security problems

○ Undo security settings

	Recommendation	Status	Fix
6	Disable IP Ident Service	Passed	
7	Disable IP source route	Not Passed	□
8	Enable Password encryption ...	Not Passed	□
9	Enable TCP Keepalives for in...	Not Passed	□
10	Enable TCP Keepalives for o...	Not Passed	□
11	Enable Sequence Numbers a...	Not Passed	□
12	Enable IP CEF	Passed	
13	Disable IP Gratuitous Arps	Passed	
14	Set Minimum Password lengt...	Not Passed	□

Total Rows: 29

Step 1: Check Disable IP Source route.

Step 2: Check the Enabled password encryption.

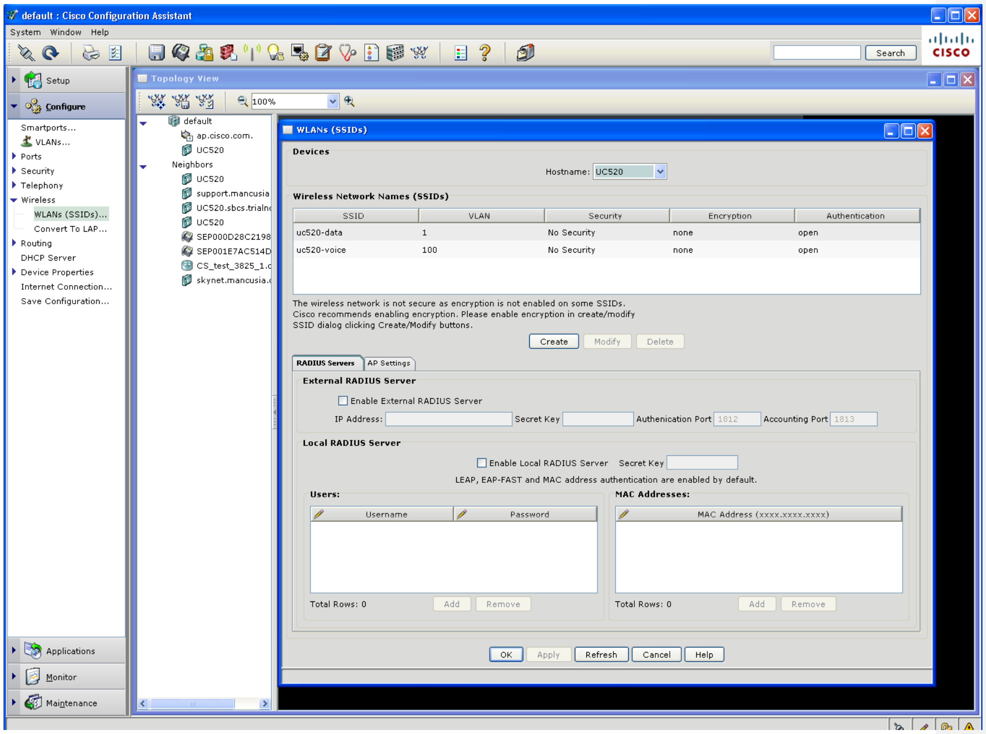
Step 3: Click OK.

Configuring Wireless

The equipment used in this lab does not have the wireless component and as such cannot be configured. These steps are included for reference purposes only. Please review the steps required to configure the wireless component on the UC520 and the 7921G Wireless IP Phone.

This section shows how to configure the wireless settings on the UC520 and how to configure a 7921G IP Phone with SSID podxx (where xx is the pod #).

Step 1: From the menus on the left select Configure → Wireless → WLANs



Devices

Hostname: UC520

Wireless Network Names (SSIDs)

SSID	VLAN	Security	Encryption	Authentication
uc520-data	1	No Security	none	open
uc520-voice	100	No Security	none	open

The wireless network is not secure as encryption is not enabled on some SSIDs.
Cisco recommends enabling encryption. Please enable encryption in create/modify
SSID dialog clicking Create/Modify buttons.

External RADIUS Server

□ Enable External RADIUS Server

IP Address: Secret Key Authenication Port 1812 Accounting Port 1813

Local RADIUS Server

□ Enable Local RADIUS Server Secret Key

LEAP, EAP-FAST and MAC address authentication are enabled by default.

Users:

Username	Password

Total Rows: 0

MAC Addresses:

MAC Address (xxxx.xxxx.xxxx)

Total Rows: 0

Step 2: Click on the UC520-Voice entry and delete it. Click on Create to add a new entry. Make the SSID "podxx" (xx is your POD #). This will be the same SSID used to configure the 7921.

Step 2: We recommend the use of WPA2-PSK on the UC520 for the voice SSID –modify. Select the below:

Security→ WPA2-PSK
Pre-Shared Key → cisco123

Step 3: Click on OK. Make note of the generated SSID, as this will be required to configure the 7921 phone.

Step 4: Click on the UC520-Data SSID and delete it.
Step 5: Click on Create and add an SSID of "podxx-data" on Vlan 1.

Step 6: Again we recommend the use of WPA2-PSK on the UC520 for the data SSID. Select the below options:

Security → WPA2-PSK
Pre-Shared Key→ "12345678"

Step 7: Click on "OK" to download the updated configuration to UC520.

On the 7921
This portion of the lab is for reference only as the lab is in a remote setting and cannot communicate with a 7921 nor is a 7921 available.

Step 1: Power on the 7921.

Step 2: Using the down arrow key browse to the Settings menu.

Step 3: Select Network Profiles and press '**#'. This will unlock the configuration on the phone.

Step 4: From the menus select to Add a new profile.

Step 5: Select Change.

Step 6: Add a profile name called UC520-xx (xx is your POD #).

Step 7: From the menus browse to WLAN configuration.

Step 8: Add the SSID 'podxx' created earlier.

Step 9: Set the Security Mode to Auto (AKM).

Step 10: Set the Key Style to ASCII.

Step 11: Set the Pre-Shared key to the key used earlier (cisco123). Do this using the phone key pad.

Step 12: Select Options and select Save.

Step 13: Navigate back to the Main Screen.

The 7921 should now register to the UC520 and receive an auto assigned extension.

Verification Steps

Place test calls to/from the wireless phone to verify correct operation.

⚠ **Pod Clean Up**
NOTE: When this exercise is complete on both buddy pods, please reset the UC520 to factory default setting using the procedure in Appendix A.

APPENDIX A: Reset to factory default

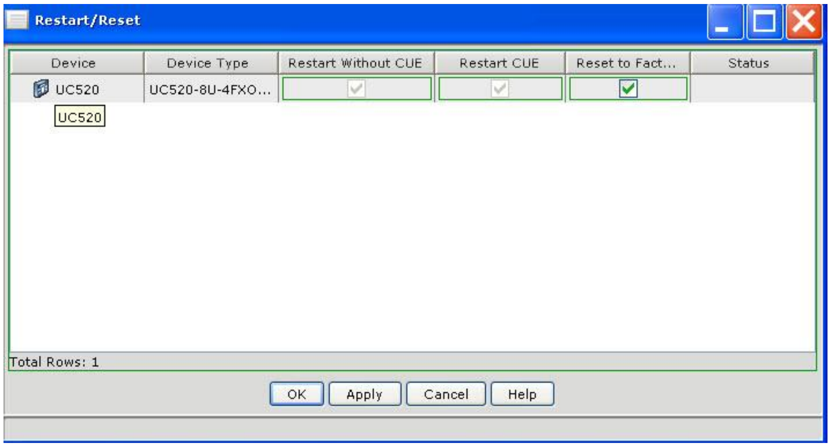
There are two methods that can be used to restore the system to factory defaults. The first is to use the GUI and the second is to telnet to the UC520 and then use the Command Line Interface (CLI).

GUI

Step 1: From the menus on the left click on Maintenance → Restart/Reset.

Step 2: Check the box Reset to Factory Default.

Step 3: Click Apply.



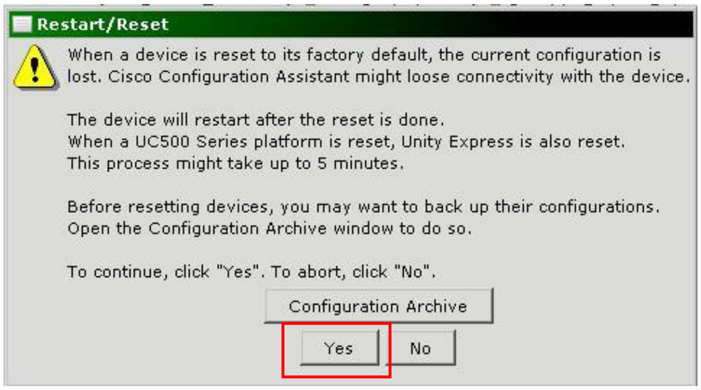
Restart/Reset

Device	Device Type	Restart Without CUE	Restart CUE	Reset to Fact...	Status
UC520	UC520-8U-4FXO...	☐	☐	☑	

UC520

Total Rows: 1

Step 4: A Restart/Reset window will appear with an option to Archive the configuration. Skip this for now and click on "Yes" to continue with the reset.



Restart/Reset

When a device is reset to its factory default, the current configuration is lost. Cisco Configuration Assistant might loose connectivity with the device.

The device will restart after the reset is done.
When a UC500 Series platform is reset, Unity Express is also reset.
This process might take up to 5 minutes.

Before resetting devices, you may want to back up their configurations.
Open the Configuration Archive window to do so.

To continue, click "Yes". To abort, click "No".

Please wait 10 minutes for this to complete.

CLI

Alternatively CLI can be used to reset the system to factory default. Resetting to factory defaults via the CLI is a two part process. CUE needs to be reset separate from CME. The reason for this is that the CUE component, written in Linux, is a separate system from CME. Follow the steps outlined below.

Establish a telnet session
Step 1: Click Start → Run.

Step 2: In the Run window type ***cmd*** to open a command window.

Step 3: At the prompt type ***telnet 192.168.10.1*** Alternatively connect a laptop to a POE port on the UC520 and telnet to 192.168.10.1.

Step 4: At the User Access Verification username prompt enter ***cisco***.

Step 5: At the password prompt enter ***cisco***.

To Reset CME

To reset CME back to factory defaults ensure the config file UC520-8U-4FXO-K9-factory.cfg is in flash. Once confirmed this file will need to be copied to the start-up config essentially over writing any configuration that is in ROM memory. Using the following commands:

Step 1: At the router prompt type *dir flash:* (with the colon).

Step 2: Verify the file name listed below and then copy the UC520 config file to the start up configuration using this exact command:

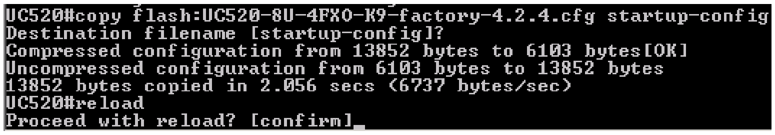
copy flash:UC520-8U-4FXO-K9-factory-7.0.3.cfg startup-config

(If the filename is different substitute the filename in this command for the correct name.)

Step 3: At the Destination filename [startup-config]? prompt press Enter to confirm.

Step 4: Once the file is copied, type "***reload***" to restart the UC520. You may see 'system configuration has been modified. Save?' Type ***'n'***

Step 5: Confirm the reload by pressing Enter.



```
UC520#copy flash:UC520-8U-4FXO-K9-factory-4.2.4.cfg startup-config
Destination filename [startup-config]?
Compressed configuration from 13852 bytes to 6103 bytes[OK]
Uncompressed configuration from 6103 bytes to 13852 bytes
13852 bytes copied in 2.056 secs (6737 bytes/sec)
UC520#reload
Proceed with reload? [confirm]
```

The telnet connection drops once the reload is initiated. When the UC520 has finished rebooting it will be in the factory default mode. **This can take up to 10 minutes.**

Step 6: To check to see if the UC520 is back online try re-establishing the telnet connection. If dithe login prompt is presented, the unit is back online.

Step 7: Once the prompt is presented close the command window.

To Reset CUE

Step 1: Session into CUE by typing the command '***service-module Integrated-Service-Engine 0/0 session***'. (Hit 'enter' twice to get a prompt).

Step 2: Type '***offline***' to go into the offline mode.

Step 3: Type in '***y'*** when you are prompted with 'Are you sure you want to go offline[n]?'

Step 4: Type in '***restore factory default'***

Step 5: Type in '***y***' when you are prompted with 'Do you wish to continue[n]?'

Step 6: Press the Enter key when prompted to 'Press any key to reload:'

This reset can take 5-10 minutes. Wait until the CUE message 'SYSTEM ONLINE' is displayed before proceeding.

APPENDIX B: Verifying VoiceView Express & IMAP

VoiceView Express

VoiceView Express (VVE) allows a user to manage their voicemail box via the display on their IP Phone. The following steps outline how a user logs in and then views header information for each voicemail in their account.

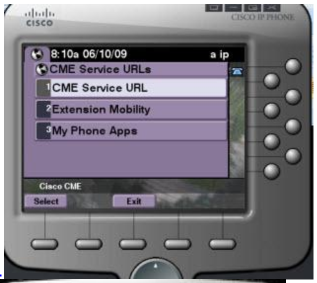
Step 1: On the phone press the Services button.

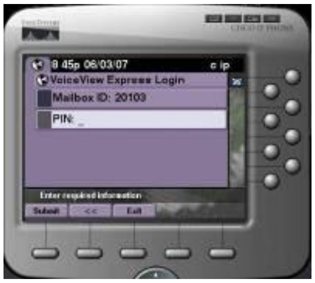
Step 2: From the menus displayed scroll down to the CME Service URL. Alternately the number displayed next to the menu can also be depressed to select that menu.

Step 3: Use the password 789 which was created during an earlier enrollment process.

Step 4: Follow the menu prompts on the IP Phone display to listen to and manage voicemail.

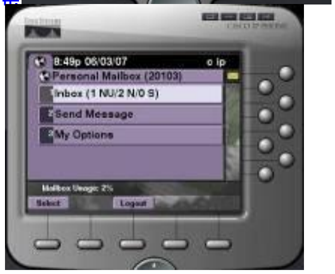
Formatted: Bullets and Numbering





Mailbox ID: 20103

PIN: _



IMAP Integration

IMAP Integration allows the user to use an IMAP client such as Outlook Express to manage voicemail on the CUE system. The following steps outline how to set up a new IMAP account using Outlook Express to view messages on the voicemail system.

Step 1: From workstation 1 or Workstation 3 launch the Outlook Express.
Step 2: From the menus at the top select Tools → Accounts.
Step 3: Click Add.

Step 4: Select Mail.

Step 5: Configure a display name. In the lab use 'aip Voicemail'.

Step 6: Click Next.

Step 7: In the email address field use username@10.1.10.1. Replace username with 'aip'.

Step 8: Click Next.

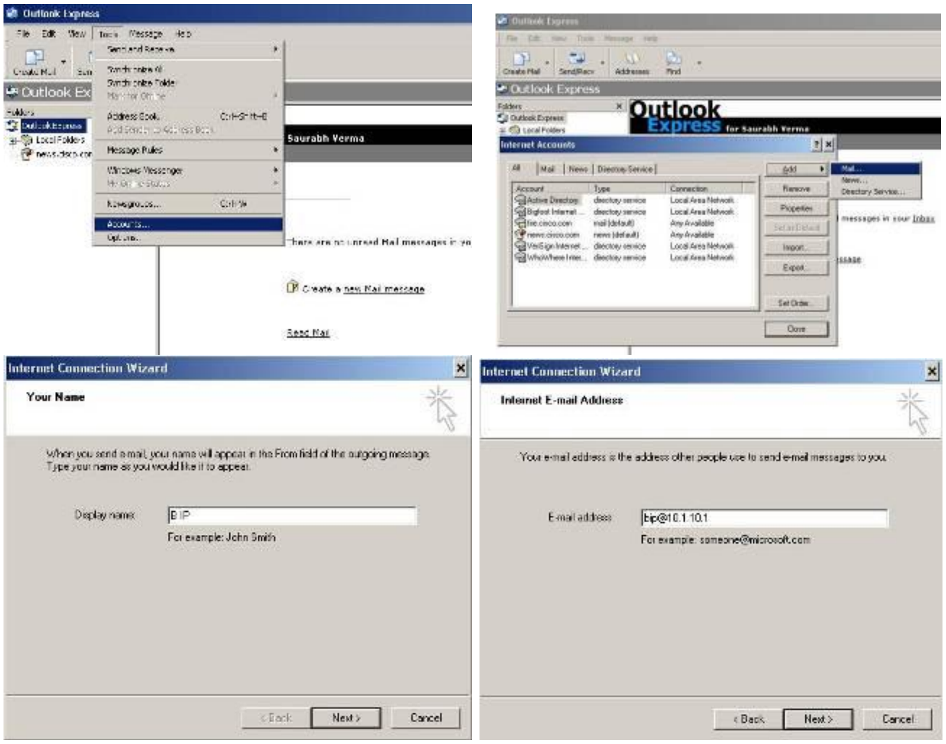
Step 9: On the Email Server setting, select the incoming mail server as an IMAP server.

Step 10: For incoming and outgoing server, configure 10.1.10.1.

Step 11: Click Next.

Step 12: Enter the Account Name as 'aip' and the Password as '1234'.

Step 13: Click Next.


Outlook Express
File Edit View Tools Message Help
Send and Receive
Synchronize All
Address Book... Ctrl+Shift+B
Message Rules
Windows Messenger
Newsgroups... Ctrl+W
Accounts...
Options...
Saurabh Verma
Create a new Mail message
Internet Accounts
All Mail News Directory Service
Add Remove Properties Set as Default Import... Export... Set Order... Close
Mail... News... Directory Service...
Internet Connection Wizard
Back Next > Cancel

Your Name

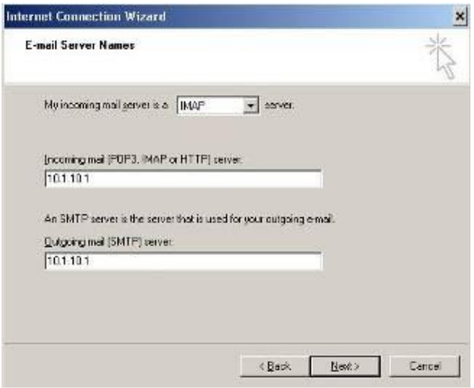
When you send e-mail, your name will appear in the From field of the outgoing message. Type your name as you would like it to appear.

Display name: BIP
For example: John Smith

Internet E-mail Address

Your e-mail address is the address other people use to send e-mail messages to you.

E-mail address: bip@10.1.10.1
For example: someone@microsoft.com



Internet Connection Wizard

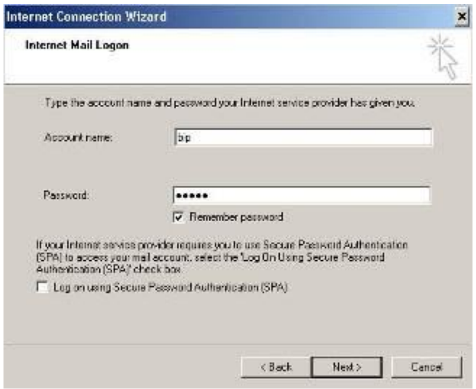
E-mail Server Names

My incoming mail server is a IMAP server.

Incoming mail (POP3, IMAP or HTTP) server: 10.1.10.1

An SMTP server is the server that is used for your outgoing e-mail.

Outgoing mail (SMTP) server: 10.1.10.1



Internet Connection Wizard

Internet Mail Logon

Type the account name and password your Internet service provider has given you.

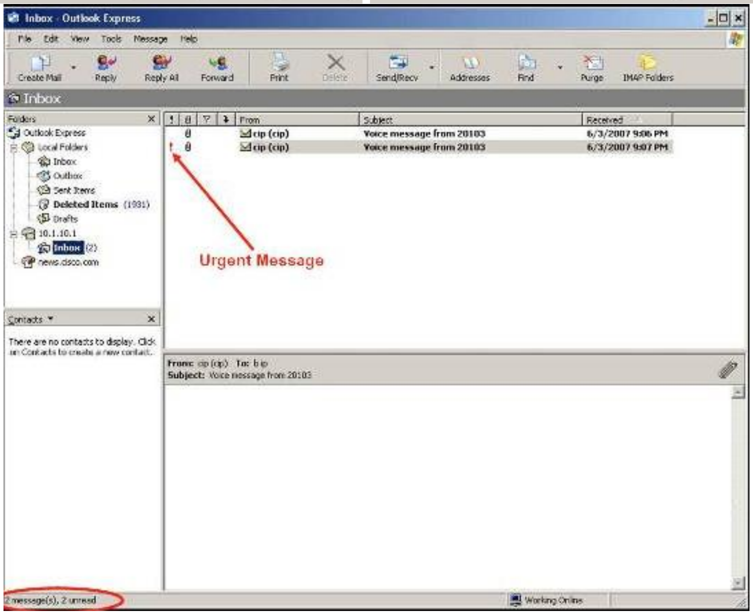
Account name: bip

Password: •••••

☑ Remember password

If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your mail account, select the 'Log On Using Secure Password Authentication (SPA)' check box.

☐ Log on using Secure Password Authentication (SPA)



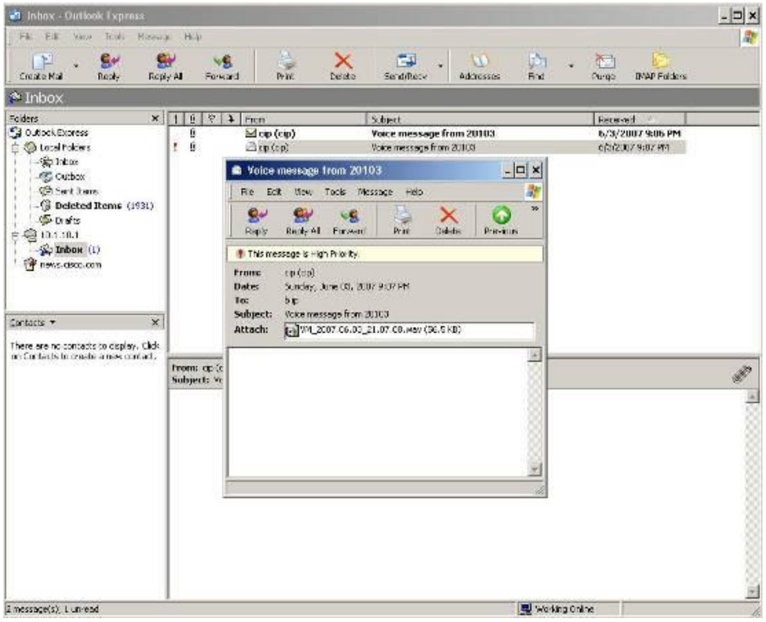
Inbox - Outlook Express

!	0	▽	↓	From	Subject	Received
	0			cip (cip)	Voice message from 20103	6/3/2007 9:06 PM
!	0			cip (cip)	Voice message from 20103	6/3/2007 9:07 PM

There are no contacts to display. Click on Contacts to create a new contact.

From: cip (cip) **To:** b ip
Subject: Voice message from 20103

2 message(s), 2 unread



From	Subject	Received
cip (cip)	Voice message from 20103	6/3/2007 9:06 PM
cip (cip)	Voice message from 20103	6/3/2007 9:07 PM

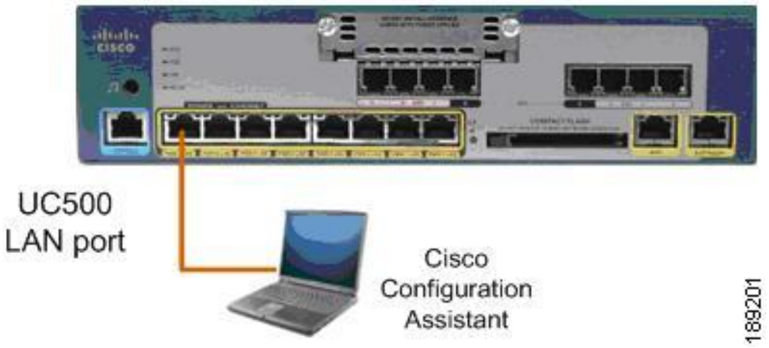
This message is High Priority.

From: cip (cip)
Date: Sunday, June 03, 2007 9:07 PM
To: bip
Subject: Voice message from 20103
Attach: VM_2007.06.03_21.07.08.wav (96.5 KB)

APPENDIX C: Configuring Security on the Cisco UC500 and SR500

Introduction:
The Cisco SR500 provided asymmetric digital subscriber line (ADSL) or FastEthernet WAN termination and advanced security features for a Cisco Smart Business Communications System (SBCS) network. This document describes how to connect a Cisco UC500 behind a Cisco SR500 in secure router mode.

Objective:
Configure the initial SR500 and UC500 setup for connectivity. Network address translation (NAT) is not required on the UC500 in this configuration, because the SR500 manages NAT for the network.



Connect your Cisco UC500 to a Windows PC, as shown

Note: Before proceeding, RESTORE the system to factory default as shown in Appendix A

Configuring the Cisco UC500

To configure the Cisco UC500 using CCA, do the following:

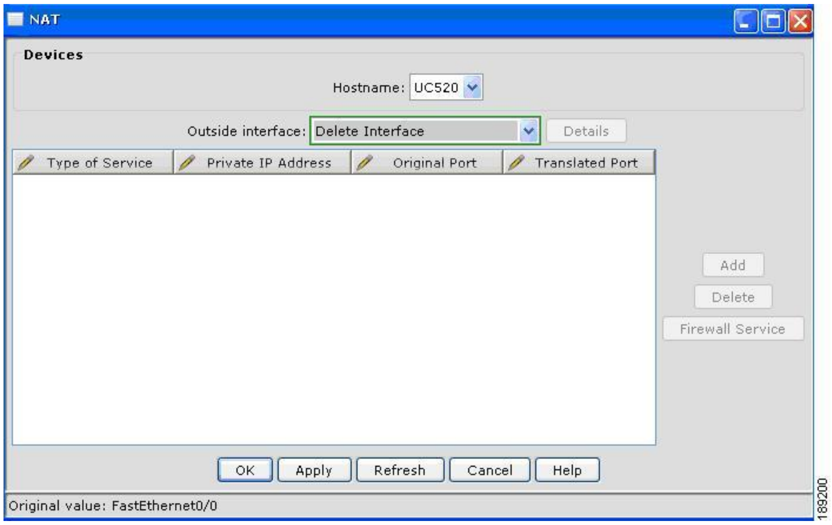
Step 1: Enter the Cisco UC500 LAN IP address in the Connect to field on the Connect window.

Step 2: Enter your Cisco UC500 administrator username and password.

Step 3: Go to Configure → Security → NAT.

Step 4: From the Outside Interface menu on the NAT window, select Delete Interface.

Step 5: Click Apply to disable NAT on the UC500. (The Cisco SR500 will NAT incoming and outgoing Internet traffic; the Cisco UC500 does not require that NAT is enabled.)

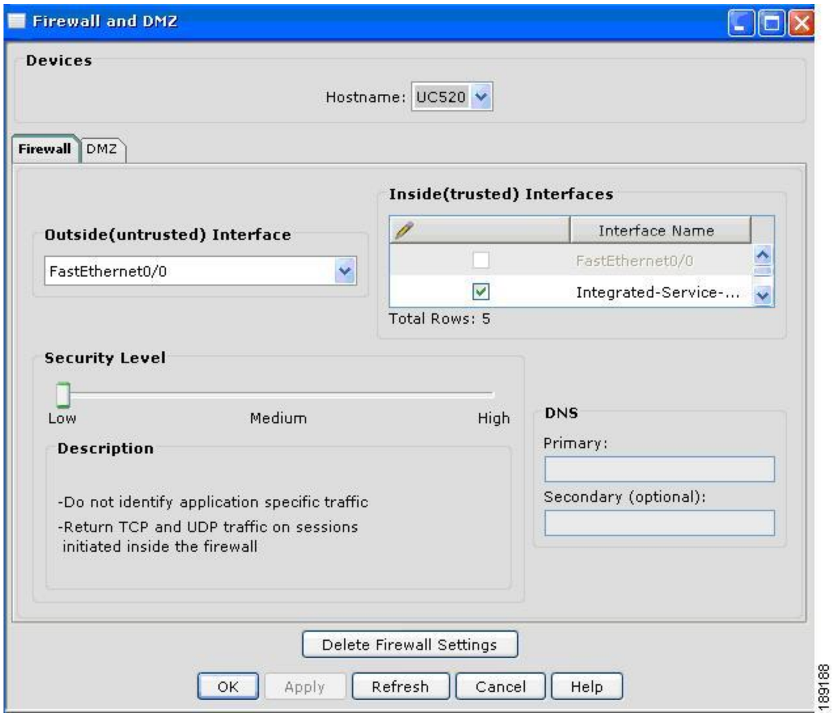


Hostname: UC520

Outside interface: Delete Interface

Original value: FastEthernet0/0

Step 6: Go to Configure → Security → Firewall and DMZ.



Firewall and DMZ

Devices

Hostname: UC520

Outside(untrusted) Interface: FastEthernet0/0

Inside(trusted) Interfaces

	Interface Name
☐	FastEthernet0/0
☑	Integrated-Service-...

Total Rows: 5

Security Level: Low

Description

-Do not identify application specific traffic

-Return TCP and UDP traffic on sessions initiated inside the firewall

DNS

Primary:

Secondary (optional):

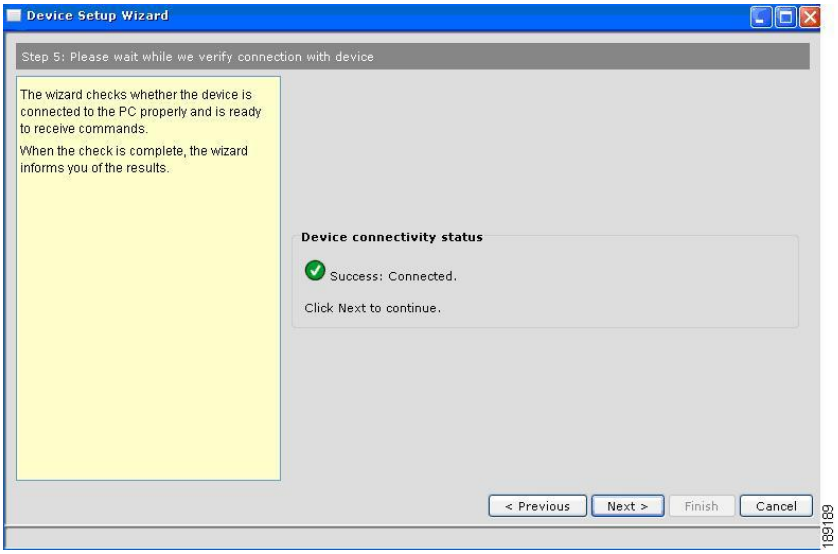
Step 7: Click Delete Firewall Settings.

Step 8: Click Yes to clear the warning message. This deletes the firewall settings from Cisco UC500. A firewall is not required on Cisco UC500, because the Cisco SR500 provides a firewall for the network.

Step 9: Go to Setup → Device Setup Wizard.

Step 10: Select UC500 from the menu and click Next.

Step 11: Click Next until device connectivity is verified. It might take 2-3 minutes to verify the device connectivity. Click Next



Device Setup Wizard

Step 5: Please wait while we verify connection with device

The wizard checks whether the device is connected to the PC properly and is ready to receive commands.

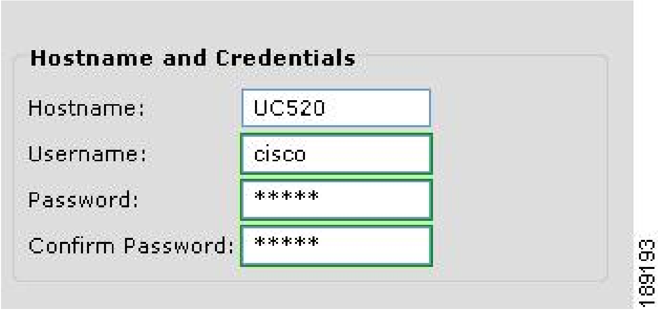
When the check is complete, the wizard informs you of the results.

Device connectivity status

✓ Success: Connected.

Click Next to continue.

Step 12: Enter your UC500 administrator username and password. The default username is cisco. The default password is cisco. Click Next.



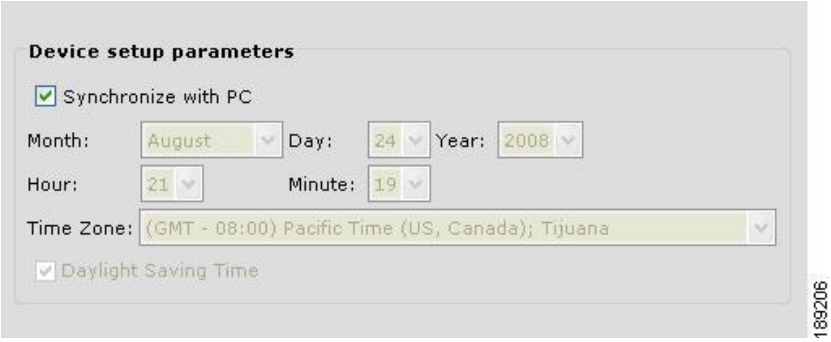
Hostname and Credentials

Hostname: UC520

Username: cisco

Password: *****

Confirm Password: *****



Device setup parameters

☑ Synchronize with PC

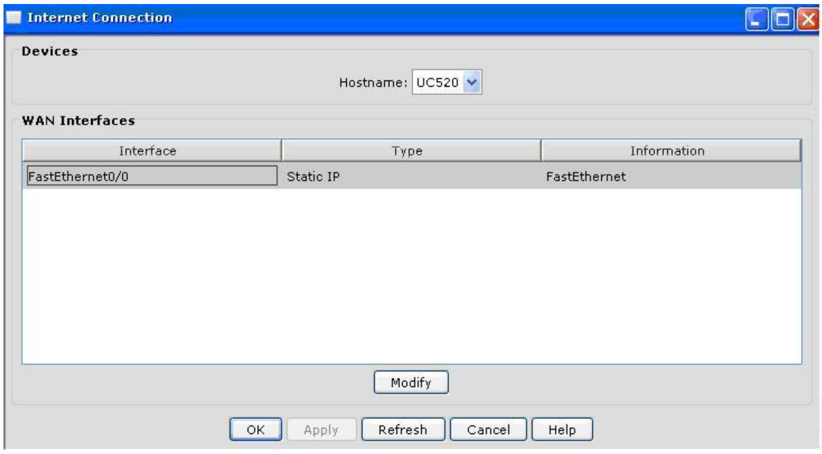
Month: August Day: 24 Year: 2008

Hour: 21 Minute: 19

Time Zone: (GMT - 08:00) Pacific Time (US, Canada); Tijuana

☑ Daylight Saving Time

Step 13: Verify that the Synchronize with PC checkbox is checked. This synchronizes the time and date settings on the UC500 with your PC and click Next.

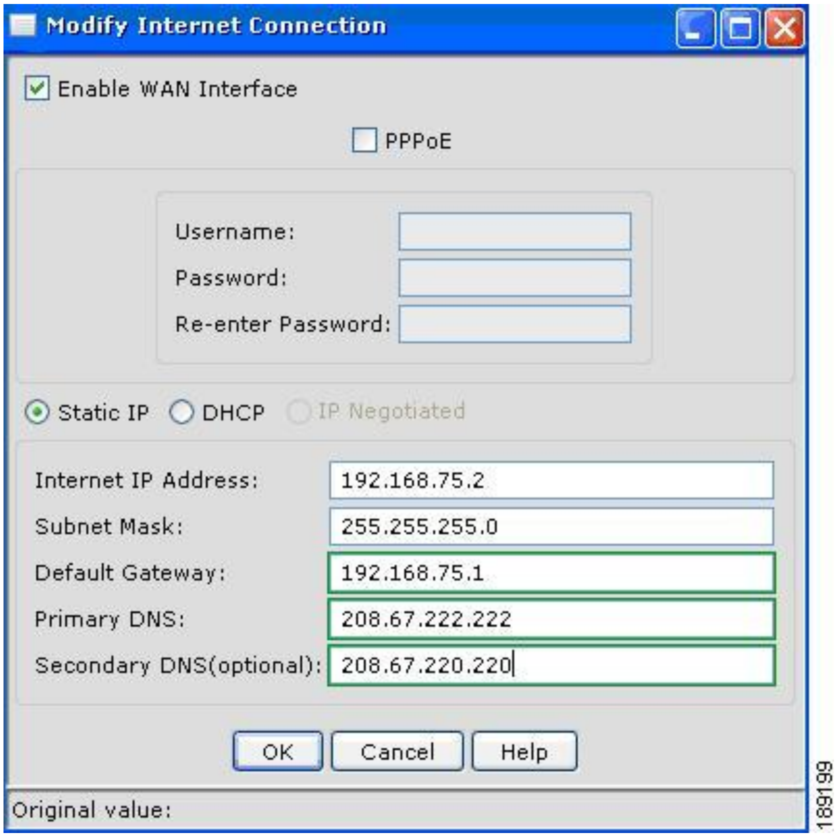


Hostname: UC520

Interface	Type	Information
FastEthernet0/0	Static IP	FastEthernet

189198

Step 14: Select Fastethernet0/0 and click Modify.



☑ Enable WAN Interface

□ PPPoE

Username:

Password:

Re-enter Password:

● Static IP ○ DHCP ○ IP Negotiated

Internet IP Address: 192.168.75.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.75.1

Primary DNS: 208.67.222.222

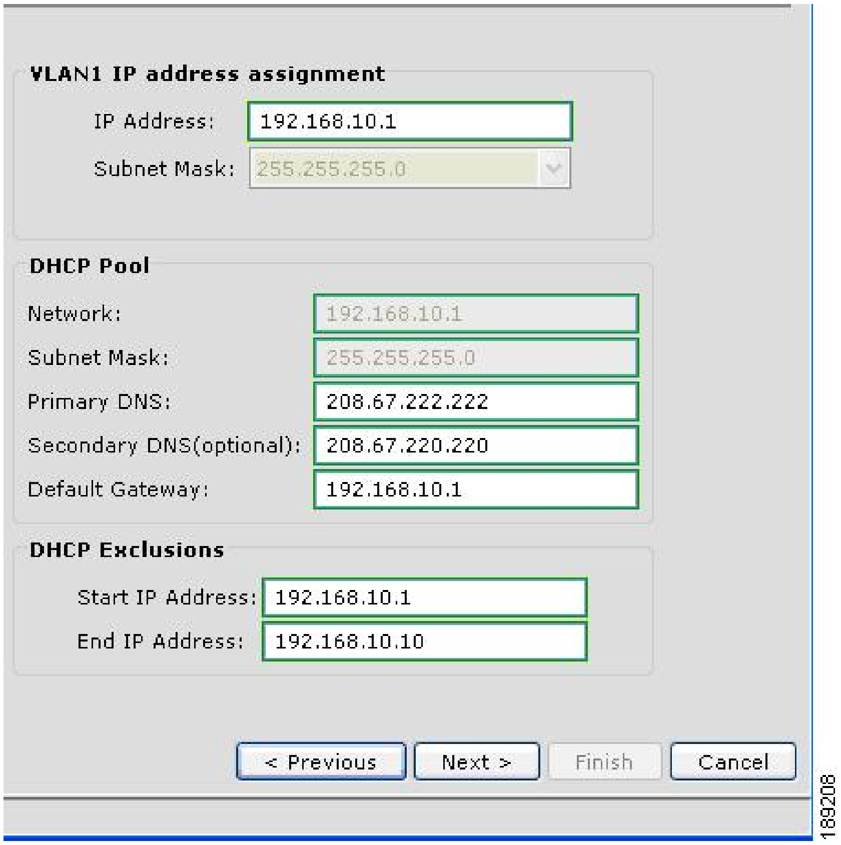
Secondary DNS(optional): 208.67.220.220

Original value:

Step 15: Choose Static IP.

Step 16: In the Internet IP Address field, enter 192.168.75.2.

Step 17: Enter the Primary DNS IP address and the Secondary DNS IP address that match the DNS server IP addresses used in your network and click OK. Then click Next.



VLAN1 IP address assignment

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

DHCP Pool

Network: 192.168.10.1

Subnet Mask: 255.255.255.0

Primary DNS: 208.67.222.222

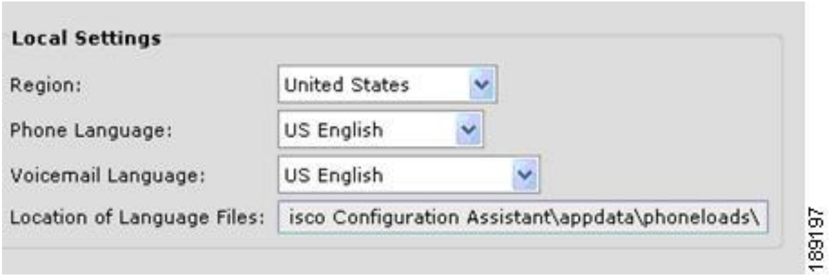
Secondary DNS(optional): 208.67.220.220

Default Gateway: 192.168.10.1

DHCP Exclusions

Start IP Address: 192.168.10.1

End IP Address: 192.168.10.10



Local Settings

Region: United States

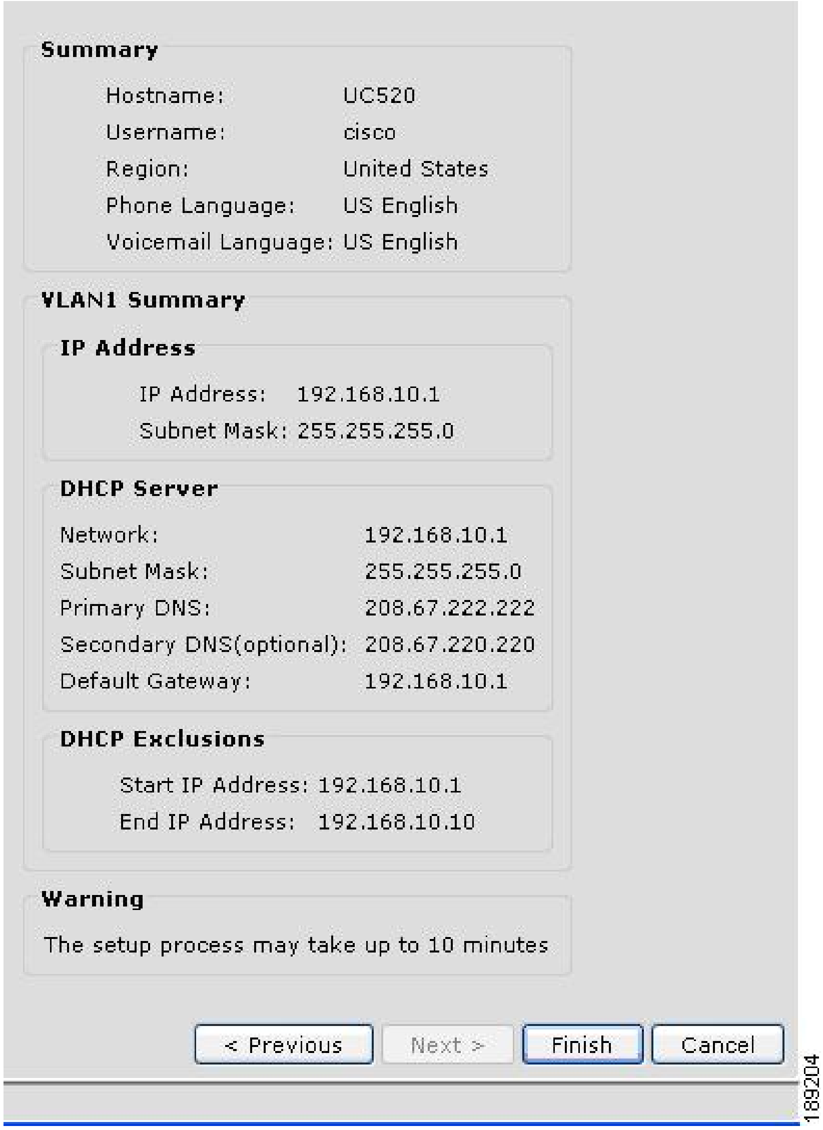
Phone Language: US English

Voicemail Language: US English

Location of Language Files: isco Configuration Assistant\appdata\phoneloads\

Step 18: Select your language from the Phone Language menu, and voicemail language.

Step 19: Select your language Voicemail Language menu click next.



Summary

Hostname: UC520
Username: cisco
Region: United States
Phone Language: US English
Voicemail Language: US English

VLAN1 Summary

IP Address

IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0

DHCP Server

Network: 192.168.10.1
Subnet Mask: 255.255.255.0
Primary DNS: 208.67.222.222
Secondary DNS(optional): 208.67.220.220
Default Gateway: 192.168.10.1

DHCP Exclusions

Start IP Address: 192.168.10.1
End IP Address: 192.168.10.10

Warning

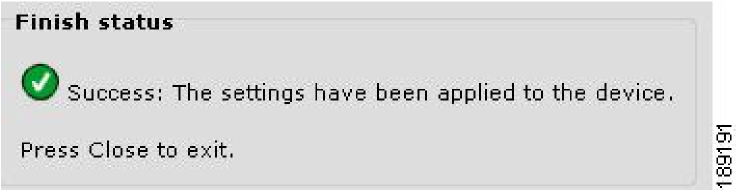
The setup process may take up to 10 minutes

Step 20: Verify your settings. To make any changes, click Previous; otherwise, click Finish.

Step 21: Click Yes when the warning displays.

Note If you retained the VLAN 1 IP address of 192.168.10.1, Cisco Configuration Assistant does not lose connectivity to the Cisco UC500 and applies the configuration settings to the Cisco UC500. This process can take 8-10 minutes

Once the process is complete, you should see the following message.



Finish status

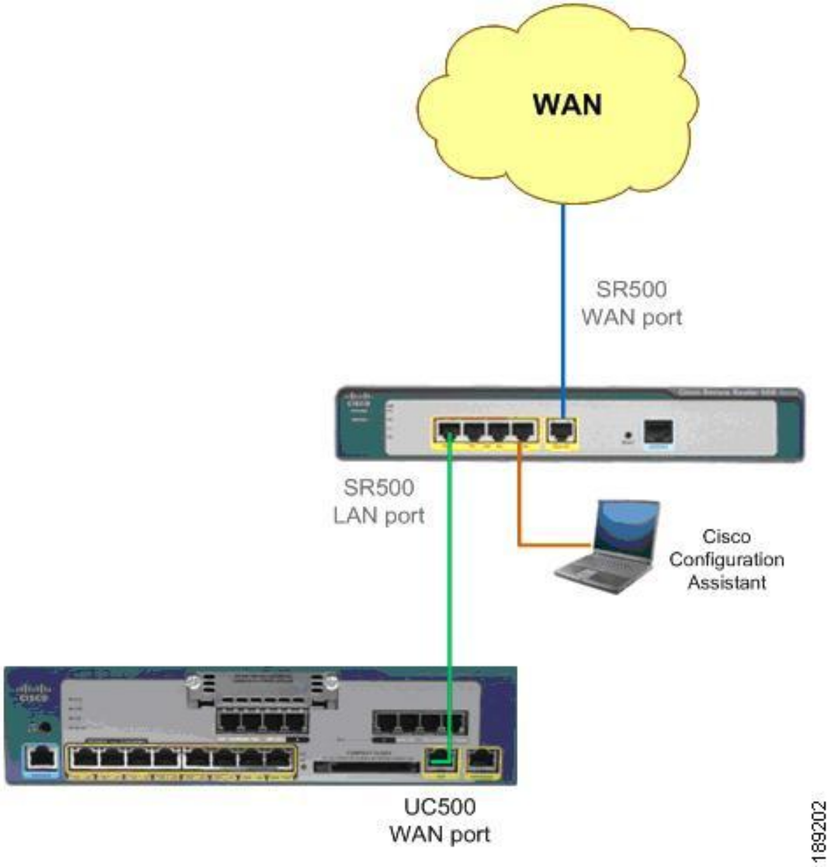
✓ Success: The settings have been applied to the device.

Press Close to exit.

Step 22: Click Close to exit the setup wizard.

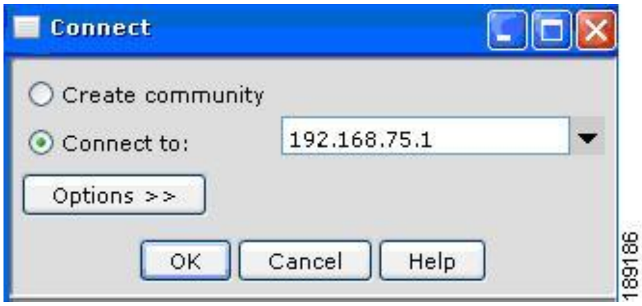
Step 23: Go to Configure → Save Configuration and click Save.

Connect your Cisco UC500, Cisco SR500, and Windows PC as shown



Your Internet/WAN connection might be an ADSL or an Ethernet connection, depending on the Cisco SR500 chassis type.

Step 1: Enter the SR500 LAN IP address in the Connect to field in Cisco Configuration Assistant.



Connect

○ Create community

● Connect to: 192.168.75.1

If your connection is rejected, it might be necessary to manually release and renew your DHCP lease to obtain an IP address from the Cisco SR500, by doing the following:

a. To open a Run window, select Start > Run

b. Enter CMD in the Open field to launch a Windows Command window.

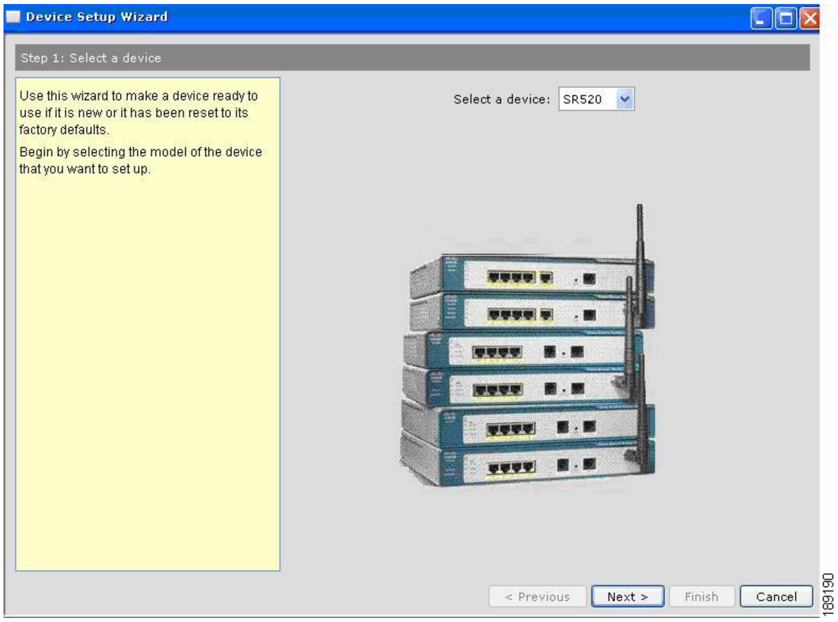
c. Enter ipconfig /release at the Windows command prompt.

d. Enter ipconfig /renew at the Windows command prompt. You should get an IP address that is in the 192.168.75.xxx network.

For example:

```
C:\temp>ipconfig /renew
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : cisco.com
IP Address. . . . . . . . . . . . : 192.168.75.11
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.75.1
```

Step 2: Go to Setup > Device Setup Wizard.



Use this wizard to make a device ready to use if it is new or it has been reset to its factory defaults.

Begin by selecting the model of the device that you want to set up.

Select a device: SR520

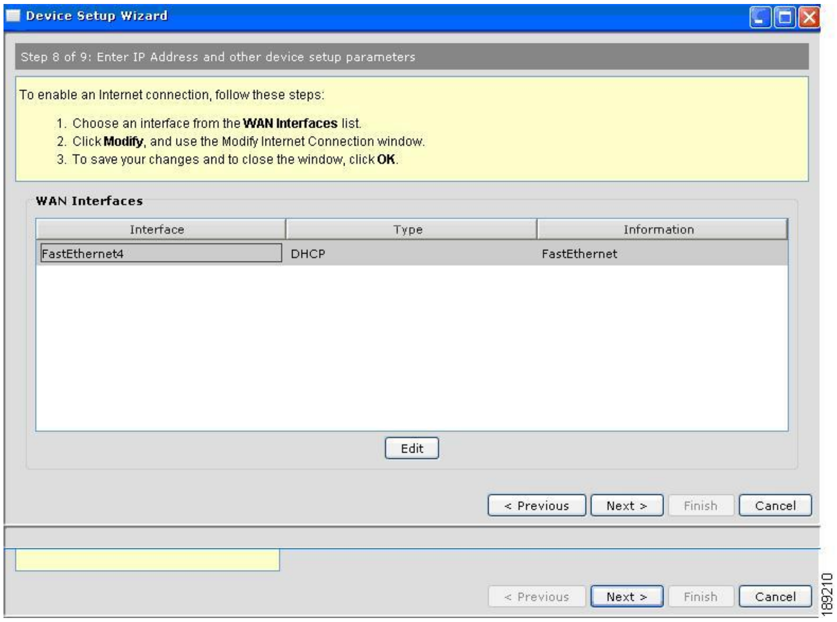
Step 3: From the Select a device menu, select SR500 and click Next.

Step 4: Click Next until device connectivity is verified. It might take 2-3 minutes to verify the device connectivity.

Step 5: Enter your Cisco SR500 administrator username and password. The default username is admin. The default password is admin.

Step 6: Verify that the Synchronize with PC checkbox is checked. This synchronizes the time and date settings on the UC500 with your PC and click Next.

Step 7A: If you are using WAN FastEthernet, the following window displays:



Device Setup Wizard

Step 8 of 9: Enter IP Address and other device setup parameters

To enable an Internet connection, follow these steps:

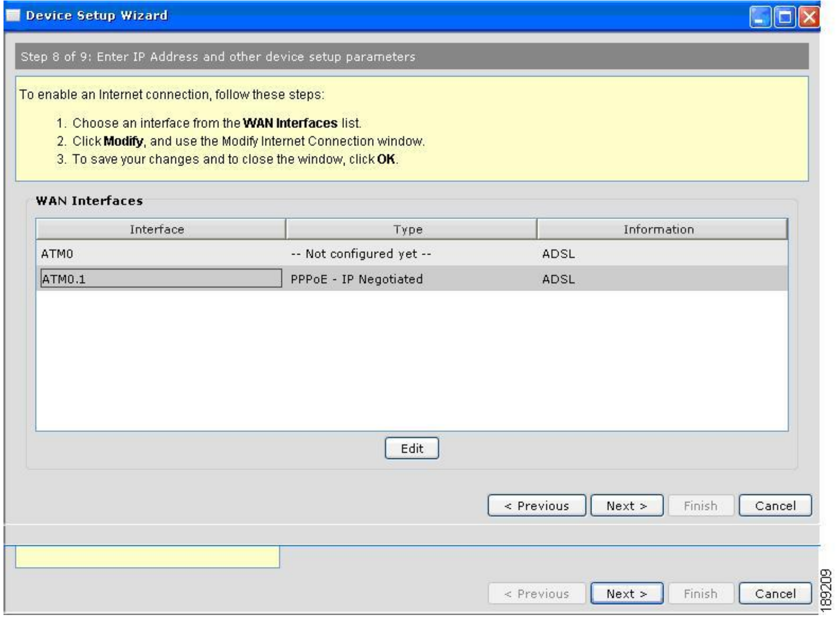
1. Choose an interface from the **WAN Interfaces** list.
2. Click **Modify**, and use the Modify Internet Connection window.
3. To save your changes and to close the window, click **OK**.

WAN Interfaces

Interface	Type	Information
FastEthernet4	DHCP	FastEthernet

Step 8A: Select Fastethernet4 and click Edit.

Step 7B: If you are using ADSL, the following window displays:



Device Setup Wizard

Step 8 of 9: Enter IP Address and other device setup parameters

To enable an Internet connection, follow these steps:

1. Choose an interface from the **WAN Interfaces** list.
2. Click **Modify**, and use the Modify Internet Connection window.
3. To save your changes and to close the window, click **OK**.

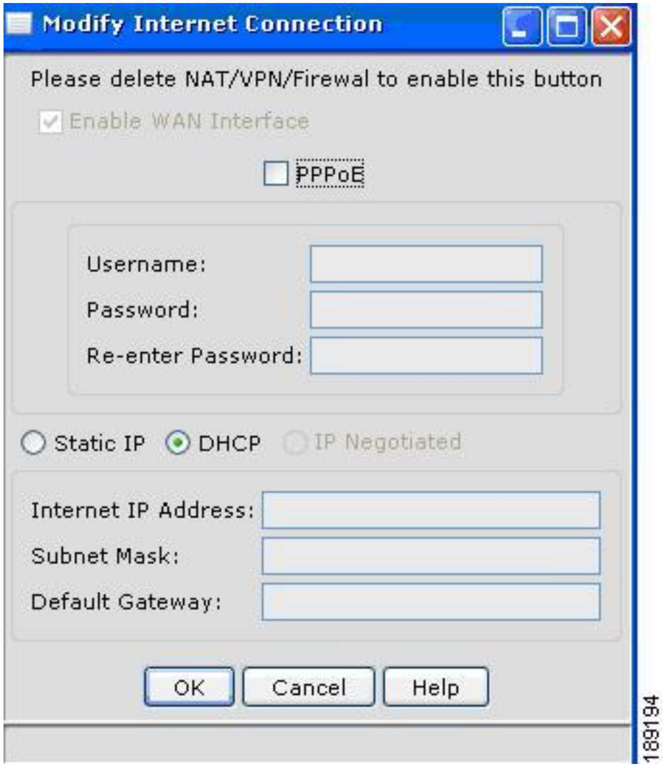
WAN Interfaces

Interface	Type	Information
ATM0	-- Not configured yet --	ADSL
ATM0.1	PPPoE - IP Negotiated	ADSL

Step 8B: Select ATM0.1 and click Edit.

Step 9: Specify your Cisco SR500 Internet connection settings and click OK. These settings vary depending on which provider and what WAN type you are using to connect to the Internet. For example:

DHCP with FastEthernet:



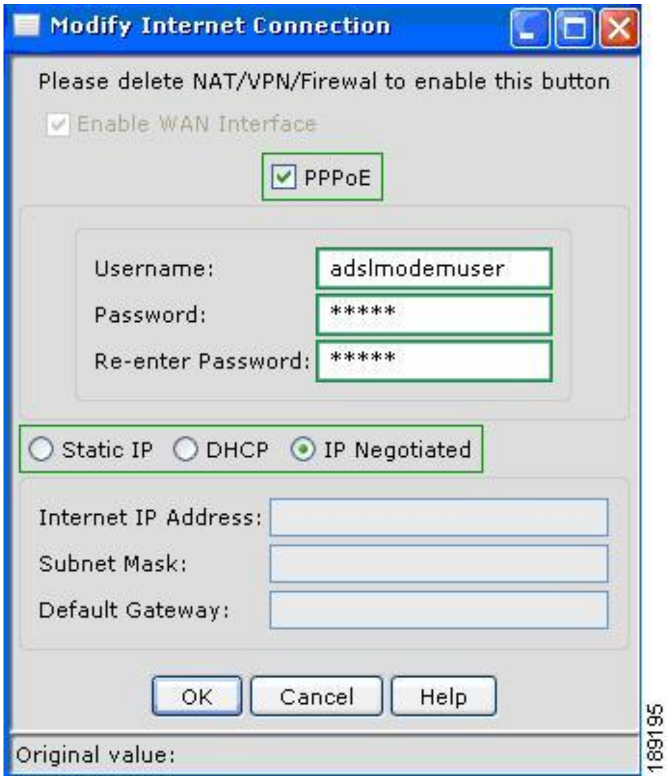
Please delete NAT/VPN/Firewal to enable this button

☑ Enable WAN Interface

□ PPPoE

○ Static IP ● DHCP ○ IP Negotiated

PPPoE with FastEthernet:



Modify Internet Connection

Please delete NAT/VPN/Firewal to enable this button

☑ Enable WAN Interface

☑ PPPoE

Username: adslmodemuser

Password: *****

Re-enter Password: *****

○ Static IP ○ DHCP ● IP Negotiated

Internet IP Address:

Subnet Mask:

Default Gateway:

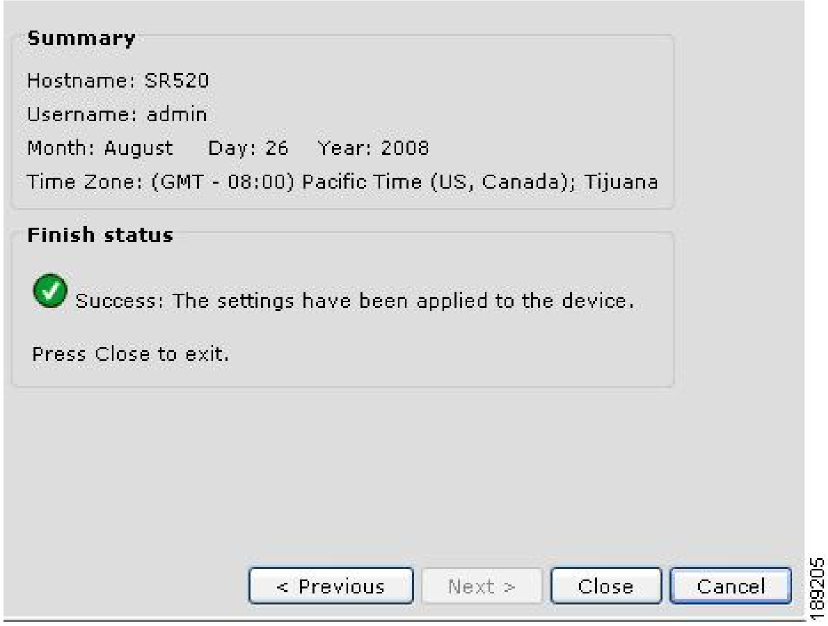
Original value:

The username and password should match the account information provided by your Internet service provider.

PPPoE with ADSL:

The username and password should match the account information provided by your Internet service provider.

Step 10: Click Next. Verify your settings. To make any changes, click Previous; otherwise click Finish. After 1-2 minutes, the Summary message displays. Click Close.



Summary

Hostname: SR520

Username: admin

Month: August Day: 26 Year: 2008

Time Zone: (GMT - 08:00) Pacific Time (US, Canada); Tijuana

Finish status

✓ Success: The settings have been applied to the device.

Press Close to exit.

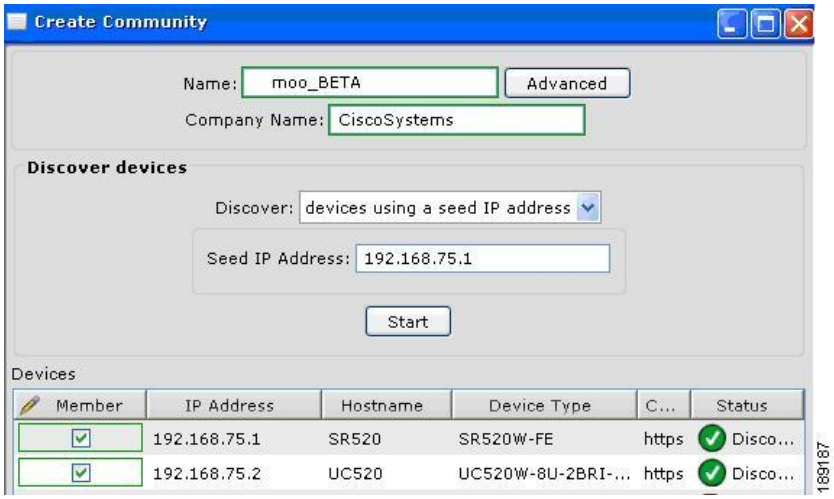
The configuration of the Cisco SR500 is complete.

Creating a Community

To create a community that includes both the Cisco UC500 and the Cisco SR500, do the following:

Step 1: Start Configuration Assistant, and select Create community in the Connect window. Click Connect.

Step 2: In the Create Community window, enter a name for the community.



Create Community

Name: moo_BETA

Company Name: CiscoSystems

Discover devices

Discover: devices using a seed IP address

Seed IP Address: 192.168.75.1

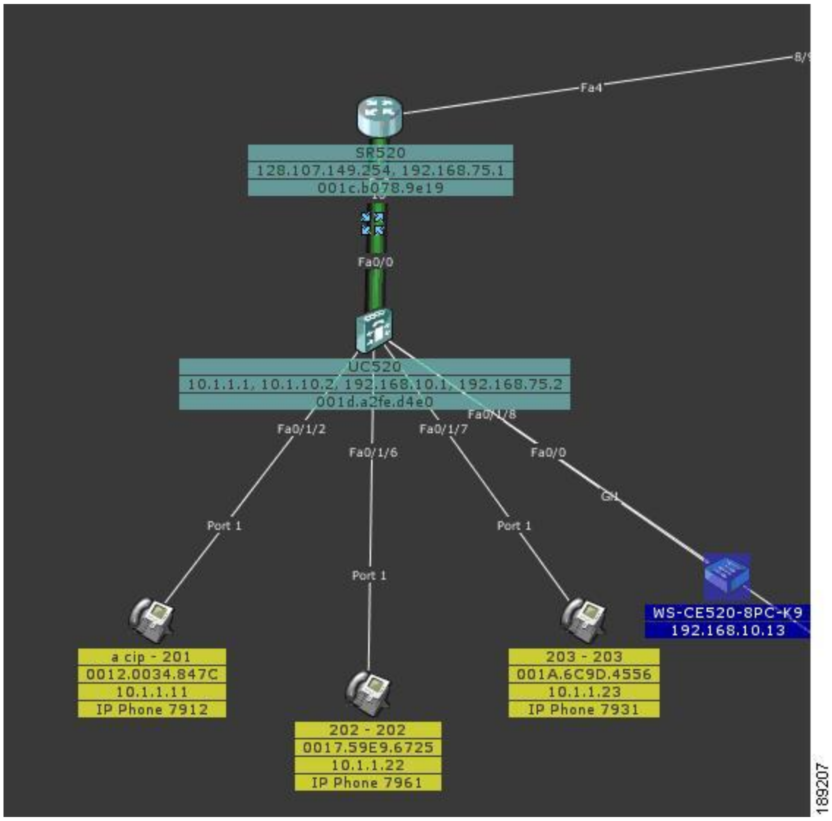
Devices

Member	IP Address	Hostname	Device Type	C...	Status
☑	192.168.75.1	SR520	SR520W-FE	https	✓ Disco...
☑	192.168.75.2	UC520	UC520W-8U-2BRI-...	https	✓ Disco...

Step 3: Enter the Cisco SR500 IP address in the Seed IP Address field. Click Start.

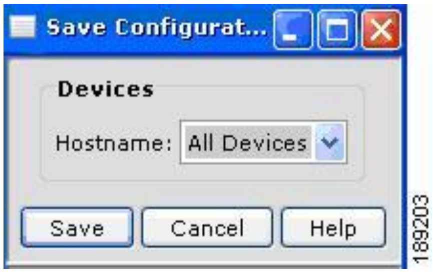
Step 4: When prompted, enter the Cisco UC500 and the Cisco SR500 administrator usernames and passwords. Click OK.

Step 5: In Topology view, verify that the Cisco UC500 is connected behind the Cisco SR500.



Step 6: Go to Configure > Save Configuration.

Step 7: Select All Devices in the Hostname menu. Click Save.



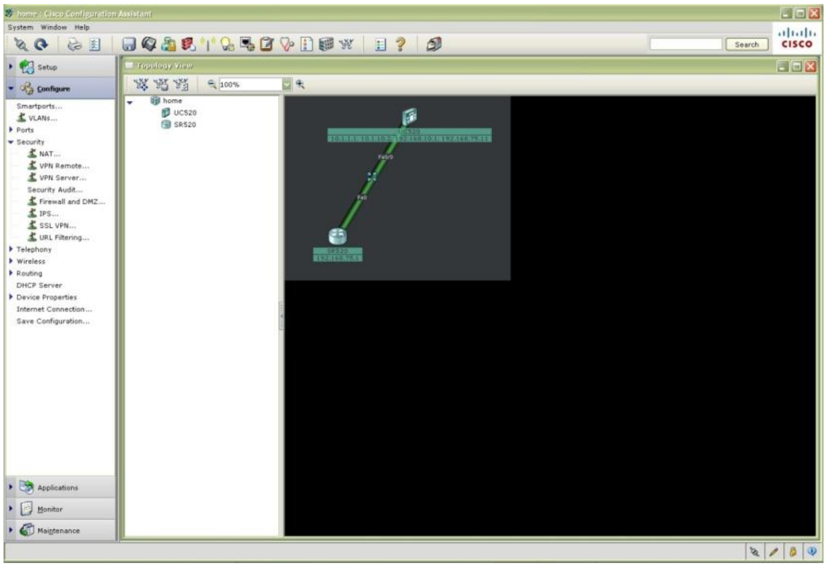
Hostname: All Devices

The configuration is complete.

You can now connect your Cisco Configuration Assistant PC to any LAN port on the Cisco UC500 or Cisco SR500 to access the community you created, allowing you to monitor the network and modify the device configurations.

You should connect all LAN devices, such as PCs, IP phones, printers, switches, and access points, to the Cisco UC500 LAN ports to access the WAN or the Internet from the LAN devices. LAN devices connected to the UC500 have secure access to the WAN and the Internet, because they are protected by the security features you enabled on the Cisco SR500.

You might choose to connect DMZ devices, such as Web servers or email servers, to the Cisco SR500.



Configuring NAT on the SR520

Step 1: Go to Configure → Security → NAT

Step 2: Some default translations exist, but to add another, click the Add button.

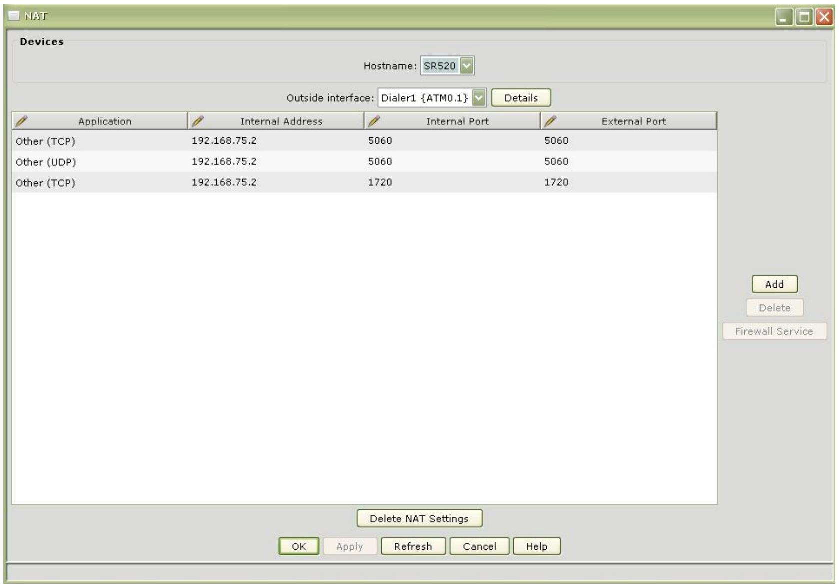
Step 3: Choose a server type from the Type of Service menu

Step 4: In the Private IP address field, enter the IP address the server uses on the internal network.

Step 5: In the Original Port field, enter a port number for the inside device. This is the port number used by the server to accept service request from the internal network.

Step 6: In the Translated Port field, enter a port number that NAT is to use for the translation. This is the port used by the server to accept service request from the Internet.

Step 7: Click OK to save and close the window.



Hostname: SR520

Outside interface: Dialer1 {ATM0.1}

Application	Internal Address	Internal Port	External Port
Other (TCP)	192.168.75.2	5060	5060
Other (UDP)	192.168.75.2	5060	5060
Other (TCP)	192.168.75.2	1720	1720

Enabling VPN Remote and Server Settings on the SR520
Consult the FirstLook Lab 8A section. The directions on the UC500 and SR520 are the same.

Enabling the Firewall on the SR520

Step 1: Go to Configure → Security → Security Audit → Firewall and DMZ

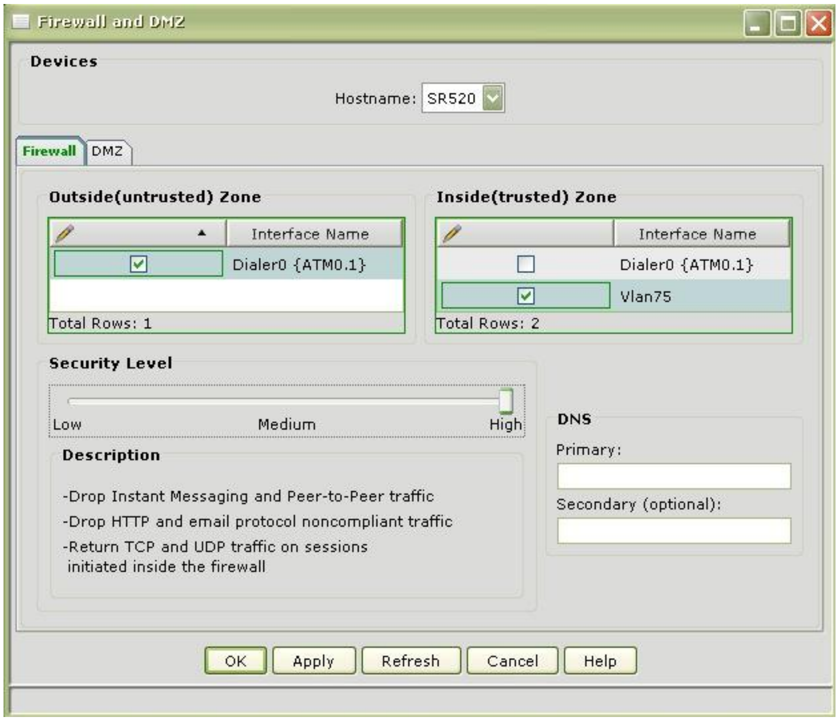
Step 2: Select the Hostname of the SR520.

Step 3: From the Outside Zone menu, select the Outside (untrusted) interface

Step 4: From the Inside Zone menu, select the Inside (trusted) interface

Step 5: Select a Low, Medium, or High security level. Medium and High security settings require DNS IP addresses.

Step 6: Click Apply to enable the firewall on the SR520



Devices

Hostname: SR520

Outside(untrusted) Zone

▲	Interface Name
☑	Dialer0 {ATM0.1}

Total Rows: 1

Inside(trusted) Zone

	Interface Name
☐	Dialer0 {ATM0.1}
☑	Vlan75

Total Rows: 2

Security Level

Low Medium High

Description

-Drop Instant Messaging and Peer-to-Peer traffic
-Drop HTTP and email protocol noncompliant traffic
-Return TCP and UDP traffic on sessions
initiated inside the firewall

DNS

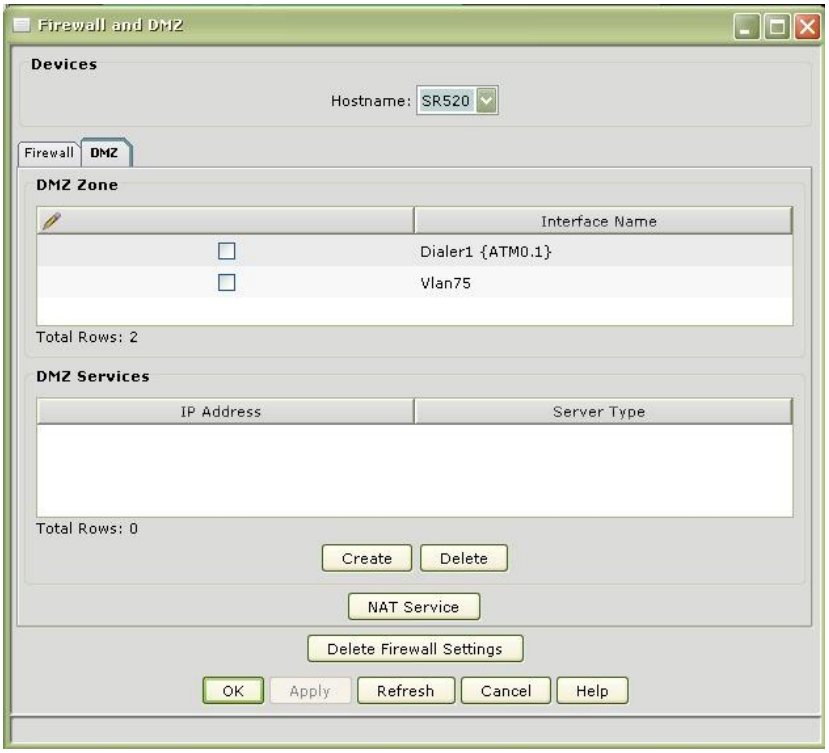
Primary:

Secondary (optional):

Enabling a DMZ on the SR520

Step 1: Select the DMZ tab

Step 2: Typically you will want to create a new VLAN before doing this step. If you select an outside or inside interface already identified with the firewall, a warning dialog appears.



Firewall and DMZ

Devices

Hostname: SR520

DMZ Zone

	Interface Name
□	Dialer1 {ATM0.1}
□	Vlan75

Total Rows: 2

DMZ Services

IP Address	Server Type

Total Rows: 0

Step 3: Click Create and use the Create DMZ Service window.

Hostname: SR520

Dialer1 {ATM0.1}

Total Rows: 2

Total Rows: 0

Enabling IPS on the SR520

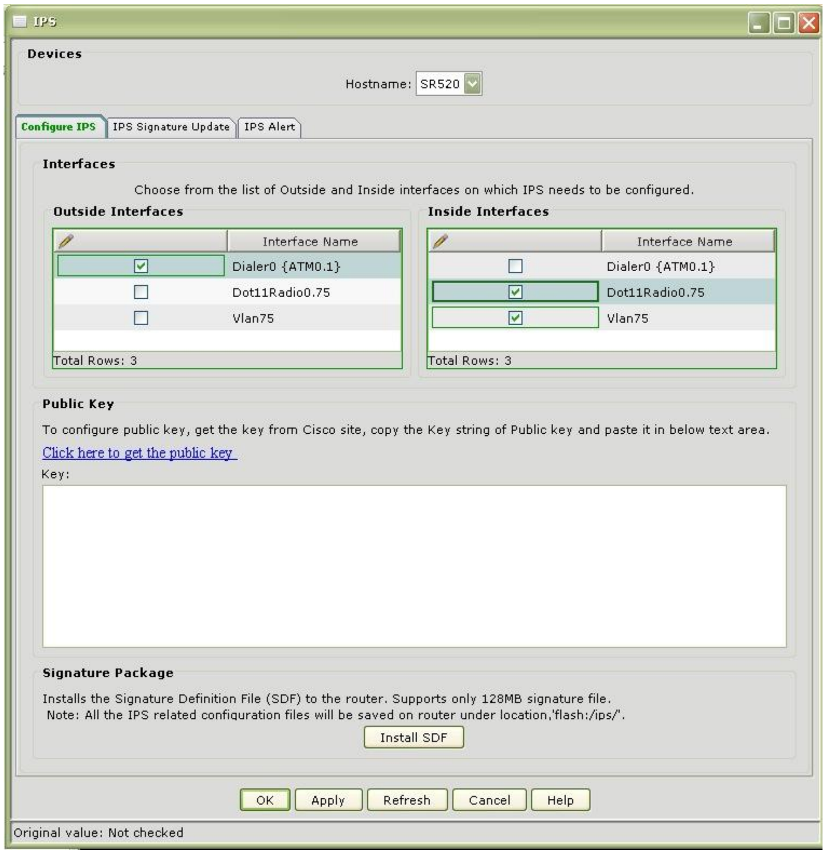
Step 1: Go to Configure→Security → Security Audit → IPS

Step 2: Select the Hostname of the SR520.

Step 3: From the Outside Interfaces menu, select the Outside interface

Step 4: From the Inside Interfaces menu, select the Inside interface. If you have a wireless SR520, the wireless LAN will also show up and can be selected.

Step 5: Click the "Click here to get the public key" link. Log in if prompted. Paste the key into the Public Key field.



Devices

Hostname: SR520

Interfaces

Choose from the list of Outside and Inside interfaces on which IPS needs to be configured.

Outside Interfaces

	Interface Name
☑	Dialer0 {ATM0.1}
□	Dot11Radio0.75
□	Vlan75

Total Rows: 3

Inside Interfaces

	Interface Name
□	Dialer0 {ATM0.1}
☑	Dot11Radio0.75
☑	Vlan75

Total Rows: 3

Public Key

To configure public key, get the key from Cisco site, copy the Key string of Public key and paste it in below text area.

Click here to get the public key

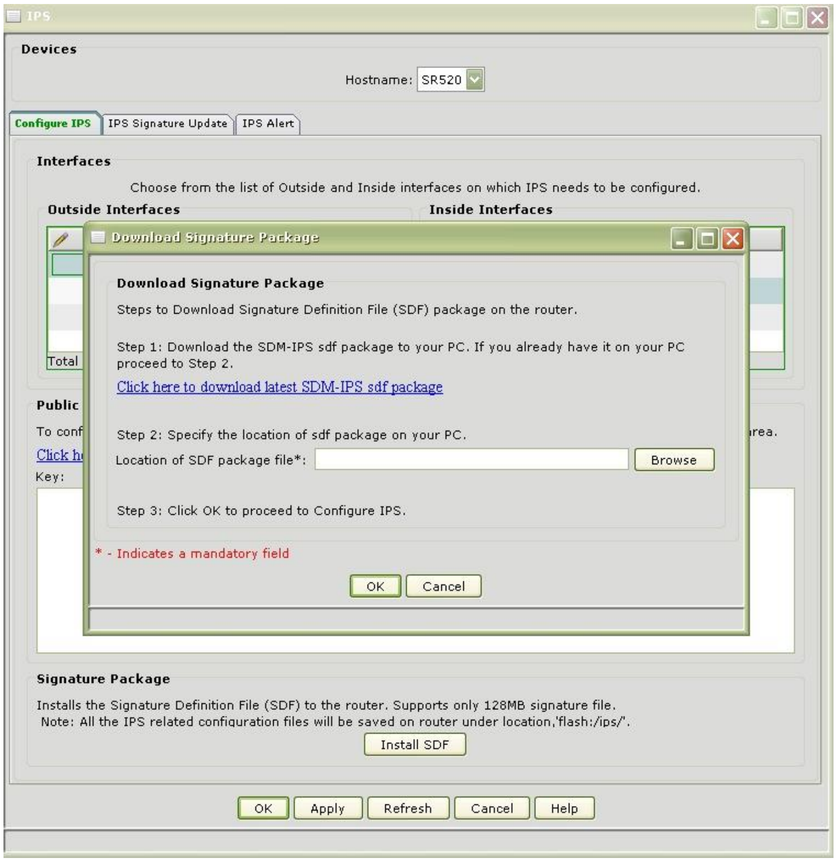
Key:

Signature Package

Installs the Signature Definition File (SDF) to the router. Supports only 128MB signature file.
Note: All the IPS related configuration files will be saved on router under location,'flash:/ips/'.

Original value: Not checked

Step 6: Click the Install SDF button. If you do not yet have the sdf package, click the "Click here to download latest SDM-IPS sdf package". Log in if prompted. Download the package to your computer, click browse and select the package, then click the OK button.



Download Signature Package

Steps to Download Signature Definition File (SDF) package on the router.

Step 1: Download the SDM-IPS sdf package to your PC. If you already have it on your PC proceed to Step 2.

Click here to download latest SDM-IPS sdf package

Step 2: Specify the location of sdf package on your PC.

Location of SDF package file*: Browse

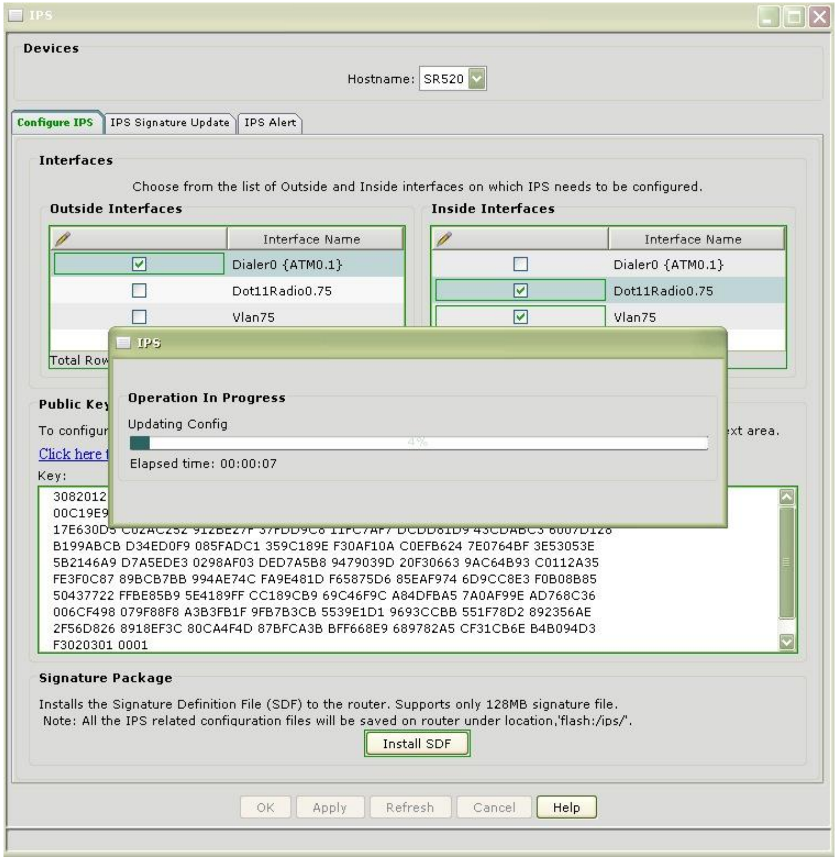
Step 3: Click OK to proceed to Configure IPS.

* - Indicates a mandatory field

Signature Package

Installs the Signature Definition File (SDF) to the router. Supports only 128MB signature file.
Note: All the IPS related configuration files will be saved on router under location,'flash:/ips/'.

Step 7: The signatures will be installed



Devices

Hostname: SR520

Interfaces

Choose from the list of Outside and Inside interfaces on which IPS needs to be configured.

Outside Interfaces

	Interface Name
☑	Dialer0 {ATM0.1}
□	Dot11Radio0.75
□	Vlan75

Total Row

Inside Interfaces

	Interface Name
□	Dialer0 {ATM0.1}
☑	Dot11Radio0.75
☑	Vlan75

IPS

Operation In Progress

Updating Config

4%

Elapsed time: 00:00:07

Public Key

To configur ext area.

Click here t

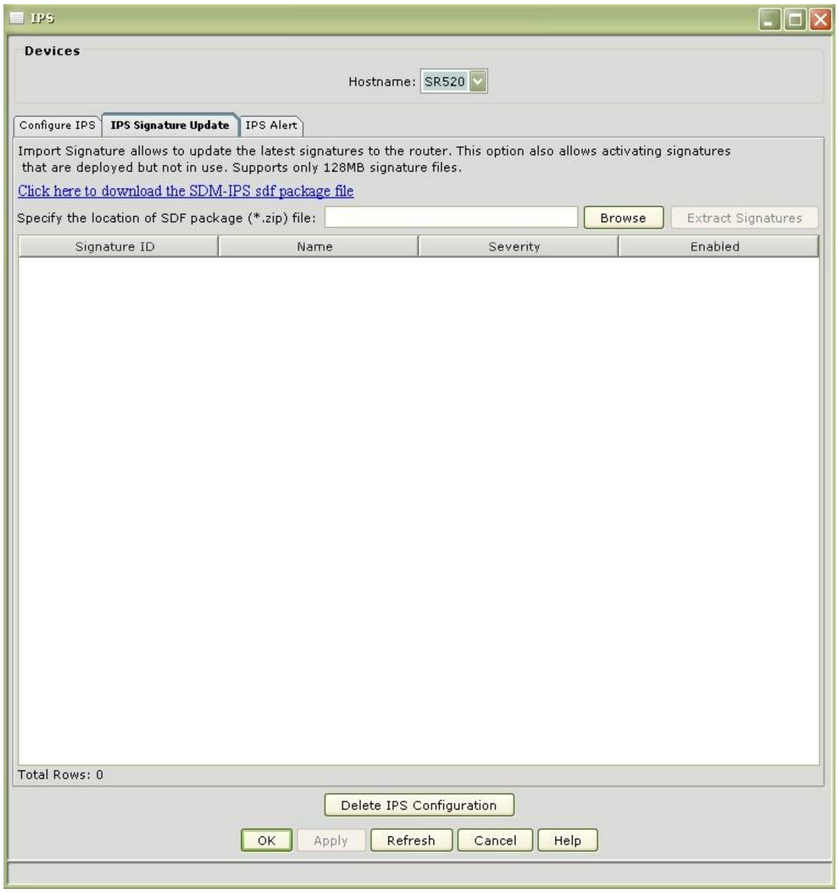
Key:

```
3082012
00C19E9
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

Signature Package

Installs the Signature Definition File (SDF) to the router. Supports only 128MB signature file.
Note: All the IPS related configuration files will be saved on router under location,'flash:/ips/'.

Step 8: IPS Signature Updates are uploaded on the IPS Signature Update tab.



Hostname: SR520

Import Signature allows to update the latest signatures to the router. This option also allows activating signatures that are deployed but not in use. Supports only 128MB signature files.

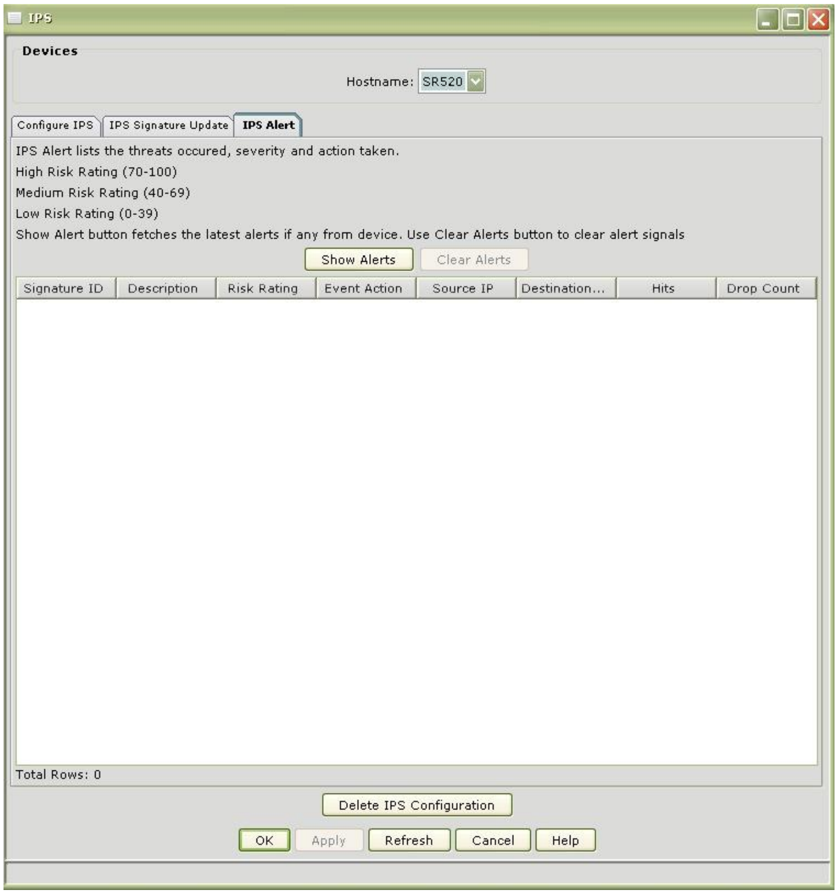
Click here to download the SDM-IPS sdf package file

Specify the location of SDF package (*.zip) file:

Signature ID	Name	Severity	Enabled

Total Rows: 0

Any traffic matching IPS signatures will be displayed on the IPS Alert tab.



Hostname: SR520

IPS Alert lists the threats occured, severity and action taken.

High Risk Rating (70-100)

Medium Risk Rating (40-69)

Low Risk Rating (0-39)

Show Alert button fetches the latest alerts if any from device. Use Clear Alerts button to clear alert signals

Signature ID	Description	Risk Rating	Event Action	Source IP	Destination...	Hits	Drop Count

Total Rows: 0

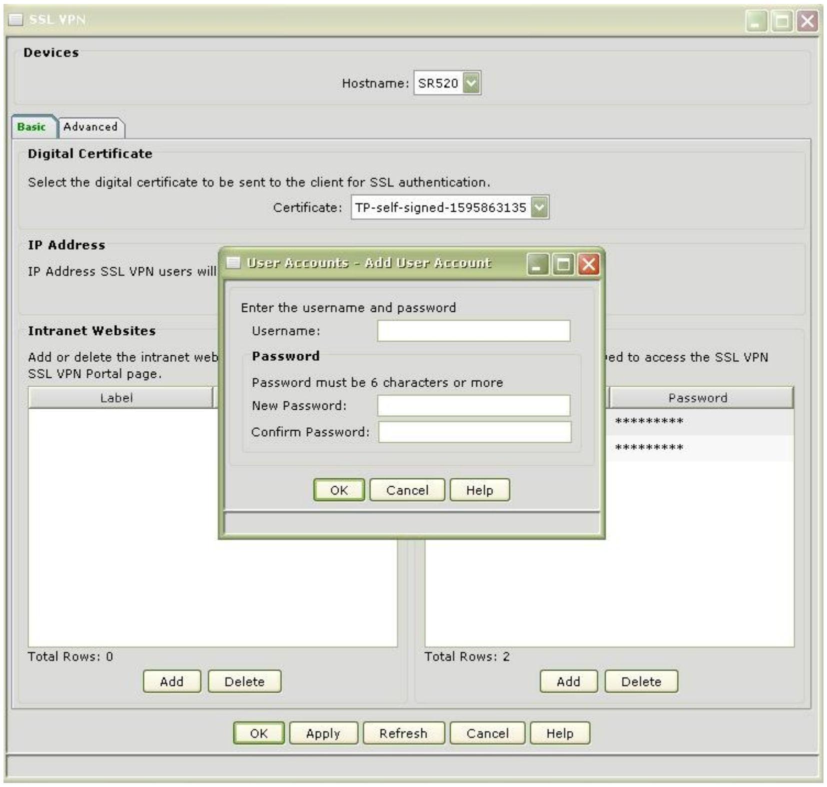
Enabling SSL VPN on the SR520

Note: A static IP address on the WAN interface is required for SSL VPN. Basic SSL VPN configuration only enables clientless browsing of a secure intranet. See the advanced tab for additional options.

Step 1: Go to Configure → Security → Security Audit → SSL VPN

Step 2: Select the Hostname of the SR520.

Step 3: Add a new user account for the SSL VPN connection.



SSL VPN

Devices

Hostname: SR520

Digital Certificate

Select the digital certificate to be sent to the client for SSL authentication.

Certificate: TP-self-signed-1595863135

IP Address

IP Address SSL VPN users will

Intranet Websites

Add or delete the intranet web
SSL VPN Portal page.

ed to access the SSL VPN

Label	

	Password
	*********
	*********

Total Rows: 0

Total Rows: 2

User Accounts - Add User Account

Enter the username and password

Username:

Password

Password must be 6 characters or more

New Password:

Confirm Password:

Step 4: To add an Intranet Website to be displayed in the SSL VPN portal page, click Add, and use the Intranet Websites Add URL window.

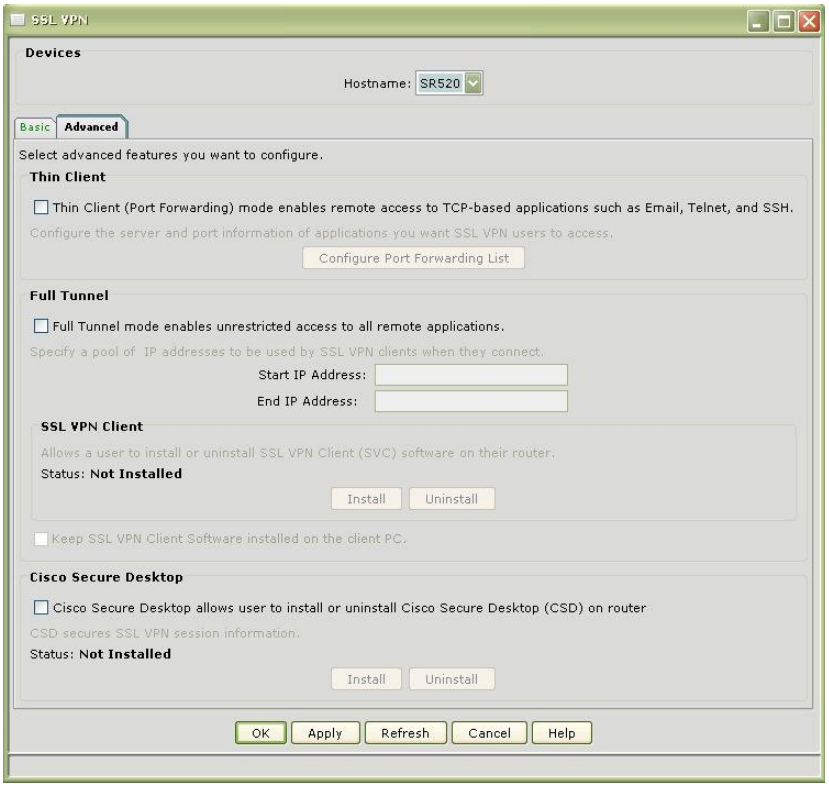
Advanced Options

There are three SSL VPN modes.

- Default - The default mode is the clientless mode allowing secure access to private web content.
- Thin Client - Enabling the Thin Client extends the default capability by allowing remote access to TCP-based application static ports.
- Full Tunnel - Full tunnel mode provides a lightweight SSL VPN tunneling client for network layer access to virtually any application.

It is recommended that the SSL VPN Client be added to the router so that it can be downloaded by clients.

Finally, enabling the Cisco Secure Desktop is recommended for optimal security. Enabling this allows CSD to write session data in an encrypted format to a special vault area of the client's disk. This is removed at the end of the VPN session. Only a machine with Cisco Secure Desktop installed can establish an SSL VPN connection when this box is checked.



Hostname: SR520

Select advanced features you want to configure.

□ Thin Client (Port Forwarding) mode enables remote access to TCP-based applications such as Email, Telnet, and SSH.

Configure the server and port information of applications you want SSL VPN users to access.

□ Full Tunnel mode enables unrestricted access to all remote applications.

Specify a pool of IP addresses to be used by SSL VPN clients when they connect.

Start IP Address:

End IP Address:

Allows a user to install or uninstall SSL VPN Client (SVC) software on their router.

Status: **Not Installed**

□ Keep SSL VPN Client Software installed on the client PC.

□ Cisco Secure Desktop allows user to install or uninstall Cisco Secure Desktop (CSD) on router

CSD secures SSL VPN session information.

Status: **Not Installed**

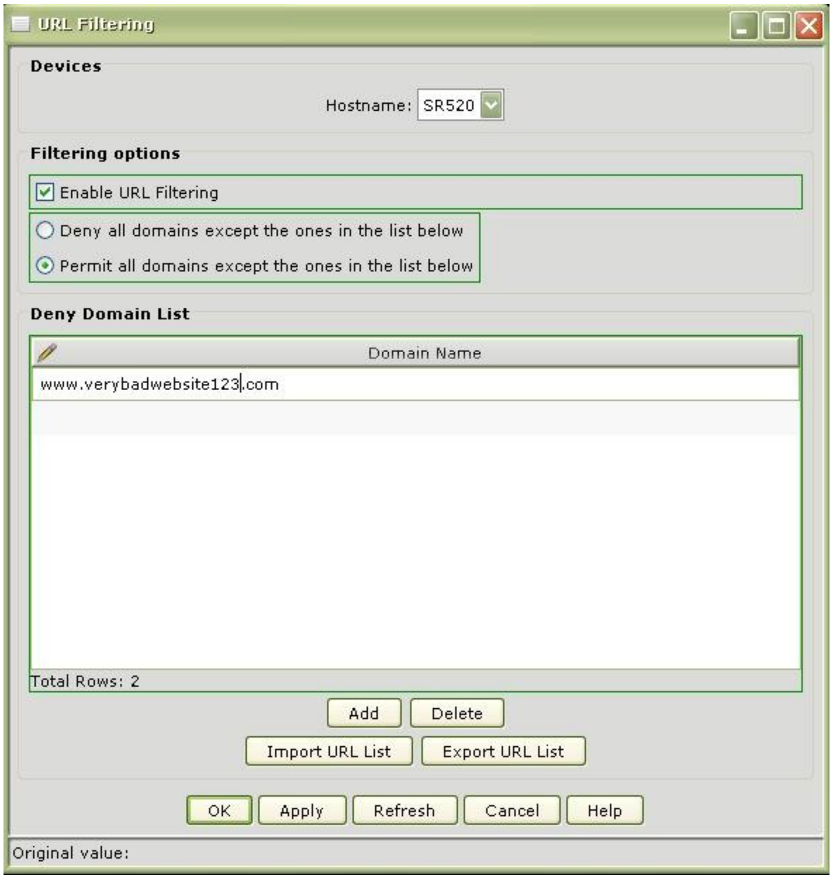
Enabling URL Filtering on the SR520

Step 1: Go to Configure → Security → Security Audit → URL Filtering

Step 2: Select the Hostname of the SR520.

Step 3: Select "Enable URL Filtering"

Step 4: This example has allowed all domains except the one manually entered into the Deny Domain List box.



Hostname: SR520

☑ Enable URL Filtering

○ Deny all domains except the ones in the list below

● Permit all domains except the ones in the list below

Domain Name
www.verybadwebsite123.com

Total Rows: 2

Original value:

Enabling Wireless on the SR520

Consult the FirstLook Lab 7B section. The directions on the UC500 and SR520 are the same.

APPENDIX D: Prompt Management

Prompt management is completed using one of two methods. The Windows Sound Recorder can be utilized or alternatively by using the Prompt Management system on Cisco Unity Express.

Note: Due to the virtual nature of this lab sound, which is required when using the Window Sound Recorder, cannot be recorded. The Sound Recorder steps have been included for your reference. Please proceed to USING PROMPT MANAGEMENT.

The following steps outline how to use the Windows Sound Recorder utility to record prompts for the Auto Attendant.

Step 1: Open the Windows Sound Recorder by selecting Start → Programs → Accessories → Entertainment → Sound Recorder.

Step 2: Click the Red Record button to start recording

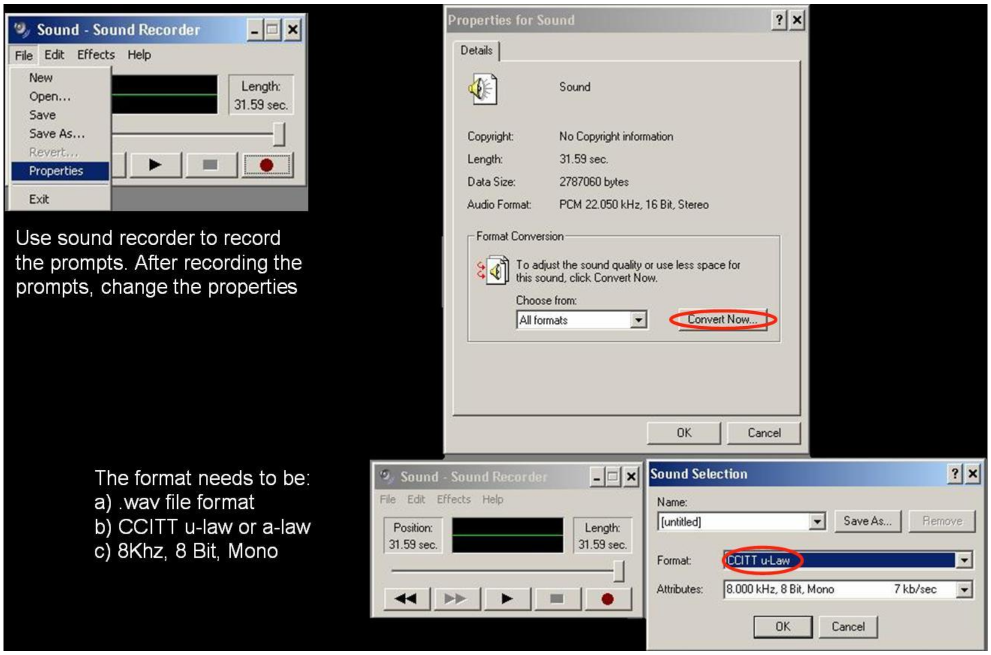
Step 3: After the prompts are recorded, click on File → Properties and change the Audio format as outlined in the screen shot below.

Step 4: In the Format Conversion section, click on Convert Now.

Step 5: In the Sound Selection window scroll up and select CCITT u-law.

Step 6: Click OK.

Step 7: Ensure that the Audio Format in the Properties page reflects CCITT u-law, 8Khz, 8 Bit, Mono.



Use sound recorder to record the prompts. After recording the prompts, change the properties

Copyright: No Copyright information
Length: 31.59 sec.
Data Size: 2787060 bytes
Audio Format: PCM 22.050 kHz, 16 Bit, Stereo

Format Conversion
To adjust the sound quality or use less space for this sound, click Convert Now.
Choose from: All formats
Convert Now...

The format needs to be:
a) .wav file format
b) CCITT u-law or a-law
c) 8Khz, 8 Bit, Mono

Name: [untitled]
Format: CCITT u-Law
Attributes: 8.000 kHz, 8 Bit, Mono 7 kb/sec

Using CUE for Prompt Management

Using CUE for prompt management requires the use of the CUE Web GUI and some CLI commands. The following configuration steps are divided into 3 main sections.

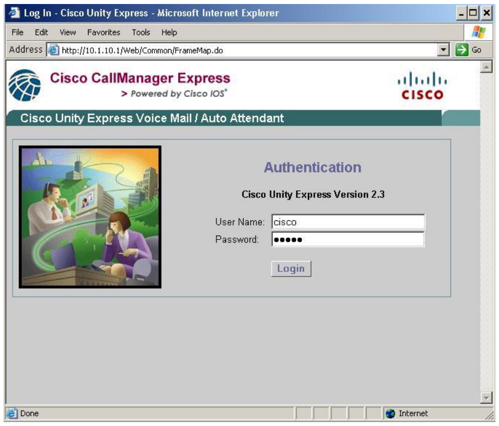
Section A configures a Call-in number for the prompt-management script,
Section B assigns admin rights to a specific extension, and
Section C provides guidance of the CLI configuration on the UC520.

SECTION A

Configuring the Call-in number or trigger for the prompt management script.

Step 1: Launch a web browser on the student desktop and go to http://10.1.10.1.

Step 2: Login using the administrator username cisco and password cisco.


Log In - Cisco Unity Express - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Go
Cisco CallManager Express
> Powered by Cisco IOS
CISCO
Done
Internet

Address http://10.1.10.1/Web/Common/FrameMap.do

Cisco Unity Express Voice Mail / Auto Attendant

Authentication

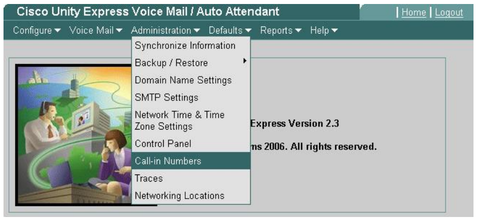
Cisco Unity Express Version 2.3

User Name: cisco
Password: ●●●●●

Login

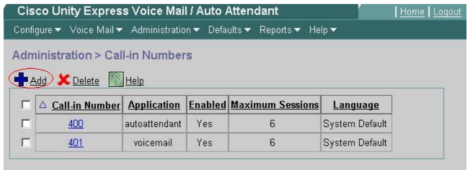
Step 3: Click on Administration → Call-in Numbers

Step 4: Click on Add



Express Version 2.3

ms 2006. All rights reserved.



Administration > Call-in Numbers

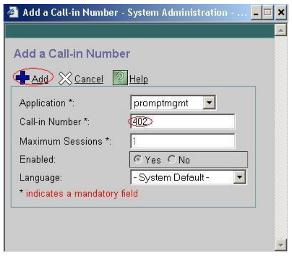
□	△ Call-in Number	Application	Enabled	Maximum Sessions	Language
□	400	autoattendant	Yes	6	System Default
□	401	voicemail	Yes	6	System Default

Step 5: In the Add a call-in Number window select promptmgmt from the Application drop down list.

Step 6: Configure the ‘Call-in Number’ as 402

Step 7: Click on Add. Close the Add a Call in Number window.

Step 8: Ensure that the new call-in number appears under Administrator → Call-in Numbers.

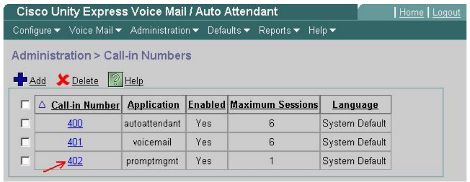


Add a Call-in Number - System Administration - ...

Add a Call-in Number

Application *:	promptmgmt
Call-in Number *:	402
Maximum Sessions *:	1
Enabled:	● Yes ○ No
Language:	- System Default -

* indicates a mandatory field



Cisco Unity Express Voice Mail / Auto Attendant

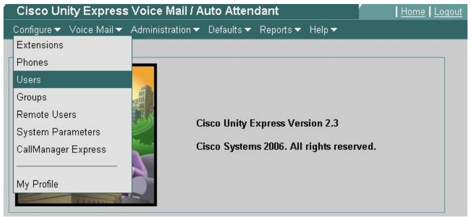
Administration > Call-in Numbers

□	Call-in Number	Application	Enabled	Maximum Sessions	Language
□	400	autoattendant	Yes	6	System Default
□	401	voicemail	Yes	6	System Default
□	402	promptmgmt	Yes	1	System Default

SECTION B

Assignment of administrator rights to extension 201.

Step 1: Click on Configure → Users



Cisco Unity Express Voice Mail / Auto Attendant

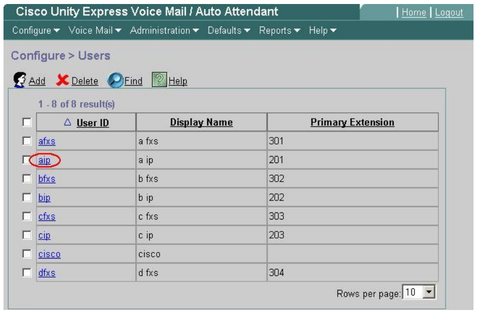
Cisco Unity Express Version 2.3

Cisco Systems 2006. All rights reserved.

Step 2: Click on the username aip. A User Profile window displays with the parameters for user A IP's account.

Step 3: Set the PIN to 789.

Step 4: Click Apply. Do not close the Parameter window.



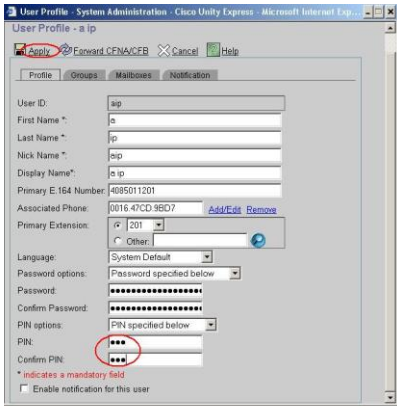
Cisco Unity Express Voice Mail / Auto Attendant

Configure > Users

1 - 8 of 8 result(s)

□	User ID	Display Name	Primary Extension
□	afxs	a fxs	301
□	aip	a ip	201
□	bfxs	b fxs	302
□	bip	b ip	202
□	cfxs	c fxs	303
□	cip	c ip	203
□	cisco	cisco	
□	dfxs	d fxs	304

Rows per page: 10



User Profile - System Administration - Cisco Unity Express - Microsoft Internet Exp...

User Profile - a ip

User ID:	aip
First Name *:	a
Last Name *:	ip
Nick Name *:	aip
Display Name*:	a ip
Primary E.164 Number:	4085011201
Associated Phone:	0016.47CD.9BD7
Primary Extension:	● 201 ○ Other:
Language:	System Default
Password options:	Password specified below
Password:	••••••••••••••••••
Confirm Password:	••••••••••••••••••
PIN options:	PIN specified below
PIN:	•••
Confirm PIN:	•••

* indicates a mandatory field

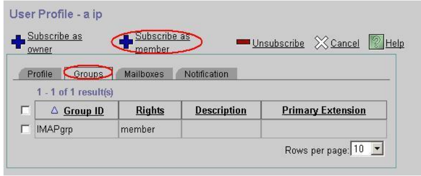
□ Enable notification for this user

Step 5: Click on the Groups tab, notice that the list contains IMAPgrp.

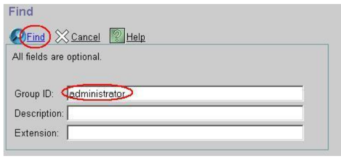
Step 6: Click on Subscribe as member.

Step 7: Type in Administrator for the Group ID.

Step 8: Click Find.



□	Group ID	Rights	Description	Primary Extension
□	IMAPgrp	member		



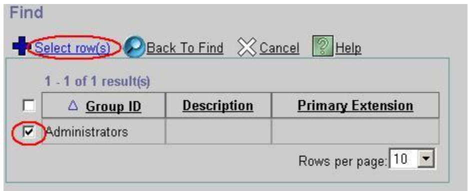
Group ID: administrator
Description:
Extension:

Step 9: Select the Group ID Administrators

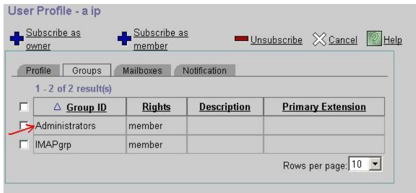
Step 10: Click on Select row(s).

Step 11: Ensure aip shows as a member of the administrator group.

Step 12: Close the User Profile window.



□	Group ID	Description	Primary Extension
☑	Administrators		



□	Group ID	Rights	Description	Primary Extension
□	Administrators	member		
□	IMAPgrp	member		

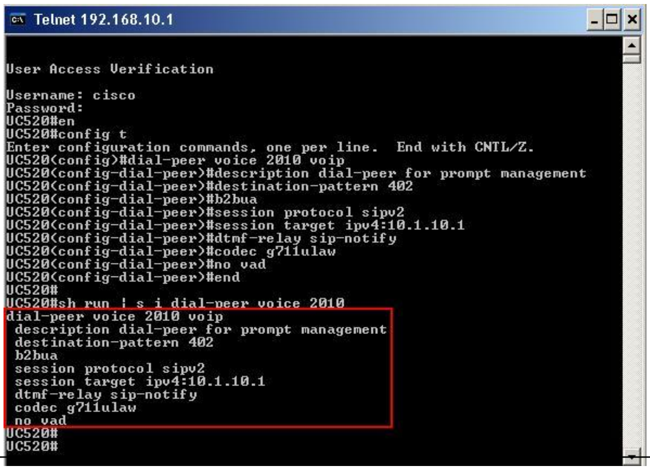
SECTION C

Step 13: Telnet to the UC520 IP Address of 192.168.10.1 using MS-DOS or cmd window. The username is cisco and password is cisco.

Step 14: Enter enable mode by typing 'en' (short for enable) at the router prompt if it does not show a # symbol.

Step 15: Use the following CLI to add a dial-peer for prompt-management. This can be cut and pasted or typed one line at a time. The 'config t' (or configuration terminal) command puts the router into configuration mode.

```
config t
dial-peer voice 2010 voip
description dial-peer for prompt management
destination-pattern 402
b2bua
session protocol sipv2
session target ipv4:10.1.10.1
dtmf-relay sip-notify
codec g711ulaw
no vad
end
```



```
User Access Verification

Username: cisco
Password:
UC520#en
UC520#config t
Enter configuration commands, one per line.  End with CNTL/Z.
UC520(config)#dial-peer voice 2010 voip
UC520(config-dial-peer)#description dial-peer for prompt management
UC520(config-dial-peer)#destination-pattern 402
UC520(config-dial-peer)#b2bua
UC520(config-dial-peer)#session protocol sipv2
UC520(config-dial-peer)#session target ipv4:10.1.10.1
UC520(config-dial-peer)#dtmf-relay sip-notify
UC520(config-dial-peer)#codec g711ulaw
UC520(config-dial-peer)#no vad
UC520(config-dial-peer)#end
UC520#
UC520#sh run | s i dial-peer voice 2010
dial-peer voice 2010 voip
 description dial-peer for prompt management
 destination-pattern 402
 b2bua
 session protocol sipv2
 session target ipv4:10.1.10.1
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
UC520#
UC520#
```

Note: The following recording of a prompt steps are for reference only and cannot be completed in this exercise due to the lack of recording capability in the remote pods. Please review this step and then proceed to step 21.

Step 16: Go off-hook on any phone and dial 402 to trigger the prompt-management script.

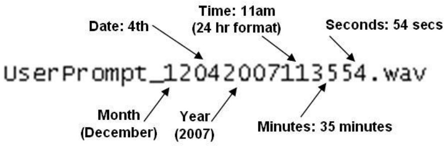
Step 17: The script will prompt for an extension/pin (followed by #). Use extension 201 and pin 789.

Step 18: Select option 2 to Administer Custom Prompt.

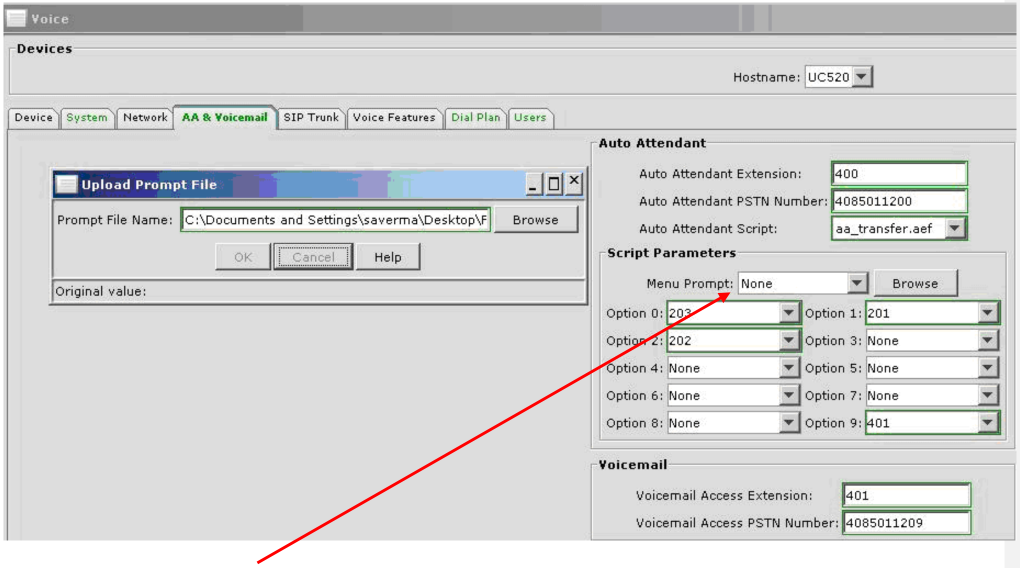
Step 19: Press 1 to record a new prompt.

Step 20: After recording the prompt, press 1 to save the prompt before terminating the call.

The prompts recorded are in the format:



If you recorded a prompt using the Windows Sound Recorder tool click on the Browse button next to the menu prompt to upload the prompt.



Hostname: UC520

Prompt File Name: C:\Documents and Settings\saverma\Desktop\F

Original value:

Auto Attendant Extension: 400
Auto Attendant PSTN Number: 4085011200
Auto Attendant Script: aa_transfer.aef

Menu Prompt: None

Option 0:	203	Option 1:	201
Option 2:	202	Option 3:	None
Option 4:	None	Option 5:	None
Option 6:	None	Option 7:	None
Option 8:	None	Option 9:	401

Voicemail Access Extension: 401
Voicemail Access PSTN Number: 4085011209

If the prompt was recorded using Prompt Management, then first refresh the voice window. This can be done by either clicking on the refresh icon on top left corner or by closing and re-launching the voice window. Once the window is refreshed, select the prompt from the Menu Prompt drop down menu.

APPENDIX E: PPPoE on the WAN

Introduction:
PPPoE can also be configured on the WAN interface of the UC520. One example of this WAN deployment would be to connect the WAN interface though Ethernet to a DSL modem. The DSL modem would be connected to a Service Provider. The PPPoE configuration would then have to reside either on the DSL modem or can also be configured on the UC520.

Objective:
In this exercise, PPPoE will be configured on the UC520 on the WAN interface using CCA. Understand the pre-requisite steps needed to enable PPPoE on the WAN interface.

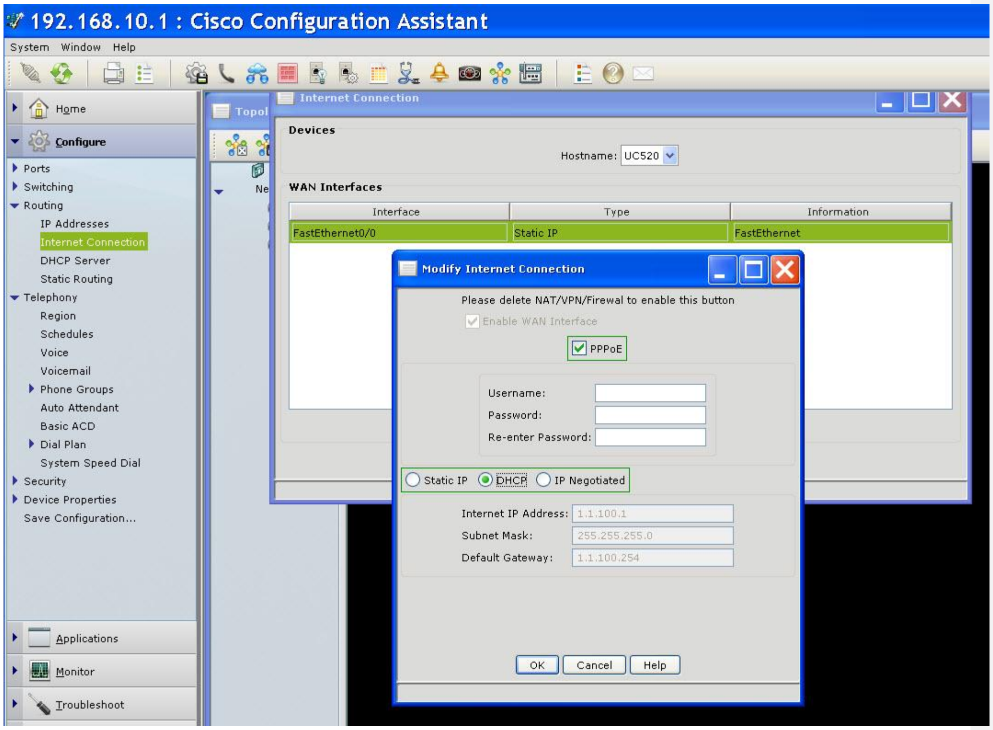
Exercise Set-up:
Refer to the main diagram.

Setup Steps:
Step 1: Launch CCA and login with the username 'cisco' and password 'cisco'.

Step 2: Let it discover the network and connected devices.

Step 3: Click on Configure → Routing → Internet Connection

Step 4: Select WAN Interface FastEthernet 0/0 and click on modify



Devices

Hostname: UC520

WAN Interfaces

Interface	Type	Information
FastEthernet0/0	Static IP	FastEthernet

Modify Internet Connection

Please delete NAT/VPN/Firewal to enable this button

☑ Enable WAN Interface

☑ PPPoE

Username:

Password:

Re-enter Password:

○ Static IP ● DHCP ○ IP Negotiated

Internet IP Address: 1.1.100.1

Subnet Mask: 255.255.255.0

Default Gateway: 1.1.100.254

Step 5: Check PPPoE button, enter username, password and select DHCP. Click OK

Step 6: Click Apply and then OK on the Internet Connection screen

Step 7: Click on Configure → Security → NAT

Step 8: Delete NAT settings and click OK

Step 9: Select Dialer0/FastEthernet0/0 as the outside Interface and click Apply and then OK

Verification Steps:

Step 1: Telnet into the UC520 from workstation 1 or workstation 3.

Step 2: Check if the Dialer0 interface is UP/UP using the ‘show ip interface brief’ command from the UC520# prompt.

APPENDIX F: Configuring IPSEC VPNs between sites on the UC520

This Appendix builds on Exercise-8 which covered inter site dialing. To configure the underlying IPSEC VPNs between sites please refer to the below link:

IPSEC with QoS:
http://www.cisco.com/en/US/products/ps6635/products_white_paper09186a0080189080.shtml

A sample config for EVEN POD (POD 2) to ODD POD (POD 1) is shown below

NOTE: The WAN IP for EVEN POD is 1.1.100.12 and for ODD POD is 1.1.100.11

```
!
crypto isakmp policy 1
authentication pre-share
group 2
crypto isakmp key sbcs address 1.1.100.11
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
!
crypto map vpn 6 ipsec-isakmp
set peer 1.1.100.11
set transform-set vpn-test
match address 199
!
!
!
interface FastEthernet0/0
ip address 1.1.100.12 255.255.255.0
crypto map vpn
!
!
!
access-list 199 permit ip 10.1.1.0 255.255.255.0 any
access-list 199 permit ip 1.1.100.12 255.255.255.0 any
```

APPENDIX G: IOS Dial-Peer Configuration

Introduction:
This appendix goes over a feature in the UC520 software (IOS) called dial peers which are the core for routing calls out the IP network (VoIP) or TDM interfaces (POTS) such as FXO, T1 / E1 PRI on the UC520. Essentially the dial-peers in the configuration define the dial plan for calls going through the UC520. The appendix will introduce this concept of dial-peers and some basics.

NOTE: In general, dialplan customization should be done through the CCA. This is section is intended only as a reference to users who have a high degree of IOS and CLI experience. If IOS CLI must be used, please make sure to follow the Out-of-Band Configuration Guidelines posted below:

Reference:

Cisco Configuration Assistant 1.9 Out of Band Configuration Guidelines
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_assistant/version1_9/out_of_band_reference/cca_oob_config_guidelines.pdf

http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080147524.shtml

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a0080080aec.html

Objective:
The default configuration on the UC520 as well as Cisco Configuration Assistant (CCA) does leverage dial-peers for a lot of the call routing / dial plan functionality. The objective is to show what the dial-peer CLI pushed down means to a certain extent. It will also go over a couple of examples of using dial-peers such as for least cost routing or translating digit strings. All configurations will be done using the command line interface (CLI). After completion of this lab – you should have a simplistic overview of dialplan and call routing in UC520 / SBCS.

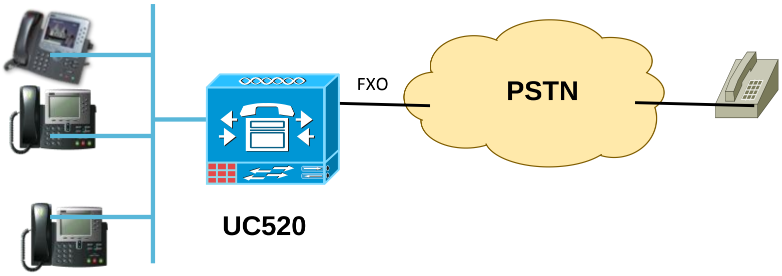
Overview:

- **Types of Dial Peers**

A dial peer is essentially a route to a particular destination. Dial peers establish logical connections, or call legs, to complete an end-to-end call. Cisco voice-enabled routers support five types of voice dial peers but two types are of greater significance for SBCS:

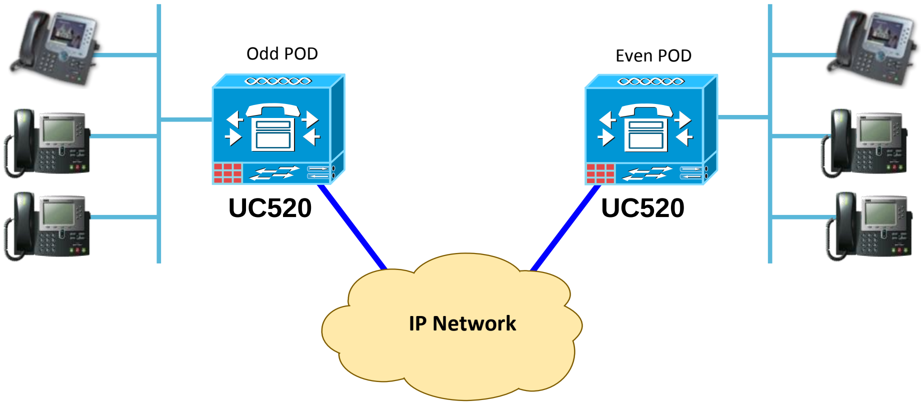
Step 1: POTS dial peers: Used for traditional telephony network (TDM) including FXO, FXS, BRI, T1 / E1 PRI etc. Below is an example of how a POTS dial peer is used to route calls starting with 9 + 7 digits i.e. a Local call in North America. Also, using [2-9] implies that the 2nd digit dial will be between the range of 2 to 9 and the remaining 6 digits can be anything from 0 to 9.

```
dial-peer voice 5000 pots
destination-pattern 9[2-9]……
port 0/1/0
```



Step 2: VoIP dial peers: Used for routing calls over the IP network to an IP address or DNS hostname. The 2 main VoIP protocols used are H.323 (default) or SIP (recommended). Typical examples for uses of VoIP dial-peers in UC520 are to route calls to voicemail / AA (via CUE), route calls over a SIP trunk to a provider or inter site dialing (as shown in Lab #8B). Below is an example of a dial-peer on the Odd pod to route calls to the even pod using 82xxx.

```
dial-peer voice 5100 voip
destination-pattern 82…
session protocol sipv2 ←Using SIP as VOIP protocol
codec g711ulaw ← Using G711 as the VOIP codec
session target ipv4:10.10.10.2 ← Defines IP address to send VOIP call to
no vad
dtmf-relay rtp-nte
```



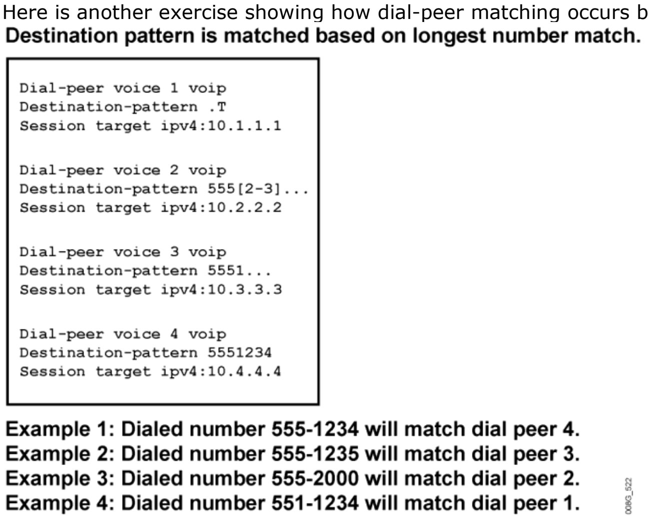
Outbound Dial-peer matching patterns

Dial-peers route on the value after the destination-pattern CLI under each dial-peer. Common destination pattern wildcards are

Pattern	Explanation
Digits such as 0-9,*,#	Digits one would dial on a phone
Period or dot (.)	Specifies any one wildcard digit
Comma (,)	Inserts a one-second pause
Square brackets [x-y]	Indicates a range of digits within the brackets
Percentage (%)	The preceding digit occurred zero or more times
T	Indicates a variable-length pattern

For the North American dial-plan, here is a typical example of what you would have
Local 7-digit dialing → **destination-pattern 9[2-9]......**
Long Distance 11-digit "1+" dialing → **destination-pattern 91[2-9]..[2-9]......**
International dialing → **destination-pattern 9011T**
Emergency or 911 → **destination-pattern 9911**

Here is another exercise showing how dial-peer matching occurs based on the below config:



Destination pattern is matched based on longest number match.

```
Dial-peer voice 1 voip
Destination-pattern .T
Session target ipv4:10.1.1.1

Dial-peer voice 2 voip
Destination-pattern 555[2-3]...
Session target ipv4:10.2.2.2

Dial-peer voice 3 voip
Destination-pattern 5551...
Session target ipv4:10.3.3.3

Dial-peer voice 4 voip
Destination-pattern 5551234
Session target ipv4:10.4.4.4
```

Example 1: Dialed number 555-1234 will match dial peer 4.
Example 2: Dialed number 555-1235 will match dial peer 3.
Example 3: Dialed number 555-2000 will match dial peer 2.
Example 4: Dialed number 551-1234 will match dial peer 1.

Least Cost routing

Outbound dial-peer matching is primarily based on the called-number matching the destination-pattern as shown above. However in case the destination-pattern is EXACTLY the same, then the tie breaker used is something known as preference that is configured under the dial-peer. The lower the preference, the higher the priority of that dial-peer getting chosen.

In the below example, let us assume that a customer has a primary route of the SIP trunk for long distance calls, in the event that the SIP trunk is down, they want to route calls over a backup analog line on FXO port 0/1/0.

```
dial-peer voice 5001 voip
 description SIP Trunk dial-peer for Long Distance
 destination-pattern 91[2-9]..[2-9]……
 session protocol sipv2
 codec g711ulaw
 session target dns:sipconnect.cisco.com
 no vad
 dtmf-relay rtp-nte
!
dial-peer voice 5000 pots
 description Backup FXO dial-peer for Long Distance
 destination-pattern 91[2-9]..[2-9]……
 preference 5
 port 0/1/0
!
```

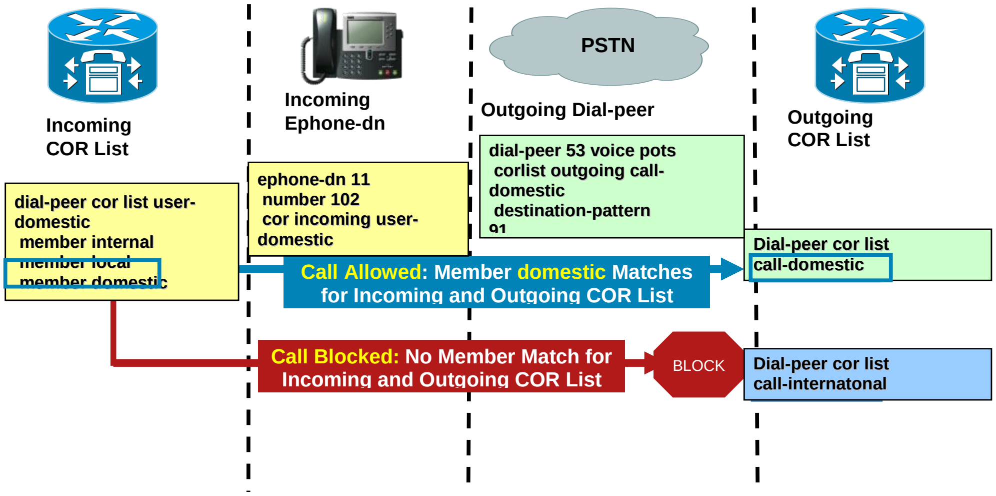
The default preference is “0” (default CLIs will NOT show up in the config) and hence the primary route chosen is the SIP trunk dial-peer versus the FXO dial peer.

Class of Restrictions (COR)

COR provides a way to deny certain calls based upon the incoming and outgoing settings on dial peers and ephone-dns. Each dial peer and ephone-dn can have one incoming COR and one outgoing COR.

The incoming COR list indicates the capacity of the dial peer to initiate certain classes of calls.

The outgoing COR list indicates the capacity required for an incoming dial peer to deliver a call via this outgoing dial peer.



Incoming COR List

Incoming Ephone-dn

PSTN

Outgoing Dial-peer

Outgoing COR List

```
dial-peer cor list user-
domestic
 member internal
 member local
 member domestic
```

```
ephone-dn 11
 number 102
 cor incoming user-
domestic
```

```
dial-peer 53 voice pots
 corlist outgoing call-
domestic
 destination-pattern
91
```

```
Dial-peer cor list
call-domestic
```

Call Allowed: Member **domestic** Matches for Incoming and Outgoing COR List

Call Blocked: No Member Match for Incoming and Outgoing COR List

```
Dial-peer cor list
call-internatonal
```

```
dial-peer cor custom
 name internal
 name local
 name domestic
 name international
!
dial-peer cor list call-domestic
 member domestic
!
dial-peer cor list user-domestic
 member internal
 member local
 member domestic
!
dial-peer voice 5003 pots
 corlist outgoing call-domestic
 description ** FXO pots dial-peer **
 destination-pattern 91............
 port 0/1/0
!
ephone-dn  11  dual-line
 number 102
 corlist incoming user-domestic
```

Reference for further information:
http://www.cisco.com/en/US/tech/tk652/tk90/technologies_configuration_example09186a008019d649.shtml

Using Translation rules

The UC500 allows for digit manipulation via a feature known as Voice Translation rules. The digit manipulation can be applied to called numbers or calling numbers (caller ID) and can be applied when the call is received or sent out to another destination by the UC500. For example, in Lab 6 during the inter site dial-plan an example was shown on how to setup inter site dialing with 5 digits – on each UC500 digit translation was done translate the called number from 5 digits to the 3 digit extension local to the UC500. The translation rules are typically applied on the basis of matching a given digit string and then manipulating that. This digit string & manipulation uses wildcard matching via regular expressions.

In the below example – the intent is to manipulate all caller ID going out the SIP trunk to match the main number (eg 408 555 1200):

Step 1: Define the match pattern and digits that this should be manipulated to:

```
voice translation-rule 10001
 rule 1 /^.*/ /4085551200/
```

Step 2: Define what is being manipulated (meaning called or calling number)

```
voice translation-profile PSTN_OUTBOUND_CID
 translate calling 10001
```

Step 3: Apply the profile to the outbound dial-peer in this case – it's the SIP Trunk dial-peer:

```
 dial-peer voice 5001 voip
 translation-profile outgoing PSTN_OUTBOUND_CID
```

Another example would be converting the main number to the internal AA extension. In this example the inbound call comes in on a T1 PRI trunk as 4085551200 and the internal AA is 400

Step 1: Define the match pattern and digits that this should be manipulated to:

```
  voice translation-rule 10002
    rule 1 /4085551200/ /400/
```

Step 2: Define what is being manipulated (meaning called or calling number)

```
 voice translation-profile AA_CALLED_NUMBER
  translate called 10002
```

Step 3: Apply the profile to the inbound dial-peer in this case – it's the POTS dial-peer:

```
 dial-peer voice 5100 pots
  incoming called-number 4085551200
  translation-profile incoming AA_CALLED_NUMBER
  direct-inward-dial
```

More complex examples are at:
http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml

APPENDIX H: Designing for a Scenario

In this lab, use the voice features that you have learned so far to fulfill the following customer's scenario.

Two employees on the system have primary extension 201 and 202. The operator has a primary extension 203. Make sure she can view the status of phones 201 and 202 as she may be required to transfer some calls to these employees' primary extension. In addition to the primary extensions, the employees have extensions 251, 252 and 253.

Extensions 201 and 202 are part of Sales department and extensions 251 and 252 are part of the marketing department.

The customer has FXO lines as well SIP trunks for PSTN access. For outbound calls, make sure to use the SIP trunk as the first choice, if the SIP trunk is down the calls should fallback to the analog FXO lines.

Incoming calls to FXO ports 0/1/0 and 0/1/1 should go directly to the Auto Attendant (AA). Use the prompt management system to record the AA greeting. The AA greeting should prompt caller to:

- Enter 1 for "Employee A" and 2 for "Employee B".
- For Sales department, the caller should be prompted to enter option 3. Unanswered calls to the sales department should be forwarded to the voicemail.
- For Marketing department, the caller should be prompted to enter option 4. Unanswered calls to the marketing department should be forwarded to the operator at extension 253.
- To be transferred to TAC helpline, the caller should be asked to enter option 5.
- Also if the caller has a mailbox on the system, he should be able to dial 9 to login and check his messages.
- Finally he should be able to dial 0 to reach the operator at extension 203.

Incoming calls to FXO ports 0/1/2 and 0/1/3 should ring all phones, and if there is no answer, then it should be forwarded to the AA.

There are DID numbers available from the SIP trunk provider. Incoming DIDs 4085xx1201 to 4085xx1203 should be mapped to the users' extension. All other DIDs should be forwarded to the AA.

A local directory should include contacts for TAC helpline at 800-553-2447 and PDI helpline at 800-462-4726. Users should be able to search and dial these numbers (configure appropriate prefixes). Users should use CME web GUI to configure their own speeddials.

BONUS SCENARIO:
Unanswered calls to sales department should hear a message "All our agents are busy, to continue to hold press 1, or press 0 to leave a message"

APPENDIX I: Device Manager Cross Launch

Introduction:
Many devices in the Cisco SBCS portfolio have embedded device managers which can be accessed from a web browser such as Microsoft Internet Explorer.

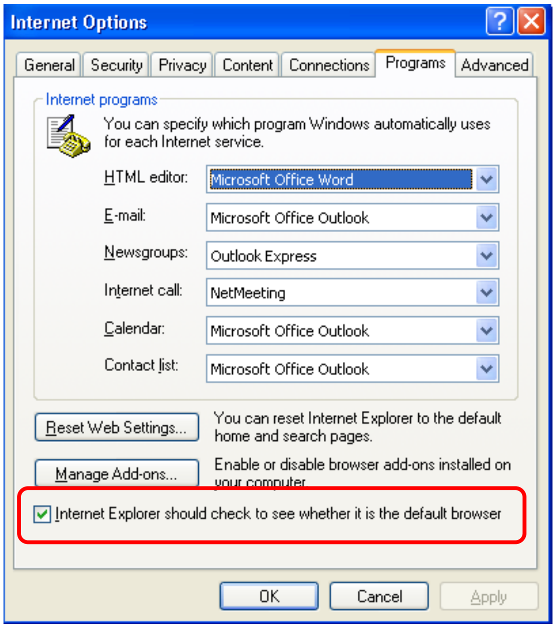
CCA can automatically launch the embedded device manager of a Cisco SBCS platform as long as the device can be discovered in the CCA network topology view and the CCA PC has network connectivity to the discovered device. This feature is called device manager cross launch.

Objective:
Using CCA, cross Launch the device manager for a switch connected to the UC500

Lab Set-up:
Refer to the main diagram. Connect a Cisco CE520 to the UC500 expansion port.

Device manager cross launch requires that a default web browser is configured on the PC that has CCA installed. While in most cases this should already be configured, the steps below outline how to set this up for common web browser software.

Microsoft Internet Explorer 6.0
Select Tools > Internet Options. Select "Internet Explorer should check to see whether it is the default browser" and click OK.



You can specify which program Windows automatically uses for each Internet service.

HTML editor: Microsoft Office Word

E-mail: Microsoft Office Outlook

Newsgroups: Outlook Express

Internet call: NetMeeting

Calendar: Microsoft Office Outlook

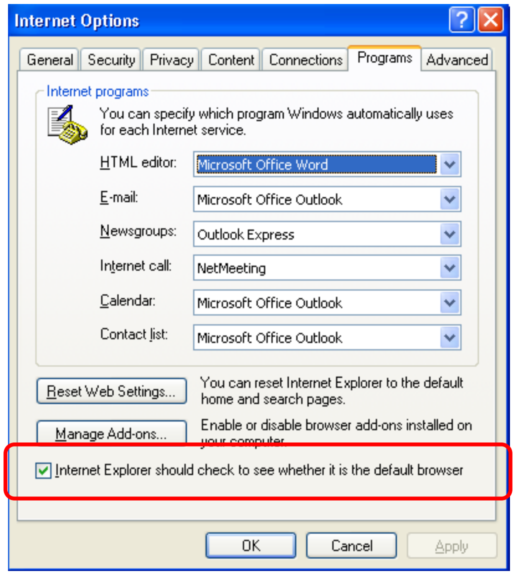
Contact list: Microsoft Office Outlook

You can reset Internet Explorer to the default home and search pages.

Enable or disable browser add-ons installed on your computer.

☑ Internet Explorer should check to see whether it is the default browser

Microsoft Internet Explorer 6.0
Select Tools > Internet Options > Programs tab. Select "Internet Explorer should check to see whether it is the default browser" and click OK



Internet programs

You can specify which program Windows automatically uses for each Internet service.

HTML editor: Microsoft Office Word

E-mail: Microsoft Office Outlook

Newsgroups: Outlook Express

Internet call: NetMeeting

Calendar: Microsoft Office Outlook

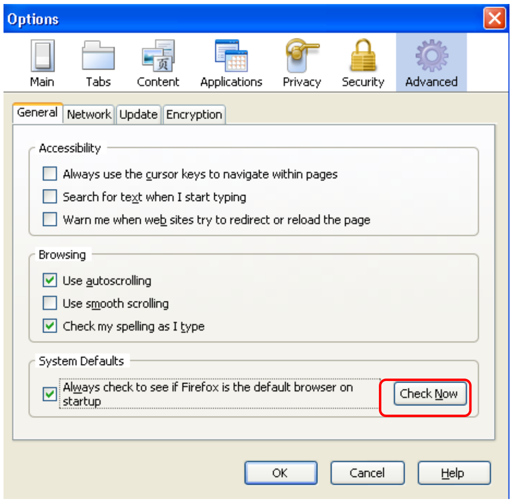
Contact list: Microsoft Office Outlook

Reset Web Settings... You can reset Internet Explorer to the default home and search pages.

Manage Add-ons... Enable or disable browser add-ons installed on your computer.

☑ Internet Explorer should check to see whether it is the default browser

Mozilla Firefox 3.0
Select Tools > Internet Options. Click Check Now. Click yes at prompt to make Firefox the default



Accessibility

☐ Always use the cursor keys to navigate within pages

☐ Search for text when I start typing

☐ Warn me when web sites try to redirect or reload the page

Browsing

☑ Use autoscrolling

☐ Use smooth scrolling

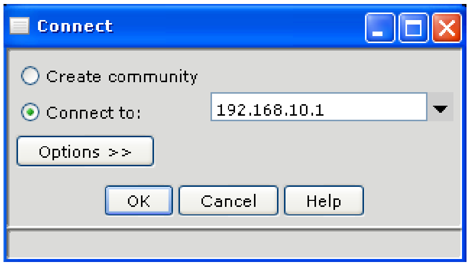
☑ Check my spelling as I type

System Defaults

☑ Always check to see if Firefox is the default browser on startup Check Now

Setup Steps:

Step 1: Launch CCA, connect directly to the IP address of the UC500 (192.168.10.1) and enter the username and password (cisco/cisco.) Let CCA discover the network and connected devices.



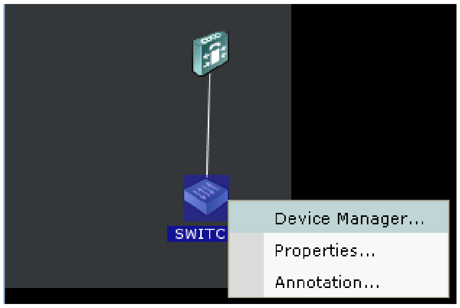
Connect

○ Create community

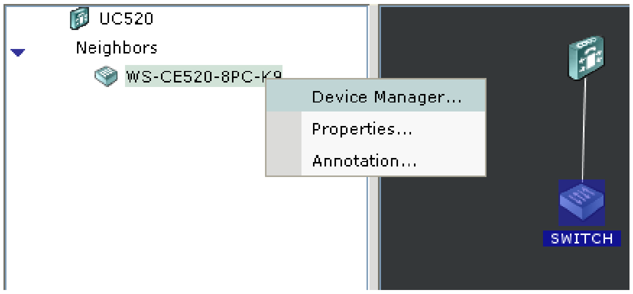
● Connect to: 192.168.10.1

Step 2: Check the topology to ensure the CE520 appears.

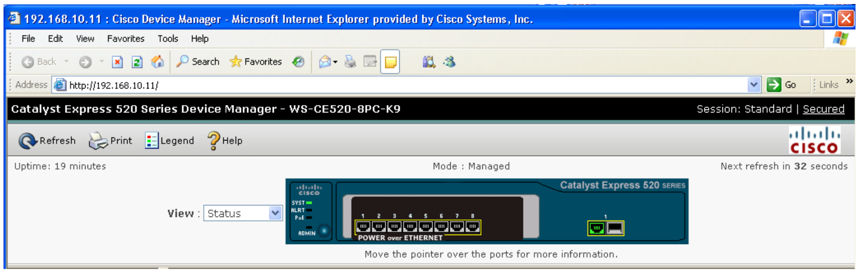
Step 3: Right click the switch icon in the Topology View window and select Device Manager.



You can also right click the switch icon under the Neighbors table and select Device Manager.



Step 4: The default web browser on your PC will automatically launch, with the URL pointing to the IP address of the switch. In the example below, the CE520 IP address is 192.168.10.11, hence the device manager cross launches with an URL of http://192.168.10.11



192.168.10.11 : Cisco Device Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address http://192.168.10.11/

Catalyst Express 520 Series Device Manager - WS-CE520-8PC-K9

Session: Standard | Secured

Uptime: 19 minutes

Mode : Managed

Next refresh in **32** seconds

View : Status

Move the pointer over the ports for more information.