4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

Building a VoIP Network with Multimedia Communication Server 5100

The First Book on Deploying Voice Over IP Products from Nortel Networks

- More VoIP phonelines than traditional PBX lines are being installed everyday. Are you prepared?
- Complete Coverage of the Nortel's Suite of Multimedia Communications Portfolio (MCP) Products
- Design, Install, Configure, and Troubleshoot the Entire Nortel Product Line

Larry Chaffin

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE
To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you will find an assortment of value-added features such as free e-booklets related to the topic of this book, URLs of related Web site, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs
Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE EBOOKS
For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These eBooks are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET
Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING
Syngress has a well-established program for site licensing our ebooks onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING
Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

Building a VoIP Network with Nortel's® Multimedia Communication Server 5100

Larry Chaffin

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Syngress Publishing, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	78GGPLM2W8
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Building a VoIP Network with Nortel's Multimedia Communication Server 5100

Copyright © 2006 by Syngress Publishing, Inc. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in Canada
1 2 3 4 5 6 7 8 9 0
ISBN: 1-59749-078-4

Publisher: Andrew Williams
Acquisitions Editor: Gary Byrne
Cover Designer: Michael Kavish
Indexer: Odessa&Cie
Page Layout and Art: Patricia Lupien
Copy Editors: Judy Eby, Edwina Lewis, and Adrienne Rebello

Distributed by O'Reilly Media, Inc. in the United States and Canada.
For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Acknowledgments

We wish to thank Nortel for permitting us to use the photos of the Nortel IP phones shown on pages 17 through 19 and to acknowledge that Nortel has not endorsed this publication and is not responsible in any way for the accuracy or completeness of its content.

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Mark Wilson, Tim Hinton, Kyle Hart, Sara Winge, Peter Pardo, Leslie Crandell, Regina Aggio Wilkinson, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Kathryn Barrett, John Chodacki, Rob Bullington, Kerry Beck, Karen Montgomery, and Patrick Dirden.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, Rosie Moss, David Lockley, Nicola Haden, Bill Kennedy, Martina Morris, Kai Wuerfl-Davidek, Christiane Leipersberger, Yvonne Grueneklee, Nadia Balavoine, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Chan, June Lim, and Siti Zuraidah Ahmad of Pansing Distributors for the enthusiasm with which they receive our books.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.

Lead Author

Larry Chaffin is the CEO/Chairman of Pluto Networks, a worldwide network consulting company specializing in VoIP, WLAN, and security. Larry is an accomplished author, and in addition to writing this book, he has contributed to Syngress Publishing's *Managing Cisco Secure Networks* (ISBN: 1-93183-656-6), Skype Me (ISBN: 1-59749-032-6), and Practical VoIP Security (ISBN: 1-59749-060-1). He has also coauthored/ghostwritten 11 other technology books on VoIP, WLAN, security, and optical technologies. Larry has more than 29 vendor certifications from companies such as Avaya, Cisco, HP, IBM, isc2, Juniper, Microsoft, Nortel, PMI, and VMware. He has been a principal architect designing VoIP, security, WLAN, and optical networks for many Fortune 100 companies in 22 countries. He is one of the most well respected experts in the field of VoIP in the world. Larry has spent countless hours teaching and conducting seminars/workshops around the world in the field of voice/VoIP and wireless networks. Larry is currently working on a Nortel MCS 5100 Service provider network and rollout scheduled for September 30, 2006, in Columbus, OH.

Dedication

This book is dedicated in loving memory of my grandmother, Jeanne Warner, who past away during the writing of this book. Her warm heart and spirit will be missed very much.

A Word from the Author

I would like to thank many people who helped me during the writing of this book. First and foremost, the staff at Syngress, Gary and Andrew. I could have not worked with two nicer people on my first solo book project. Also I would like to thank members of the Nortel team: Steve Cook, Denis Fortier, Curt Nelson, and Gary Shook. Without their help with providing screen shots or making systems available to me for screen shots, this book would be incomplete. Also thanks to my two puppies, Jordan and Clyde, who put up with many sleepless nights while I was writing through all hours of the night.

Even though we did not have room in this book for the Microsoft Outlook Client, Web Collaboration, or IP Phones options, we will be making this information available on the Syngress Web site when the book is purchased. This adjunct material should be available by September.

All proceeds from the royalties of this book will be donated to charity by Larry Chaffin on behalf of Pluto Networks and its Save the Homeless Campaign.

Contents

Foreword

The first thing I think of when talking about the MCS 5100 is what's not to like? It has everything that you would need for a system that will grow with your company, and it provides multimedia and IP phone support. When customers see this system, they react by saying, "Wow, it does all of that and more?" It is the kind of system that administrators who begin using it wonder how they got along without it.

But let's talk about the writing of this book. It took some time to write this book because many different people helped me obtain access to a system that I could mold and set up to meet my needs. They allowed me to take a full system, rip it bare, and reinstall everything just to get the screen shots and setup I needed. Friends are a great thing to have when you need help. Most of the writing for this book came when I was traveling back and forth to London, Tokyo, and Hong Kong.

Most of my friends wonder how I have time to do all of the work I do, travel, and write an entire book by myself. Well, it takes a lot of time management to do everything plus do other work. But if you want to know the truth, I would not have it any other way right now; being wanted and being busy are good things. When customers stop calling, and you are sitting around surfing the Web, you know there is a problem. So accessing a VPN to Canada all the time to configure an MCS 5100 and make other changes is not so bad.

Some people have already asked me what is next for me. Well, I am thinking of a follow-up to this book already. There is some good news about the new partnership between Nortel and Microsoft for use of the SIP Client. Don't be surprised if you see the PC Client from the MCS 5100 in use with the Microsoft LCS soon. Remember you heard it here first.

I have found it is easy to stop and smell the roses when you do something great, such as writing a book. But it is even better when you can take time to smell the roses while you are running with them in your hand.

—Larry Chaffin,
CEO/Chairman of Pluto Networks

Chapter 1

Getting Started with the MCS 5100

Solutions in this chapter:

- **What Is the MCS 5100?**
- **Application Tools**
- **Alliances**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

The Nortel Multimedia Communications Server (MCS) 5100 is one of the first systems to push SIP to the forefront ahead of its competitors in the voice over IP (VoIP) arena. It takes the best of both worlds from a PBX system and a computer application system and combines them into the system we will be looking at throughout this book. This first chapter provides a high-level overview of what the system is and what it is not, and a look at some of the major services provided by the MCS 5100.

To understand how this system works and how it operates with other systems, you need to have somewhat of an understanding of the SIP Protocol (see Chapter 8). Although the MCS 5100 can also provide and use H.323, most users and enterprise users are moving to SIP due with is complexity compared to H.323. Currently there are a few other major players that are following the lead of Nortel using SIP; for example, Cisco and Microsoft. In the Microsoft LCS and the new version of Call Manager both have gone to a SIP-based presence for their clients.

But Nortel has continued to evolve in front of the competitors by offering more than just a phone and voice mail. It has expanded into other areas of mobility such as personal digital assistants (PDAs) and wireless clients. The ability Nortel has to do SIP to endpoints such as those from Polycom has proven the potential of the MCS 5100 to expand outside the normal realm of a VoIP PBX. The system has the capability to move communication toward a single platform.

A group of components and applications that can all work on a single system provides users and administrators with a better experience than a dispersed system. An example of this is a user who is on the Nortel PC Client, using the instant messenger—at the same time he or she can receive and make calls to others, send files, and perform a whiteboard task. Also the user could be using a video call between one or more people at the same time. In a dispersed system a user would have to have three to nine different applications open at one time to do the same tasks as the MCS 5100.

This is the beauty of the Nortel MCS 5100 system in comparison to other PBXes or VoIP PBXes—it gives you everything you need at your fingertips and in easy reach for outstanding communications to users in and out of the enterprise.

What Is the MCS 5100?

The Multimedia Communications Server 5100 (MCS 5100) is a SIP-based application server (for information on SIP, see Chapter 8). It can deliver SIP-based multimedia and collaborative applications in either a LAN or WAN network. As with all VoIP PBX systems, you can have a choice between either a Nortel IP Phone at your desk and the PC Client softphone on your computer. If you would like the best of both worlds, the Nortel IP Phone and the PC Client will work together, or the PC Client can be used with the Nortel CS 1000 family of products for a PBX Converged Desktop.

Conferencing, collaboration, and video are main components within the MCS 5100. These components provide users with a full multimedia office experience not seen on other VoIP PBX systems.

Users of the MCS 5100 do not have to pay for costly audio conferencing and videoconferencing; the MCS 5100 provides these services within the system. These services are very scalable to any network. The system also provides a Web collaboration tool that allows users to not only make an audio or video call but also share or create documents in moments.

The MCS 5100 has addressed the issue of current security concerns about instant message usage within a network. Now you can have instant messaging in a secure VoIP network to and from your IP phone or PC Client. Being able to provide a secure instant messaging environment is a great feature of the MCS 5100; in collaboration with SIP-based user presence, this feature allows users to communicate in real time. Knowing who is available, if they are talking on the phone, or away from their desk provides users with valuable information during the day. This allows users to make better use of their time and have better control of their day.

As stated earlier, the MCS 5100 is an application server; this statement may be very puzzling to people who thought it was just a PBX. Nortel has stated that the MCS 5100 is not a PBX and not a VoIP PBX, but an application server that has the capability to transform enterprise communications. It

has the capability of your normal PBX and VoIP PBX, but brings much more to the user. If you are wondering why it is an application server, the MCS 5100 is made up or either a two- or four-server configuration; these servers are Sun Fire V100s or Sun Netra 240s (see Figures 1.1 and 1.2). Most people view a PBX as a chassis with many cards inserted into it, much like the Nortel CS 1000.

Figure 1.1 Two-Server Configuration

Figure 1.2 Four-Server Configuration

NOTE

The MCS 5100 platform runs on Solaris with an Oracle database. It is recommended that the engineer in charge of the installation, configuration, and troubleshooting of the system be very familiar with these systems. It does make working on the system much easier if you understand how the platform and database work.

Nortel was looking to provide the user with more than a simple phone to dial from; instead, the company wanted to provide a full and rich multimedia communications platform. The MCS 5100 combines communications services and collaborative services on a single platform. It brings together such services as Meet Me Conferencing, Ad Hoc Conferencing, Web Collaboration, White Boarding, File Exchange, Call Screening, and Presence-Based Routing. All of these services will be discussed in more detail later in the book and can be used with the IP phones and clients shown later.

The MCS 5100 can use any of the IP phones shown in Figure 1.3 plus the Multimedia PC Client, Multimedia Web Client, PC Client integrated with Microsoft Outlook, and Multimedia Wireless BlackBerry Client.

We will not discuss all the features on all the IP phones in great depth, but we will go over the 2004 and PC\Web Clients in other chapters. As it is described earlier, as a multimedia application server the users can still use an IP phone like a regular desk phone. The difference is what the MCS 5100 brings to the IP phone when compared to a regular phone. There are many more features than the normal pick up and dial. Users also have the choice of using a computer-based softphone like the PC Client.

Figure 1.3 IP Phones

NOTE

The MCS 5100 currently uses SIP and SIP T as its primary server protocol. Between the client and the MCS 5100, the system uses UNIStim, IPv4, and SIP as intercommunication protocols (for more information on SIP, see Chapter 8). Management protocols are handled by the system using XML, FTP, SNMP, Accounting, and IPDR (XML based). These are covered in more detail in another chapter.

Application Tools

The MCS 5100 provides the user with an array of application tools to use with an IP phone or the PC Client. Whether you're at your desk, on the road, or in the sky with the MCS 5100, you have ability to have full multimedia audio and videoconferences, as well as whiteboard, clipboard, and file exchanges using the PC Client. Another application tool is the Web Collaboration feature used in conjunction with a browser. This allows users to have the ability to share documents and other material in a Web-based environment.

In this section we briefly explain the applications used as tools within the MCS 5100. These tools are covered in more detail in different chapters throughout the book.

Collaboration Tools

The collaboration tools are what some people say set the MCS 5100 apart from its rivals at Avaya and Cisco. It provides all the tools listed in this section, while using your IP phone and PC Client. Whereas most companies require you to have multiple clients or applications open on your PC, the MCS 5100 requires only that you have the PC Client open to utilize these tools.

Audio and Videoconferencing

Conferencing services are provided by the MCS 5100 in the form of both audio and video. These services can be used with or without a PC Client or IP phone. These services can be point-to-point between two users, or more than two users may participate. Recognized endpoints and the local PSTN can be utilized with the MCS 5100.

Web Collaboration

This service allows users who are on a browser to share files interactively over the system. It is similar to Webex in that you may share files, but when used in conjunction with the PC Client you also have all of the tools, video, and conferencing at your fingertips.

Whiteboard, Clipboard, and File Exchange

This is a feature within the PC Client that allows users to work on a virtual whiteboard for drawings, send a Web page to another user, and also exchange files while on the PC Client.

Dynamic Presence and Routing

Since the MCS 5100 uses SIP as its protocol of choice, presence is used heavily within the system. Presence can be used within the PC Client or an IP phone. Presence works with routing to correctly send calls and users to proper routing endpoints.

Messaging

On the Internet, messaging, from instant to chat, has become a way of life. But the problem is that most companies rely on outside messaging services. The MCS 5100 provides a safe haven for all instant message users on one system. Since the instant message is integrated into the PC Client, it provides a secure platform for the company to use instant messaging within an enterprise environment.

This is the same for the chat rooms that are provided on the MCS 5100 system; rather than having to use public chat rooms to discuss work, employees can access their companies' chat rooms using the PC Client. This also provides a secure haven for your users to use chat rooms within your enterprise environment. Also if they happen to get a message while they are not at their desks, they can route the message or screen the message using the PC Client.

Instant Messaging

A great feature of the system is an internal instant messaging system on the MCS 5100; this can be used on the PC Client or IP phone. Having a secure instant messaging system is a goal of any enterprise network. The MCS 5100 provides this as well as encrypts the sessions from PC Client to PC Client or IP phone.

Chat Rooms (Public, Private, and Password Protected)

Along the same lines as an instant message, chat rooms have become very popular with online communities. The MCS 5100 provides users with an online chat system that can be used at anytime. So at anytime users can start their own chats and invite others; they could join a chat already established, such as a help desk chat. Also, chats can be private or public and can be password protected.

Message Screening and Routing

This feature allows the user to take messages being sent over the IP phone or PC Client and route them to different outlets or applications on the system.

Telephony Services

The following services are available on the MCS 5100 when using either the PC Client or an IP phone. Since these services are running off an application database, they have significant advantages over the same feature you would have on a normal POTS phone. In later chapters we will cover how and why these are some of the most utilized services on the MCS 5100.

Call Screening and Personalized Routes

The ability to move calls and route them effectively is what this feature is all about. Seeing who is calling and being able to send callers to another person or directly to voice mail are good features to have, but you may also respond to the call with an IM or reply from your PC Client or IP phone. Routes may be created for any phone number, user, or group that you would like to create. Calls can be sent anywhere for any number from the MCS 5100. Calls may be sent to multiple numbers one after the other and/or simultaneously.

Meet Me and Ad Hoc Conferencing

Meet Me Conferencing is a service that allows you to do either voice or video as described earlier. Ad Hoc Conferencing is the service that allows you to put one person on hold and add another, then another, and so on. This may be done on either voice or video calls.

Music on Hold

No one wants a user to sit on hold or in a conference room with no music. The MCS 5100 allows administrators to add whatever music they would like to the system for on-hold music.

Call Park and Pick Up

This feature allows the user to put a call on hold and pick up the call at another IP phone or PC Client on the system. The user is given a token for the call that has been parked, and they use the token to retrieve the call. A call may also be parked against another user on the system.

Professional Assistant Services

An assistant console may be added to any user so that they can take, screen, and handle all calls for another party. This also allows the attendant to see who is on hold for the other party, use instant messaging, and move the calls accordingly.

Mobility

The whole idea with the MCS 5100 is to be able to get what you need anywhere and anytime. This would mean you need to have the mobility on the system to stay connected. The MCS 5100, as shown in the following options, provides these services in the form of personalization and registration that you have on the Web, the PC Client, or IP phone.

Dynamic Registration

The ability to register to the system from any place in or out of the network is a great feature of the MCS 5100. A user can register, move, and then reregister to the system in a very dynamic way.

Personalization

On the system, users can manage their calls, messages, and conferences in a way that is personalized for them. Using the PC Client and Personal Agent, the user can customize all the features needed within the system. There is no more one profile or identity fits all, and when you are mobile with the system, you need these tools more to stay connected.

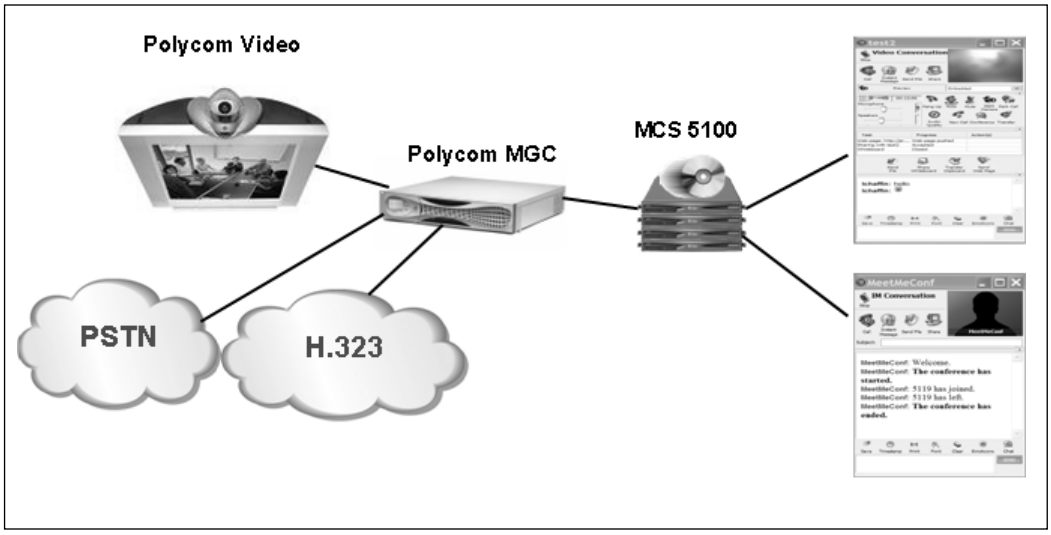
Alliances

Over the last few years Nortel has expanded its MCS 5100 solution to include other vendors. These vendors, such as RIM, which makes the BlackBerry handheld device; Polycom; and TANDBERG, have helped the MCS 5100 portfolio expand into new areas. In the following sections we will discuss the Polycom solution, which allows multipoint video to and from the MCS 5100. We'll taking your functions of the MCS 5100 on the road with your BlackBerry. Also Nortel has added application gateways to the portfolio. One company that has helped provide these services is Citrix.

Multipoint Video

One of the great features of the MCS 5100 is its capability of interacting with other machines to provide a full converged desktop using voice and video. This is very true with the partnership Nortel has with Polycom in the video arena. Although having all the aforementioned applications, features, and ability to perform audio and videoconferencing at your fingertips is good, being able to connect to business partners the same way is even better. The MCS 5100 can connect to other audio and video platforms using SIP advanced multipoint video conferencing, which enables full videoconferencing as seen in Figure 1.4.

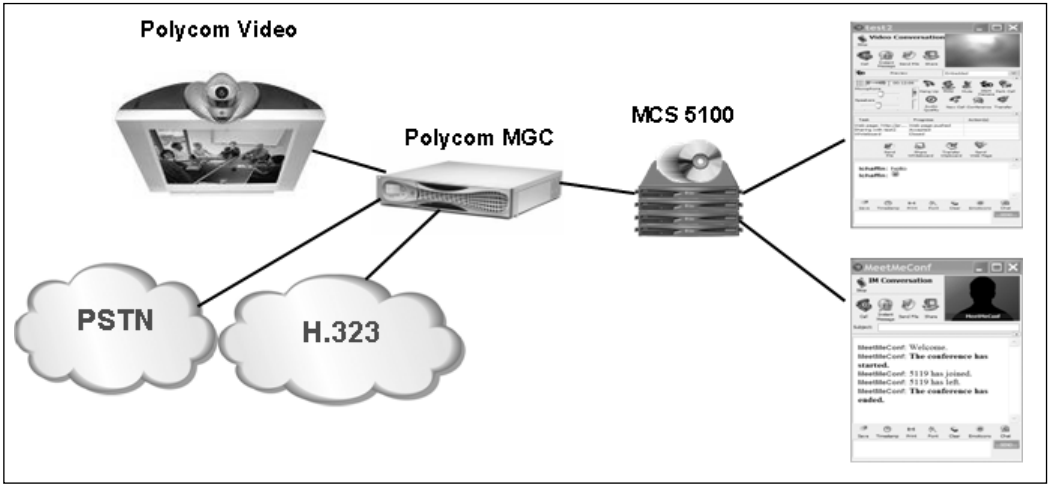
Figure 1.4 Multipoint Video



The SIP Polycom MGC platform registers as SIP endpoints with MCS 5100 to provide the MCU (Multipoint Control Unit) function on the system. Multiuser videoconferencing is now possible between all audio and video devices. So users from the outside can register to the MCU from other networks and also the PSTN. Now you may have secure audioconferencing and videoconferencing within your network, to a business partner, and to other platforms.

In Figure 1.4 this representation could be a configuration on a single network or in fact it could be two networks. The MCS 5100 could be within one network and the Polycom MGC could be in another network that in fact belongs to a partner, as seen in Figure 1.5. The MCS 5100 enables the network to communicate and connect to endless SIP points within and outside of the network. Multiple SIP endpoints can be added very simply to provide the user a much wider array of communications tools. The system also can connect to legacy videoconferencing devices, such as those based on H.320 and H.323.

Figure 1.5 Partner Network Video



BlackBerry Client

Nortel has teamed up with RIM to allow users access from the MCS 5100 to a client residing on a BlackBerry handheld device. The software is downloaded to the BlackBerry from your desktop and then it is as simple as changing network settings and logging in. The client will work on the BlackBerry service outside your network just as a regular BlackBerry does. It will also work on certain BlackBerry devices that have an option for WLAN.

If you are asking what you can expect on the BlackBerry, well, it won't look like the PC Client, and you won't be able to send or receive video, but the options listed in the next section will be available to you.

Multimedia Services on BlackBerry

Users of the MCS 5100 can access the following multimedia services on BlackBerry handheld devices:

- Presence indication of contacts status
- Presence management of own status, for example, "In meeting," "Available"
- Secure Instant Messaging
- Click to call from personal/global directories
- Click to call connection over GSM to BlackBerry or to nearest phone, for example, home phone
- View call logs
- Routes management (activate predefined Personal Agent routes or temporary redirection of calls)

BlackBerry SIP Client

Users of the MCS 5100 can utilize BlackBerry's onboard SIP Client for campus mobility.

Currently the following devices are supported: 6200, 7200, 6700, 7700, 6500, 7500, and the 7100 series. In Figures 1.6 through 1.9 you can see screenshots from a BlackBerry device.

Figure 1.6 BlackBerry Login

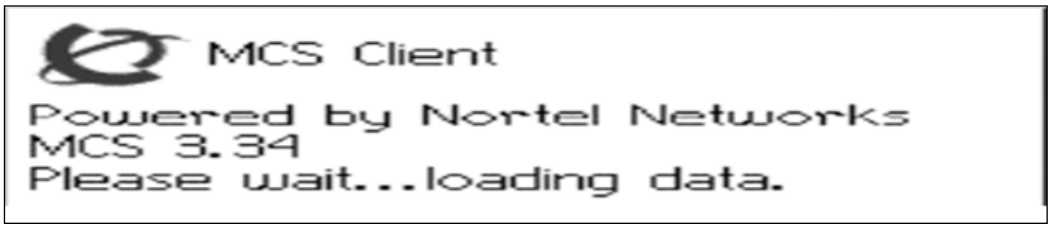


Figure 1.7 BlackBerry Menus

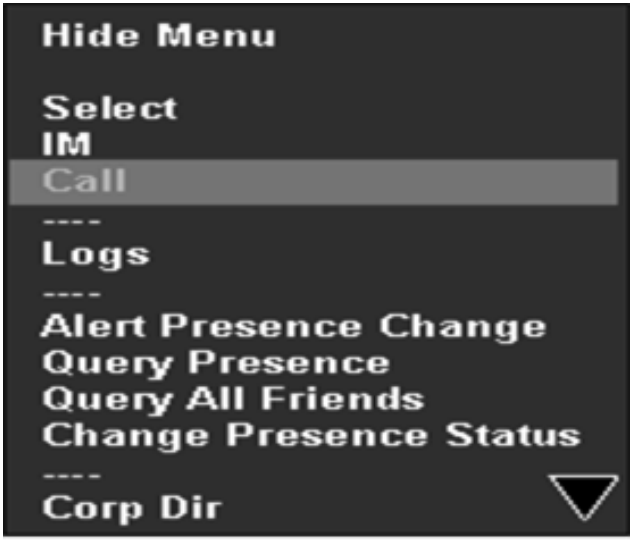
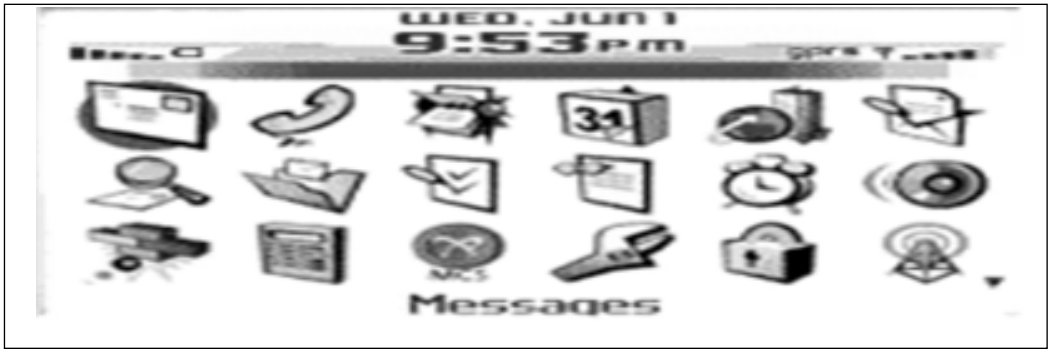


Figure 1.8 BlackBerry Menus 2

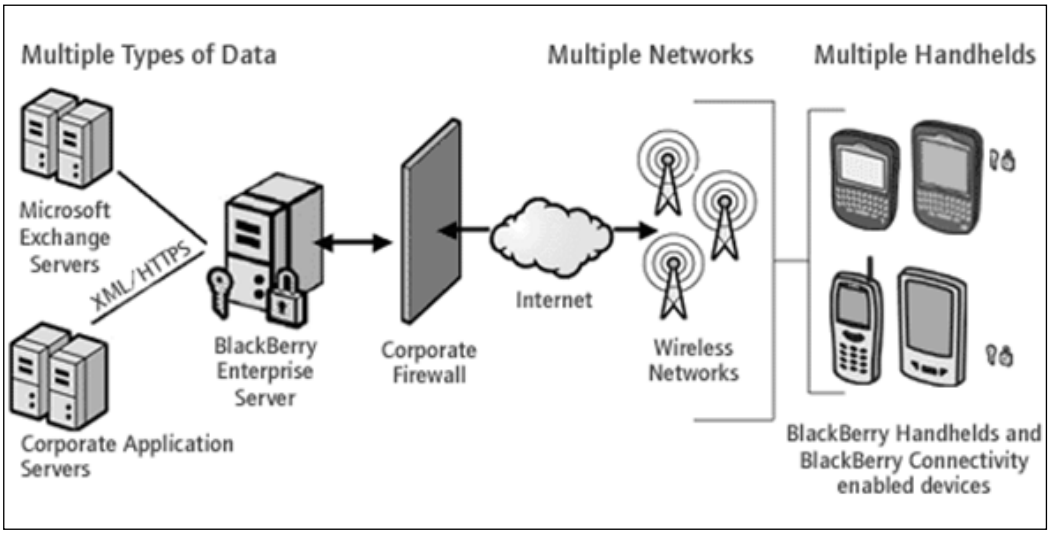
Figure 1.9 BlackBerry Screen



Supported Network

The following network configuration is required on both the MCS 5100 and the BlackBerry Enterprise Server for the client to work: a dedicated Nortel Wireless Client Manager on a Sun V100 server, the appropriate amount of SIP port licenses, and a BlackBerry Enterprise Server 3.0 or later, plus Mobile Data Services. In Figure 1.10 you can see what a network diagram could look like.

Figure 1.10 MCS 5100-BlackBerry Architecture



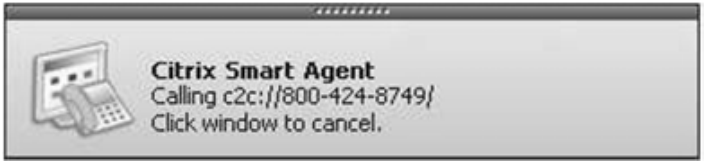
Citrix IP Telephony Applications

Citrix has teamed up with Nortel to provide some very cool and robust application solutions for the 1000 and 2000 series IP phones. These applications are meant to be used on just the IP phones and not any other part of the system or on the softphones. The current product offering provides five different types of service packages from Citrix. These five offerings come in the Citrix Voice Office Application Suite and the Citrix Applications Gateway.

Click-to-Call

This application uses the Citrix Smart Agent and enables users to dial their telephones by simply clicking on telephone numbers within e-mails and applications and information that can be accessed using Internet Explorer. Also the Smart Agent alleviates the need to install and maintain TAPI service providers or softphones on each personal computer. This will also reduce cost when users have to buy other systems. Figure 1.11 shows you what the application will look like after a number is clicked on a Web page or in e-mail.

Figure 1.11 Citrix Smart Agents for Click-to-Call



Broadcast Server

This server provides priority messages such as emergency, IT, fire, and weather alerts in the form of text, graphics, and audio to IP phones and PC Clients. This can be programmed per the company request for more specific or more generalized material based on such things as by department or floor. Figure 1.12 shows an alert on different IP phones for a fire in a building.

Figure 1.12 Citrix Broadcast

© Copyright Nortel Networks

Express Directory

This application provides an LDAP organizationwide directory. This new application directory reduces the search time and dial time by 75 percent, compared with current solutions on the market. Figure 1.13 shows how the express directory would look on multiple IP phones.

Figure 1.13 Express Directories

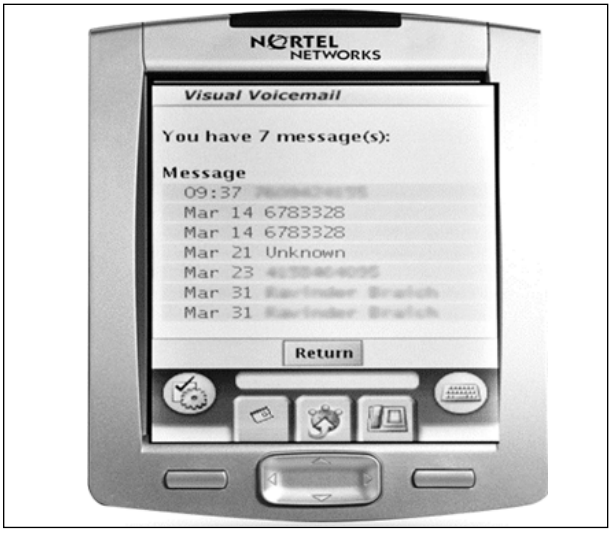
© Copyright Nortel Networks

Visual Voicemail

This application enables users of IP phones to see a visual list of their voice messages, select the most important messages for preview, and listen to or review messages without having to listen to each message like normal voice

mail. During message playback the user can play, pause, forward, delete, reply, and rewind using labeled soft keys rather than using and having to remember number keys that would represent each of these options on a normal voice mail system. Figure 1.14 shows a screen shot of how the Visual Voicemail would look on an IP phone.

Figure 1.14 Visual Voicemail



© Copyright Nortel Networks

Zone Paging

Zone paging allows users to page to groups of IP telephones in specific zones or domains without the expense of installing an overhead paging system in the building. This helps with the overall cost reduction of the system being installed.

Guest Services Application Package

This package has been designed for hotels, restaurants, bars, and retail stores. It allows the company to pick a package (either gold or silver) and use the IP Phone 2007 to display information, broadcasts, slideshows, and marketing material. The Package also allows companies to use one-touch dialing to different departments while using the company logos to push their service or brand to the customer. This Citrix system also can take existing applications from a network and put them on the IP phones, such as a time clock, atten-

Summary

The MCS 5100 is one of the first systems to come around that can be a stand-alone system or can be an overlay to an existing system (e.g., CS 1000). It offers the user a full multimedia communications experience unlike most common forms of a PBX or VoIP PBX. The system can be sized to accommodate a small organization, large enterprise, or a carrier class system as we will discover in further chapters of this book. The ability to bring applications and systems in house for a business that was paying huge outsourcing fees is a sure sign of a product's ability to produce a good ROI. The MCS 5100 does that today.

In chapters to come we will discover two of these applications, called Meet Me Conferencing and Web Collaboration. Most companies outsource voice and videoconferencing features to a local PSTN provider on a per-minute or per-call charge. Being able to bring that in house and then into one system provides great savings to any company. If you add that to the cost of using online Web tools to do meetings such as Webex or Placeware to savings provided by the MCS 5100 to an enterprise, you can see how it provides great value to the customer.

The chapters to come will provide you with an understanding of how all the applications and options work together. Learning how these applications work together will provide a greater understanding of the system and how it provides value to the enterprise and user.

Solutions Fast Track

What Is the MCS 5100?

- ☑ It is a SIP-based multimedia and collaborative applications server that also provides PBX-based features.
- ☑ It is an applications-based, communications-based server that can provide a soft computer-based IP phone or a hard desktop IP phone.
- ☑ The MCS 5100 is an all-in-one applications-based server that provides not only the preceding features but also all the

communications tools your user will need, such as videoconferencing, Web collaboration, instant messaging, and much more.

Applications Tools

- ☑ The MCS 5100 provides collaboration tools in the system such as audioconferencing and videoconferencing to users at anytime. MCS 5100 users don't need to schedule a call with someone else, in a room down the hall or on an Outlook calendar. Their contacts are always available either on a PC Client, IP phone, or outside the network in a PSTN.
- ☑ Instant messaging has become common in today's workplace; when used with the PC client,the MCS 5100 provides a secure and encrypted instant messaging service. When you are using instant messaging over an IP phone, there is no encryption. This can be used inside or outside the network and will provide secure transmissions.
- ☑ Call routing is becoming the new wave on communication systems. The MCS 5100 takes it to the next level by enabling users to personalize calls from anyone, any number, and any group to anywhere. It is a follow-me option that will always keep you connected or direct your calls to the applications or place of your choosing.

Alliances

- ☑ Having a meeting with your business associates or business partners is a day-to-day chore; the MCS 5100 allows you to have these meetings over video in your office. By using SIP to connect to endpoints, users reduce travel expenses and save money.
- ☑ Being always on the go and always connected is why people carry a BlackBerry. The MCS 5100 allows you to stay connect even more. By integrating a MCS 5100 client into a BlackBerry you have some of the same options you have while at work on your PC Client or IP phone.

- ☑ Rather than having to pay for a PDA, a soft client, and WiFi service from your local carrier, you can just add a client to your BlackBerry and stay connected to your MCS 5100 at all times, saving money for the user by offering better communications savings.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Why is the MCS 5100 called an applications server and not a regular PBX?

A: The difference would be that when you have a normal VoIP PBX you would have to add all the features in the base MCS 5100 configuration with the applications server. The MCS 5100 put both together in one package.

Q: Can the MCS 5100 be used with either a softphone or an IP phone?

A: The system can be used with either a PC Client softphone or a regular IP phone; also the two can be used together at the desktop to form a converged desktop.

Q: How does the MCS 5100 provide videoconference calling?

A: We will be looking at that later in another chapter, but it is through the PC Client and a Web camera plugged into a computer. Also, a MAS (Multimedia Application Server) is added to the MCS 5100 to provide audio and videoconferencing services.

Q: How does the MCS 5100 provide instant messaging to users?

A: This is also done mostly through the PC Client, but you do have the ability to use an IP phone if needed.

Q: How is call routing controlled by the user?

A: This is done on a Personal Agent Web page that will be covered in another chapter. This Web page may be accessed from the PC Client or a normal Web URL.

Q: The MCS 5100 provides Web collaboration, as it is called. Is this similar to Webex and Placeware?

A: It is similar in the sense that you can do online collaborations with each other, but the MCS 5100 provides this in the system and with all the other features of the PC Client. This is much more than you would ever get from another online service that you have no control over.

Q: The MCS 5100 provides a client for the BlackBerry handheld. Does it provide one for others?

A: As of now there are no other clients for PDAs available for use on the MCS 5100.

Q: Does using SIP for presence-based routing mean that I can see what a user is doing at that moment?

A: Yes, when presence is used on the system, you can see if the user is connected, offline, on a call, unavailable, or any other user response they have posted for their availability. This will allow the user to be able to find people in real time and communicate with them, rather than not knowing what they are doing before calling, e-mailing, or sending an instant message.

Chapter 2

MCS 5100 Architecture

Solutions in this chapter:

- Component Overview
- Network Topology
- IP Addressing
- Domains and Subdomains
- Call Flow
- AudioCodes Gateway

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

In this chapter we will take a look at the system itself and what makes up the MCS 5100. As you saw in Chapter 1, the MCS 5100 can come in different packages. There are many different options that, when added to the MCS 5100, need to run on a dedicated server for optimal use. We will also look at call routing and security within the system and outside the system. Although these two could be listed separately, it is better to discuss and show the ports used by the system when making a call or communicating to other devices. This way, security professionals would understand what ports are used and what needs to be secured in or out of the network.

Knowing what you will need before you start your initial installation or configuration is a critical point, so we will discuss how IP addresses and domains work within the MCS 5100. This allows the administrator to understand how many different IP addresses and virtual local area networks (VLANs) are needed on the system. Understanding the domains structure of the MCS 5100 in the beginning will help the administrator avoid unwanted mistakes and pitfalls in the initial configuration. By creating an incorrect domain structure, the administrator will create endless work that will need to be redone on the MCS 5100. For any installation to succeed, you must understand your network, users, and how the company will use the MCS 5100.

Within the MCS 5100 there are two main ways to send user calls to the outside world: either through a Primary Rate Interface (PRI) gateway or Session Initiation Protocol (SIP) gateway. For most companies a PRI gateway to the local Public Switched Telephone Network (PSTN) is normally what is used, but there is another way. Many companies are realizing the savings when using SIP to communicate to the local PSTN or business partners. The local PSTN in some areas is now providing direct SIP trunks to systems over a wide area network (WAN) link instead of PRI gateways.

Understanding the use of the SIP trunk to the PSTN and business partners is a great way for any engineer to show return on investment (ROI) to its company or customer. Rather than having to buy a new gateway every time you need to add more lines to the PSTN, you just add SIP trunks over a WAN link. We will discuss how this works with the MCS 5100 and the configuration.

Component Overview

There are four different configurations that can be implemented for an MCS 5100; one is called an MCS 5200 now. The MCS 5100 uses either a Sun Fire V100 Server or a Sun Netra 240 server for its core components. Figure 2.1 shows a typical two-server MCS 5100 using two Sun Fire V100 servers, a four-server MCS 5100 using four Sun Fire V100 servers (see Figure 2.2), and an eight-server MCS 5100 using four Sun Fire V100s for the primary servers and four Sun Fire V100s for the backup servers (see Figure 2.3). With this configuration, an extra Sun Fire V100 server may be added for an H.323 gatekeeper.

Also shown is an eight-server MCS 5100 using four Sun Netra 240 servers for the primary and four Sun Netra 240 servers for the backup (see Figure 2.4). Nortel now calls this system an MCS 5200, but the documentation has this set up in a possible configuration for the MCS 5100. The difference between the two systems is the different software load for the 5100 and the 5200. The MCS 5200 also has a few different features.

Figure 2.1 MCS 5100 Configuration with Two Sun Fire V100 Servers

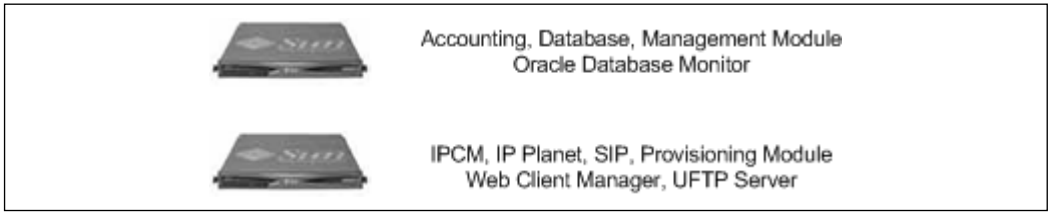


Figure 2.2 MCS 5100 Configuration with Four Sun Fire V100 Servers

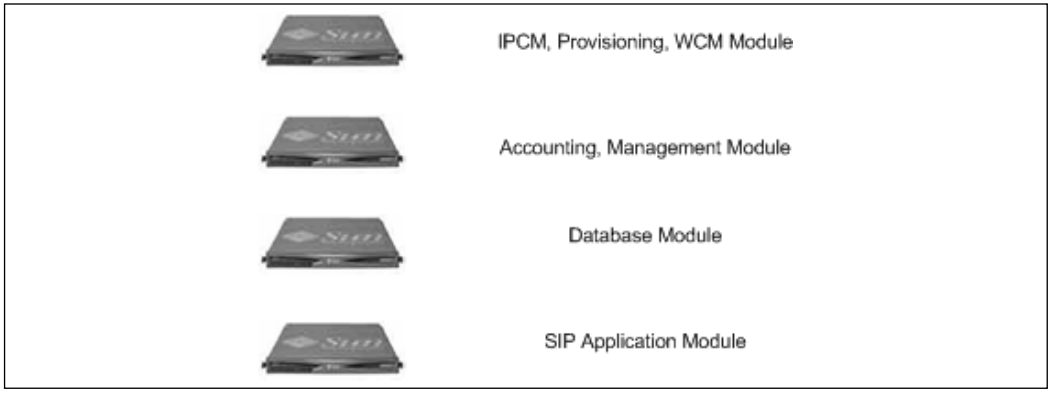


Figure 2.3 MCS 5100 Configuration with Eight Sun Fire V100 Servers

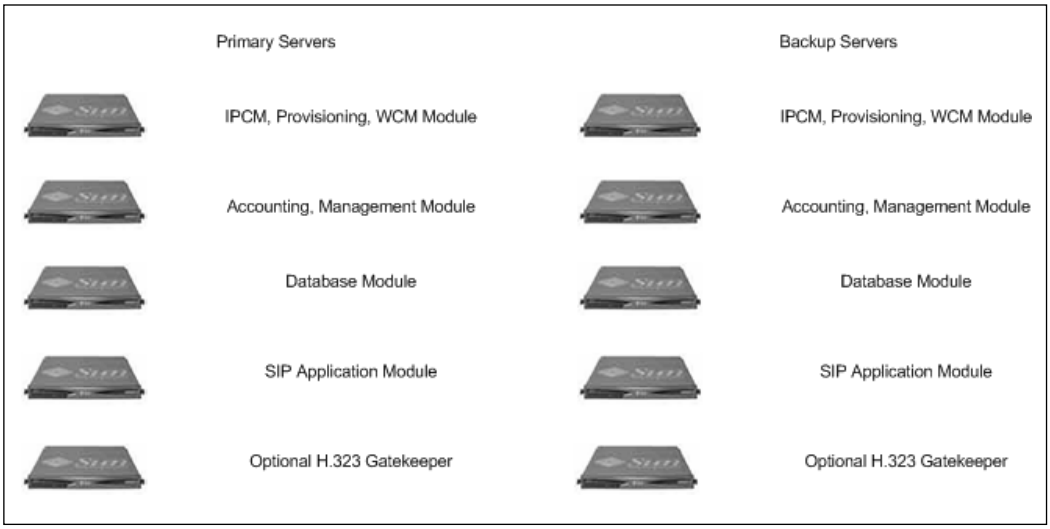
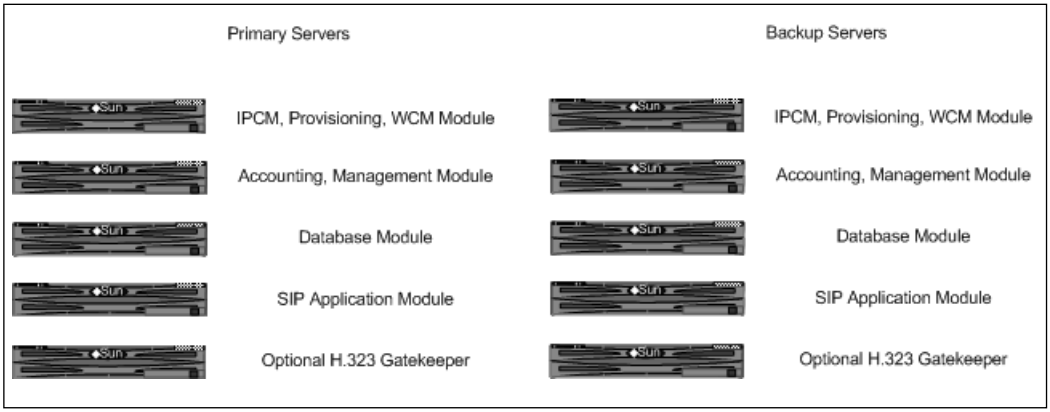


Figure 2.4 MCS 5100 Configuration with Eight Sun Netra 240 Servers



Component Descriptions

In this section, we'll take a look at the core components on the MCS 5100. We'll explain what they do and what they provide within the system. Here is a list of the MCS 5100's core components:

- Accounting Module
- SIP Application Module

- IP Client Manager (IPCM)
- Web Client Manager (WCM)
- Provisioning Module
- Database Module
- Management Module

The first component that we will look at is the SIP Application Module (for more information on SIP, see Chapter 8). This module processes SIP signaling messages, handles SIP sessions, and provides core services that communicate between SIP clients. The SIP Application Module communicates through SIP to the endpoints in and out of the network. It identifies the SIP clients and their method of connecting through a process of authentication and registration. It also supports presence and Call Processing Language for call screening.

The Database Module holds all the subscriber information, Call Processing Language scripts, component, service data, and configuration data. The IPCM performs SIP and UNIStim (Unified Network IP Stimulus) protocol conversion and transfer for the Nortel IP Phones. The IPCM provides all service and options for the Nortel IP Phones; it also sends all outgoing messages to the SIP Application Module.

The H.323 Gatekeeper Module, which is an optional server on the MCS 5100, provides users an interface between H.323 networks and the MCS 5100. Because some networks and network devices are not SIP-enabled as of yet or are legacy devices, you may use this module to allow them access as endpoint into the MCS 5100 network. All H.323 endpoints would be managed from this device before being allowed to interact with the core MCS 5100 modules. This module does support Coordinated and Universal Dialing plans or Private Dialing plans.

The Web Client Manager (WCM) provides and manages the Multimedia Web Client. It manages the logins and secure Web browser for the Web client. The WCM also controls all activity, calls, and options on the Web client. The WCM takes the WCSCP (Web Client Session Control Protocol) and transfers it to the SIP protocol used on the MCS 5100.

Within the Accounting Module resides the processes and information to provide billing and call information for all customers on the MCS 5100. It

also provides storage for these records and formats them in an IPDR (Internet Protocol Detail Record) format for use. The Management Module provides a Java-based tool to provide administration and maintenance access to the MCS 5100. This module also deploys new loads of firmware to IP phones and PC clients.

Today, administration of the Provisioning Module gets the most work out of any module. It provides a Web-based GUI for the administrations of the MCS 5100. It provides this GUI to make it easier to configure users and systems in a timely manner. We will discuss this GUI, called the Provisioning Client, in a later chapter. It is accessible by a number of different Web-based clients like Internet Explorer and Firefox.

Sun Hardware Features

In this section, we'll discuss the features that are standard on each Sun Fire V100 and Netra 240 within the MCS 5100 platform.

Sun Fire V100

The Sun Fire V100 includes the following features:

- One 550MHz processor
- 512 KB of external cache
- 1 GB of RAM
- Two 40GB hard drives
- One 24X CD-ROM
- Two 100BaseT Ethernet ports
- Two USB ports
- Two RS-232C/RS-423
- 19-inch rack mount kit
- Sun Solaris 8
- Lomlite2
- Sun DiskSuite

Sun Netra 240

The Sun Netra 240 includes the following features:

- DC or AC power supply
- Two 1.28GHz UltraSPARC IIIi processors
- 1 MB of internal cache
- 4 GB of memory
- Two 73GB disk drives 15,000 RPM Ultra 160 SCSI
- Four10/100/1000BaseT Ethernet ports operating at 100Mbps
- One10Mbps Ethernet port for network management, console, and LOM
- Two USB ports, OHCI-1.0 compliant interfaces, supporting dual speeds of 12 and 1.5 Mbps for each port
- One TIA/EIA-232F (RJ45) serial port
- One TIA/EIA-323-F asynchronous (DB9) serial port
- One Ultra 160 SCSI multimode (SE/LVD) port
- Two 400W power supplies
- Solaris 2.8
- Sun Volume Manager (disk suite)
- Sun JVM

Capacity

As we described in the preceding section, there are many different configurations to the MCS 5100, from a simple and small two-server MCS 5100 to a full eight-server configuration. Each has different maximum configurations that are allowed on each, based on the number and type of servers used. In this section, we'll show you the maximum configurations allowed on each server.

A Two-Server Configuration

The maximum configuration for the MCS 5100 with two Sun Fire V100 Servers is as follows:

- Database Module: one
- Management/Accounting Module: one
- SIP Application Module: one
- IP Client Manager: one
- Web Client Manager: one
- MCP Trunking Gateways: two
- Media Application Servers: one
- RTP Media Portal: zero
- Provisioned subscribers: 250
- Domains: 25
- SIP PRI DS0 trunks: 50
- SIP BHCA for SIP-to-SIP basic calls: 1,250

A Four-Server Configuration

The maximum configuration for the MCS 5100 with four Sun Fire V100 Servers is as follows:

- Active Database Module: one
- Primary Management and Accounting Module: one
- Active SIP Application Module: three
- IP Client Manager: six
- Web Client Manager: six
- MCP Trunking Gateways: 200
- Media Application Servers: 12
- RTP Media Portal: four
- Provisioned subscribers: 10,000

- Domains: 1,000
- SIP PRI DS0 trunks: 5,000

An Eight-Server Configuration

The maximum configuration for the MCS 5100 with eight Sun Fire V100 Servers is as follows:

- Database Module: one active plus one backup
- Primary Management and Accounting Module: one active plus one backup
- Active SIP Application Module: three active plus three backup
- IP Client Manager (4 load sharing pairs): six active plus six backup
- Web Client Manager: six active plus six backup
- MCP Trunking Gateways (two-span devices): 200
- Media Application Servers: 12
- RTP Media Portal: four
- Provisioned subscribers: 10,000
- Domains: 1,000
- SIP PRI DS0 trunks: 5,000

MCS 5100 8 Sun Netra 240 Server Configuration

The maximum configuration for the MCS 5100 with eight Sun Netra 240 Servers is as follows:

- Database Module: one active plus one backup
- Primary Management and Accounting Module: one active plus one backup
- Active SIP Application Module: four active plus four backup
- IP Client Manager: eight active plus eight backup
- Web Client Manager: eight active plus eight backup
- MCP Trunking Gateways: 2,500

- Provisioned subscribers: 60,000
- Domains: 10,000
- SIP PRI DS0 trunks: 60,000
- SIP BHCA for SIP-SIP basic calls: 400,000

Designing & Planning…

Server Details

Note the following information for each server; it will come in handy when designing your network.

- The Sun Fire V100 server can support 3,300 subscribers and is capable of 60,950 weighted SIP transactions per hour.
- Sun Netra 240 server can support 15,000 subscribers and is capable of 230,000 weighted transactions per hour.
- An IPCM configuration with two Sun Fire V100 Solaris-based servers can support up to 250 i2002/i2004 clients. Four- and eight-server V100 Solaris systems can support a maximum of 1,500 clients, including Multimedia Web Clients, i2002 and i2004 Internet telephones. An eight-server Netra 240 Solaris system can support a maximum of 10,000 clients.
- A Web Client Manager configuration consisting of a two-server V100 Solaris system can support up to 250 Multimedia Web Clients. Four- and eight-server V100 Solaris systems can support a maximum of 1,500 clients, including Multimedia Web Clients, i2002, and i2004 Internet telephones. An eight-server Netra 240 Solaris system can support a maximum of 10,000 clients.

Optional Components

Besides what resides within the core MCS 5100 system, there are different services that may be added to the system. These services reside on what are called

MAS (Multimedia Application Server) servers. These servers are either located on an IBM 335 eServer or the new IBM 336 eServer. These can also now be placed onto an IBM Blade Server or Center for further cost savings over individual servers. The following services will be discussed in later chapters:

- Media Application Server (MAS) Announcement Services
- Media Application Server (MAS) Ad Hoc Audio and Video Conferencing
- Media Application Server (MAS) Chat Service
- Media Application Server (MAS) Meet Me Audio and Video Conferencing
- Media Application Server (MAS) Music on Hold
- Media Application Server (MAS) Web Collaboration

Two pieces that are required but outside the core system are an MRV Terminal Server and a PC for system management. Other optional components that can be added outside the core system are

- RTP Media Portal
- H.323 Gatekeeper
- MCP Trunking Gateway (needed for PRIs)
- Wireless Client Manager

Network Topology

In this section we will take a look at how the preceding components and others connect in a network to bring the MCS 5100 to life. Even though there is really no big difference between a two-, four-, or eight-system topology, we will look at all of them individually. Also discussed will be a few items not really talked about yet—Call Pilot Voice Mail and CS 1000 private branch exchange (PBX) systems. These connect to the MCS 5100 to provide such options as voice mail for the MCS 5100 and network routing to other PBXes such as the CS 1000.

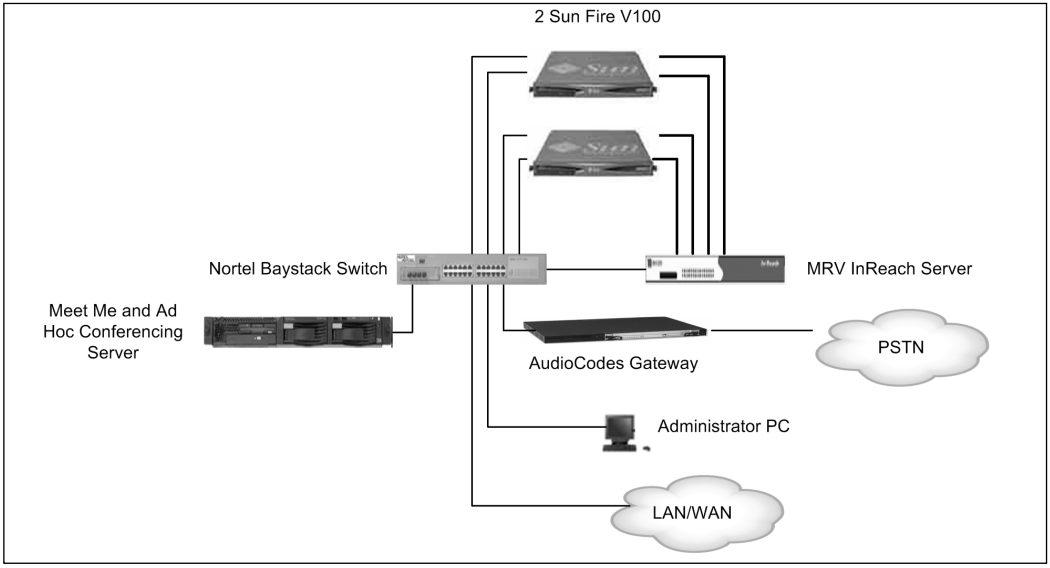
MCS 5100 Two-, Four-, and Eight-Server Topology

The first system is a two Sun Fire V100 Server Configuration with some optional components added to the system such as Meet Me Conferencing and Ad Hoc Conferencing (see Figure 2.5). These systems are connected to a layer 2 switch, which provides 802.1q and 802.1p to the system and its users. This switch then is connected into a layer 3 switch, which handles other functions for the system into the enterprise backbone. The MRV InReach Server is mandatory since it provides access to the Sun Servers.

NOTE

You are not allowed to have more than one MAS on a two-server system. The one MAS can have multiple applications on it—Adhoc conferencing, MeetMe conferencing, IM Chat, Music on Hold, and Recorded Announcements—and there are hard restrictions on the max number of ports for each application. Video conferencing and Web collaboration are not allowed on a two-server system.

Figure 2.5 A Configuration with Two Sun Fire V100 Servers

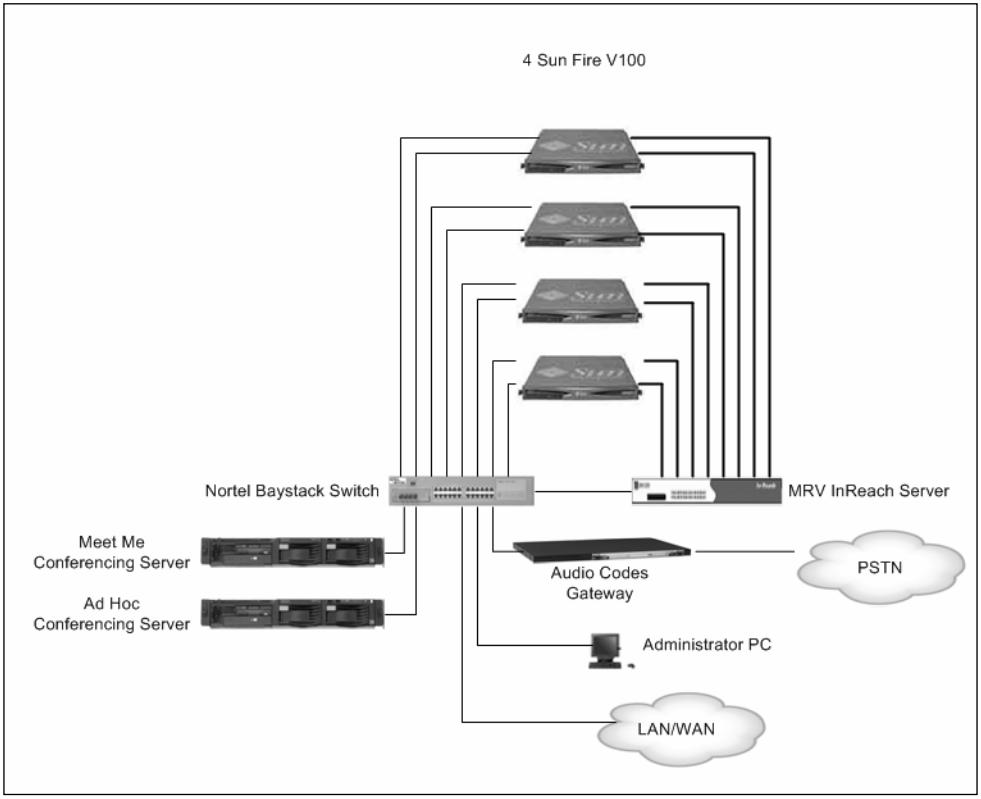


NOTE

When designing the system please note that in these drawings there is one switch, but as a standard practice it is always good to have two switches. This would be so that the Sun Fire, MRV, AudioCodes Gateway, Meet Me, and Ad Hoc servers all have dual paths into the network in case one switch fails.

The next system is going to be arranged in the same way, but this will be a configuration with four Sun Fire V100 Servers (see Figure 2.6).

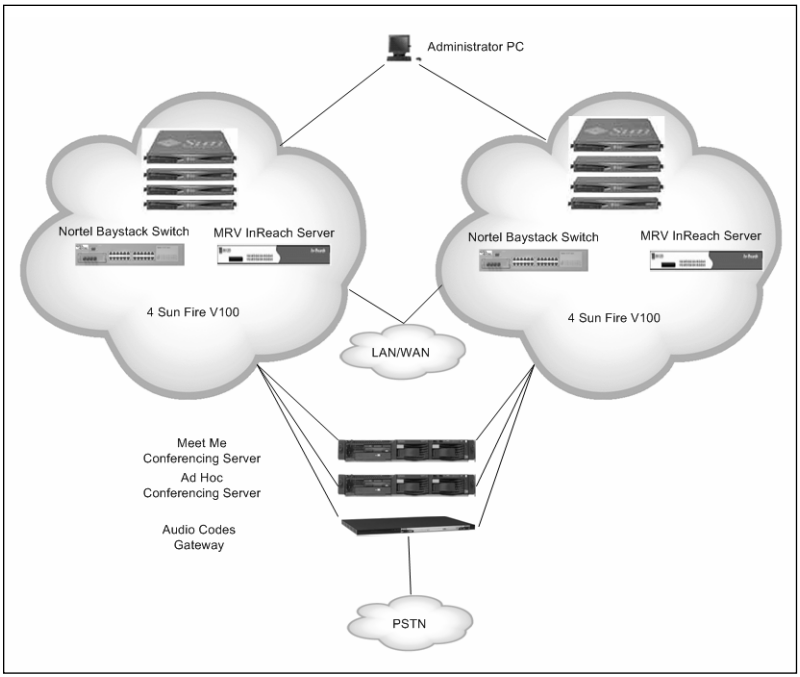
Figure 2.6 A Configuration with Four Sun Fire V100 Servers



In Figure 2.7, we will see how the eight-server system is architected; this drawing will be the same for both the V100 and Netra 240 servers. In this

drawing, we are using a Sun Fire V100 for our purposes. Note that in the drawing there are now two MRV InReach Servers; this would be one per MCS 5100 Core System. As in the earlier remarks about having two switches for your system, the same is true in this case. Having both systems on one MRV InReach Server is not a good idea or a common practice. The optional servers and the gateway now have dual routes to each switch in each CS 1000 Core System.

Figure 2.7 A Configuration with Eight Sun Fire V100 Servers



NOTE

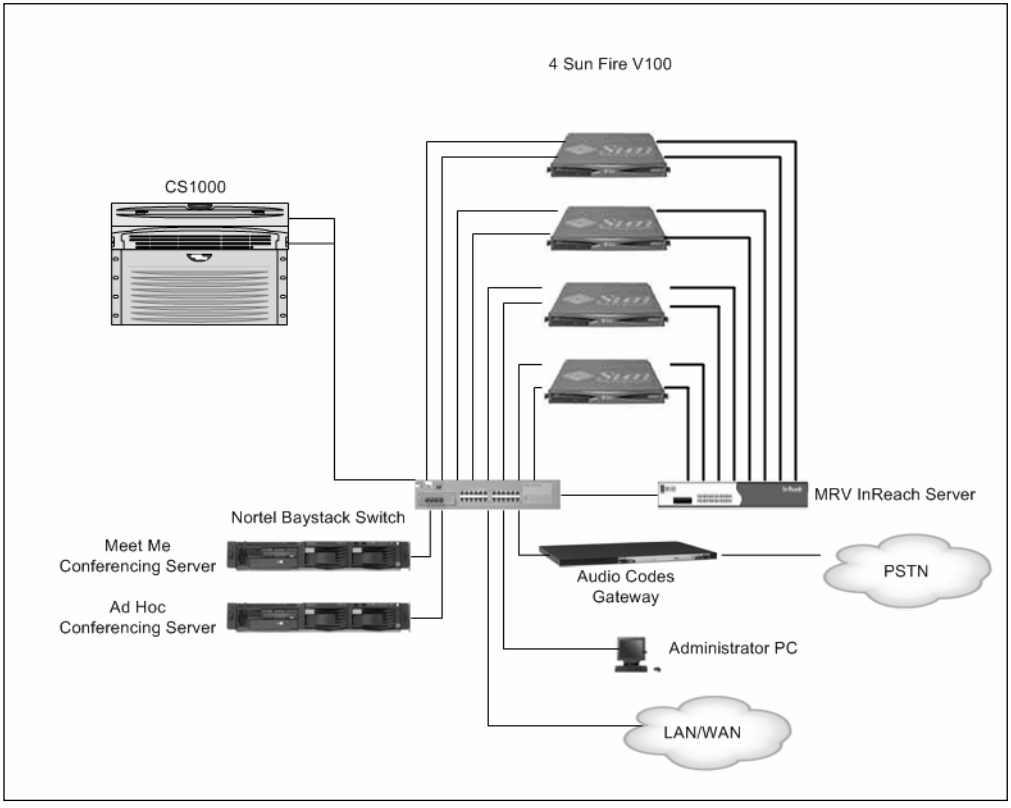
It is an option within the system to use an IBM Blade Server instead of using separate IBM servers for such things as Meet Me and Ad Hoc Conferencing, Chat, Music on Hold, and Web Collaboration. This can be a cost-saving measure for some companies based on the size and future expansion of the system.

MCS 5100 and CS 1000 Topology

The MCS 5100 can be connected to a CS 1000 via SIP or H.323 trunks in order to provide direct link calling to the system. Some might ask why this would be necessary or needed in a network. Before systems were able to connect over an IP network topology, calls had to be routed through a gateway and out to the PSTN to be able to connect to another PBX. This caused added expense to companies because they would have to buy more vendor equipment and also additional PSTN resources to process the calls. This would take up a huge part of most company's capital asset money for a year.

Now that we can connect two PBXes over an IP link, we are able to eliminate those costs in the network. As you can see in Figure 2.8, the MCS 5100 and the CS 1000 connect through the LAN backbone. They can also connect over a WAN backbone if needed in the network.

Figure 2.8 MCS 5100 and CS 1000 Topology

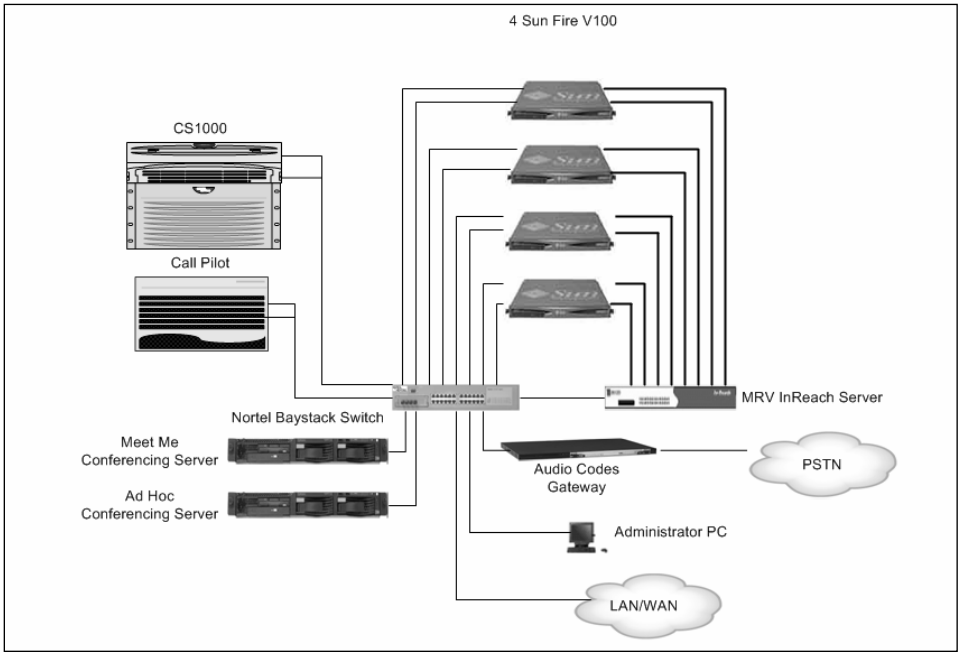


Besides the value of being able to connect the MCS 5100 and CS 1000 over Ethernet to save money; there is one other reason why this is needed. The current MCS 5100 has no voice-mail system provided within the Sun servers or IBM servers. Nortel relies on the current Call Pilot system to provide voice mail via a CS 1000. So if you want to use the MCS 5100, you have to buy a Call Pilot voice-mail system and a CS 1000 PBX.

The reason for this is that Nortel has not yet put a SIP interface on its Call Pilot voice-mail system. This means that the MCS 5100 needs to be able to do time-division multiplexing (TDM) signaling to a Call Pilot voice-mail system. In the current architecture of the MCS 5100, it does not have anything that can change a SIP or H.323 signal to TDM and provide that to the Call Pilot. In comes a CS 1000 system, which through an MGate Card in its system, provides TDM signaling to the Call Pilot. The MGate Card on the CS 1000 connects directly to the Call Pilot via a cable through the back plane of the CS 1000.

In Figure 2.9 you can now see a Call Pilot voice-mail system added to the topology and connected by Ethernet to the LAN switch (remember it still is directly connected to the CS 1000 via the back plane).

Figure 2.9 MCS 5100, CS 1000, and Call Pilot Topology



IP Addressing

When you are designing your voice network, assigning IP addresses plays a huge part in the overall success of your network and how it will work. The MCS 5100 makes it easy—when adding this system into a network, it can be added in by a single plane. By that we mean a single plane of IP addresses can be used for the entire system. A plane is another word for a subnet, so to speak. A single subnet needs to be set aside for the MCS 5100 to use for its equipment and one for the IP phones. If you are working on a small system, you can use the same subnet for both the equipment and the IP phones. Just remember to specify the range of IP addresses in the subnet for Dynamic Host Configuration Protocol (DHCP).

For example, if you have a subnet of 10.1.1.0 and a subnet mask of 255.255.255.0, you can split this up so all your equipment and IP phones are on the same subnet. A recommendation is to use 10.1.1.49 and earlier for equipment, then 10.1.1.50 and later for all IP phones. If you want to split up the subnets to put your equipment behind a firewall or DMZ, then you can use one subnet for the equipment and one or more for the IP phones. Many subnets can be put together or added if you happen to run out of IP addresses for the IP phones.

Overall, there are no restrictions on where you put IP phones on a subnet; they could go anywhere, but it is much easier to troubleshoot issues if you have them subjected to a certain range.

If in your system you are going to have Call Pilot voice mail, you will need to set aside a few more subnets for the CS 1000 and the Call Pilot. Three different LANs are needed for the CS 1000 and Call Pilot: the Customer LAN (CLAN), Equipment LAN (ELAN), and the Telephony LAN (TLAN). All of these need to be separate subnets to prevent interaction with the systems. Here is a list of subnets that you will need for the Call Pilot and CS 1000:

- Call Pilot Voice Mail
  - CLAN and ELAN
- CS 1000
  - CLAN, ELAN, TLAN

As a standard for best practices, it is always better to use your existing DHCP server for soft clients and IP phones connecting to your network. When phones connect to your network they access DHCP from the information on the switch port that they attach to and then connect to either the Application Server or IPCM. This depends on which you will have running your IP phones. If you are going to have the IP phones do UNIStim, which is the Nortel proprietary protocol, then you need to use the IPCM. If you just want to do SIP to the IP phones, then you can just use the Application Server.

NOTE

When using just SIP instead of using UNIStim, remember that on the IP Phone 2004 you will be allowed to have only one user sign into the IP phone. When using SIP as a dedicated path to the IP phone where if using UNIStim you can have multiple people sign into one IP Phone at the same time.

Domains and Subdomains

The MCS 5100 uses SIP domains as a way to control subscribers, routing, services, and translations. A domain is controlled and configured within the Provisioning Client, which will be discussed in a later chapter. Domains allow the administrator to control and assign such things as service packages, call routes, subdomains, E911, and translations. This allows changes to be made to a group such as a domain and not affect all users on the MCS 5100.

Root Domain

This is the highest level of domains in the structure used within the MCS 5100. When designing your network from the top down, this would be your

main company domain, such as PlutoNetworks.com in Figure 2.10. You do not have to just set up one Root domain and then issue Subdomains in your network. You may put all users on Root domain for the company, depending on the size and location.

Subdomain

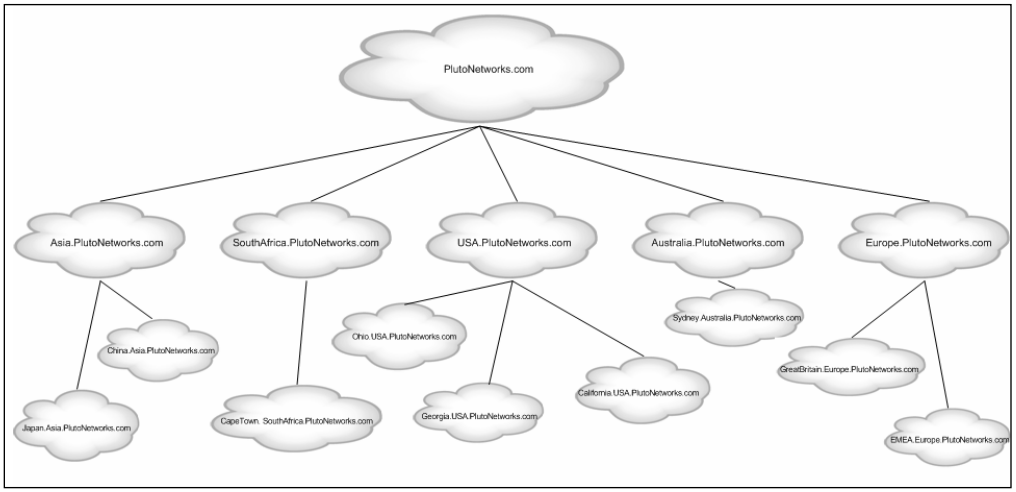
This domain sits below the Root domain and allows the administrator to break up big Root domains into smaller, more manageable groups. These could be areas around the world or even down to company offices if need be. Subscribers of users are assigned to these Subdomains under the main Root domain. There is no limit on the amount of levels provisioned for Subdomains that you can have under any one given Root domain. One thing to remember is that each Subdomain will receive the parameters assigned to the Root domain.

Foreign Domain

A Foreign domain is really what it sounds like, a domain that is not local to the MCS1500. This is a domain that is not controlled by the system, and one that you would have to get to by IP address or DNS through the network.

Figure 2.10 is an example of how a Root and Subdomain architecture is designed for Pluto Networks. The Root domain is the domain for the entire company worldwide, whereas the Subdomains are different countries around the world. Also, there are Subdomains below Subdomains, so within each country it can be separated by city.

Figure 2.10 Pluto Networks Domain Design

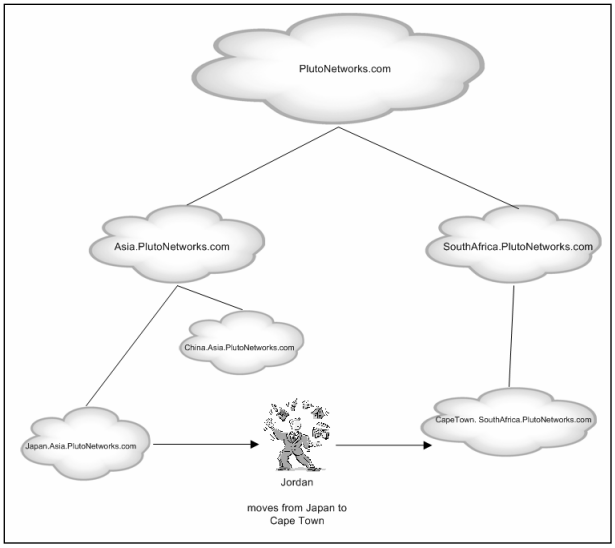


Domain Limitations

When you do design your SIP Domain network, you should be aware of a little limitation on the system so that you do not have any major problems. When a user within a Root domain or Subdomain is being moved to another, certain items will be lost and or will need to be provisioned again. These items are within the IP Client Manager, Call Pilot Voice Mail Servers, Application Server, service packages, call routes, and E911 provisioned locations.

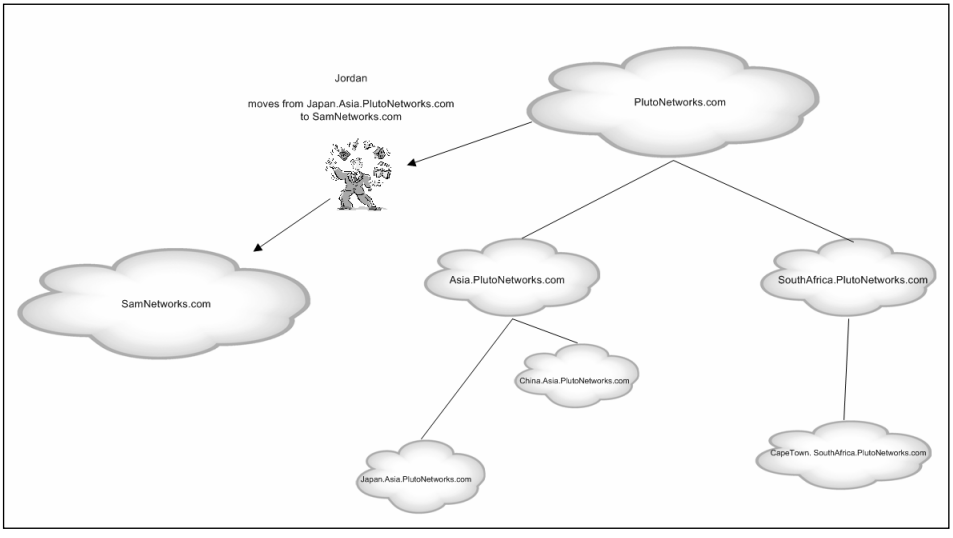
Let's look at an example of how this would work within your system. If we have only one main Root domain and all your other Subdomains are under that, a move is simple from one Subdomain to another (see Figure 2.11). In this example we are moving the user Jordan from one Subdomain to another with in the same Root domain. Now since these Subdomains are under the same Root domain, the user will not lose any items. This is because items are provisioned from the top down.

Figure 2.11 User Move within Root Domain



Now, if the same user, Jordan, moves from the Subdomain of Japan, which is under the Pluto Networks Root domain, to another Root domain of, let's say, Sam Networks, then the user will need to be provisioned again since everything in the service package under their old Root domain will be lost. This is shown in Figure 2.12.

Figure 2.12 User Moves to Different Root Domain



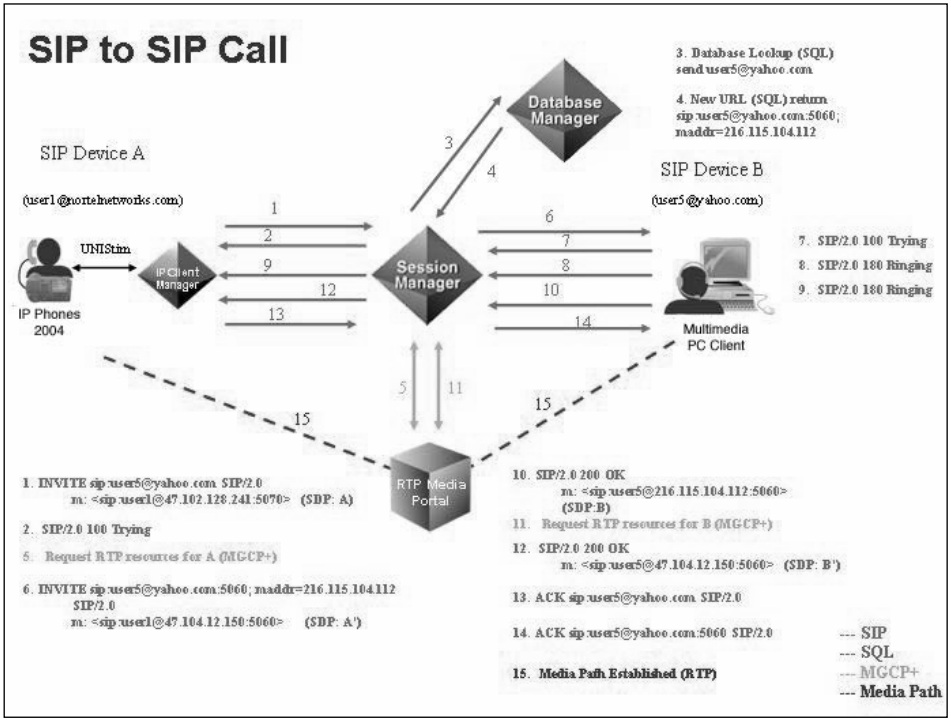
Call Flow

How a call is made within any system plays a role in how you define your architecture in the network. The MCS 5100 is not any different in that respect; you could have as many as eight Sun Servers, six IBM Servers, PRI Gateway, CS 1000, and a Call Pilot within your call flow architecture of the system. In this next section we will show some call flows from within the current systems part and some optional parts as well. This will provide you with a greater understanding of how the SIP translations work within the system.

SIP-to-SIP Call

In Figure 2.13 we are looking at a SIP-to-SIP call using a Nortel IP Phone 2004 and a PC Client. This figure will take you step-by-step on how the call flow works between the two and what you can look forward to in troubleshooting a SIP call.

Figure 2.13 Nortel SIP-to-SIP Call

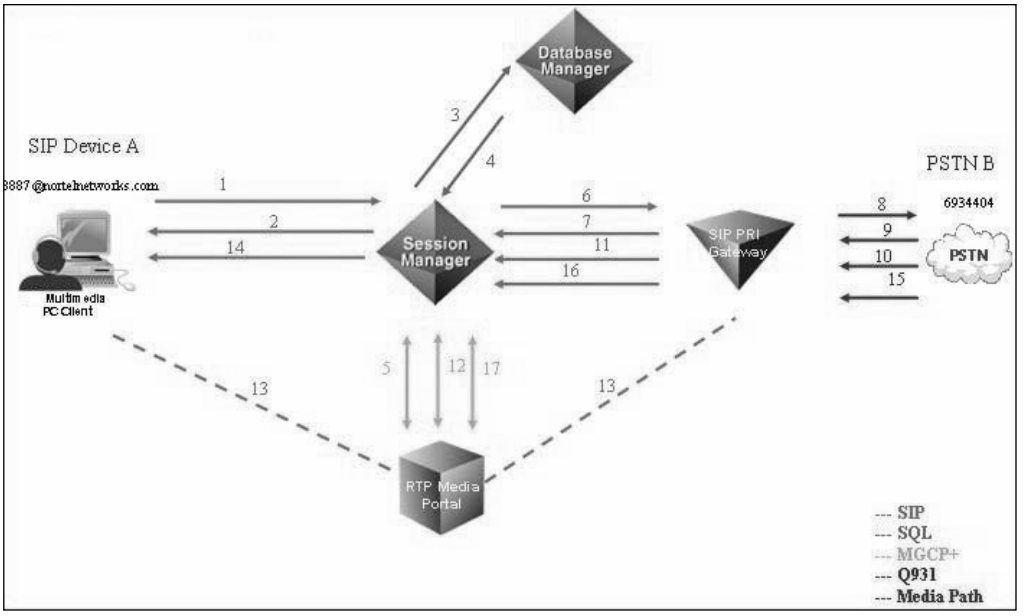


Here is the step-by-step call flow for a SIP-to-SIP call using Nortel's MCS 5100. The numbers in the following list correspond to the numbers shown in Figure 2.13:

1. Invite (SIP)—INVITE sip:user5@yahoo.com SIP/2.0 m: <sip:user1@47.102.128.241:5070>(SDP: A)
2. Trying (SIP)—SIP/2.0 100 Trying
3. Database Lookup (SQL)—send user5 @ yahoo.com (refer to "Database Lookup 2")
4. (New URL (SQL)—return sip:user5@yahoo.com:5060; maddr=216.115.104.1125.Request RTP resources for A (MGCP+) (A', B')(Map A to A')
5. Request RTP resources for A (MGCP+) (A', B')(Map A to A')
6. Invite (SIP)—INVITE sip:user5@yahoo.com:5060; maddr= 216.115.104.112 SIP/2.0 m: <sip:user1@47.104.12.150:5060> (SDP: A')
7. Trying (SIP)—SIP/2.0 100 Trying
8. Ringing (SIP)—SIP/2.0 180 Ringing
9. Ringing (SIP)—SIP/2.0 180 Ringing
10. OK (SIP)—SIP/2.0 200 OK m: <sip:user5@ 216.115.104.112:5060> (SDP: B)
11. Update RTP resources for B (MGCP+)(Map B to B')
12. OK (SIP)—SIP/2.0 200 OKm: <sip:user5@47.104.12.150:5060> (SDP: B')
13. ACK (SIP)—ACK sip:user5@yahoo.com SIP/2.0 (Note: Originating client will start sending packets.)
14. ACK (SIP)—ACK sip:user5@ yahoo.com:5060 SIP/2.0 (Note: Terminating client will start sending packets.)
15. Media Path Established (RTP) (A sends media packets to B', Portal double NAPTs the packets (both SRC & DEST), and forwards to B from A')

In Figures 2.14 and 2.15 we will look at a call from a SIP device like a PC Client to the PSTN. The call flow is split up into two figures to make it easier to follow the call flow with little clutter in the figure.

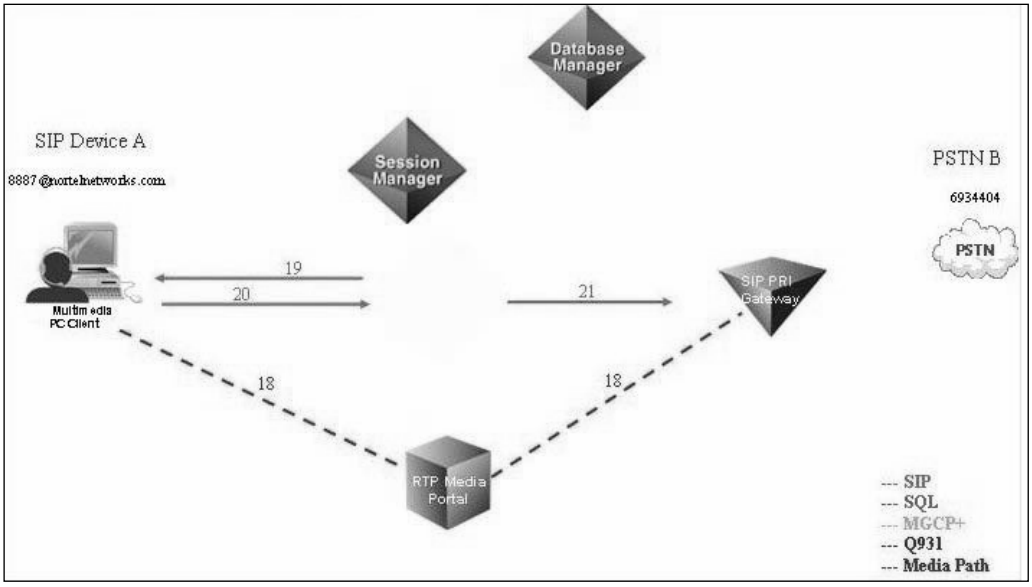
Figure 2.14 SIP to PSTN A



As in Figures 2.14 and 2.15, the following list shows the call flow by the numbers for SIP-to-PSTN call flow.

1. Invite (SIP) –> INVITE sip:66934404@nortelnetworks.com SIP/2.0 m: <sip:8887@47.100.234.159:5060> (SDP: A)
2. Trying (SIP)—SIP/2.0 100 Trying
3. Database Lookup (SQL)—send 66934404@nortelnetworks.com (refer to "Database Lookup 2")
4. New URL (SQL)—return sip:4404@nortelnetworks.com,maddr=47.100.234.140, user=phone, norteldevice=pri,norteltrkgrp=pria_t1_8000

Figure 2.15 SIP to PSTN B



5. Request RTP resources for A (MGCP+) (A', B') (Map A to A')
6. Invite (SIP)—INVITE sip:4404@private.nortelnetworks.com:5060;maddr=47.100.234.140; user=phonenorteltrkgrp=pria_t1_8000 SIP/2.0 m: <sip: 8887@47.104.12.150:5060>(SDP: A')
7. Trying (SIP)—SIP/2.0 100 Trying
8. SetUp (Q931)
9. Call Proceeding (Q931)—equates to the SIP Trying
10. Alerting or Progress (Q931)—depends on NT or TE mode
11. 183 Ringing (SIP)—SIP/2.0 183 Session Description(SDP: B) (Note: The Terminating Gateway will start sending ringing tones.)
12. Update RTP resources—flag for one-way RTP media (MGCP+)(Map B to B')

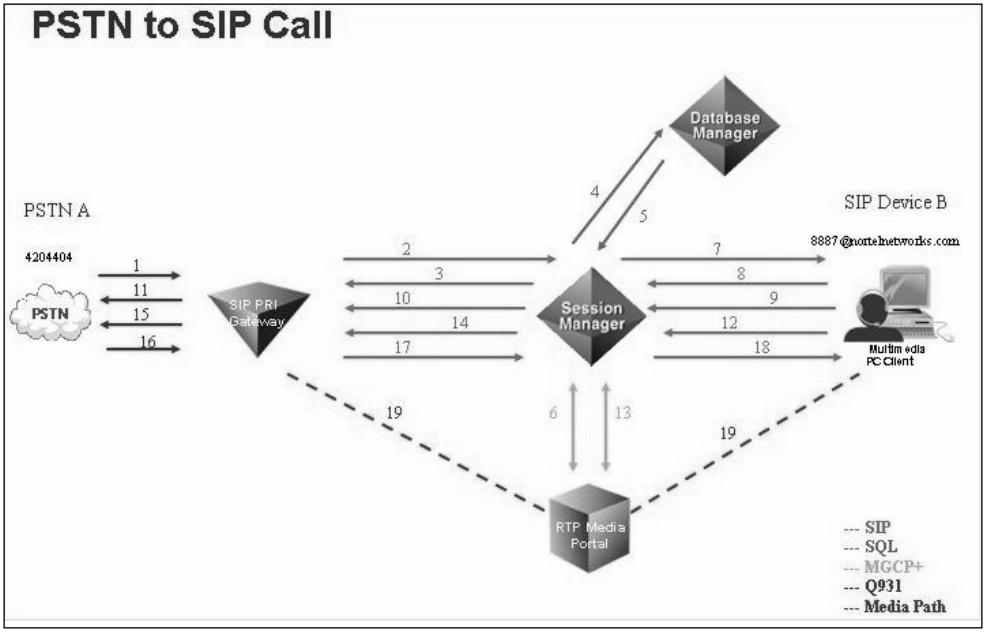
13. One-way Media Path Established for Early Media Note: This is a one-way media path from the Gateway to Device A. Information is not mapped in the reverse order.
14. 183 Ringing (SIP)—SIP/2.0 183 Session Description (SDP: B') (Note: The originating client will start sending packets when it receives the 183 with SDP information.)
15. Connect (Q931)
16. OK (SIP)—SIP/2.0 200 OK m: <sip: 66934404@47.100.234.140:5060> (SDP: B)
17. Update RTP resources for B (MGCP+)—flag for 2-way RTP media (This sets up the 2-way RTP path. If 16 contained new SDP for B, then this new B would be mapped to B'. However, the Gateway will send the same SDP.)
18. Media Path Established (RTP) (A to B', then NAPTed and forwarded A' to B)
19. OK (SIP)—SIP/2.0 200 OK m: <sip: 66934404@47.104.12.150:5060> (SDP: B')

NOTE

If the OK contained new SDP information, the client would begin sending its packets to the new SDP.)20.ACK (SIP)—ACK sip:66934404@47.104.12.150:5060 SIP/2.0 21.ACK (SIP)—ACK sip:4404@private.nortelnetworks.com:5060; maddr=47.100.234.140; user=phone; norteltrkgrp=pria_t1_8000 SIP/2.0

To make a complete circle on the phone call, in Figure 2.16 we look at a PSTN-to-SIP phone call.

Figure 2.16 PSTN to SIP



Here are the steps by the numbers within the call flow for the PSTN to SIP call.

1. SetUp (Q931).2.Invite (SIP)—INVITE sip:8887@private.nortelnetworks.com; maddr=47.104.12.150; transport=udp; user=phone;
2. Invite (SIP)—INVITE sip:8887@private.nortelnetworks.com; maddr=47.104.12.150; transport=udp; user=phone; nortelTrkGrp=pri_t1_8000 SIP/2.0 m: <sip: 4404@47.100.234.140:5060> (SDP: A)
3. Trying (SIP)—SIP/2.0 100 Trying
4. Database Lookup (SQL)—send 8887@nortelnetworks.com
5. New URL (SQL)—return sip:8887@nortelnetworks.com:5060;maddr=47.100.234.159
6. Request RTP resources for A (MGCP+) (A', B') (Map A to A')
7. Invite (SIP)—INVITE sip:8887@nortelnetworks.com:5060;maddr=47.100.234.159; ttl=1;

transport=udp SIP/2.0 m: <sip: 4404@47.104.12.150:5060> (SDP: A')

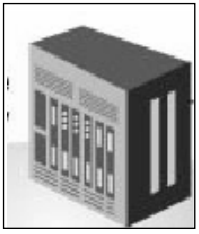
8. Trying (SIP)—SIP/2.0 100 Trying
9. Ringing (SIP)—SIP/2.0 180 Ringing(SIP clients do not send SDPin the 180)
10. Ringing (SIP)—SIP/2.0 180 Ringing
11. Alerting (Q931)
12. OK (SIP)—SIP/2.0 200 OK m: sip: 8887@47.100.234.159:5060 (SDP: B)
13. Update RTP resources for B (MGCP+)(Map B to B')
14. OK (SIP)—SIP/2.0 200 OK m: <sip: 8887@47.104.12.150:5060>(SDP: B') (Note: Originating Gateway will start sending packets.)
15. Connect (Q931)
16. Connect ACK (Q931)
17. ACK (SIP)—ACK sip:8887@private.nortelnetworks.com;maddr=47.104.12.150; transport=udp; user=phone;nortelTrkGrp=pria_t1_8000 SIP/2.0
18. ACK (SIP)—ACK sip:8887@nortelnetworks.com:5060; transport=udp SIP/2.0 (Note: Terminating client will start sending packets.)
19. Media Path Established (RTP) (A to B', then NAPTed and forwarded A' to B)

AudioCodes Gateways

The gateway of choice and the one that would be shipped with your MCS 5100 system is a Mediant gateway made by AudioCodes Limited (see Figure 2.17). These gateways come in many different sizes and shapes, depending on what your current needs are in the system. The gateway that we will be looking at in our examples is a Mediant 2000 configured with two PRI ports. The system can handle more PRI ports if ordered and depending on

your bandwidth. Figure 2.17 shows a Mediant gateway. These gateways come in different sizes, and units are available for the small office user and users of carrier-class enterprise systems.

Figure 2.17 AudioCodes Gateways



NOTE

Although most companies still and will continue to use PRI's links to the PSTN for service, the MCS 5100 can do a regular SIP trunk to a PSTN gateway. This has become more of an option now in the telco world since it is much cheaper to do SIP trunk over a data line than install and provide costly PRI circuits.

After the initial CD install to set up the gateway, you will be able to log on to the system via a Web page browser. This browser is available via the IP address assigned to the gateway at the time of the initial CD install. The Web page is a secure Web page, in which you will need to know the username and password to access the system. Please be aware that the login and password are case-sensitive on the system.

The system you are about to look at is a working system and the configuration can be changed to suit other setups. Although we will not be going through every option, this section is more of an overview to the gateway.

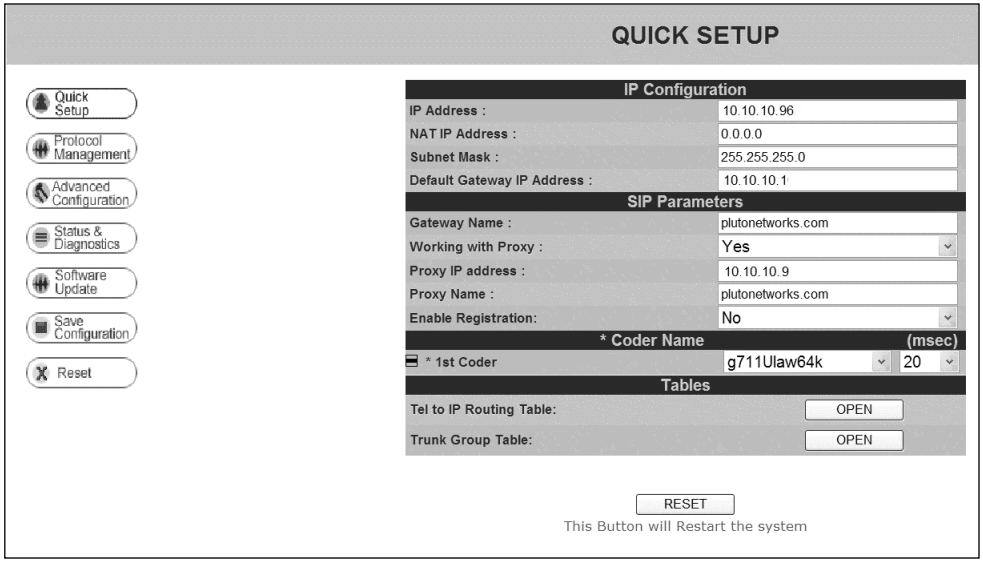
Quick Setup

In the first figure, you can see information that has been put into the Web page. The items that will need information added or inserted to them are the IP address for the gateway, subnet of the gateway, the default gateway IP address, gateway name, proxy IP address, and proxy name. The other fields are filled in by default but they can be changed. These would be the fields for working with proxy and enabling registration. The coder name field is very important since this will be the code used when the gateway send calls to your proxy.

The coder can be changed from such codes as G711 to G729, based on the administrator needs. The time, or msec, for these codes can be specified, also based on what is needed. They can be set for as low as 20 msec or as high as 120 msec. All these options and more are available on the CD that comes with the gateway. It is recommended that you keep this in a safe place since it does have help files on it.

In Figure 2.18 you can see an example of the Web page used for administration. To the side are the areas in which you may browse and configure.

Figure 2.18 Quick Start



Protocol Management

The next button on the left hand side is one for Protocol Management. After clicking on this button a new row of suboptions will be displayed at the top. This is the same for other buttons on the left-hand side of the Web page. There are six new subareas under Protocol Management; under Manipulation Tables there are four other subsections to that table. These all can be seen by just moving your mouse or cursor over the selected areas.

Protocol Definition

In Figures 2.19 through 2.21 you can see that we have clicked on the Protocol Definition in the Protocol Management section. In this area you will find the SIP Definition; under this definition you will have the following:

- General area
- Proxy Server and Authentication area
- Coder name
- DTMF and dialing parameters
- Early media parameters
- Number manipulation and routing modes
- Supplementary services
- ISDN and CAS parameters
- Miscellaneous parameters

Figure 2.19 SIP Definitions

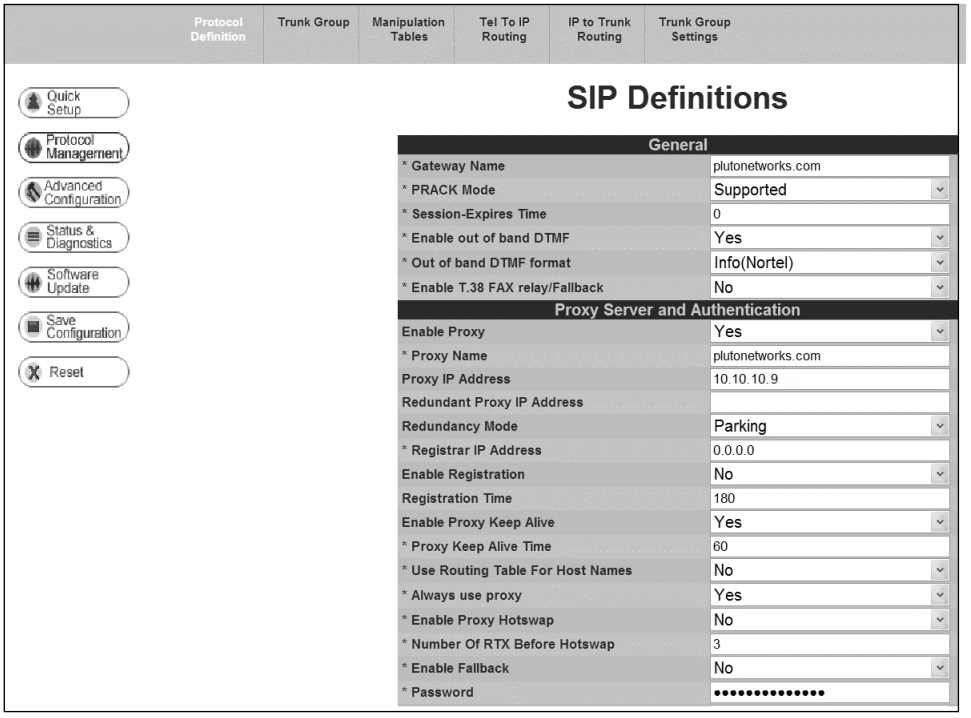


Figure 2.20 SIP Definitions

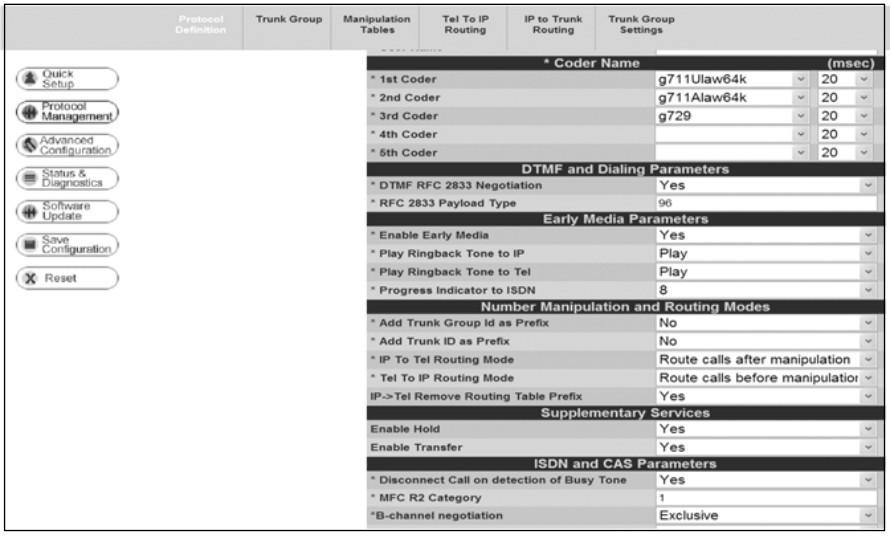
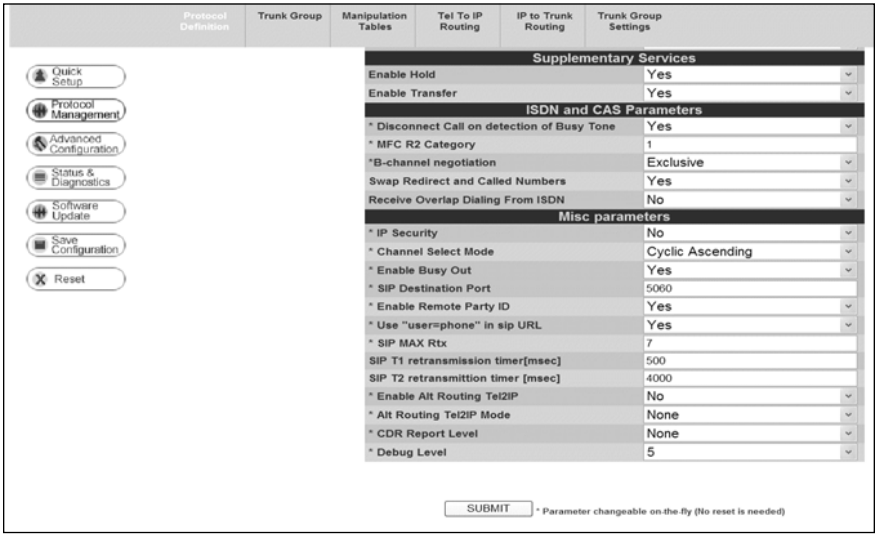


Figure 2.21 SIP Definitions



NOTE

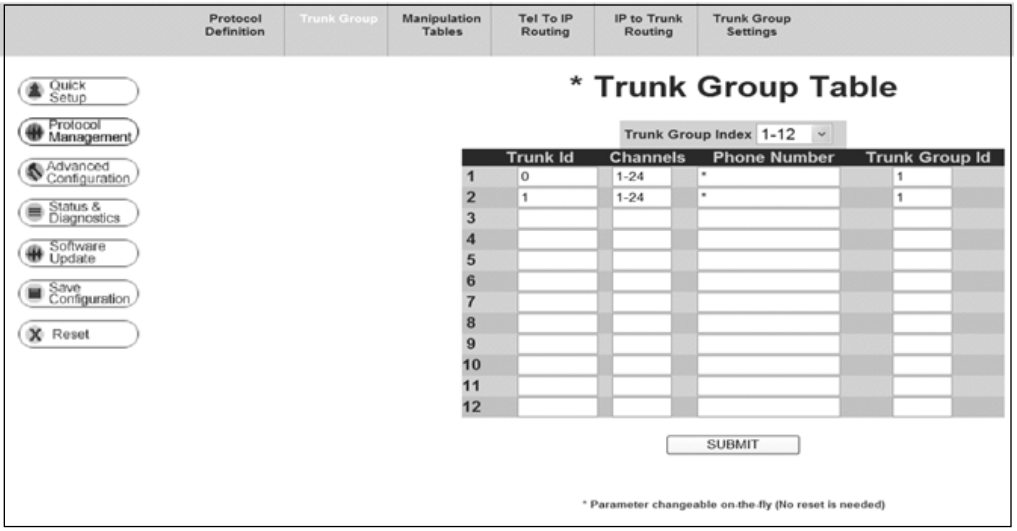
As you can see from these screen shots, there are certain options that have a * symbol. These are the options that you will need to fill based on how your system is configured. The settings configured in this section are sample default settings.

Trunk Group

Figure 2.22 shows the Trunk Group table, which is also under the Protocol Management configuration tab. Within this table, the Trunk Id's are configured based on your current network PSTN requirements as well as how many channels will be used on each Trunk. Different Trunk Group IDs may be used on the system as well. So you may have four or five Trunk Groups, and then have a different number of Trunk IDs within those Trunk Groups.

This section also is intended to be used to separate customers or sections of the company to different Trunks. Also, different applications can be separated to different trunks or Trunk Groups based on need.

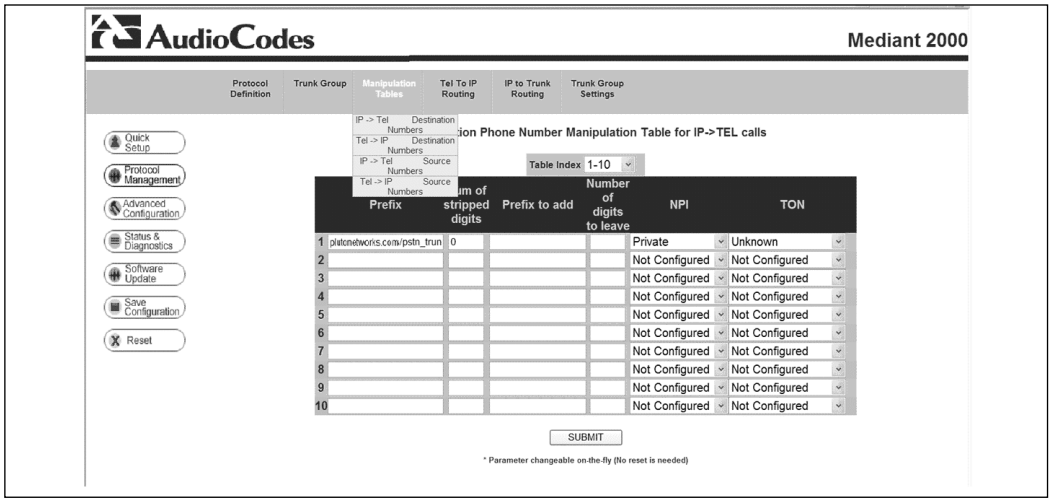
Figure 2.22 Trunk Group



Manipulation Tables

In Figure 2.23, as is the case in many of the top tables on the Web page when highlighted, there is a drop-down menu. Within these drop-down menus you will see submenus of the tables you have highlighted. In this figure, the Manipulation Tables are highlighted; below this are four submenus that we will go through one at a time.

Figure 2.23 Manipulation Tables

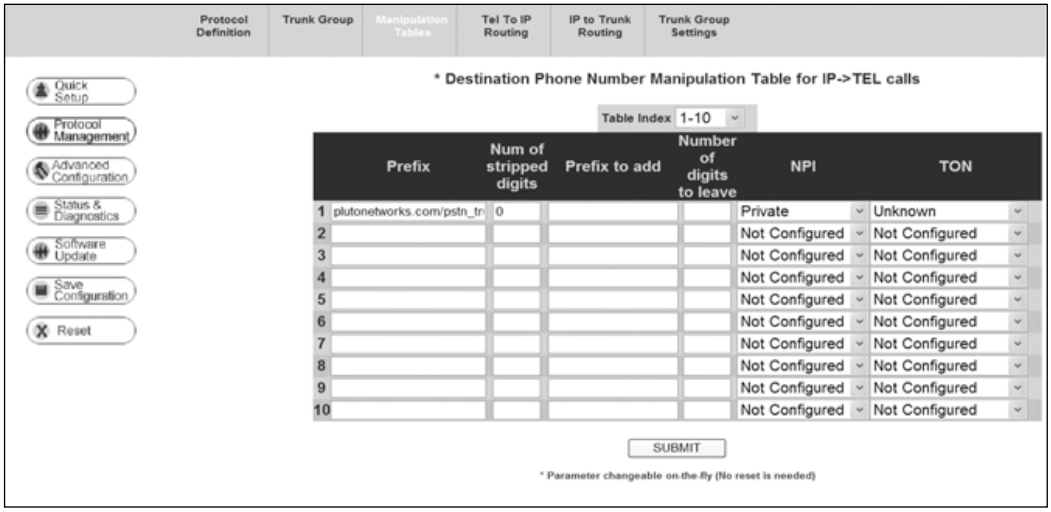


Well before configuring this part of your gateway, as seen in Figure 2.24, you should discuss it with your telco carriers. Based on the following information, telco will know how to send the calls to your gateway. The prefix you enter will be unique, like the following, plutonetworks.com/pstn_trunk _group. The Number of Stripped Digits refers to how many numbers will your gateway takes off the front of the incoming number.

If a number such as 9195551212 is sent to your gateway, and as shown the number of stripped digits is set to zero, the whole number will be sent from the gateway to your PBX. Now let's say we want to strip three digits from the incoming number; then the number being passed to the PBX will be 5551212. The system does not allow you pick which numbers are being stripped, like the three and five digits of the phone number; it always starts from the beginning of the incoming number.

The NPI refers to the dialing plan you have chosen for the system and TON means the type of number used.

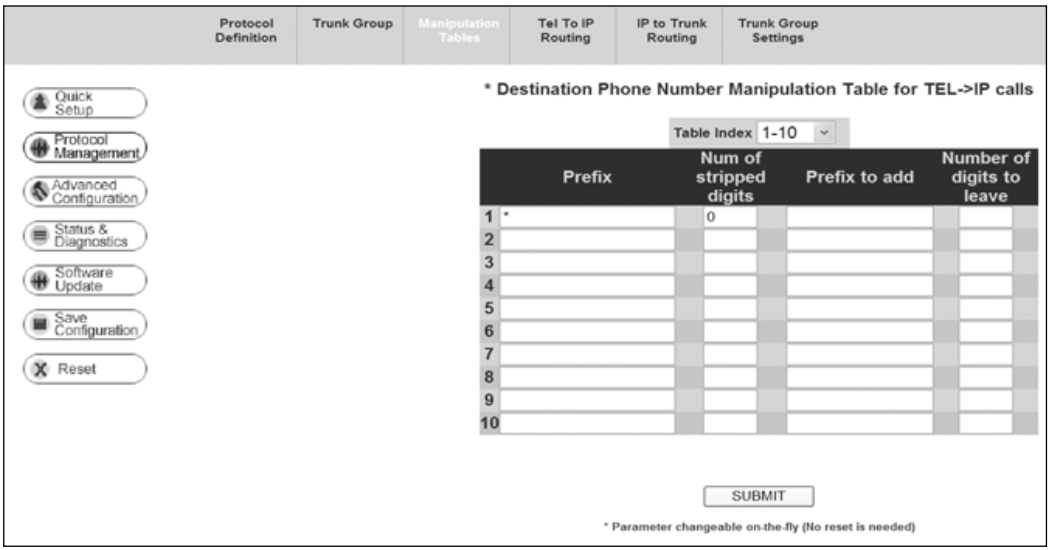
Figure 2.24 Manipulation Tables Destination IP>TEL Calls



The next shot we will look at is the Telephone-to-IP calls within the same table. As you can see in Figure 2.25, it is very similar to what was provisioned earlier, since this is for the destination phone number. It is important to remember this when provisioning or troubleshooting a problem on the

system. The * symbol listed in the prefix area is just a wild card list in place of something else. This maybe used in the system from time to time.

Figure 2.25 Manipulation Tables Destination TEL>IP Calls



Now we have moved form the destination phone number tables to the Source Phone number tables as listed in Figures 2.26 and 2.27. As you can see, these are essentially the same figures as the ones earlier; the only difference is that these are Source Numbers. Remember which you are working on when you get to these pages, it will help in the end.

TEL-to-IP Routing

Within this table (see Figure 2.28) the destination phone prefix refers to the routing table of the incoming call from the PSTN to the gateway. The IP Address listed in the table refers to your SIP Proxy Domain. These tables can be used for IP Security also if the options have been turned on; for this screen shot it is not. There can be up to 50 separate routing indexes chosen from the drop-down box in the middle of the page.

Figure 2.26 Manipulation Tables Source IP>TEL Calls

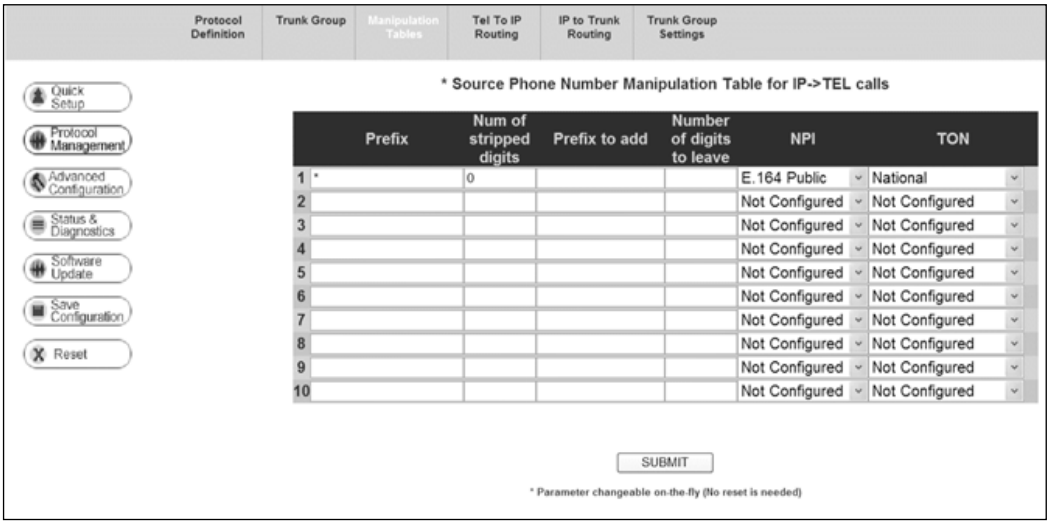


Figure 2.27 Manipulation Tables Source TEL>IP Calls

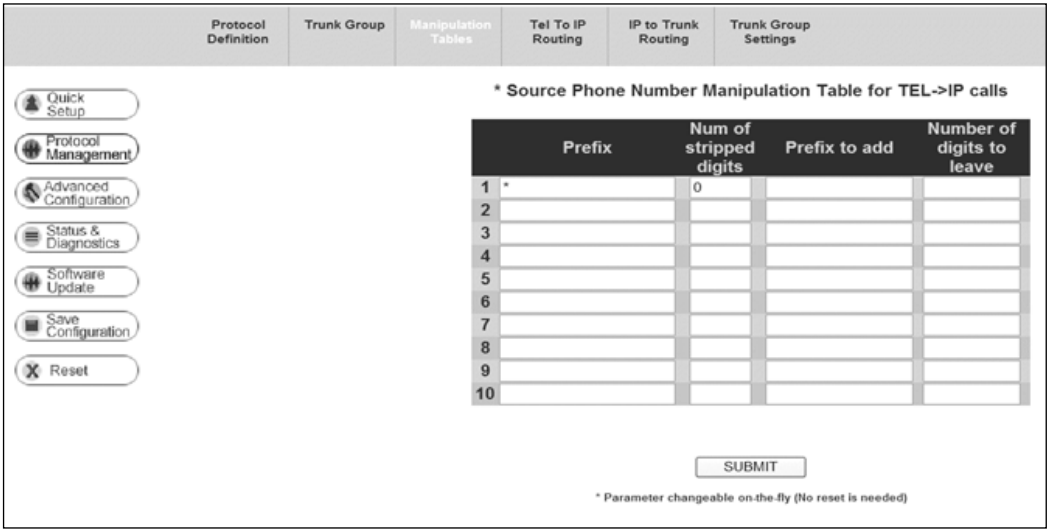
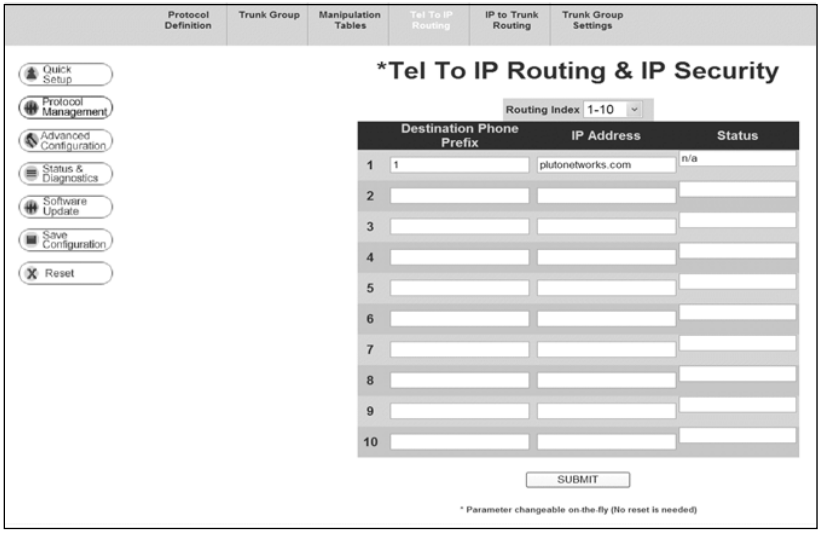


Figure 2.28 TEL-to-IP Routing



IP-to-Trunk Routing

In Figure 2.29 you may have up to 24 different Routing Indexes from the drop-down menu in the middle. The Prefix table once again has our trunk group Routing table with the Trunk Group ID assigned to it. You may have many different indexes for your network, as mentioned earlier, unless you are using multiple carriers or are acting as a service provider, when you will not use more than a couple for your network.

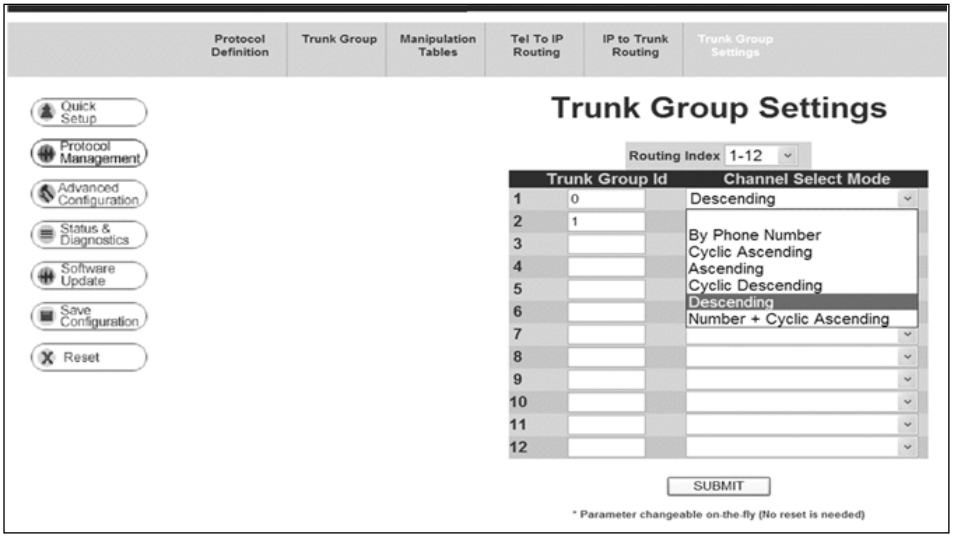
Figure 2.29 IP-to-Trunk Routing

Trunk Group Settings

Within the Trunk Group Settings you are able to choose how you would like the calls coming from the PSTN to arrive and process on the gateway. As you can see in Figure 2.30, we have our Trunk Group IDs listed as zero and one and also on our Channel Select Mode we have chosen Descending. But there are many others to choose from, listed in the drop-down menu, based on your needs in the gateway. As a reminder, before you choose your options, work with your carrier.

You should work with your carrier because many people don't know about Glare and what it can do on your network. This is a problem that happens when two calls—one inbound and one outbound—try to take the same DSO at the same time. This can be eliminated or reduced by the customer starting at the top of the trunk and the PSTN starting at the bottom when delivering calls. Otherwise, if both started at the top or bottom, the Glare effect can happen and cause problems on your gateway.

Figure 2.30 Trunk Group Settings



Advanced Configuration

The next tab is called Advanced Configuration, and it consists of seven subareas that will be listed once again at the top. These areas will be for Network

Settings, Channel Settings, Trunk Settings, TDM Bus Settings, Configurations File, Regional Settings, and Change Password. To be honest I am not sure why these are called advanced settings when you really need to have these configured before the gateway will work.

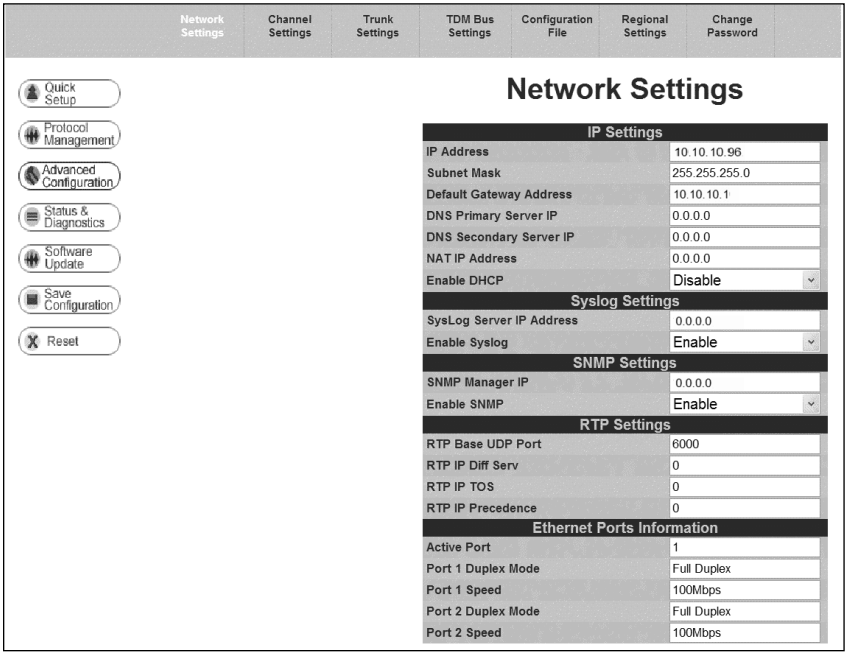
The company that makes the gateway should have made one tab for configuration, so this has to be done before starting. The quick setup does not get everything configured you need for the gateway to work.

Network Settings

In Figure 2.31, we can see that the first item listed under this area is Network Settings. The first subarea listed is for IP settings; this is where you put the IP address of the gateway. You also need to fill in the subnet mask, default gateway, and enable DHCP. The other listings can stay at 0.0.0.0 if they are not going to be used in your setup. If left blank they will go to the default for the gateway.

The Syslog settings may be filled in or left at 0.0.0.0, as well as the SNMP settings. The other settings may remain at the defaults or may be changed based on your gateway setup.

Figure 2.31 Network Settings



Channel Settings

In the next area we will take a look at the Channel settings under Advanced Configuration. Figures 2.32 and 2.33 show all the Channel settings that you can adjust to meet your needs. Within the Channel settings, the area that needs the most attention are the Voice settings. The other areas are all set to default settings for the gateway. In the Voice settings, you can adjust your DTMF Transport Type, MF Transport Type, and CAS Transport Type based on information from your PSTN provider.

When troubleshooting a problem or on the initial calls after the gateway is set up, you may adjust your Voice Volume, Input Gain, Silence Suppression, and DTMF Volume Type based on your system needs. These settings come in handy when adjustments are needed; they can be made on the gateway, thereby not having to go through your PSTN provider for small changes.

Figure 2.32 Channel Settings

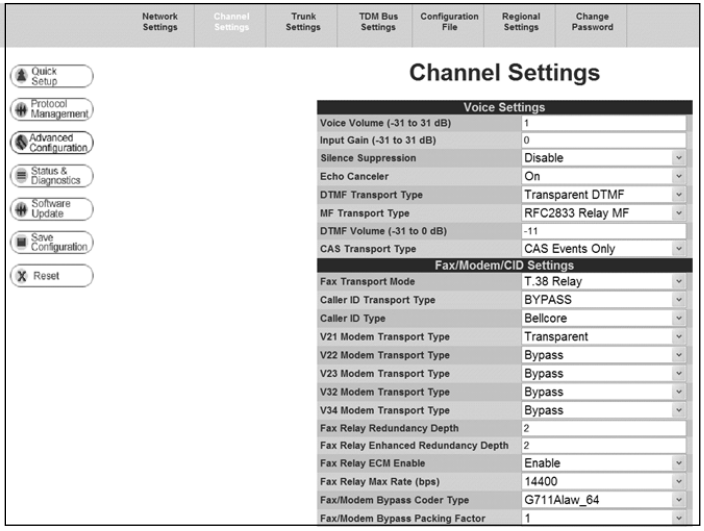
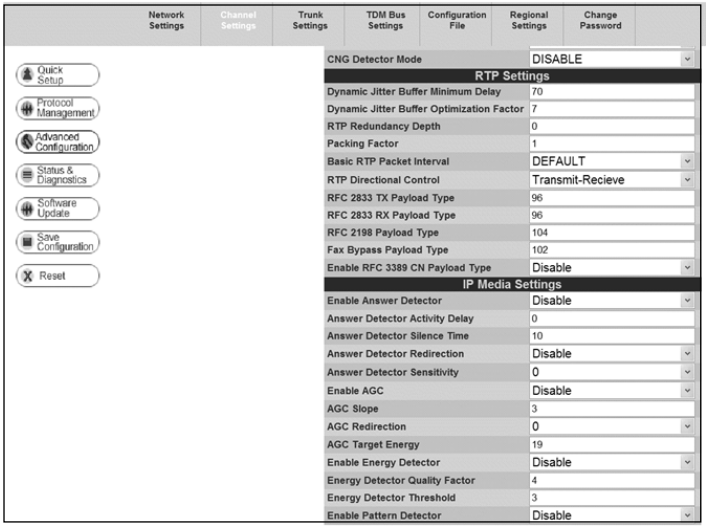


Figure 2.33 Channel Settings



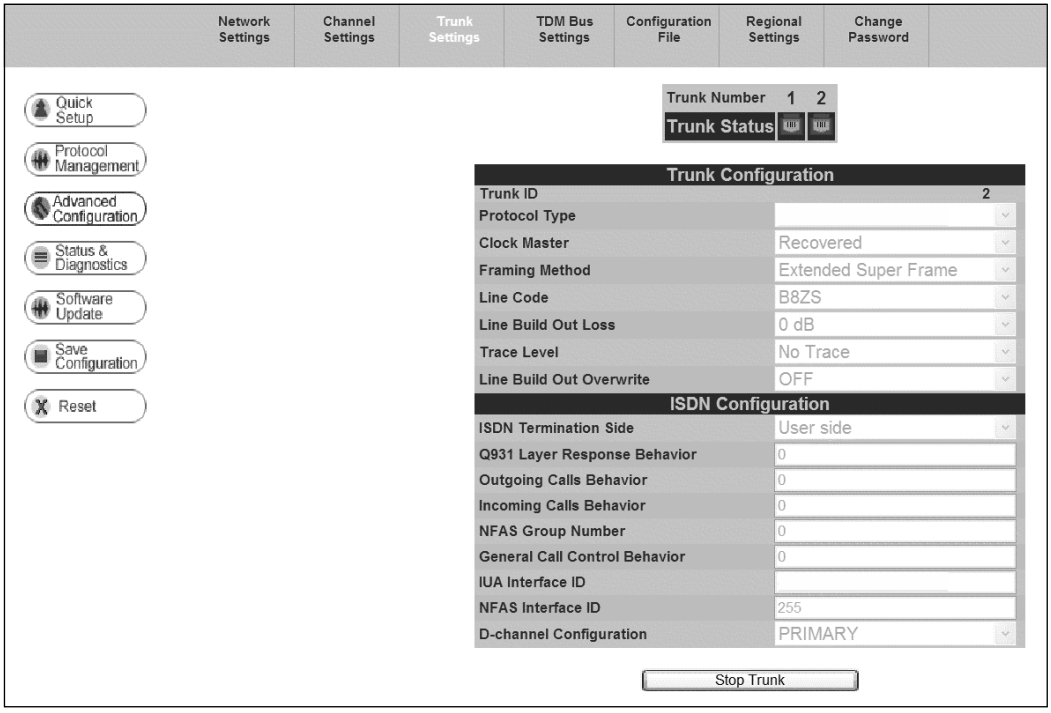
Trunk Settings

Trunk Settings are how you get your gateway to talk to the switch within the PSTN carriers cloud. In Figure 2.34 we see that we now have settings for our Trunk Configuration and ISDN Configuration. Don't get confused—a PRI coming into the gateway is referred to as an ISDN PRI in many different areas. I have unplugged both PRIs going into the test switch so you would see the red shown in the Trunk Status area for each Trunk Number.

Under the Trunk Configuration area you may choose the Protocol Type used by the PSTN switch; there are many different types to choose from. All these settings under Trunk Configuration will be options that your PSTN carrier will give you based on their local switch. Most of the time these setting cannot be changed since it will be the local PSTN switch that services your area.

Within the ISDN Configuration, all the options are default except for the ISDN Termination Side, which is set now for User Side based on PRIs coming from the PSTN Carrier. Now if you were setting up the gateway to send its calls to another PBX, you would set it up as a Network Side. The D-Channel Configuration is now set to Primary since both PRIs coming in have separate d-channels. If there were multiple PRIs per d-channel you could change the setting to Backup or NFAS.

Figure 2.34 Trunk Settings



TDM Bus Settings

In this small area shown in Figure 2.35, there are only three things to change during setup. One is the PCM Law Select, which can be either Mulaw or Alaw. Next is the TDM Bus Clock Source setting, which can be either Network or Internal. If using PRIs from a PSTN carrier it is suggested to use the network setting. Also you may enable or disable the TDM bus PSTN Auto Clock setting.

Configuration File

A good way to back up your config file for the gateway is to retrieve the INI file from the gateway and store it somewhere safe. In Figure 2.36 you may receive the INI file form the gateway that will help you restore the gateway incase of a problem. Also as you can see, you can select an INI file from your computer and send it to the gateway in case a restore is needed on the system.

Figure 2.35 TDM Bus Settings

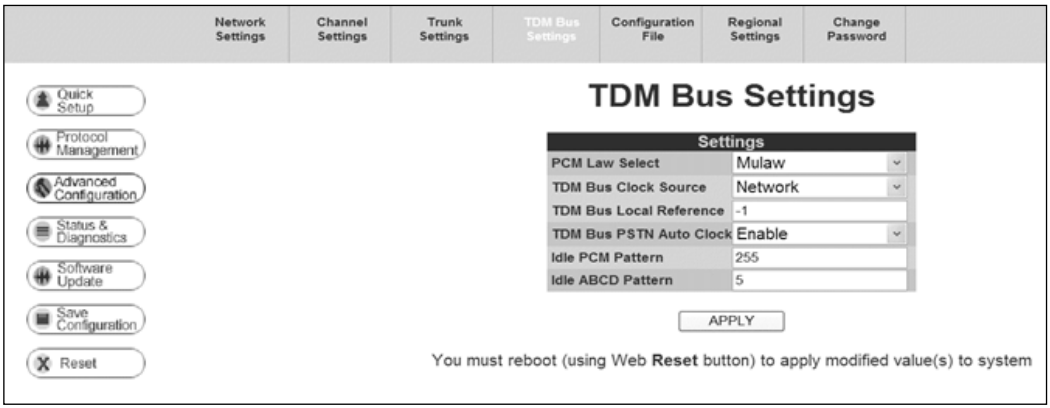
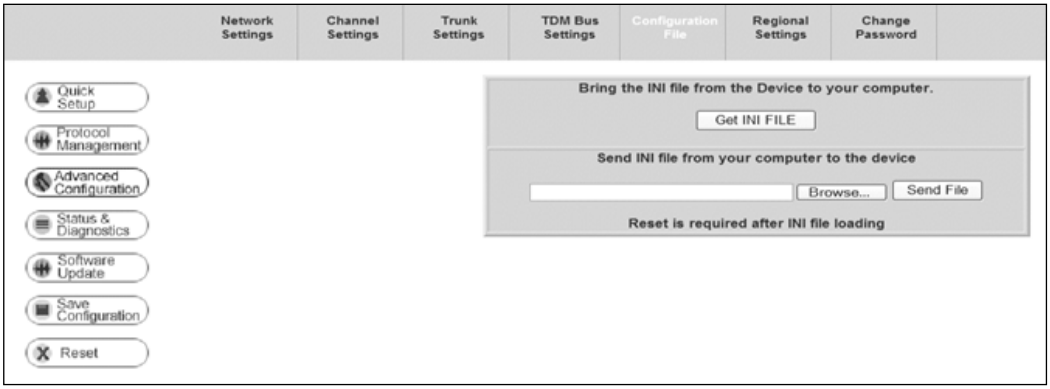


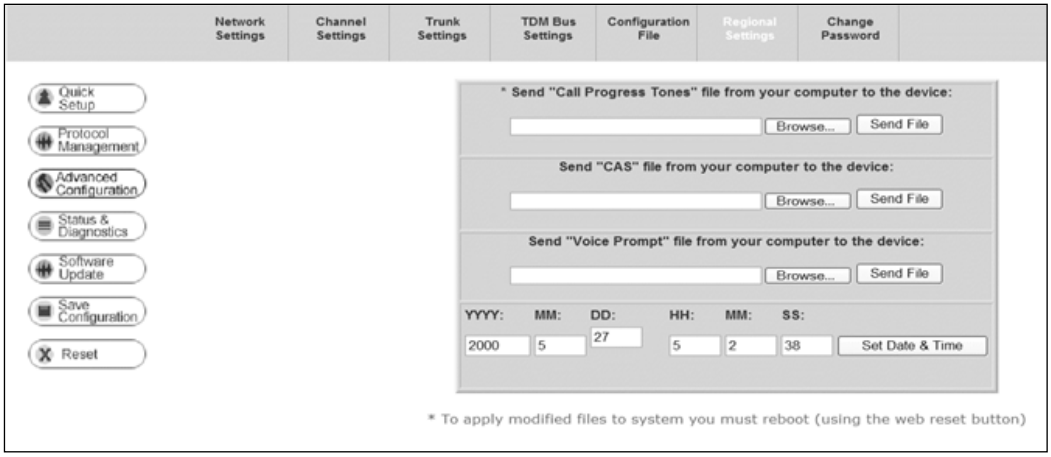
Figure 2.36 Configuration File



Regional Settings

Within the Regional Settings area you can see this is for uploading files to the gateway for different purposes. The first (as shown in Figure 2.37) is to upload Call Progress Tones to the gateway from your computer. Next you have the ability to send a CAS file to the gateway, and last to upload Voice Prompt to your gateway. Most users will never use these features since everything is controlled on something other than the gateway for these options. Also this is the area to set or change your date and time for the gateway.

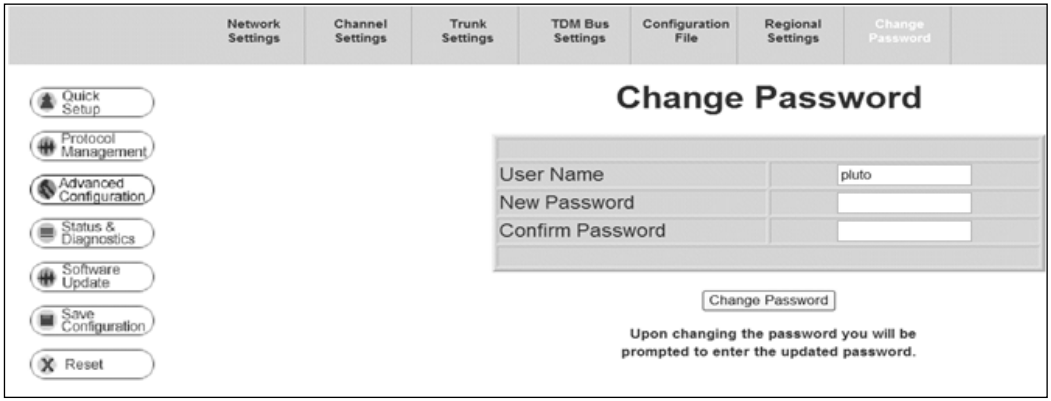
Figure 2.37 Regional Settings



Change Password

To be able to log onto the gateway via direct cable or over a Web page you must have a username and password to do so. In Figure 2.38 you can see the username listed; this can be changed to whatever you would like; then you just put in a password and retype your password below. Remember to put your password and username in a safe place. You don't want to lose them and have to start all over again. But if you do, just remember to always save your work and retrieve the INI file each time to your laptop—it can be a life saver.

Figure 2.38 Change Password



Status & Diagnostics

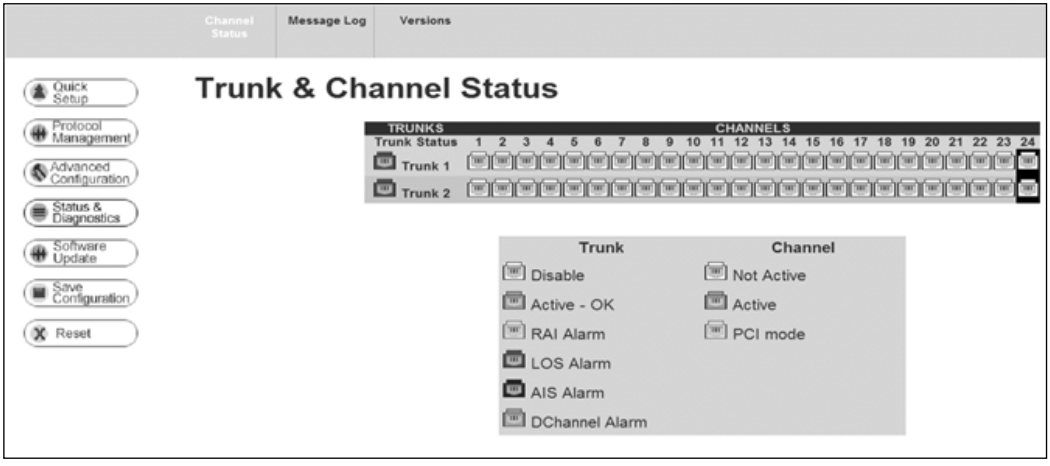
The tab on the left called Status & Diagnostics will be one that you use most often to watch what is transpiring on the gateway. It is a real-time section that provides information on the trunks that are coming into the gateway and their status, and also helps troubleshoot problems. If you have configured the message log to be on it will provide you that information also in this section. Also provided will be the version information for your gateway, which can help with many different problems or upgrade issues.

Channel Status

When troubleshooting the PRIs coming into the gateway, this next section is most helpful since it will give the administrator the information they need to work through problems. In Figure 2.39, you can see that we have two trunks or two PRIs coming into the gateway. Along with the trunks you can see the 24 channels to the right. Starting with Figure 2.40, we will show what you can see when you click a channel. On the bottom of Figure 2.39 you see that there are different color codes for the trunk and channel. These will change when the status of either the trunk or channels changes.

As calls starts to come in over the trunk the channels will begin to fill and go from Not Active to Active and change colors. The same can be said for the trunks; there is really only one good color and the rest will show you have a problem.

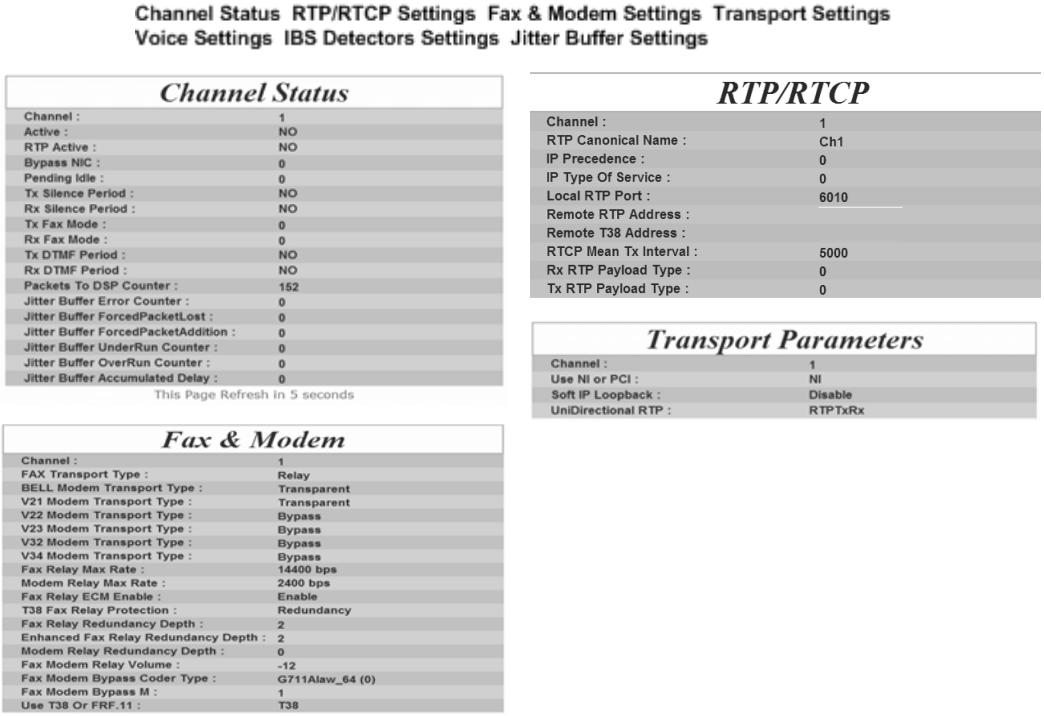
Figure 2.39 Channel Status

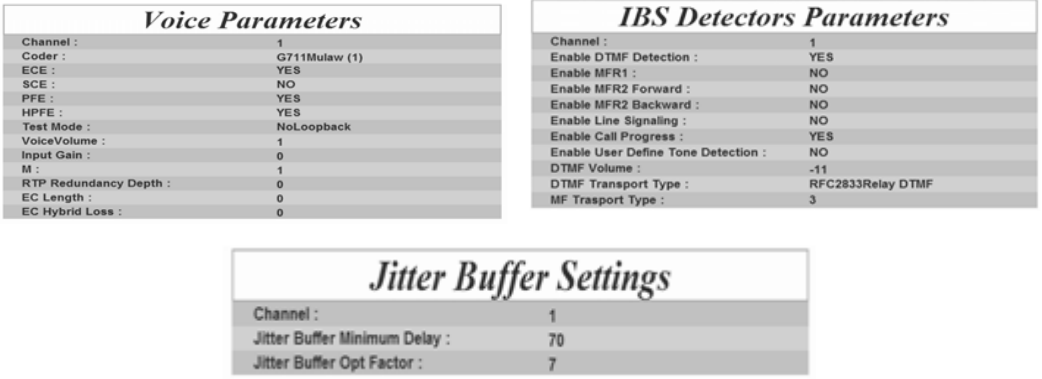


In the following section, we have many different screen shots from after we clicked on channel one. When you click on a channel it allows you to watch what is going on with a current call in progress or an idle channel. If you are having problems with a call you can see the jitter buffers, voice and transport settings, plus much more to help with troubleshooting the issue.

Here are the options you can use after selecting a specific channel on the trunk along with individual screen shots of what each option looks like. One certain option like the Channel Status will refresh the page every five seconds to update the information. This works well when you can see the activity in real time along with any jitter problems you might be having.

Figure 2.40 Channel 1





Voice Parameters

Channel :	1
Coder :	G711Mulaw (1)
ECE :	YES
SCE :	NO
PFE :	YES
HPFE :	YES
Test Mode :	NoLoopback
VoiceVolume :	1
Input Gain :	0
M :	1
RTP Redundancy Depth :	0
EC Length :	0
EC Hybrid Loss :	0

IBS Detectors Parameters

Channel :	1
Enable DTMF Detection :	YES
Enable MFR1 :	NO
Enable MFR2 Forward :	NO
Enable MFR2 Backward :	NO
Enable Line Signaling :	NO
Enable Call Progress :	YES
Enable User Define Tone Detection :	NO
DTMF Volume :	-11
DTMF Transport Type :	RFC2833Relay DTMF
MF Trasport Type :	3

Jitter Buffer Settings

Channel :	1
Jitter Buffer Minimum Delay :	70
Jitter Buffer Opt Factor :	7

NOTE

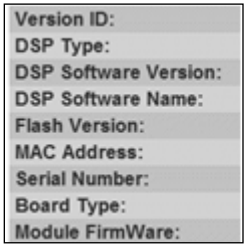
When you are using these tables to troubleshoot problems with issues such as jitter or buffers, remember that these represent only the gateway to PRI Trunk. If you are having issues with jitter to a phone and there are no problems shown in these tables during a call, the problem is on the LAN/WAN.

Message Log and Version

These are two very short areas that need to be covered in this section. If you have the message log enabled or not it will tell you that when you click on that area as shown in Figure 2.41, and if you stay on that page it will refresh with logs as long as you stay there. In Figure 2.42 for the Version area we have blued out the Mac Address and Serial number for security reasons, but you can see the other information that can be displayed in this area.

Figure 2.41 Message Log

Figure 2.42 Version



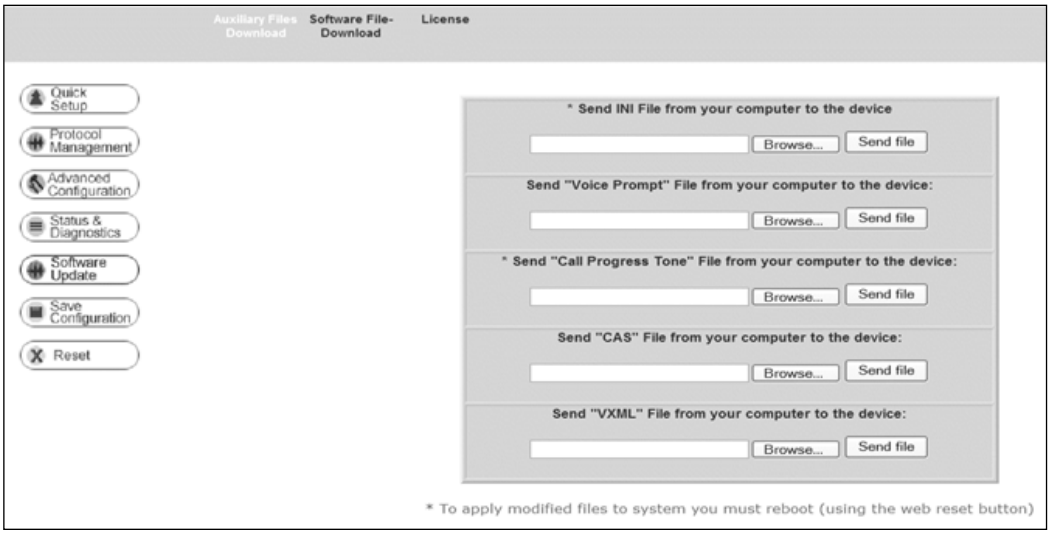
Software Update

As you can tell by the title of this section, we will show how to update software to the gateway. This can be done by a computer and Web page as shown next. Before we take a look at the different areas within the Software Update, there are few things to remember. One, always double-check what files you are uploading to the gateway for any type of updates. This will eliminate problems of uploading or loading the wrong files that can bring your gateway and system to a halt.

Auxiliary Files Download

In Figure 2.43 there are many different file types that can be sent from your computer to the gateway. You may upload INI files, Voice Prompt files, Call Progress Tone files, CAS files, and VXML files. More than likely you will not use any of these other than the INI file. Most of the time, you would upload the INI file to the gateway only if technical support gave you instructions to do so or you made changes to an INI File off the gateway.

Figure 2.43 Auxiliary Files Download



Software File Download and License

The last areas of this section deal with the upload of the CMP file from your computer to the gateway and the gateway license. In Figure 2.44 you can see there is a warning to retrieve the INI file from the gateway to your computer before uploading a new CMP file to the gateway. Any time you see these suggestions on the gateway, it is a common practice to follow them. The area that shows the license will not be shown in this book for security reasons, since it shows the license and keys for the gateway.

Figure 2.44 Software File Download

Save Configuration and Reset

The last sections that will be covered are the Save Configuration and gateway Reset. After making any changes to the system you will need to save these changes by clicking the button shown in Figure 2.45 to Save Configuration. If you make changes to the system and those changes were not saved, they could be lost if the gateway is reset. If the gateway needs to be reset for any reason this may be done by clicking the Reset button; then you would receive the message as listed in Figure 2.46.

The gateway will be offline for three minutes and all calls will be rejected. It is a common practice to do any reset after hours when the system may be taken down. Also remember that if the system is reset there will be no access to that system via direct link or Web page until the system restarts from the Reset.

Figure 2.45 Save Configuration

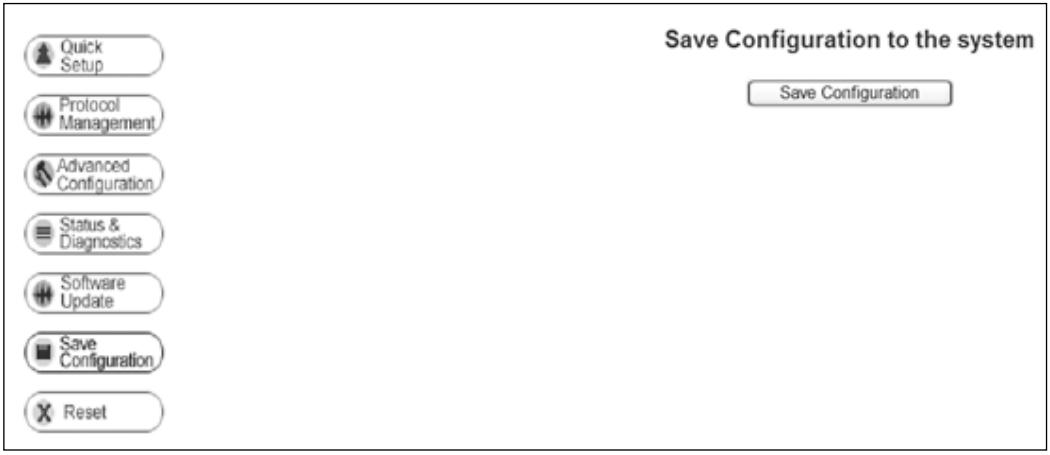
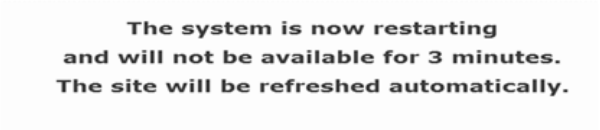


Figure 2.46 Reset



NOTE

This gateway is not mandatory for the MCS 5100 to work; it the gateway of choice and sold by Nortel with the system. Any gateway that has the same features for SIP or H.323 can be used for the system.

Summary

In this chapter we have looked at many different areas of the MCS 5100 that have architectural design concerns. The MCS 5100 has many different components and can be arranged in several different configurations. Just as an example, if your network or another provider can accept protocols such as H.323 or SIP, voice mail can be sent to an off-site vendor. This would mean you can keep your current voice-mail system. If your company does not need a quote conferencing server, you may use just the Ad Hoc server for this servicing. People would need to be added on one by one, but it will work.

The system has been designed in such a way that it can be used for a small company or a very large service provider. Even small companies can and will want to create their own subdomains for better management of the system. It will allows for better service package administration, user administration, and also the problems having to deal with E911 on a system. The one thing to take away from this chapter is that you can have a small system and it can be just as well optioned as a bigger system.

Solutions Fast Track

Component Overview

- ☑ The MCS 5100 can be configured with both two, four, or eight Sun Fire V100 Servers or eight Sun Netra 240 Servers.
- ☑ In order to have a redundant system, the number of original Sun Servers is multiplied by two.
- ☑ In a bigger enterprise network the use of an IBM Blade Server instead of separate IBM Servers could be money well spent for future expansion.

Network Topology

- ☑ A CS 1000 PBX is needed to provide TDM service to the Call Pilot Voice Mail system since this system does not have SIP as an option.

- ☑ The MCS 5100 can send voice-mail traffic to a system that is not within the current system, provided that outside system can do SIP or H.323.
- ☑ It is suggested that a port count is taken on all equipment within the system; this will help in port assignments to the network switches. It will provide information on how many switches will be needed on the network.

IP Addressing

- ☑ The MCS 5100 by itself can work off a single subnet to all IP Phone and PC Clients.
- ☑ If a CS 1000 or Call Pilot voice-mail system is added to the MCS 5100, other VLANS such as a CLAN, ELAN, and TLAN will need to be added. These are all separate subnets on the network.
- ☑ When configuring the network and DCHP for IP Phones, remember to leave enough for expansion of the system.

Domains and Subdomains

- ☑ Domains and subdomains should be used by both large and small systems to provide better administration to the system.
- ☑ Before starting with a configuration, take time to ensure that the plans for these domains and subdomains are correct and allow for growth. It is hard to go back a year later and have to reconfigure the network when time was not taken up front.

AudioCodes Gateway

- ☑ This is the gateway of choice for the MCS 5100 system within Nortel System.
- ☑ This provides support from a MCS 5100 and CS 1000 for SIP protocol to and from the system as well as PRI configuration from a PSTN provider.

- ☑ The system has more options than will ever be used with a normal MCS 5100 configuration.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Can I use servers other than the current Sun Servers in this chapter for my MCS 5100 system?

A: Not at this time. The system is built around the current Sun Server configuration and will not work with another vendor.

Q: Why is there a need to use another PBX just to provide a connection to the Nortel Call Pilot?

A: Nortel has not provided support as of yet for the Call Pilot system to provide SIP to and from other systems. As of this moment the only supported way is to go through a CS 1000.

Q: Why would I need to configure multiple subdomains in my company?

A: The best reason is for better administration, provisioning, user-defined packages, and E911 support.

Q: I have seen mentioned that there are as many as four different subnets needed for a system. Why not use just one to make it easier?

A: When adding Call Pilot to the MCS 5100 system, a CS 1000 is added, which has three separate VLANS on its system alone. There is no way to use less than three when this is added, but using four is better.

Q: If I am using an MCS 5100, CS 1000, and Call Pilot, do I need to use a separate gateway for PRI trunks from the PSTN?

A: You can add PRI Cards to the CS 1000 to provide calls to and from the PSTN.

Q: How are calls sent to and from the MCS 5100 and CS 1000?

A: They are sent via SIP from the MCS 5100 to the Signaling Server within the CS 1000.

Q: Can calls be connected to other systems outside my company?

A: If the system provides SIP support you can do a SIP-to-SIP call to another system outside your network. This is configured a foreign system on the MCS 5100 and must be allowed and be a recognized IP addresses.

Q: In the drawings I see, there are dual paths from the MCS 5100 to the network connections. Is this really needed?

A: No, it is not needed. You can use connection to one switch, but it is recommended and a best practice always to use a different switch when you have more than one connection going out to the network. This is for disaster recovery in case a path is lost on one switch; you have a back up switch to provide a path.

Chapter 3

System Management Console

Solutions in this chapter:

- **Installing MCP Client**
- **Configuration of MCP Client**
- **IPCM Device Maintenance**
- **Alarm Browser**
- **System Options**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

In this chapter we will look at the installation and the configuration of the MCP Client, which is called the Multimedia Communications Platform Management Console (MCPMC) in other documentation. This software is used to manage the MCS system within the network environment. The console specifically provides the following to the administrator:

- Administering system, database, and service components
- Deploying and configuring system sites, servers, components, and component services
- Monitoring system using alarms, logs, and performance measurements
- Managing collection of operations, administration, and maintenance information

The software should be installed on a Windows PC that will have direct access to the MCS and other system components. It can be used and left in an operating mode 24x7 for alarm-based activities, or it can be used when needed if another system will be used for network alarms. It is a common practice to have engineers who will be supporting the system use a copy of this software on a remote computer for service. The software is GUI-based, and all changes are made and stay on the MCS and not on the local client.

In the next section we start with the installation of the MCP Client, after the current Sun servers have been loaded with the current MCS software. We do not cover the loading of the Sun servers with MCS software because it is basic; all that is needed is a copy of the Software Installation PDF that comes with the system. It is a step-by-step process of what to do on each server. Before you start the installation, though, you should complete the IP addressing scheme to save many hours of problems.

Table 3.1 lists the steps for configuring the MCP Client. Then in the rest of the chapter we go over each area, screen by screen, to show what needs to be configured in each area. This table is a good overview of the steps.

Table 3.1 Configuration of MCP Client Step by Step

Step	Task
Configure the system-level elements	Add sites, servers, and service components
Configure the accounting server	In the System Management Console: (1) select the server to host the accounting module; (2) select components, add, component; (3) select the software version; (4) configure the accounting module service components name; and (5) configure the properties within the accounting module
Configure the SIP application server	In the System Management Console: (1) select the server to host the SIP application module; (2) select components, add, component; (3) select the software version to install; (4) configure the SIP application module service components name; and (5) configure the properties within all the tabs of the SIP application module
Configure the IP client manager	From the System Management Console: (1) select the server to host the IP Client Manager; (2) select components, add, component; (3) select the software version to install; (4) configure the IP Client Manager service components name; and (5) configure the properties within all the tabs of the IP Client Manager
Deploy the UFTP bundle	From the System Management Console: (1) select the server to host the UFTP bundle; (2) select components, add, basesoftware; and (3) select the software version to install

Continued

Table 3.1 continued Configuration of MCP Client Step by Step

Step	Task
Configure the provisioning server	From the System Management Console: (1) select the server to host the provisioning server; (2) select components, add, component; (3) select the software version to install; (4) configure the provisioning module service component name; (5) configure the properties within all the tabs of the provisioning module
Configure the Web client manager	From the System Management Console: (1) select the server to host the Web Client Manager; (2) select components, add, component; (3) select the software version to install; (4) configure the Web Client Manager service component name; and (5) configure the properties within all the tabs of the Web Client Manager.
Configure the RTP media portal	From the System Management Console: (1) select the server to host the RTP Media Portal; (2) select components, add, component; (3) select the software version to install; (4) configure the RTP Media Portal service component name; and (5) configure the properties within all the tabs of the RTP Media Portal

Installing MCP Client

As with most other Windows-based software packages, the installation of the MCP Client is very straightforward. It is important that you have your IP addresses in hand when starting this installation; these should have been completed and used in the installation of the MCS Sun servers. This software can be installed on multiple machines for an engineer to use while in the field or in a remote situation. Changes to the system made on each MCP stay on the MCS and do not stay on the remote client.

Table 3.2 includes a list of requirements for the PC-based computer on which the MCP Client will be installed.

Table 3.2 Requirements for Installing an MCP Client on a PC-Based Computer

Category	Minimum Requirements	Recommended Requirements
Processor	600MHz Pentium-class or equivalent processor	1.0GHz (or higher) Pentium-class or equivalent processor
Free RAM	64 MB of RAM (This requirement is in addition to the memory requirements of the operating system and other concurrent applications.)	64 MB of RAM This requirement is in addition to the memory requirements of the operating system and other concurrent applications.)
Free hard disk drive space	50 MB (If the console is installed on a drive other than drive C, then 50 MB of free space is required on that drive as well. In this case, the free 50 MB on drive C will not be used.)	50 MB (If the console is installed on a drive other than drive C, then 50 MB of free space is required on that drive as well. In this case, the free 50 MB on drive C will not be used.)
CD-ROM drive	Optional (Only required if CD is the mechanism for installing the Management Console.)	Optional (Only required if CD is the mechanism for installing the Management Console.)
Mouse	Required	Required
Video graphics card	640x480 @ 8bpp (256 colors) VGA	800x600 @ 16bpp (65,536 colors) VGA or better
Sound card	Not applicable	Not applicable

Continued

Table 3.2 continued Requirements for Installing an MCP Client on a PC-Based Computer

Category	Minimum Requirements	Recommended Requirements
Operating systems	Microsoft Windows 98(SE)/ME/2000/XP/ Microsoft Windows NT 4.x with Service Pack 5 (SP5)	Microsoft Windows 2000/XP/98(SE) Microsoft Windows NT 4.x with Service Pack 5 (SP5)
Network connectivity	56Kbps modem	10BaseT or other fast network connection (DSL, cable, LAN, etc.)
Internet browsers	Netscape Communicator 7.0 Microsoft Internet Explorer 6.0	Netscape Communicator 7.1 or greater Microsoft Internet Explorer 6.0 or greater
Cookies	Enabled	Enabled
Javascript	Enabled	Enabled

After you have made sure that the requirements have been met, you can then install the client on your computer. In the following steps, we will show the installation process for MCP Client. The client can be downloaded from the Nortel Web site or it will be given to you by your installation partner. In Figure 3.1 we start the installation process; after double-clicking on your .exe file, you will come to this first screen. Click **Next** to go to the next screen (see Figure 3.2).

In Figure 3.2 you can chose the destination folder of the MCP program you are about to install on your computer. If you wish to choose a folder other than the default, click **Browse**. After you have selected your destination folder, click **Next**. At any time, you can click **Back** if you made a mistake and need to change it, or **Cancel** to start over at another time.

As shown in Figure 3.3, you can name the program folder or use the default. It is recommended that you use the default name, MCP, unless you have to change it.

Figure 3.1 The InstallShield Wizard for MCP

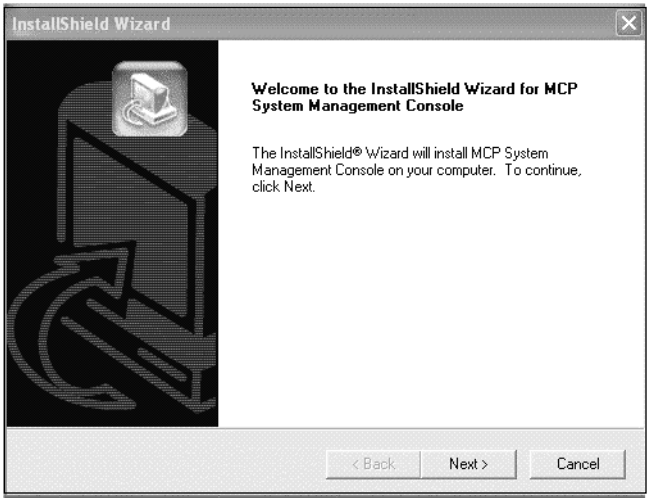


Figure 3.2 Choosing a Location for Setting Up the MCP System Management Console

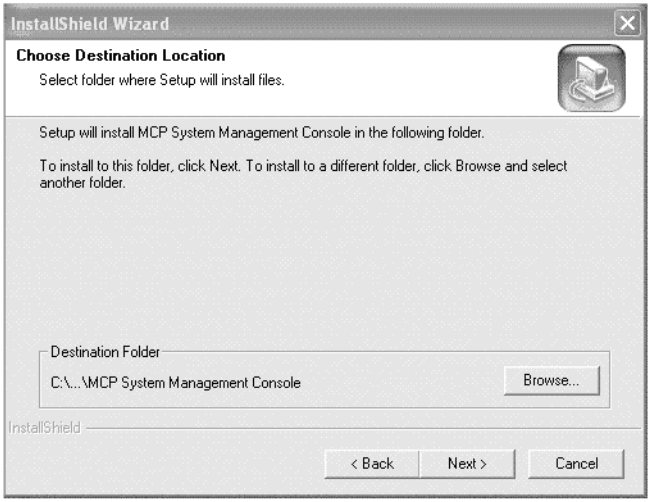
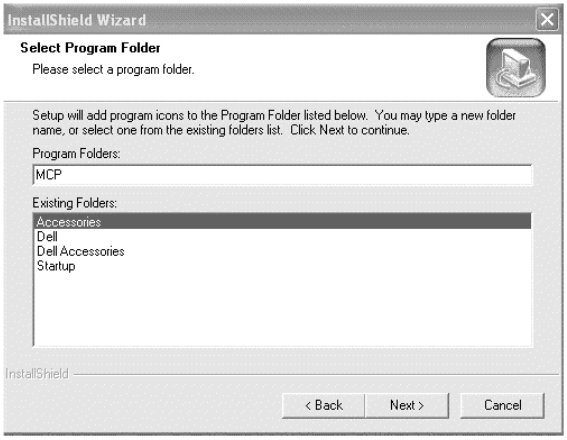
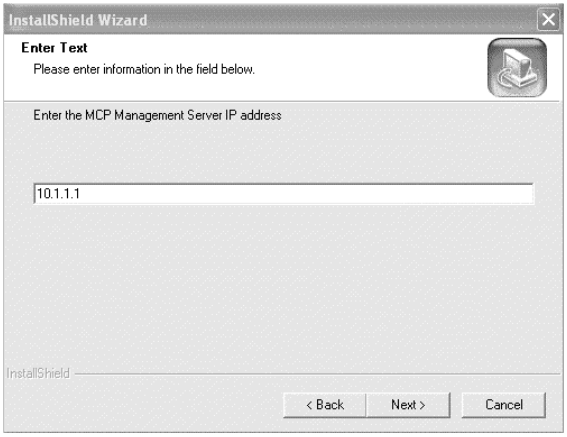


Figure 3.3 Default Name for Program Folder



In Chapter 2 we discussed the IP addressing and architecture of the MCS 5100 system, and how this information would be needed in the installation process. In Figure 3.4, you can see that you will need the IP address of the Management Server. Enter the address in the space provided and click **Next**. Remember to double-check your Management Server IP address—sometimes people get the Database and Management Server confused.

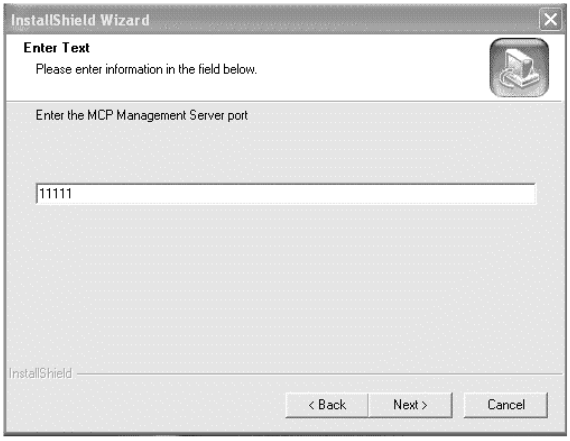
Figure 3.4 Entering the IP Address of the MCP Management Server



Returning to your installation of the MCS 5100 (more specifically, to the installation of the Nortel Software on the Sun servers), you notice that an address was entered for the service port. Refer to your Nortel Installation

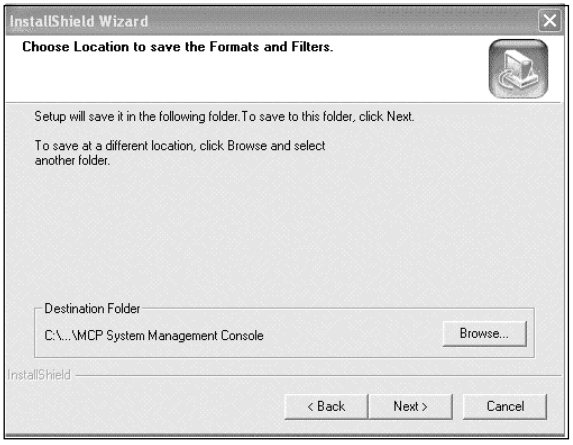
Checklist if necessary; it is a list of IP addresses, ports, and Web address used in the installation of the MCS 5100. This port in the installation documentation is set to 11111, but you can change it. Enter the correct port number and click **Next** (see Figure 3.5).

Figure 3.5 Entering the Port Number of the MCP Management Server



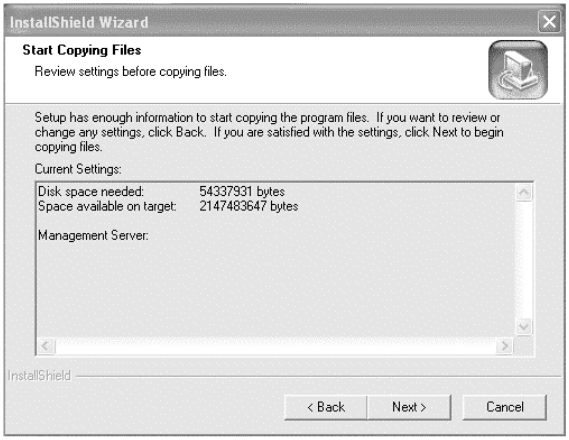
In Figure 3.6, the software will install the format and filter used with the MCP Client onto your computer. It is recommended that you leave the destination folder as the listed folder (a default folder). Changing the folder can hamper troubleshooting down the road in case you have a problem with the client and have moved the destination folder to somewhere else. After you chose a folder, click **Next**.

Figure 3.6 Installing the Format and Filter



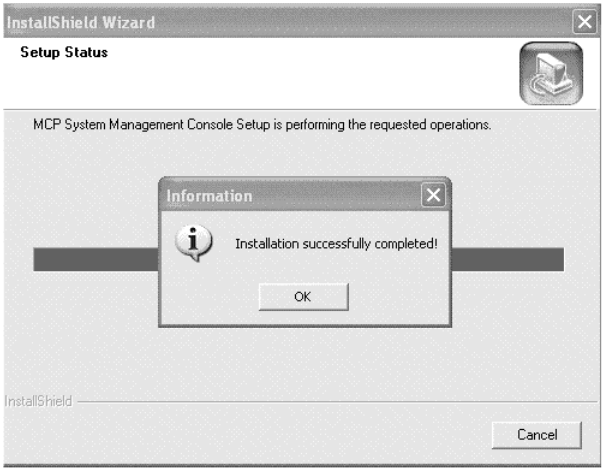
In Figure 3.7, the installation process is about to take place; the files are copied from the MCP.exe file to your designation folder on your computer. If you think you have missed anything or have a port or IP address wrong, now is the time to go back and correct those settings. If you have entered all settings correctly, Click **Next**.

Figure 3.7 Reviewing Settings



After you have selected **Next**, as shown in Figure 3.8, the program will start to install. While the program is installing, its progress is indicated by displaying a colored bar across to screen. If the program has been installed correctly it will display (see Figure 3.8). Click **OK** to end the installation program.

Figure 3.8 Installation Completed



Configuration of MCP Client

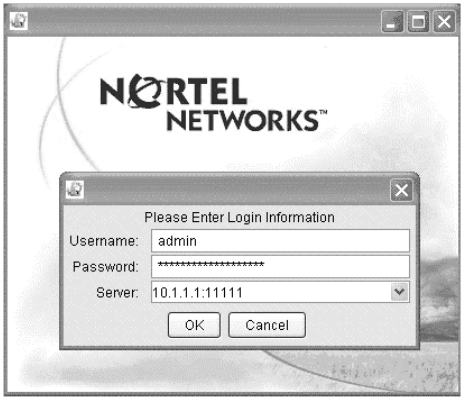
In this section we will look at the configuration of the MCP Client. Although most of the configuration settings can remain as the default, you will need the IP addressing of the MCS 5100 system as well as other addresses. These addresses could be the Signaling Server or NRS for a CS1000, a Call Pilot Voice Mail System, or any other system or end point that will be connected to this system. Remember to have your IP addresses for your Ad Hoc and Meet Me Conferencing Servers, Web Collaboration, Music on Hold, and Chat server available.

In Figure 3.9 you can see the first login screen after your successful installation of the MCP Client. The admin login and password for this account will also be the same one used for the Provisioning Client in Chapter 4. There can be three different accounts set up within the Provisioning Client for access to this MCP Client. The three account types and their roles are:

- **General Admins** General Admins have management console access allowing them to configure sites, servers, components, and services. They can monitor operations and maintenance information, and provision end-user information.
- **Database Admins** Database admins can log into the Oracle Enterprise Manager and use the management tools to perform database administration tasks. In addition, they have management console access, allowing them to perform the same tasks as general administrators.
- **System Admins** The system admins is the system superuser assigned during the initial deployment. System admins have access rights to all component modules, and are responsible for adding and defining the roles of other admins. The system administrator has access to all the tasks and tools available through the System Management Console.

If you have entered the incorrect port or IP address of the Management Server, you may correct it in the box labeled Server. After entering the correct information request, click **OK**. There are no remember me or password saves on this MCP Client.

Figure 3.9 Logging In



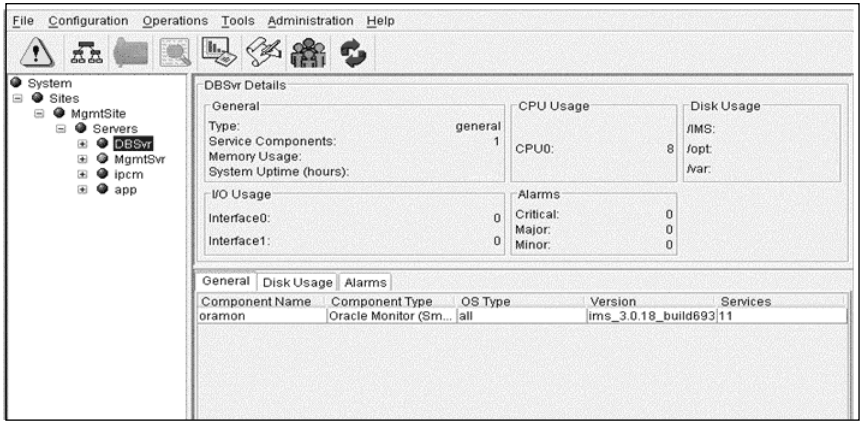
Once you have logged in to the MCP Client, you will come to a screen that will look something like the one shown in Figure 3.9. This client is working from a MCS 5100 that is in the Pluto Network Lab in France. The reason that I say this will look something like it is because the naming or objects listed could be different. But the overall look of the client window will always be the same.

Designing & Planning…

Names

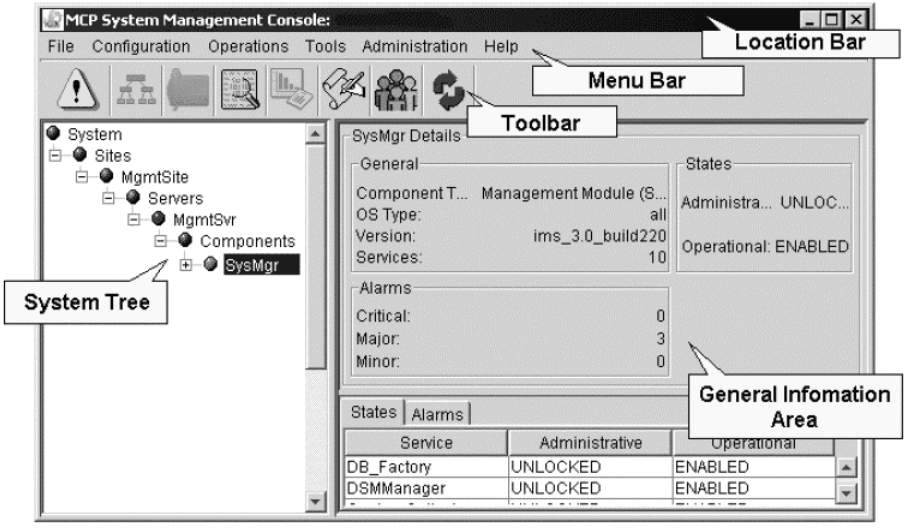
In Figure 3.10 you will see that we could have different names for our sites, servers, and components than you might have in your system. These names can be different from system to system, so please be aware of this when adding sites, server, and components to your system. It is much easier to give names to your items that make sense and will be easy to use and troubleshoot. We have installed more than a few systems and use these names in ours as a best practice along with the IP addressing scheme. Since most systems will be behind a firewall for security, the IP addressing scheme on the backend can be made easier.

Figure 3.10 Naming Sites, Servers, and Components



To understand what the main points of the screen shown in Figure 3.10 are, you need to look at Figure 3.11, which shows the layout of the MCP Client. Also listed are explanations of what the different parts of the MCP Client are used for in the MCS 5100 system.

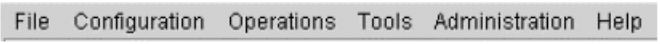
Figure 3.11 MCP Client Layout



Menu Bar

Figure 3.12 shows the Menu bar of the MCP Client. The bar allows the user to navigate through the System Management Console to other components or servers.

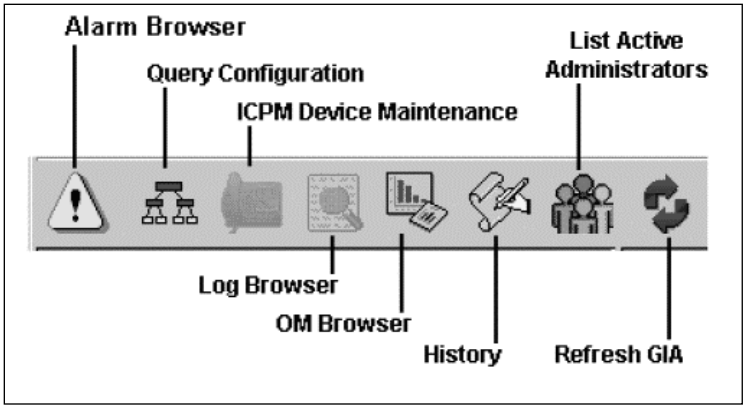
Figure 3.12 MCP Client Menu Bar



Tool Bar

The tool bar shown in Figure 3.13 is used by admins for more frequent options. It makes the configuration, troubleshooting, and optioning easier when you can just click rather than having to use the Menu bar. With this Tool bar it can be pulled away from the MCP Client and placed on the desktop by a drag-and-drop in Windows. Then it may be returned to the MCP Client using the same drag-and-drop feature.

Figure 3.13 MCP Client Tool Bar



Configuring & Implementing …

The MCP Client

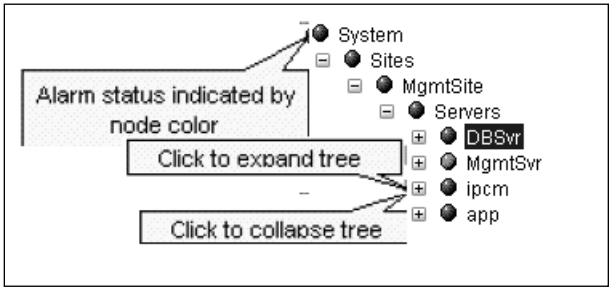
When using the MCP Client, remember that not all options are available for use by users. As you can see in Figure 3.13, the IPCM Device Maintenance has been grayed out, which means that the user logged on now does not have access to that feature. Please be aware of this option when assigning user rights to admins.

System Tree

The System tree in Figure 3.14 displays sites, servers, components, and services for the MCS 5100 System. When installed the system by default already will have the management site (MgmtSite), management server (MgmtSrv), and Management Module (SysMgr) installed and listed in the tree. As you can see by the different colors shown in Figure 3.14, these represent the following alarms for those objects in the tree:

- Green: no alarm or warning
- Yellow: minor alarm
- Orange: major alarn
- Red: critical alarm

Figure 3.14 System Tree



General Information Area

The General Information Area (GIA) of the MCP Client, shown in Figure 3.15, is different for each item you select within the tree. When an item is selected in the tree, the information will change within the GIA to accommodate the choice made in the system tree. In this section we list areas and meanings for the GIA; these can change based on the item selected in the system tree.

General

The general area includes:

- **Servers** The total number of servers on the site or sites
- **Components** The total number of components deployed on the site or sites

Highest Usage

The highest usage area includes:

- **CPU** The Site Server with the highest percentage CPU usage
- **I/O** The Site Server handling the highest number of packets
- **Memory** The Site Server using the highest percentage of memory
- **Disk** The Site Server with the highest percentage disk usage

SIP Information

The SIP information area includes:

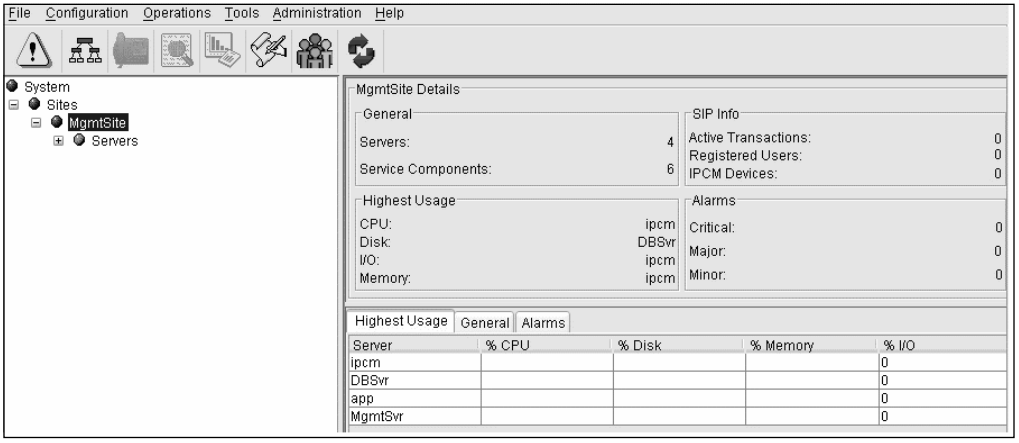
- **IPCM Devices** The number of hard clients (e.g., i2004) registered for the site
- **Active Sessions** The active number of SIP sessions across the site
- **Registered Users** The number of users registered with the site Application modules

Alarms

The alarms include:

- **Critical** The total numbers of current critical alarms generated by the site components
- **Major** The total number of current major alarms generated by the site components
- **Minor** The total number of current minor alarms generated by the site components

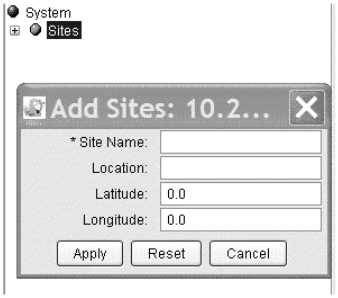
Figure 3.15 General Information Area



Adding a Site

When adding a new or additional site to the System Tree you will need to right-click the **Sites** object. Click the small **Add** button, which takes you to the screen shown in Figure 3.16. Here you can add a new Site Name, Location, Latitude, and Longitude if needed. After entering the information, click **Apply** and your site will be added.

Figure 3.16 Adding a Site



Adding a Server

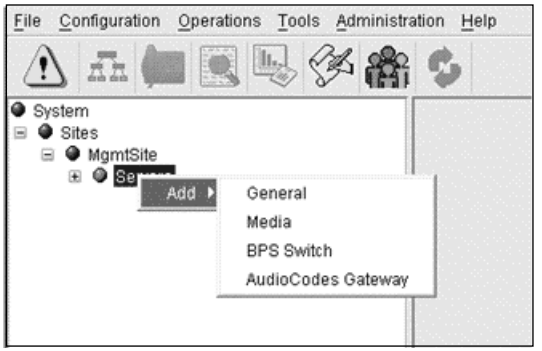
After you have added your new site, you can add a server to the site. As you can see in Figure 3.17, we added a site called MgmtSite to our system tree. Right-clicking the **MgmtSite** enables you to add a new server, one of four different types, including a general Server, Media Server, BPS Server, and an AudioCodes Gateway.

- **General server** Hosts the Database, Accounting, Management, Application modules, and RTP media portal.
- **BPS switch** Hosts the Business Policy Switch (BPS) application. A BPS server enhances the quality of service (QoS) of time-dependent network traffic.
- **AudioCodes Gateway** Hosts the MCP Trunking Gateway functionality. This is your line to the PSTN.

NOTE

You can add a Media Server in the tree, but it is not used by the MCS 5100.

Figure 3.17 Adding a Server



General Server

Figure 3.18 shows the screen to add a General Server to the tree. As you can see, some of the information is the same as when adding a site, but this can be changed. Table 3.3 lists the names and options for the fields. General Servers will run either Sun- or Linux-based systems. A General Server can host Management, Database, Accounting, Application modules, and RTP media portal.

Figure 3.18 Adding a General Server

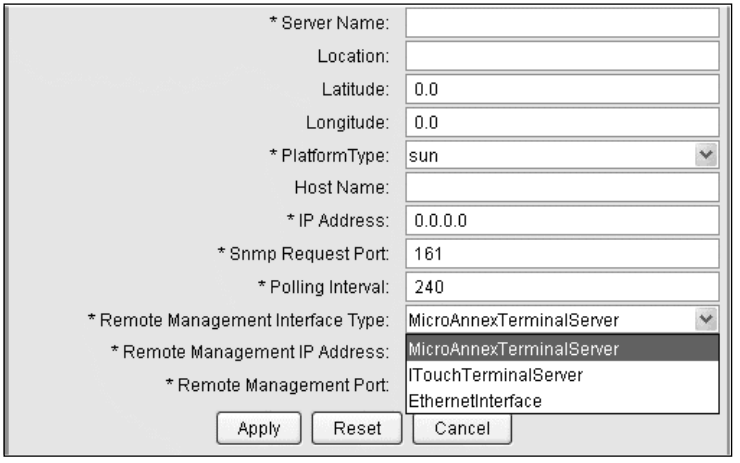


Table 3.3 Names and Options for General Server Fields

Property Field	Format (Default)	Description (Range)
Server name	Alphanumeric (n/a)	A unique name identifying the server (1–20 characters)
Location	Alphanumeric (n/a)	Geographic location of this server (1–20 characters)
Latitude	(0.0)	Geographical latitude (n/a)
Longitude	(0.0)	Geographical longitude (n/a)
Platform type	Server OS (Sun)	Indicates the type of server being added (Sun, Linux)
Host name	Alphanumeric (n/a)	Host name of the server machine. The host name of the server is configured during the installation and commissioning of the server. This field has to match exactly the host name configured on the server for LOM commands sent from the System Management Console to be allowed.
IP address	IP address (0.0.0.0)	Physical address of the server
SNMP request port	Integer (161)	Server port on which the SNMP agent is running. This is the port on the server where the SNMP daemon listens for SNMP requests (240–1800).
Remote management interface type	Dropdown menu (MicroAnnex, TerminalServer)	The type of Lights-out Management (LOM) interface (Touch TerminalServer, MicroAnnex TerminalServer, Ethernet interface). A terminal server is used for remote access.

Continued

Table 3.3 continued Names and Options for General Server Fields

Property Field	Format (Default)	Description (Range)
Remote management IP address	IP address (0.0.0.0)	IP address of remote management interface used to access this server (0.0.0.0). I BFN x.xx.x{(Blade_number0] An IP address of 0.0.0.0 tells the Management Module that no terminal server exists for this system; therefore, no attempt to connect to the terminal sever occurs.
Remote management port	Integer (0)	The LOM interface port this server is connected to [0-65536).

Configuring & Implementing …

Required Fields

When adding new servers in the MCP Client, be aware that the items marked with an asterisk are required fields in the MCP Client. These fields will need to be filled in and be unique for the adding or changing to be successful.

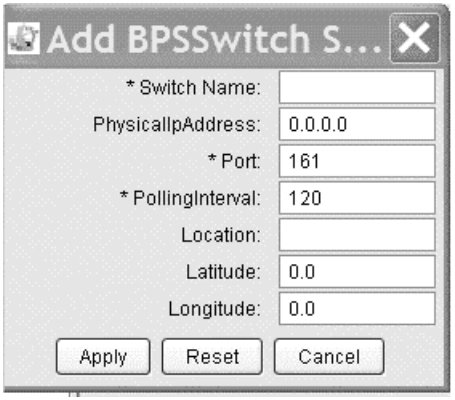
BPX Server

Table 3.4 and Figure 3.19 contain information similar to what you will find in the General Server. Figure 3.19 provides the options for the BPX Server. The BPX Server will host Business Policy Switch or BPS. The server when added will enhance the quality of the QOS on network traffic.

Table 3.4 BPX Server Options

Property field	Format [default]	Description [range]
Switch Name	Alphanumeric [n/a]	Unique name identifying the BPS switch [1-20 characters]
PhysicalIpAddress	IP address [0.0.0.0]	Physical IP address of the BPS switch
Port	integer [161]	BPS port on which the SNMP agent is running. This is the port on the switch where the SNMP listens for SNMP requests [0-65536].
PollingInterval	Integer [120]	Indicates how frequently, in seconds, the switch is polled for SNMP updates [0-60000 secs].
Location	alphanumeric [n/a]	Geographic location of this server [1-20 characters].
Latitude	[0.0]	Geographical latitude [n/a].
Longitude	[0.0]	Geographical longitude [n/a].

Figure 3.19 BPX Server



AudioCodes Gateway

Nortel uses the AudioCodes Gateway to connect to the PBX or local loop telephone system. The Mediant 2000 is the primary gateway used by AudioCodes for the MCS 5100 system. But as with any system you can use different SIP gateways for your connections to the PSTN. Just be aware that you will not be able to add them into the MCP Client—this is not saying they will not work since they will. At this time in our system we have an AudioCodes Gateway that is not added to the MCP Client but is still working to provide our connections to the PSTN.

Table 3.5 lists the fields for the AudioCodes Gateway and describes what can be put into those fields. Also, Figure 3.20 shows the fields you will see in

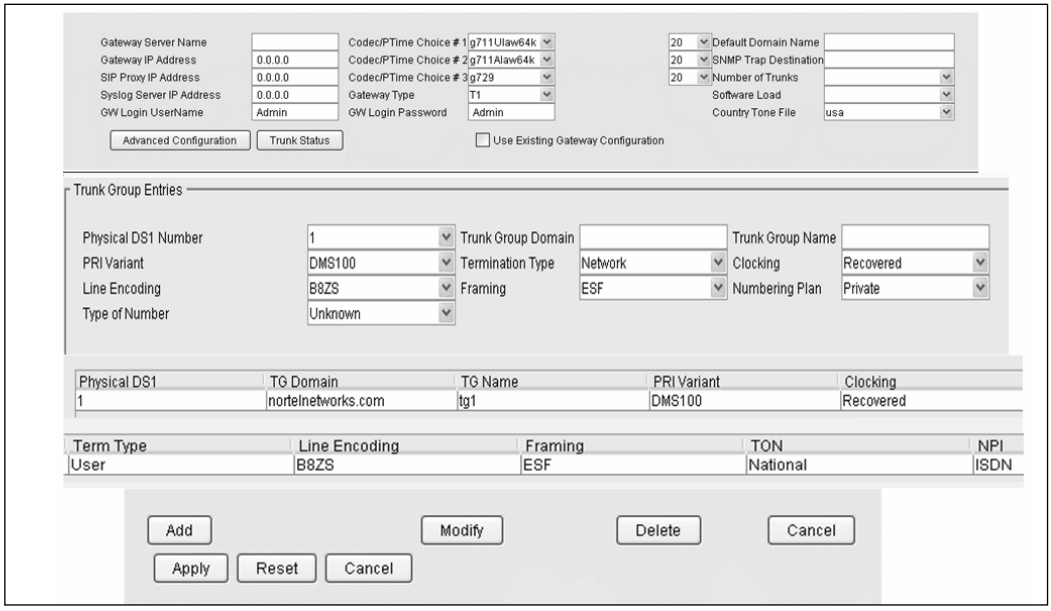
the MCP Client when adding your gateway. Once you have completed your configurations, click **Add**. Within the Trunk Groups area you can add more than one physical T1 for your system by inserting the information and clicking **Add**. It will then add that information as shown in Figure 3.21.

There are also buttons at the bottom so that you may change information or modify a physical T1 from the list above. This is done by selecting the physical T1 in the field and then clicking **Modify**. Once changes have been completed, click **Add** or **Apply** to save those changes.

Table 3.5 AudioCodes Gateway Fields

Field	Description
Gateway Server Name	The server name as it will appear in the system tree of the System Management Console.
Gateway IP Address	The IP address of the AudioCodes PRI Gateway.
SIP Proxy IP Address	The Application Server Service IP address.
Syslog Server IP Address	The Mediant 2000 uses syslogs to log its behavior. This field contains the IP address these logs are to be sent to. The Syslog messages are sent to a PC. AudioCodes is not a UNIX based platform, so the messages are not sent to the Management Module (SysMgr) like the syslog messages of the SUN servers.
Codec/Ptime Choice #1	The primary choice for codec/ptime for this gateway. Please note that a codec can only be listed once.
Codec/Ptime Choice #2	The second choice for codec/ptime for this gateway.
Codec/Ptime Choice #3	Third choice for codec/ptime for this gateway.
Gateway Type	The gateway can either be a T1 or E1 configuration.
GW Login UserName	The username for the account allowed to log in through the AudioCodes Web Interface.
GW Login Password	The password for the account allowed to log in through the AudioCodes Web Interface
Default Domain Name	The domain which calls originating from the gateway will use to originate call to the Application Server.
SNMP Trap Destination	Enter the IP address of the Management Server.
Number of Trunks	The Mediant 2k gateways come in 1,2,4, or 8 port logical gateways. This field should contain the actual number of ports available on the gateway.
Software load	The load to be sent to the AudioCodes PRI Gateway once the configuration is complete.
Country Tones File	The country specific tones file used for Call Progress Tones on the gateway.
Use Existing Gateway Configuration	Selecting this causes the Management server to override the fields being set here to the existing configuration set on the gateway.
Advanced Configuration	Clicking on this button launches the AudioCodes Web Configuration screen.
Trunk Status	Clicking this launches the AudioCodes Channel Status Screen which displays the current state of the Gateway's trunks.
Physical DS1 Number	The port (starting with 1) which the trunk is connected to on the gateway.

Figure 3.20 AudioCodes Gateway



Options within the System Tree

While you are within the system tree you may make changes to different components of the system tree under your sites. As you can see in Figure 3.21, in the system tree we have highlighted the DBsur. Now we can make changes to different servers or components within the tree. So if you right-click a server a menu will pop up as shown in Figure 3.21. These menus are not all the same for each server; most are different and it depends on the server. This gives you an understanding of what you can do within the MCP Client to make changes to a server or component. Also be aware that you do not need to lock the server to make changes; only the component must be locked for changes to be made.

The commands or options shown are different for the server and components in the system tree (see Figure 3.22). The servers can be powered on and off from the system tree, as long as you have access to the tree. You may also reset the server and modify the SNMP string of the server for alarms.

Figure 3.21 System Tree Pop-Up Menu

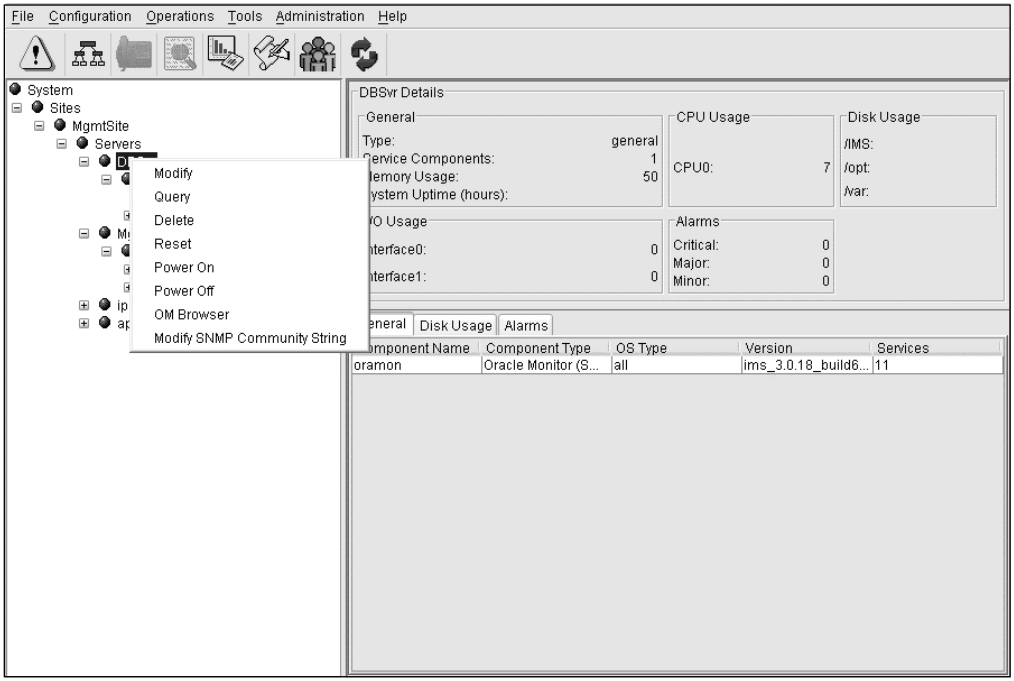
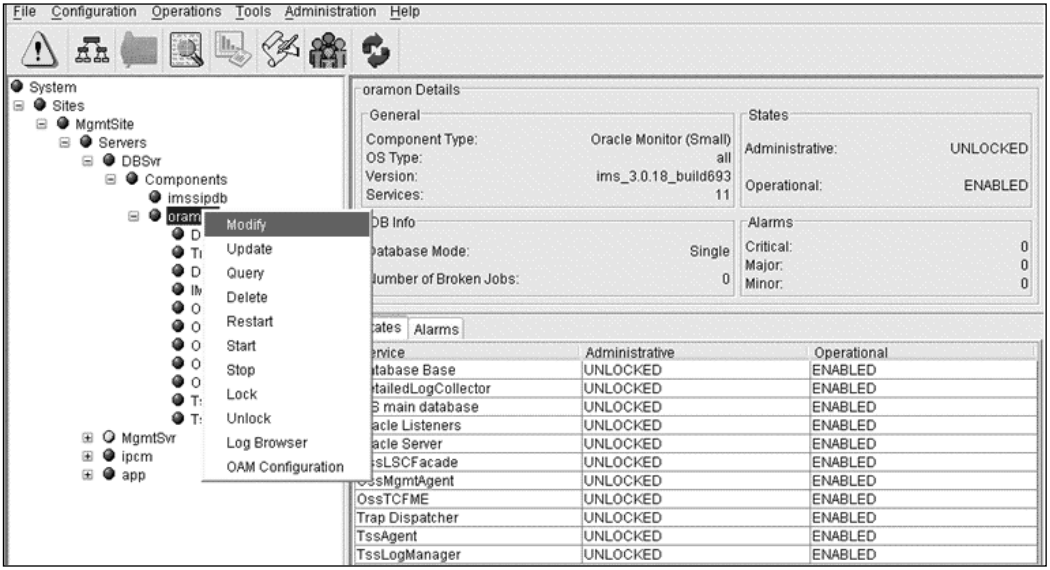
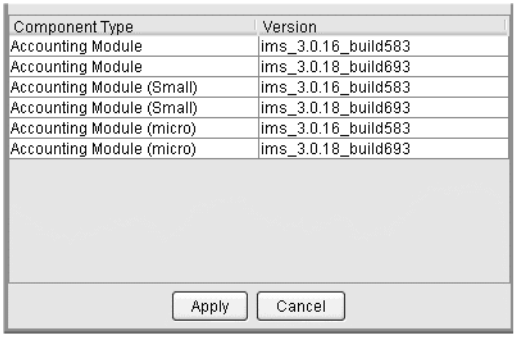


Figure 3.22 System Tree Options



Since this is the first time we have looked at this we will make sure you understand what the options in Figure 3.22 mean. The modify, query, and delete options really need instructions. But the update options will allow you to update the server or component you are working on at that time. As seen in Figure 3.23, it will provide a list of components and a load list of software that may be chosen for that server. These are broken out by component type and version for you to choose. The start and stop options are in no need of explanation at this time other than to say it will enforce the command on whatever component you chose.

Figure 3.23 Component List



When you are adding a component under a server, refer to Table 3.6, which provides information that will be needed for your choice. You must select the right component base for the system you have in hand. These systems can range from large to small, and if the wrong component is chosen to be added to the wrong server, it could cause problems on the system.

Table 3.6 Selecting a Component

Component	2 x V100	4 x V100	8 x V100
Accounting Module	micro	small shared	small
IP Client Manager	micro	small shared	small shared
Oracle Monitor	micro	small	small
Provisioning Module	micro	small shared	small shared
SIP Application Module	micro	small shared	small
Web Client Manager	micro	small shared	small shared
iPlanet Monitor	micro	small shared	small

Configuring & Implementing…

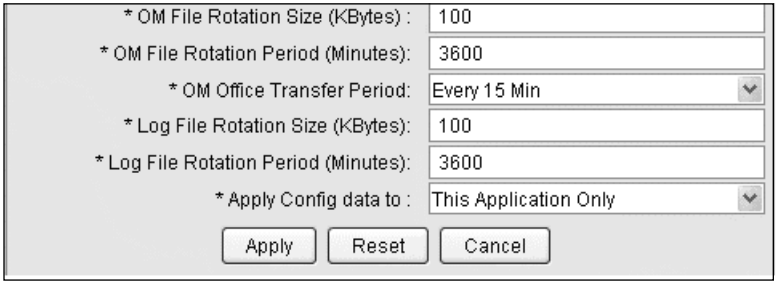
Making Changes

When selecting the restart, stop, stop, modify, delete, unlock, lock, or update options listed in Figure 3.22, be sure to notice if you are making changes on a server or component. If changes are made to a component it will have effect on a server.

When changes need to be made the system must be locked into place for this to happen. Choose the lock option from the list, but be aware that when you lock a component it can halt the server. This means service will stop and the customer will go down. The system will warn you that this could impact service. Sometimes it is best to do this after hours or when there is downtime on the system. When changes have been completed you must unlock the system to bring it back up to normal operational status.

The log browser option will bring up a window for logs, leave the window up, and provide logs for the server or component you have chosen. Also you may select OAM Configuration in the options listed in Figure 3.22. Figure 3.24 is a sample of what you might see when selecting this option. You may change these options while locking the component.

Figure 3.24 OAM Configuration Option



Designing & Planning…

Lock Operation

Following is a list of what will happen to each component as a result of the lock operation performed earlier. Be aware of the results in your planning sessions so that you will not unwillingly drop users or the system.

- **SIP Application Module** If the system is in a warm standby arrangement with the application server nothing will happen; if not, then the component in the module will be affected until the system is put back into an unlocked state.
- **Management Module** Cannot lock the module
- **Database Module** Cannot lock the module
- **Oracle Monitor** Not service impacting
- **IPlanet Monitor** Not service impacting
- **Provisioning Module** Not service impacting
- **RTP Media Module** Although you can lock the module and it is service-affecting, it is recommended that the module be shutdown to get it into a lock administrative state.
- **IP Client Manager** Locking this service will impact the module; however it can be modified in the tab fields.

Component Configuration

There are many different components that can be added to a server within the MCP Client. Even though we do not cover all of them in this book, we will cover the most important once that you will use. We will go through each server under our site here at Pluto Network and Nortel to show you the options and fields that can be modified under each component. In the following screen shots you will see some screens that are grayed out and some that are not. If they are grayed out that means the system is up and unlocked. If they are not that means the system is being halted and could be down.

Database Server—Oracle (Oramon)

Our first component we will look at is under the Database Server and is called the Oramon. This component is used for the Oracle Server and Database on the MCS 5100 system. In Figures 3.25 through 3.29 you can see the options that you can chose from. The items with an asterisk are important and are mandatory when configuring your component. When configuring the component you may place your mouse over the item to provide more information about the item, such as more of a description and the range allowed for the value needed.

The settings that you see in the figures are really default settings that we used in our setup. Except for the IP addresses, hostname, and SNMP agent these settings can be used for a new setup.

Figure 3.25 Oracle Server Option

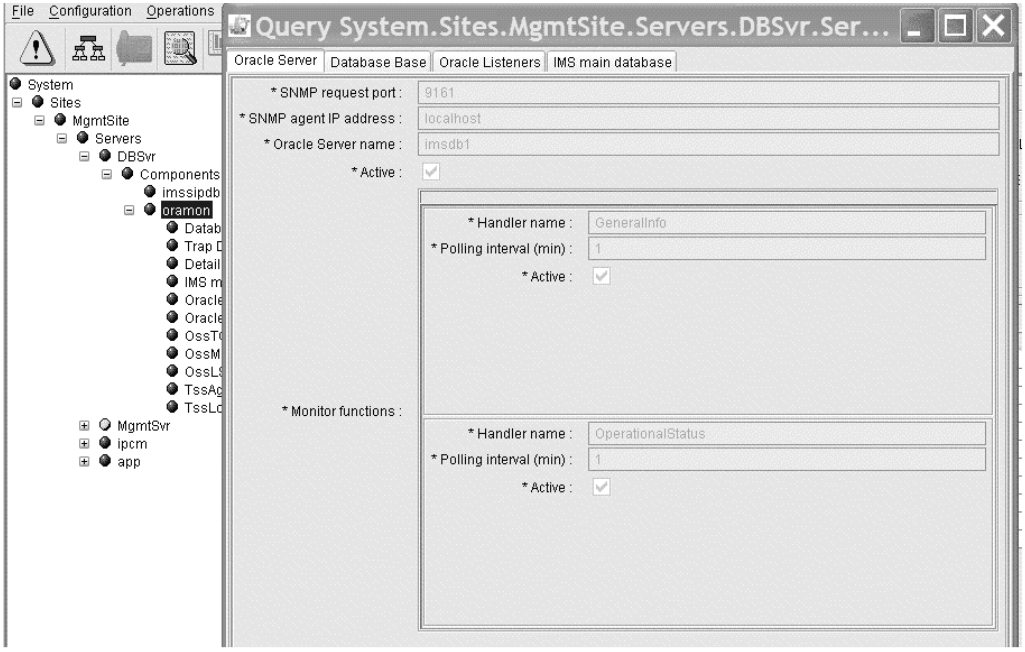


Figure 3.26 Database Base Option

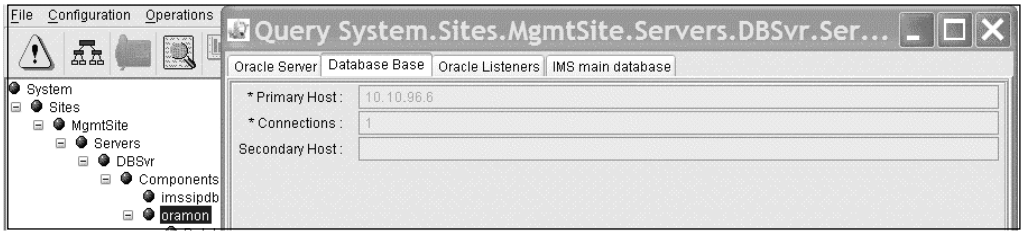


Figure 3.27 Oracle Listeners Option

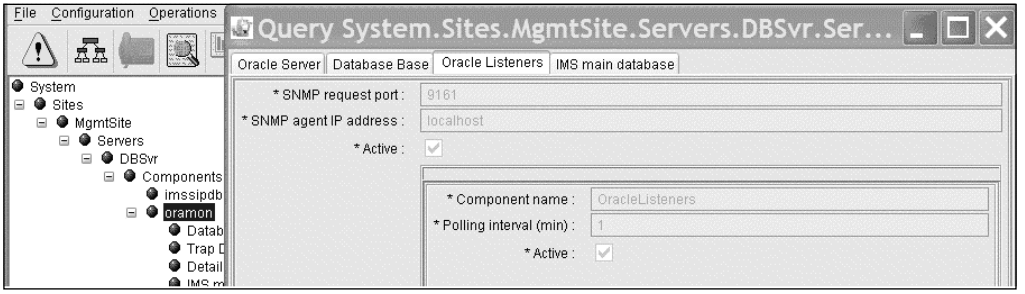
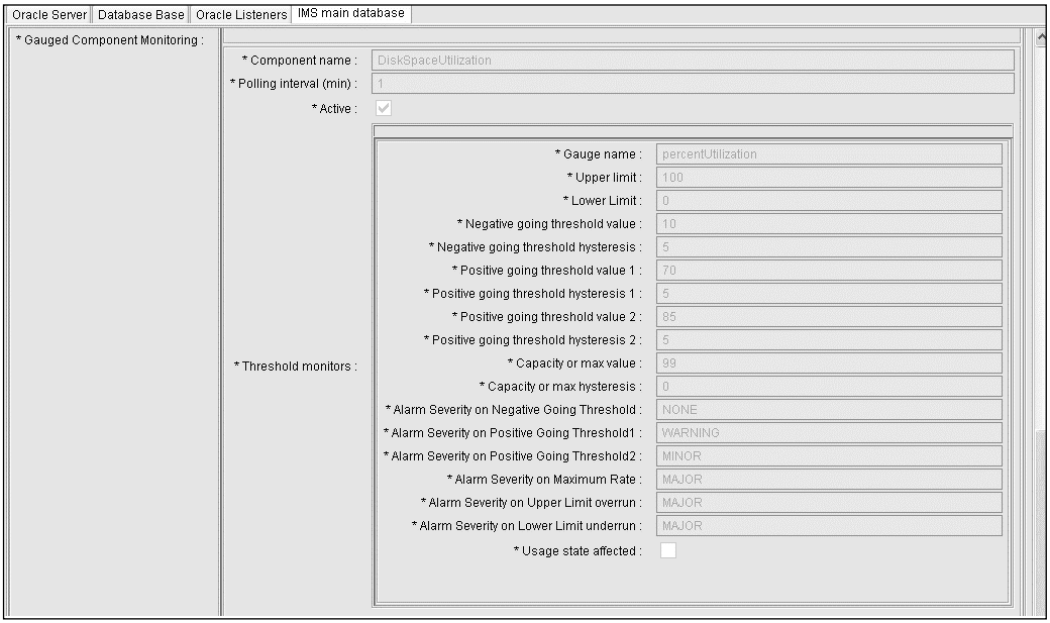


Figure 3.28 IMS Main Database Option

Figure 3.29 Gauged Component Option



Management Server—Central Account Manager (Acctg)

Next we are going to look under the MgmtSvr at the acctg component in Figure 3.30. As you can see on the right in the States information box, it shows the service that is associated with the acctg component. When a server or component is select in the tree it will show this type of information in the window. In Figure 3.31 a query was selected for the Central Accounting Manager; make sure that your IP address that is entered for the CAM IP address is the Machine Logical IP address of the Management Server.

Management Server—System Manager (SysMgr)

The next component under the Management Server that will be covered is the System Manager. As seen in Figure 3.32, there are many services under the component. There are only two that can be changed and we will show those in this section. The only options that may be modified within the System Manager are shown in Figure 3.33. The values shown in Figure 3.33 are default for this component; however you may move your mouse over the entry to provide a value range.

Figure 3.30 Acctg Component

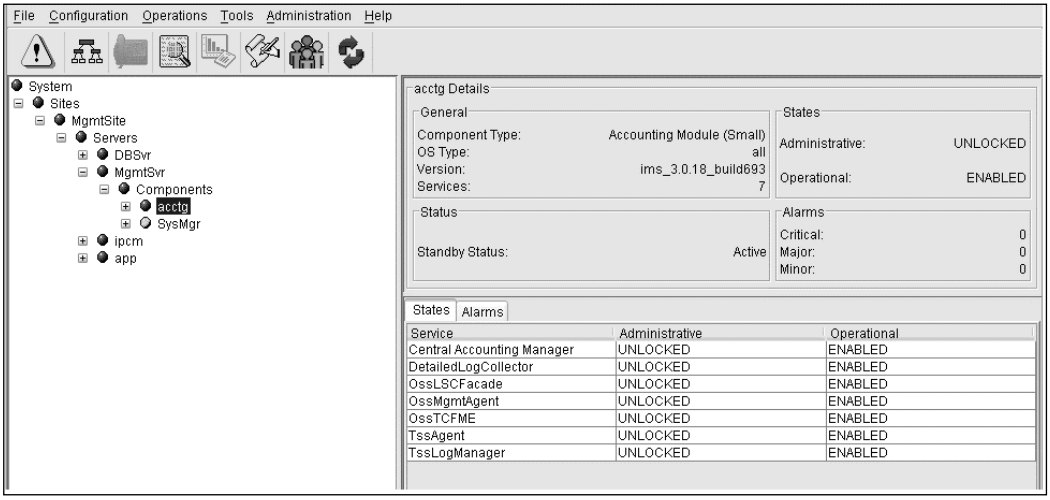


Figure 3.31 Acctg Query

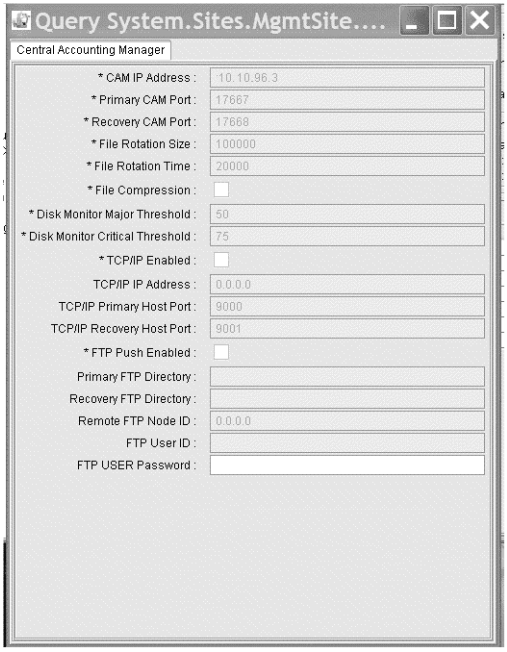


Figure 3.32 System Manager Services

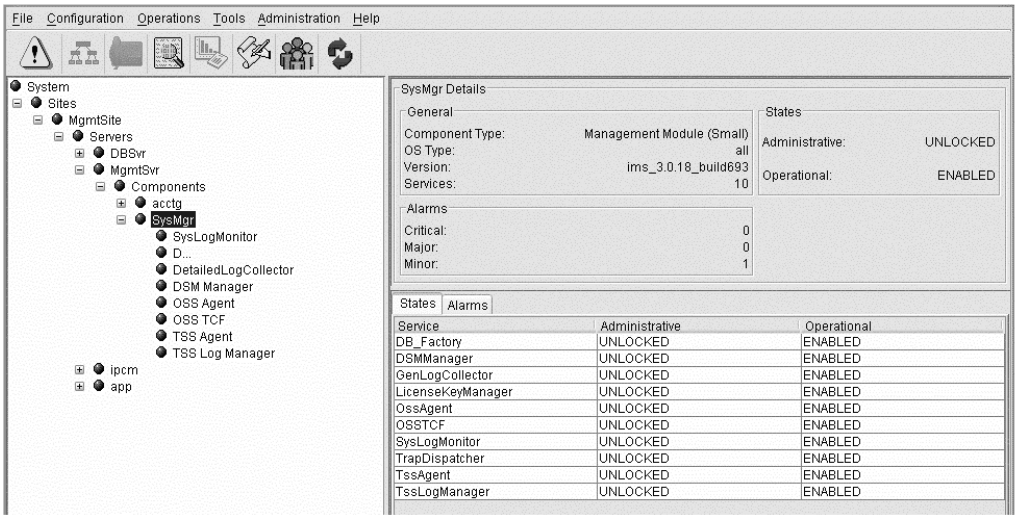
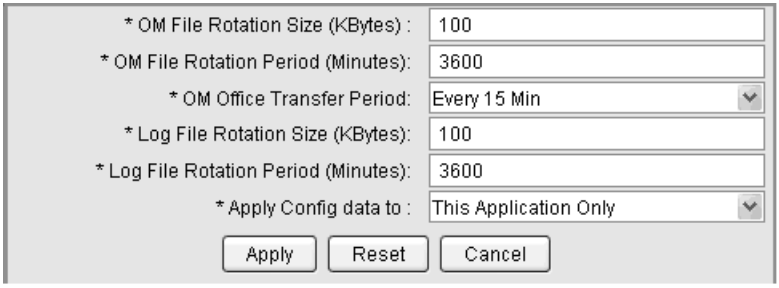


Figure 3.33 Default Values for SysMgr



The next two figures show the only two services that can be modified under the SysMgr Component. SysLogMonitor (shown in Figure 3.34) has only two fields, and both fields need to be completed. The next service is the DB Factory (shown in Figure 3.35); you will need to input the IP address of the Database Server as well as the amount of connections coming in to the server. If there is a secondary Database Server, that IP address can be entered at the bottom. Even though it has an asterisk as a mandatory field, it is only mandatory if there is a secondary server.

Figure 3.34 SysLogMonitor Service

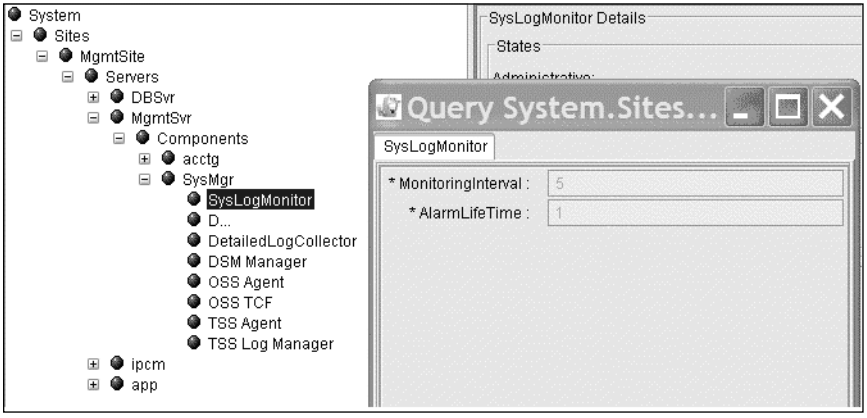
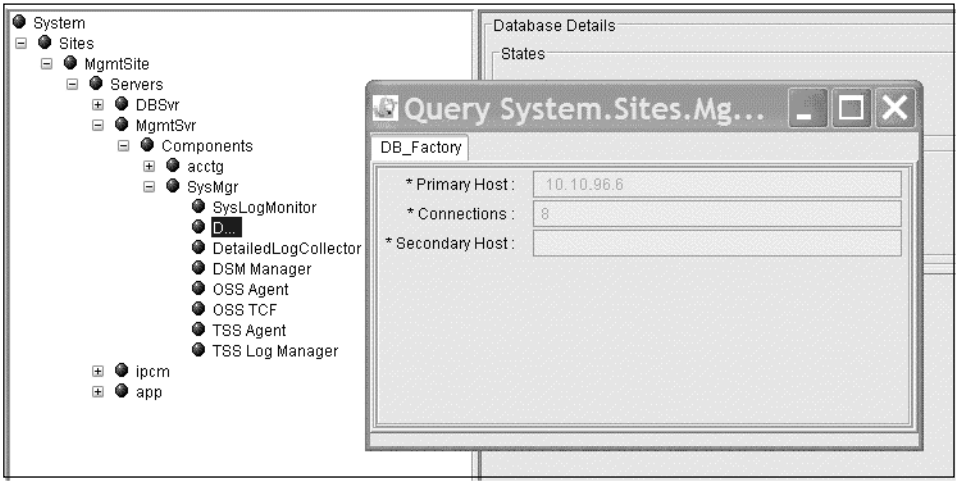


Figure 3.35 DB Factory Service



NOTE

During configuration if an item is highlighted and right-clicked, it might produce a menu. As seen in Figure 3.35, only two services can be modified by a menu. Be aware of this when configuring your system; it will save you time in troubleshooting a problem that does not exist.

IPCM Server—Provisioning (Prov)

The IPCM Server is the next area we will be looking at; as seen in Figure 3.36, there are a few components under the IPCM. As in the last server and as seen in Figure 3.37, these are the only changes that can be made to the IPCM. You must add the IP Address of the IPCM, name, remote IP Address, and remote management interface. This will more than likely be the iTouch Server since it is bundled in with the MCS 510 Package from Nortel.

Figure 3.36 IPCM Server

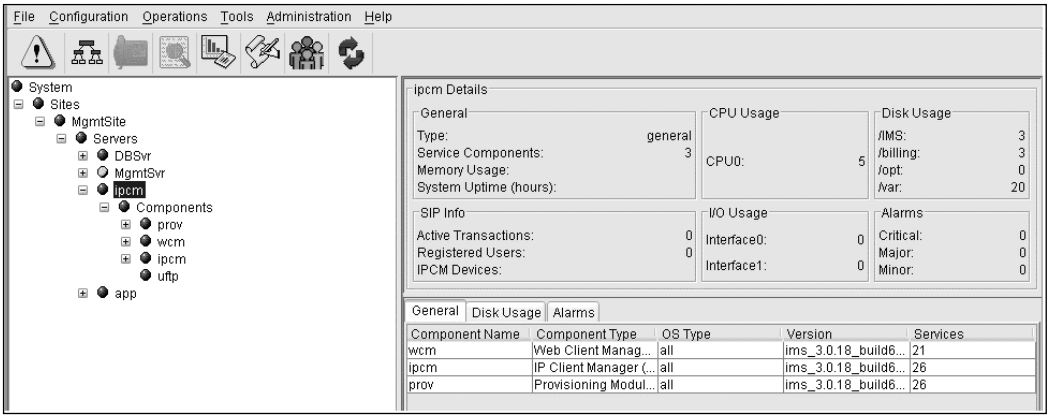
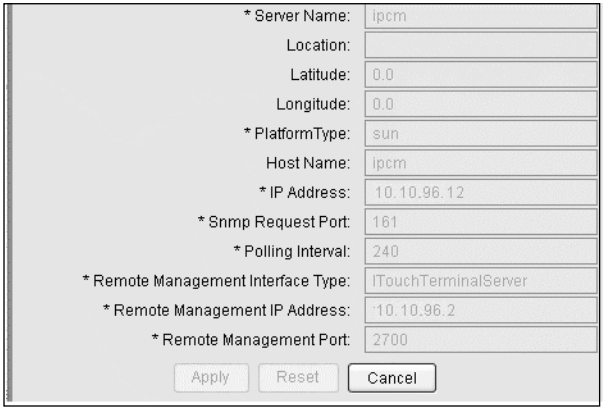


Figure 3.37 IPCM Server Options



The Provisioning component under the IPCM has many services that will need to be configured for the IPCM to work properly. After you highlight the provisioning component within the system tree, right-click and select

Modify to see a menu like the one in Figure 3.38. The items you see will not be grayed out like ours, since we did ours in query mode to get the menu, so we didn't have to stop or lock or system while users were working on it.

There are seven tabs we will show within the provisioning component; the first tab (in Figure 3.38) is the User Agent Server, and each of the fields listed need to be completed. Even though you are working on the IPCM it is asking for the Application Server Host IP address and the Applications Server Port. Since the system uses SIP, the port that will be used is 5060, which is the default port used for SIP. The Click to call Cancel Delay is a default setting, but can be changed. Just highlight the field with your mouse and the system will show the values allowed.

Figure 3.38 User Agent Server Tab

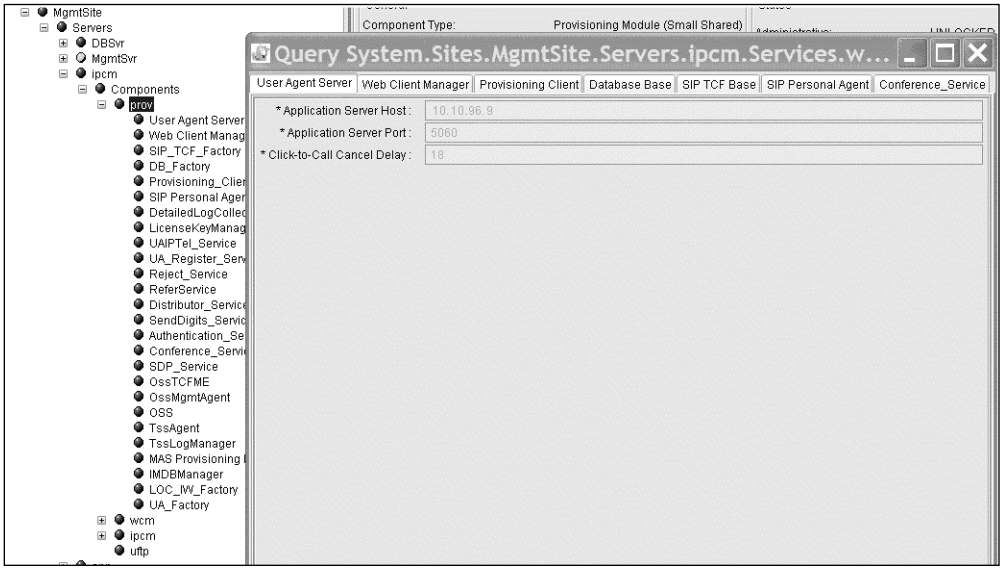
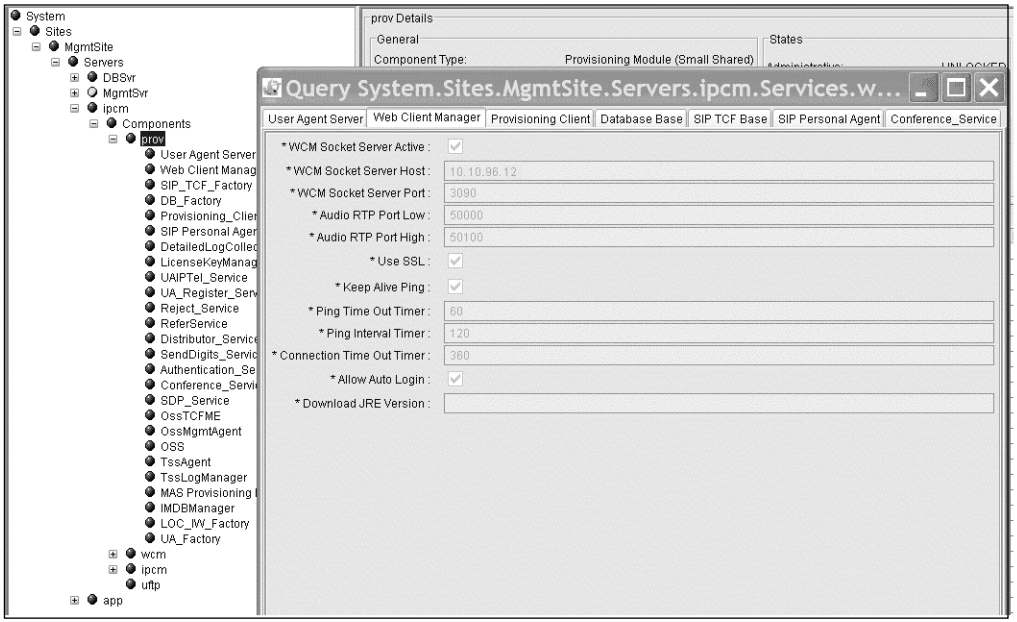


Figure 3.39 shows the Web Client Manager, and as you can see, the box for the WCM Socket Server Active is checked. Remember to check this box; if this is not done, even though you make changes to the tab, they will not work. The WCM Socket Server Host is the IP address of the IPCM Server on your system. Make sure the other three boxes for Use SSL, Keep Alive Pings, and Allow Auto Login are all checked. The other settings can be left at default or changed.

Figure 3.39 Web Client Manager Tab



The next two services or tabs that need to be configured are shown in Figures 3.40 and 3.41. These are for the Provisioning Client and Database Client. In Figure 3.40, the provisioning host is set to the IPCM Server IP address, and the other values may be used at default or changed. The Database Client in Figure 3.41 should have the Primary Host IP address set to the Database Server IP address. The connections will need to be set and we have added a Secondary Host IP address; this is a little-known secret that if the Primary connection fails for some reason it will go to a secondary.

Even if the secondary is the same host IP address as the primary it will reconnect by default looking for a secondary before reconnecting the primary. So if you put the same IP address in here, it could save you down the road in case of a problem. This was tested with our system, Pluto Network, and it worked better and faster with the secondary IP address the same as the primary. If you have a secondary server; that is better, and that can be added.

Figure 3.40 Provisioning Host Set to IPCM Server IP Address

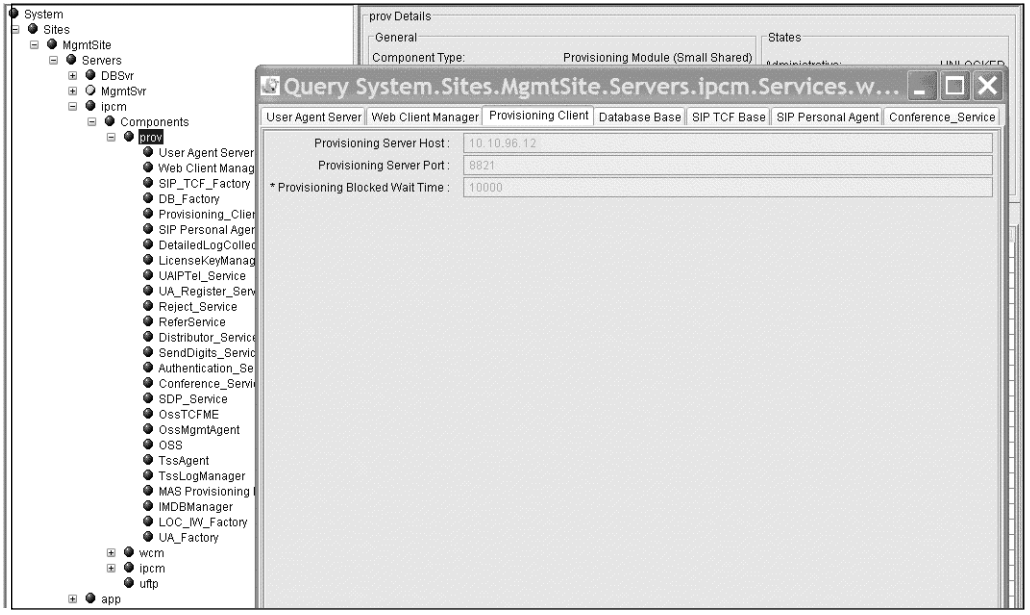
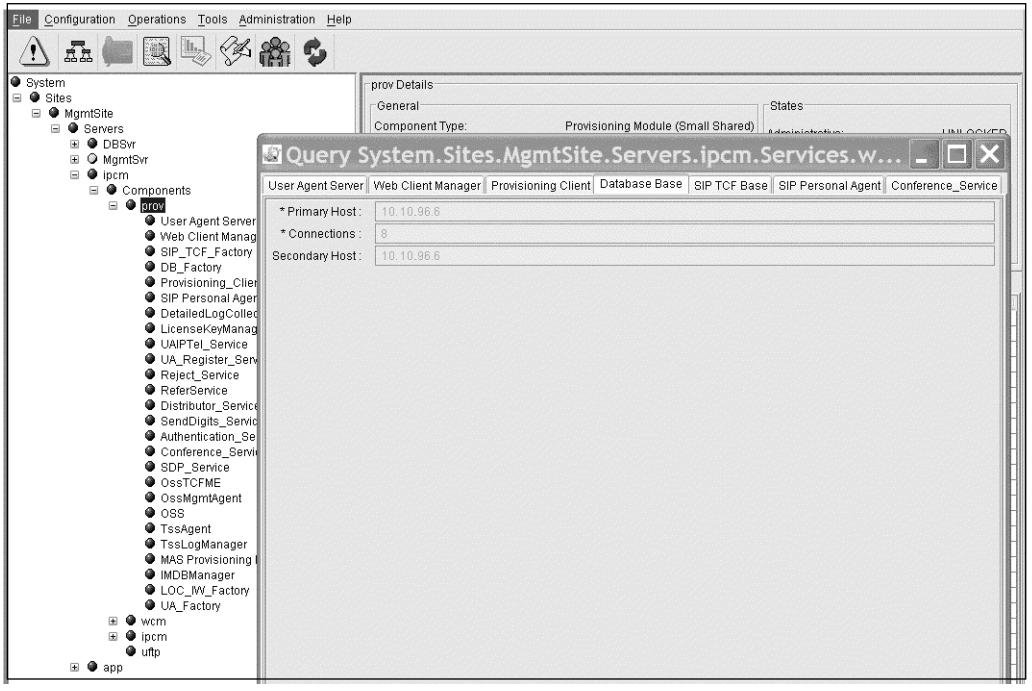
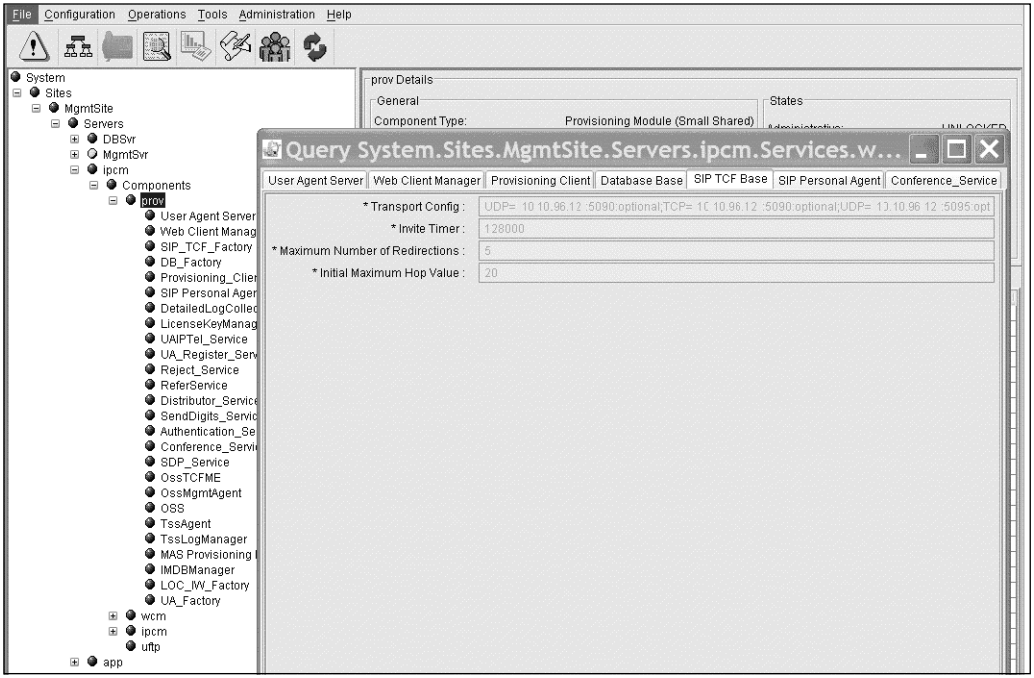


Figure 3.41 Primary Host IP Address Set to the Database Server IP Address



The next three services or tabs we will look at are shown in Figures 3.42 through 3.44. Figure 3.42 shows the SIP TCF Base. As you can see, this is a string for configuration transport of SIP TCF. This could be different for each system and the user's preference. But as you can see in the figure, in the tab we use UDP and TCP within the string on the same IP address of the IPCM and the same port. These ports change in the string with different ports further on, but it is recommended that you use both UDP and TCP in the string.

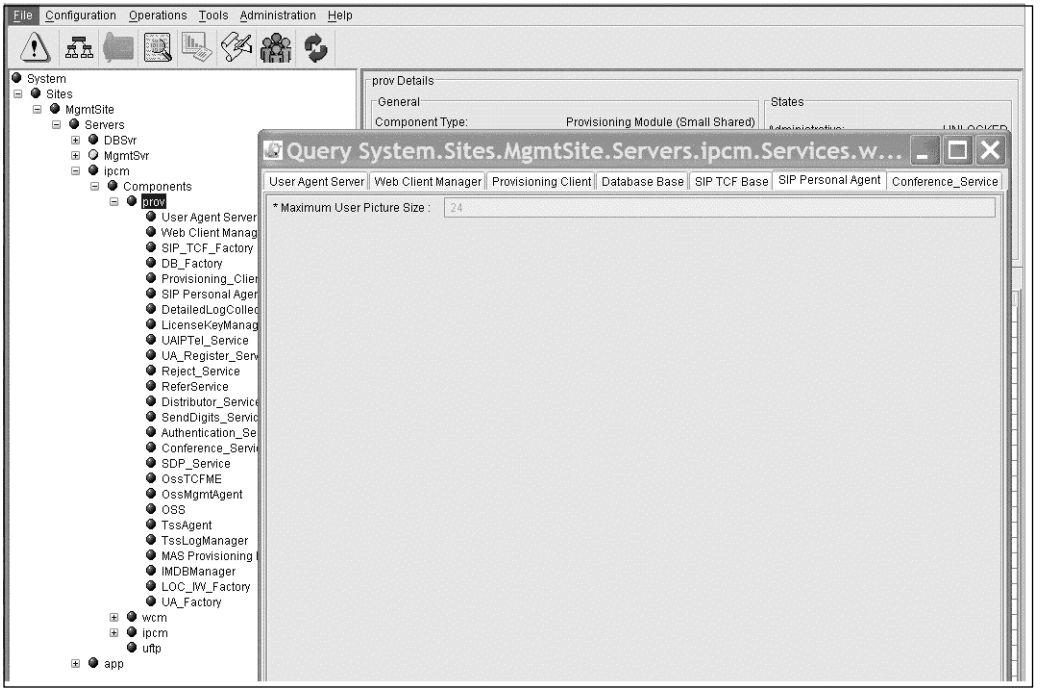
Figure 3.42 SIP TCF Base Tab



As shown in Figure 3.43, the SIP Personal Agent service or tab allows the user to change the size allowed for user picture within the Personal Agent. We will discuss the personal agent in a later chapter. You may set this to the default or to what you see in the figure for now. After using the Personal Agent you may come back and change this to suit your needs. Figure 3.44 shows just one value needed and that is for the conferencing service URL. The Conferencing Service used by the MCS 5100 is called Meet Me

Conferencing. In the value shown we use the protocol, which is SIP and just a simple name.

Figure 3.43 SIP Personal Agent Tab



IPCM Server—Web Client Manager (WCM)

The next component that will be covered under the IPCM Server is the Web Client Manager. This component has five different services that can be configured. These settings are the same as discussed in the Provisioning Component listed earlier. Since the settings used are the same we will just show the settings in Figures 3.45 through 3.49. Please refer to the earlier discussion for settings needed.

Figure 3.44 Enter Conferencing Service Value

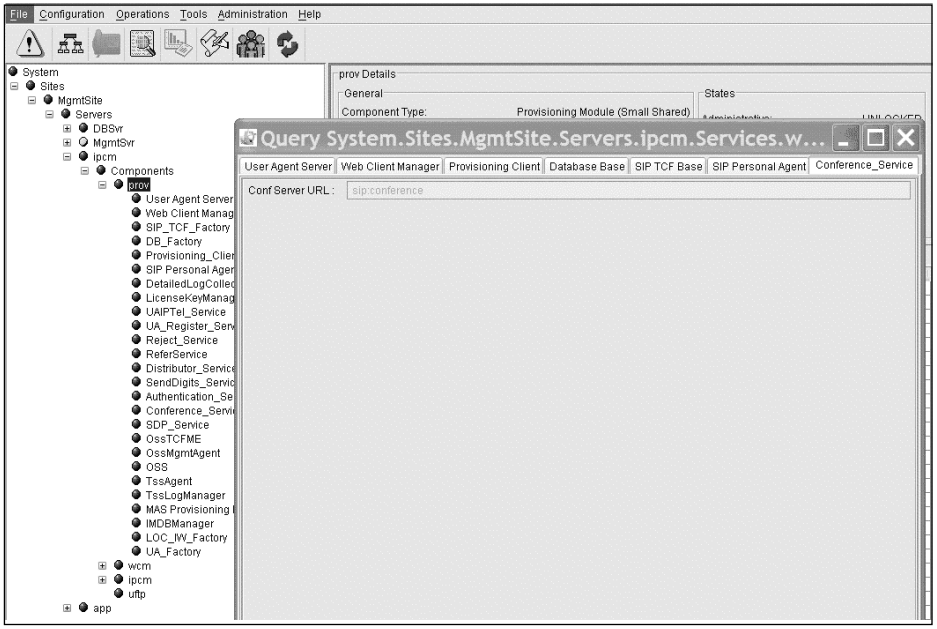


Figure 3.45 WCM User Agent Server Tab

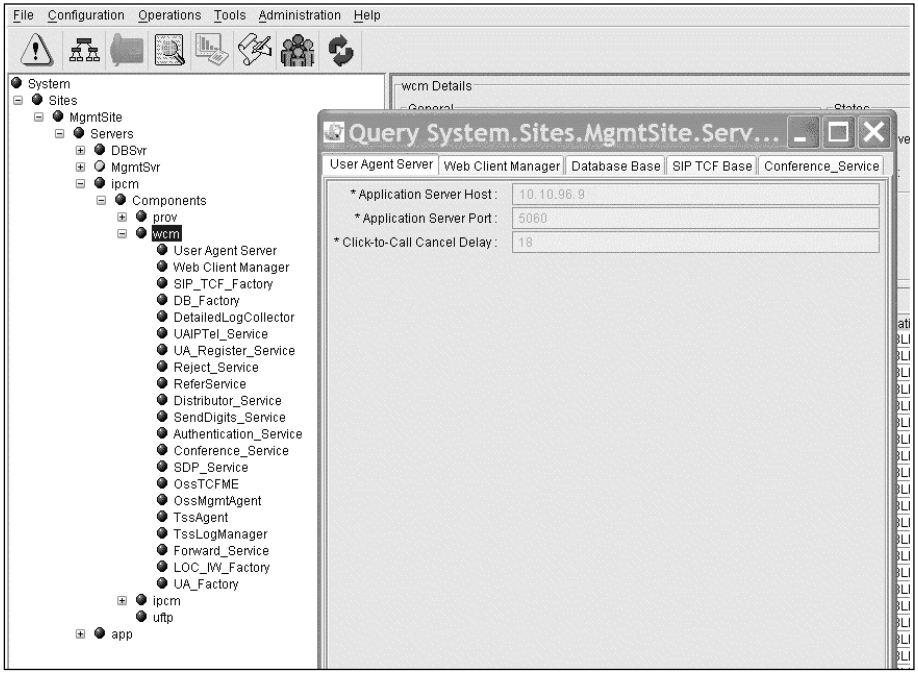


Figure 3.46 WCM Web Client Manager Tab

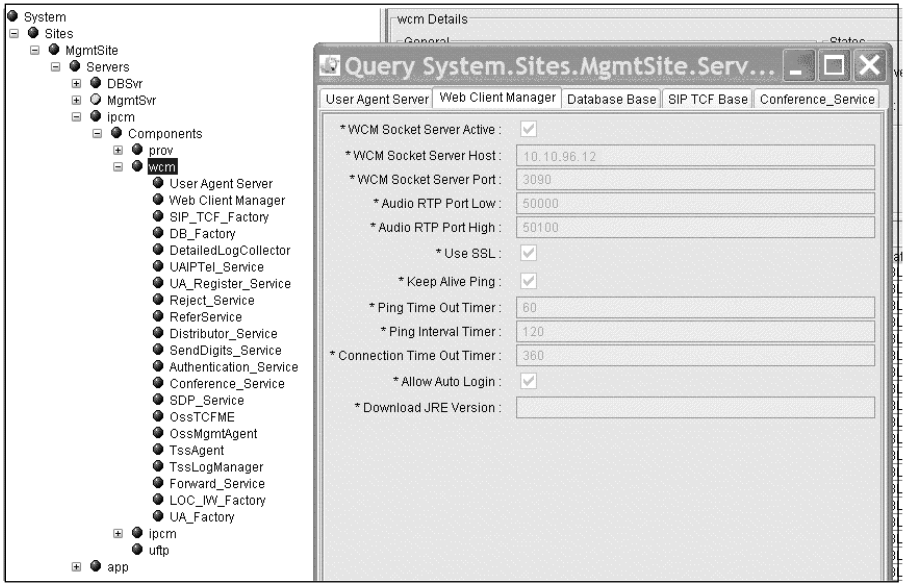


Figure 3.47 WCM Database Base Tab

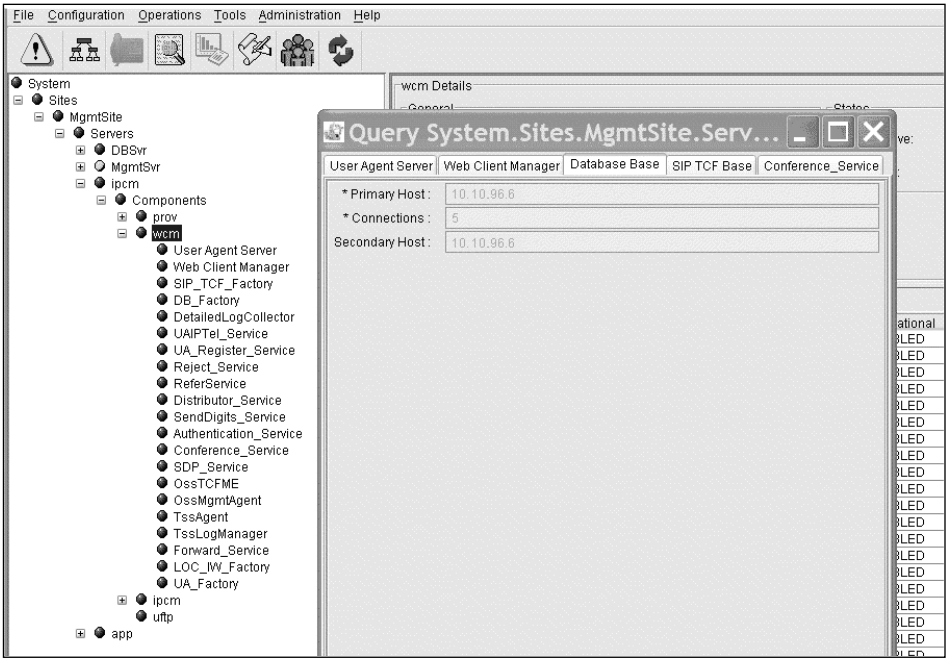


Figure 3.48 WCM SIP TCF Base Tab

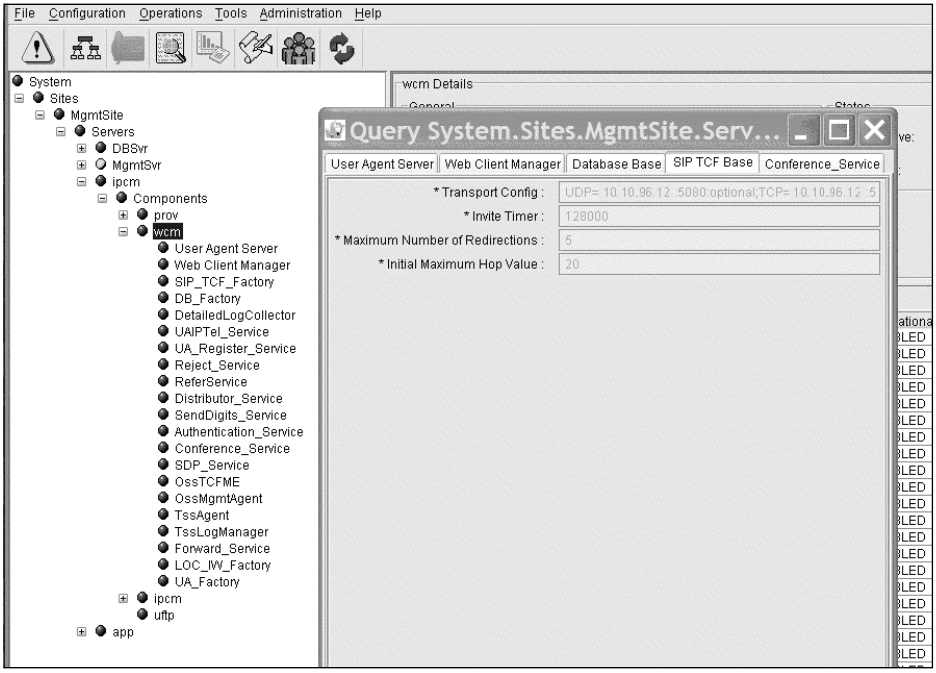
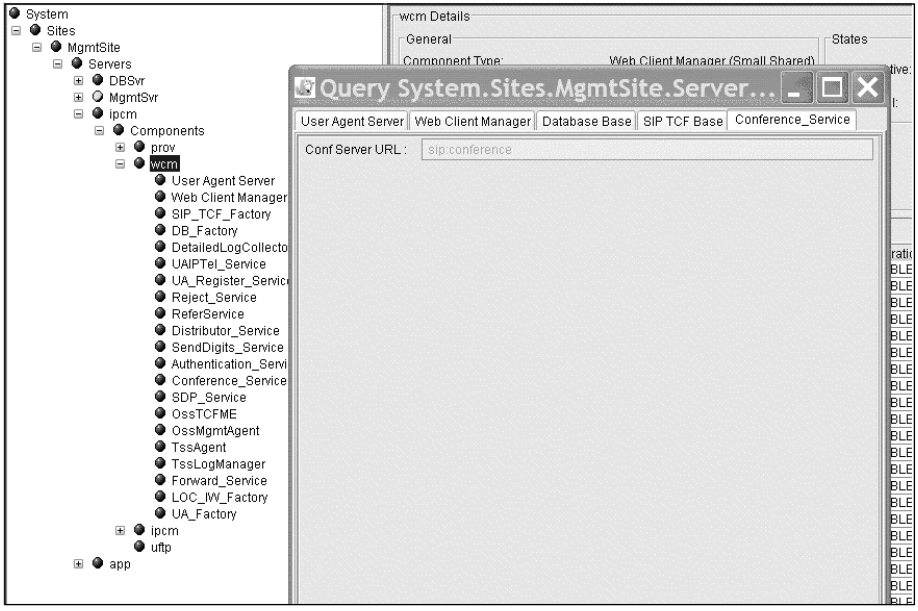


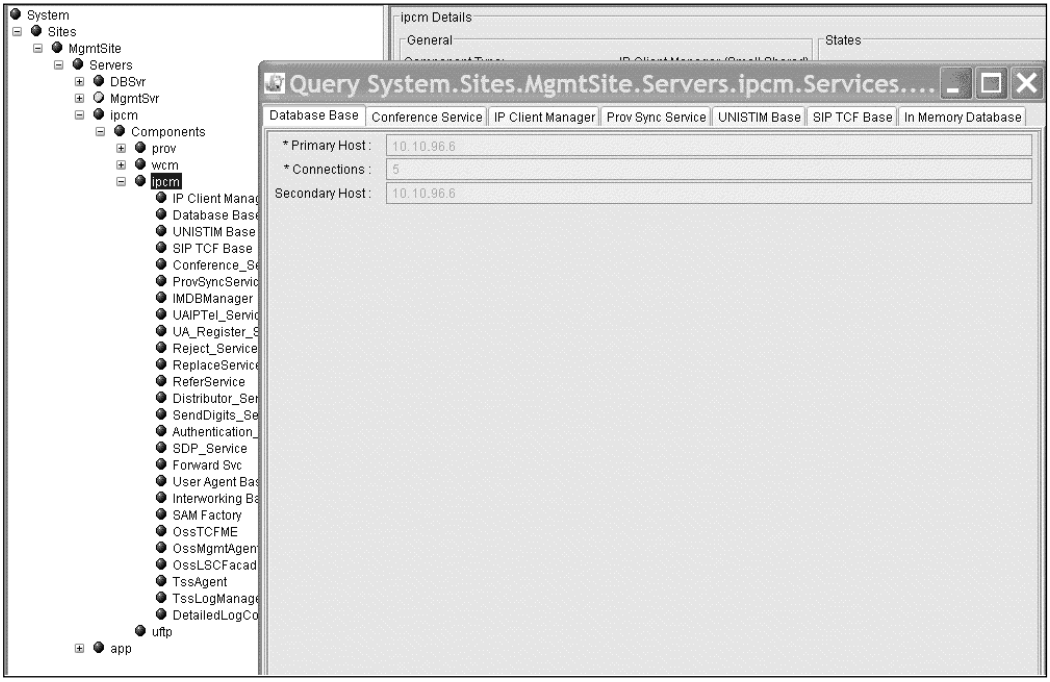
Figure 3.49 WCM Conference_Service Tab



IPCM Server—IPCM

Under the IPCM Server there is an IPCM component that will need to be configured. Some of the settings that you will see in this component are the same settings you have seen before but there are a few new tabs to be configured, for a total of seven, shown in Figures 3.50 through 3.55. The first service, shown in Figure 3.50, is the database base. Input the IP address of the database server, then the number of connections. As shown before we have added a secondary IP address, which is the same as the Primary IP address of the Database Server.

Figure 3.50 IPCM Server Database Base Tab



As shown in Figure 3.51, enter the same information as done before for the Conferencing Server. The IP Client Manager Service or tab shown in Figure 3.52 will be configured next. A simple name for the VM client contact can be used as shown, such as voicemail. The cluster name will be the domain used for the system. In our system is it Plutonetwork.com, our company domain. The IP address in the next field is the IP address for the Application Server.

The locales, max number devices, overflow server will be completed based on your network setup. You may use the values shown as defaults. Next check the box for auto provisioning and input the IP address of the IPCM in the F/W download server. This is used to configure your IP Phones and download software to the IP Phones from the system. The next two fields will be used for IP Phone firmware codes that will be downloaded to the different kinds of IP Phones on your network.

When adding the IP Phone firmware codes please make sure to enter the correct code for each type of IP Phone. These will be the same types of firmware that you would have loaded onto the IPCM Sun Server through the command line interface and Putty Client. If the wrong software is entered for the wrong IP Phone or a different type of software from what was loaded, the IP Phones will not work. Double check what was loaded on the server; it will save time when booting IP Phone.

Next check the box called Use UFTP; this will allow the firmware to be downloaded to the IP Phone. If this is not checked the IP Phones will not get loaded with firmware or updates. When booted up originally, the IP Phones will have a firmware already loaded on to them, but if you want to download new firmware you will need this box checked. The other values under this box may remain at default or you may change them based on the values allowed on each box.

The Prov Sync Service (see Figure 3.53) will need to be configured or it can be left as the default. In Figure 3.54, the UNISTIM Base will also need to be configured. The local host for this service is the IP address of the IPCM Server. The port used is the standard port for UNISTIM, which is port 5000. This is the same port used on other Nortel PBX's such as the CS1000 and BCM.

Figure 3.51 Conference Service Tab

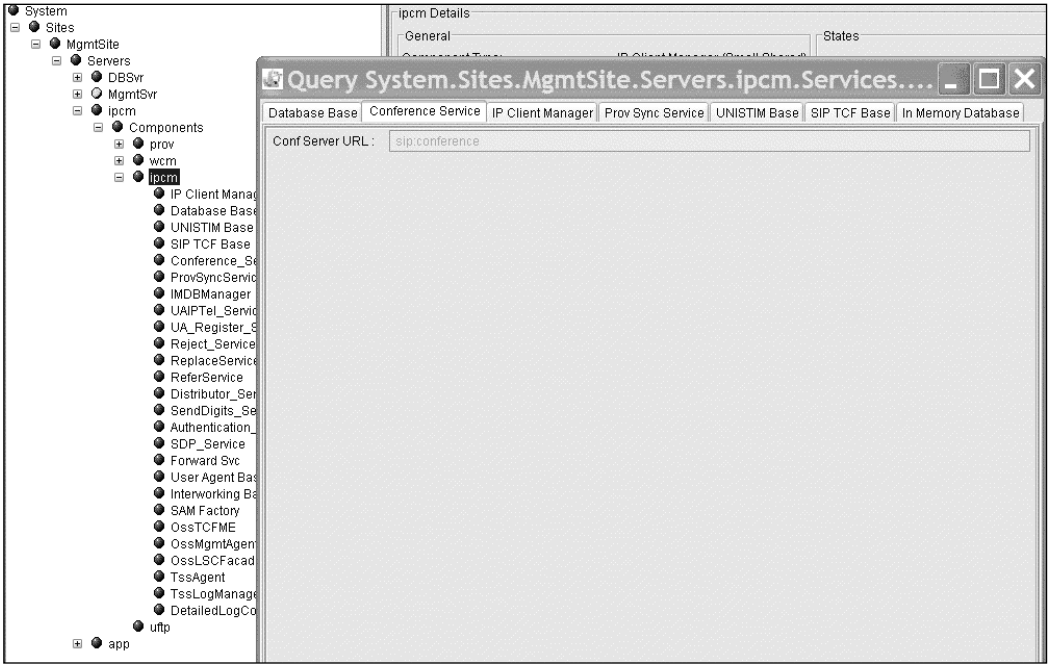


Figure 3.52 IP Client Manager Tab

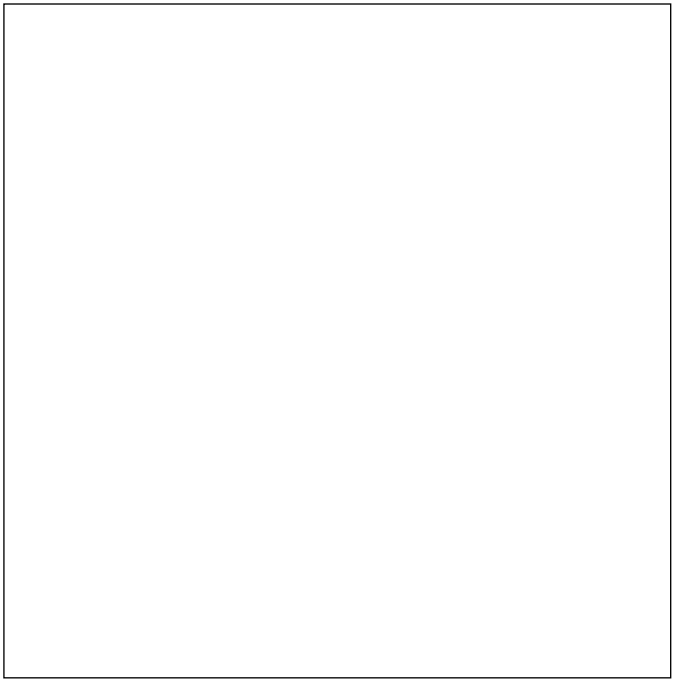


Figure 3.53 Prov Sync Service Tab

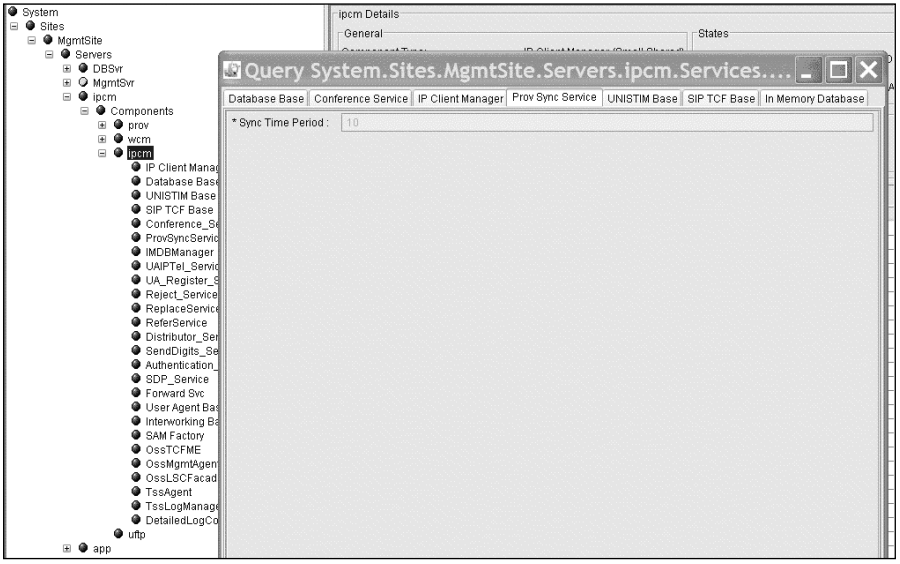
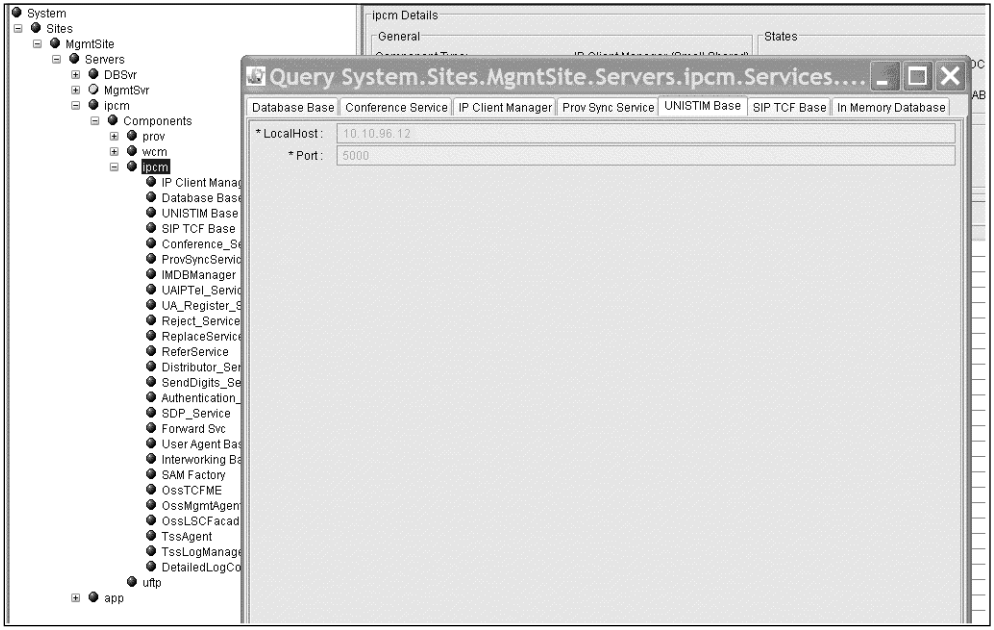


Figure 3.54 UNIStim Base Tab



Designing & Planning…

UNIStim

The protocol called UNIStim is a proprietary protocol used by Nortel Networks. The IP Phones, when configured to the MCS 5100, are configured with port 5000. The reason for this is that up until this past year, the MCS 5100 did not offer SIP on IP Phones like the 2004. Now if you have a phase two IP Phone you may either do UNIStim or SIP to the MCS5100. If you do SIP to the MCS 5100 you will not be able to log more than one person into a phase two IP Phone. If you use UNIStim to the MCS 5100 then you may log up to six users on one phase two IP Phone.

The SIP TCF Base shown in Figure 3.55 has the same settings as the tab configured earlier. The settings may be copied or you may change the settings based on values allowed. As shown in Figure 3.56, the In Memory Database, you will need to configure the number of domains and number of users, based on your system and what you have set as limits in your system. The limits can be set to the max value with no harm, but it is recommended to set them based only on your network design.

The other values that need to be set may be set based on the default value in each area. You may also change these based on your system and on what you would like to see in your system.

APP Server—APP1

The next server that will need to be configured is the Application Server; this is the one component that we have listed under our system that is an application component. The Application Server is used for the PC Client and Web PC Client. In Figure 3.57 these are the settings that can be changed on the APP server itself. These are the same setting changes as the other servers listed earlier.

Figure 3.55 SIP TCF Base Tab

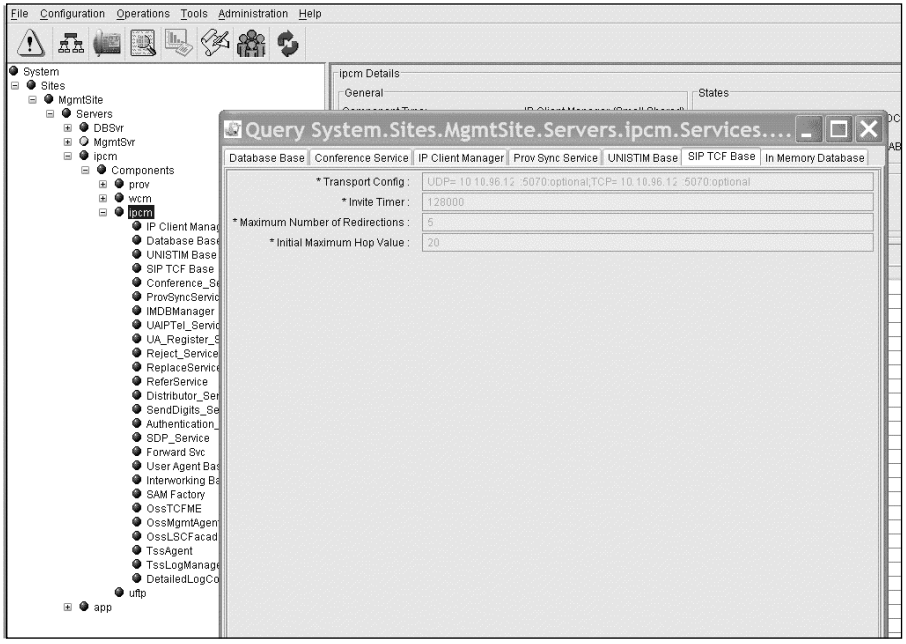


Figure 3.56 In Memory Database Tab

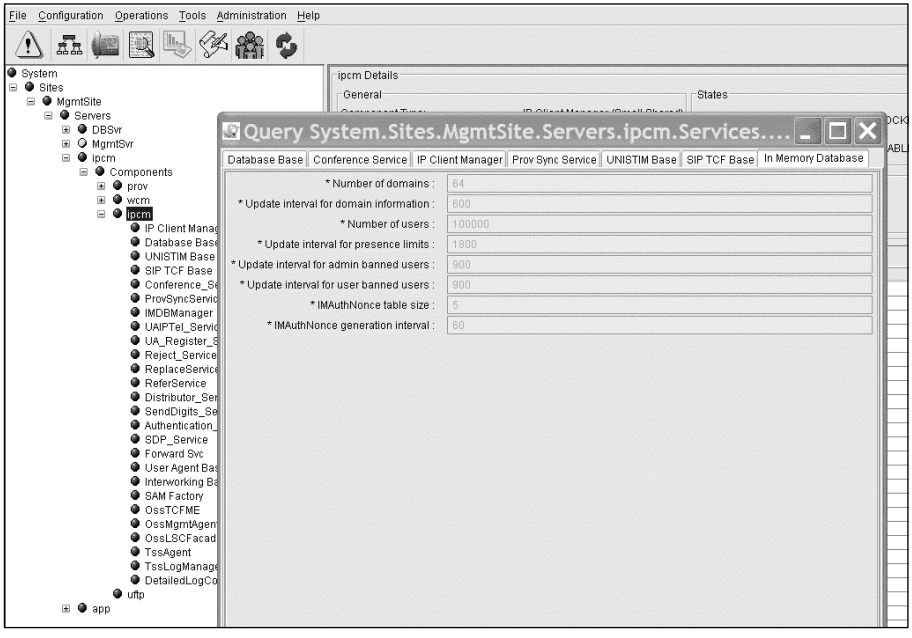
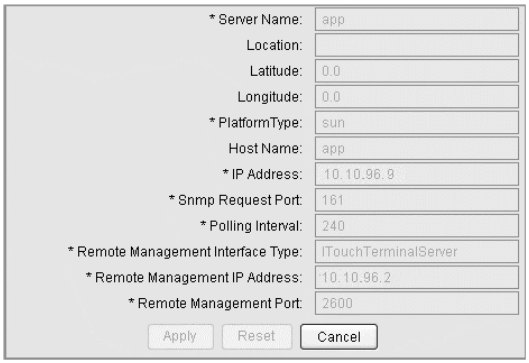
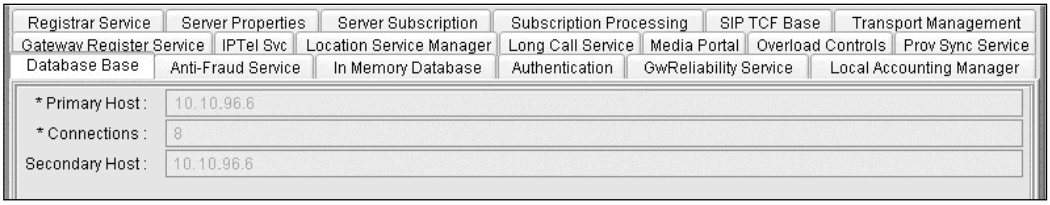


Figure 3.57 APP1 Server Settings



As you can see starting with Figure 3.58, there are many services that will need to be configured under the APP1 Component. The first, shown in Figure 3.58, is the same as we have seen before in other components. The primary host needs to be set to the IP address of the Database server and the amount of connections that need to be set. As before, you may add a secondary host if you have one or you may use the same address as primary.

Figure 3.58 APP1 Database Base Tab



In the next two services or tabs, the Anti Fraud Service may be checked and used on the APP1 component in Figure 3.59. Figure 3.60 shows the In Memory Database; these settings are the same as a prior component configured. The number or domains and number of users will need to be configured based on your system. The other values may be kept at the default or changed to other values allowed.

Figure 3.59 APP1 Anti-Fraud Service Tab

Figure 3.60 APP1 In Memory Database Tab

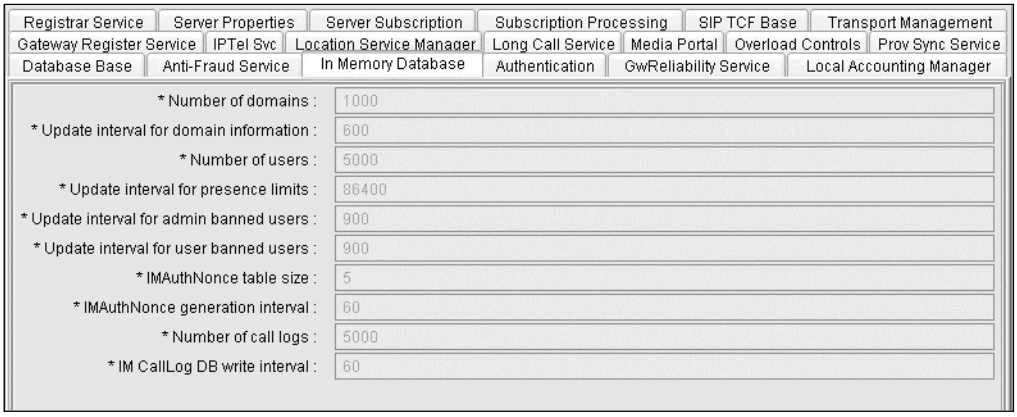
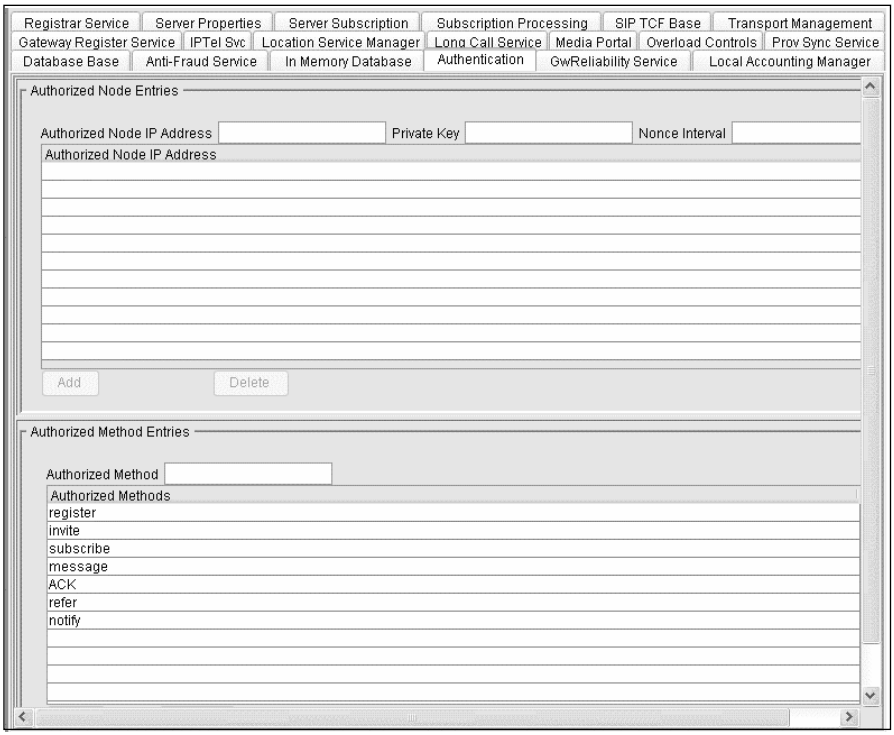


Figure 3.61 shows the Authentication Tab Nodes and Methods being configured. These addresses would be the IP addresses of servers within the MCS5100, AudioCodes Gateway, Meet Me, and Ad Hoc Conferencing Servers, Web Collaboration Servers, Blackberry Server, Wireless Server, CS1000, Call Pilot, and other nodes such as an Avaya Server and Citrix Server. These are all servers that would be listed in the Authentication Tab. These servers need to be listed in the Authentication Tab by IP address before they can communicate with the system.

The authentication methods are how the node communicates with the MCS 5100. These methods could be different depending on the system and those methods.

Figure 3.61 APP1 Authentication Tab



In Figure 3.62, you may activate the Gateway Reliability Service on the MCS 5100; check the Service active flag box, and then select the **Performance** feature active flag box. The Service active flag maybe be left at 600 or default, but may be changed based on the current system needs. In Figure 3.63, the local accounting manager tab, you will need to input the IP address for the database server. This goes into the primary cam IP address. All other settings in the tab can be left at the default or changed if needed. The recovery cam IP address is for networks that will have more that one management server. If you do not have a secondary address, you may input the primary address into this space.

The next two tabs that will need to be configured are the Gateway Register Service in Figure 3.64, where the maximum gateway registration duration may be left at the default or changed. I recommend that you use 300 for the duration. Going any higher in the number range did show some problems with our system. When adding your nonoverflow response codes in the

IPTel service, make sure you separate the codes by commas (see Figure 3.65). These codes can be either numeric or alpha characters.

Figure 3.62 APP1 Gateway Reliability Service Tab

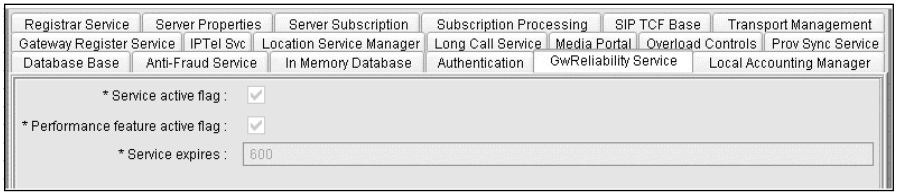


Figure 3.63 APP1 Local Accounting Manager Tab

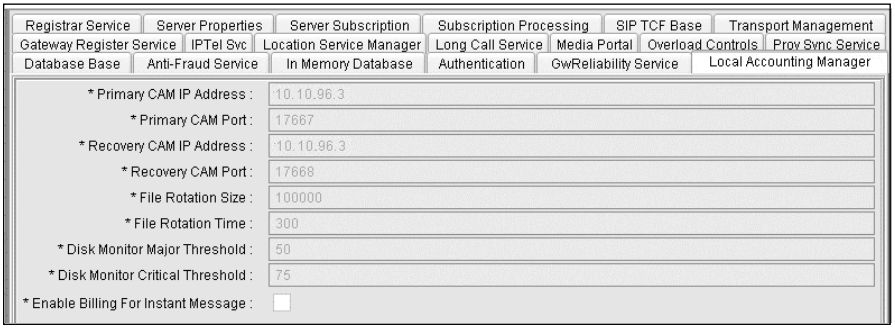


Figure 3.64 APP1 Gateway Register Service Tab

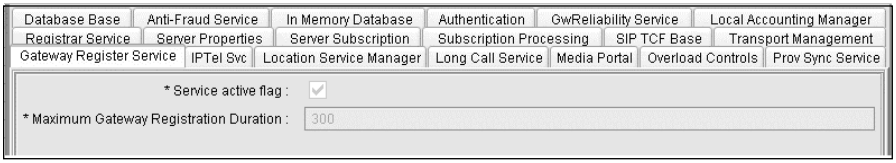


Figure 3.65 APP1 IPTel Service Tab

In the Locations Server Manager tab, you can set up DNS to be used on the MCS 5100. The transport used is usually UDP, unless you want to use TCP (I do not recommend this). You will also need to configure the DNS server URL and then check the box to use the server (see Figure 3.66). In

Figure 3.67, the Long Call Service is set to a default of 60 for the duration; you may add time to this range.

Figure 3.66 APP1 Location Service Manager Tab

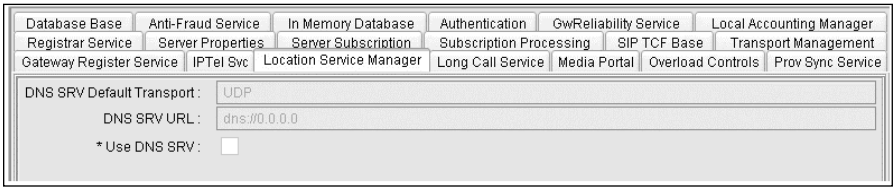
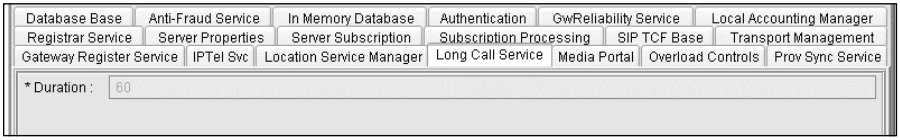


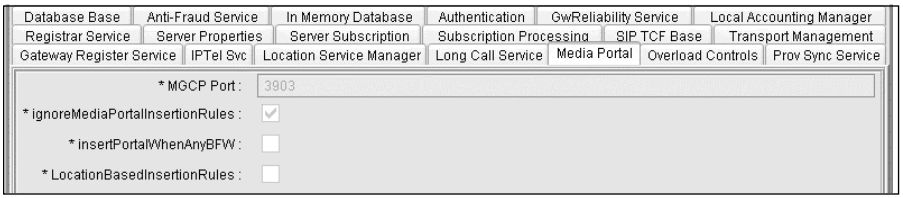
Figure 3.67 APP1 Long Call Service Tab



If you are using a media portal in your system, you will need to pay attention to this tab in the screen shown in Figure 3.68. The port used in our system for MGCP is 3903. You may change this but I would recommend keeping it the same as shown here. If you are not using a media portal in your system, you need to check the box as shown. If you are using a media portal, then leave the first box called Ignore Media Portal Insertion Rules. If this is not done the correct way you will have problems when using the media portal.

If you are using a media portal and it is going to be behind a firewall then you will need to check the second box called Insert Portal When Any BFW. If your media portal is going to be behind a firewall or at another location other than where your MCS 5100 is located, it is recommended that you check the location-based insertion rules.

Figure 3.68 APP1 Media Portal Tab



In Figure 3.69, these settings are default and recommended on the system. These settings all may be changed but it is recommended to use these default values. If you need to change the values, remember you may highlight the value in the tab to produce a system box for each that will give you more information on each option and the range allowed for the value. In Figures 3.70 and 3.71, the values listed are the default and recommended range for those values.

Figure 3.69 APP1 Overload Controls Tab

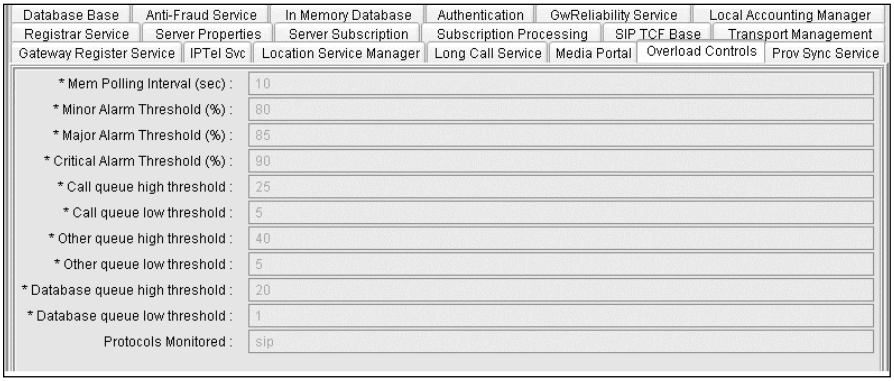
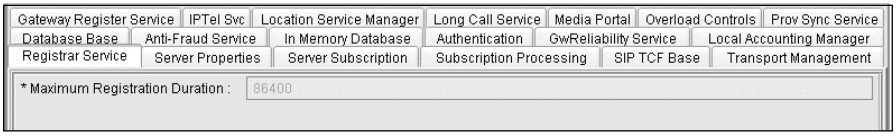


Figure 3.70 APP1 Prov Sync Service Tab

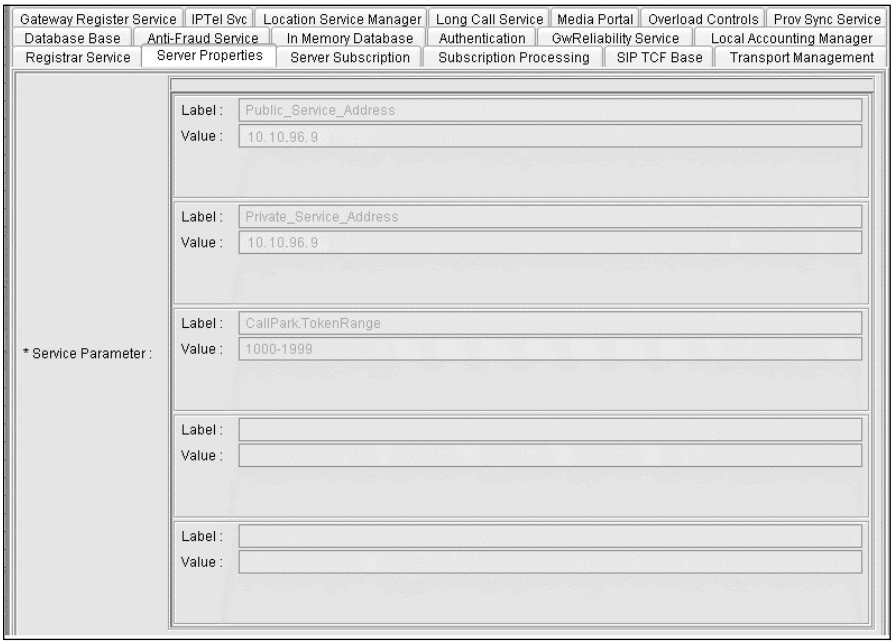
Figure 3.71 APP1 Registrar Service Tab



In Figure 3.72, information about the application server will need to be added. This is done by adding a pubic and private service addresses as shown. The IP addresses for both stay the same but the label changes. Another label will need to be created for call park token range, which is a feature of the MCS 5100 that can be used on the IP Phones and PC Client. Your range may

be greater or you may have less for your value. The items listed in the range are defaults used in the system.

Figure 3.72 APP1 Server Properties Tab



The IP address for the IPCM server is being used in the Server Subscription tab (see Figure 3.73). In the provserverURL space you will add this IP address, a port number on the server, the port number for the World Wide Web (which is 80), and the http. In Figure 3.74, the maximumExpires works with the Server Subscription tab just configured and your default value is listed in the figure. The administrator can change this if he or she wants to shorter the subscription time on the server.

Figure 3.73 APP1 Server Subscription Tab

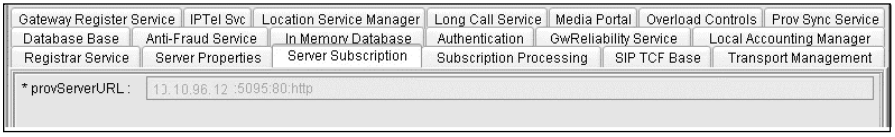
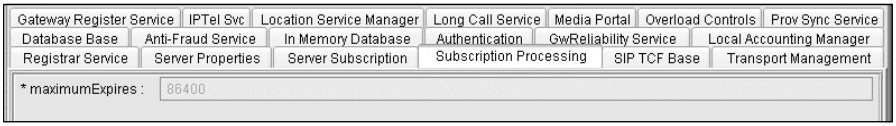
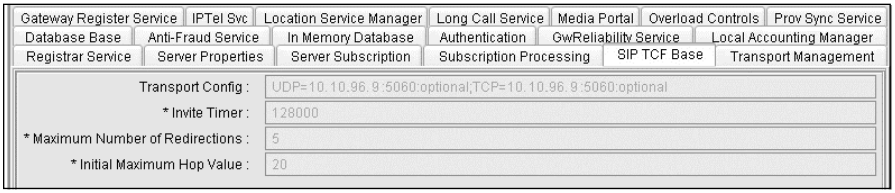


Figure 3.74 APP1 Subscription Processing Tab



The SIP TCF Base will be configured as shown in Figure 3.75. This is similar to the other SIP TCF Bases tabs that have been configured before. In the transport config area you will need to enter a UDP transport going to your application server with a SIP port configured. This will be set the same for TCP (both are set to optional), which makes it easier since you can change from TCP SIP to UDP SIP and not have to reconfigure your whole system.

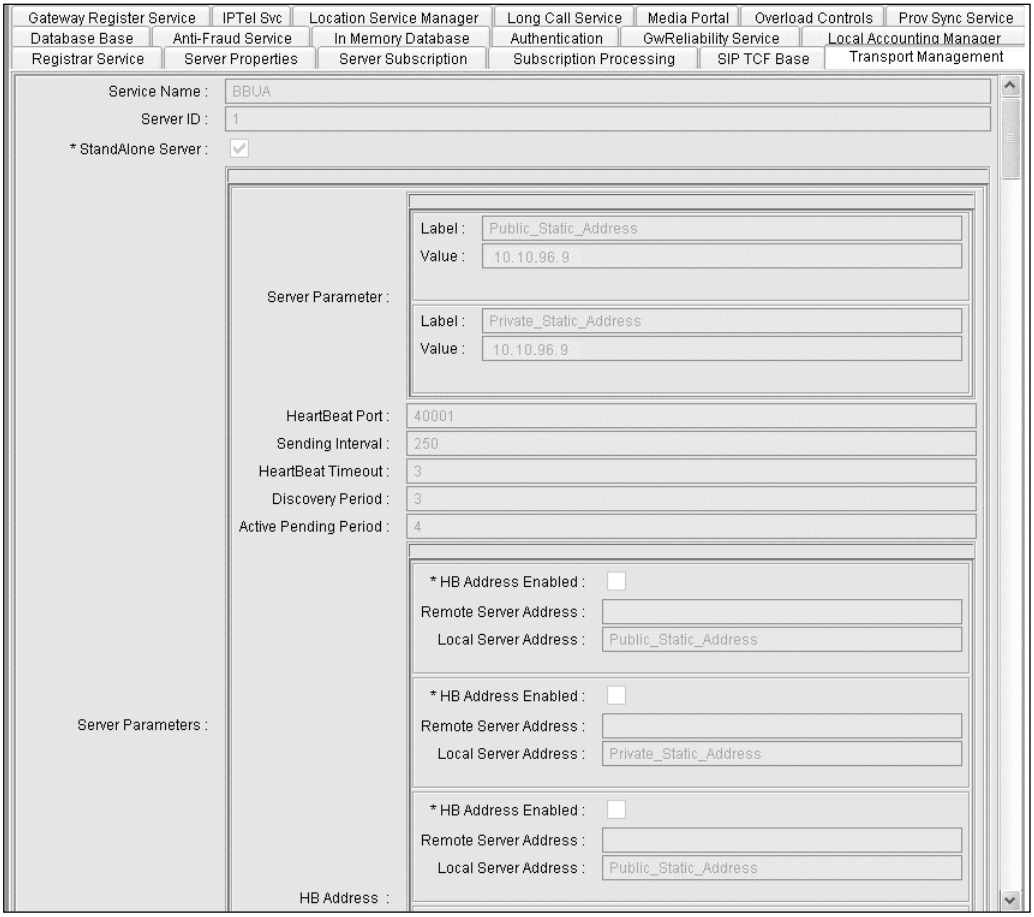
Figure 3.75 APP1 SIP TCF Base Tab



The next tab that will be configured is the Transport Management Service (see Figures 3.76 to 3.84). The first value that needs to be configured is the service name, which can be any name; we used a default of BBUA and a server id of 1. You may change these or leave them as shown here. Next, check the Standalone Server box. The next values you see in the server parameters are the same settings entered in prior services for public and private addresses; these will change for your system based on what addresses you use.

All other settings within the server parameters are default, and if you were using a heartbeat port you would add the addresses of the remote server and check the box below. Also in the NSD Fields shown in Figure 3.77, there are four different NSD services that can be used; each box must be checked before it can be used. The values and parameters within the NSD areas are similar to what has been shown before for SIP addresses using UDP and TCP plus a private and public address for the IP addresses.

Figure 3.76 APP1 Transport Management Service



NOTE

Users of the MCS 5100 do not have to pay for costly audio conferencing and videoconferencing; the MCS 5100 provides these services within the system. These services are very scalable to any network. The system also provides a Web collaboration tool that allows users to not only make an audio or video call but also share or create documents in moments.

Figure 3.77 APP1 Transport Management Service

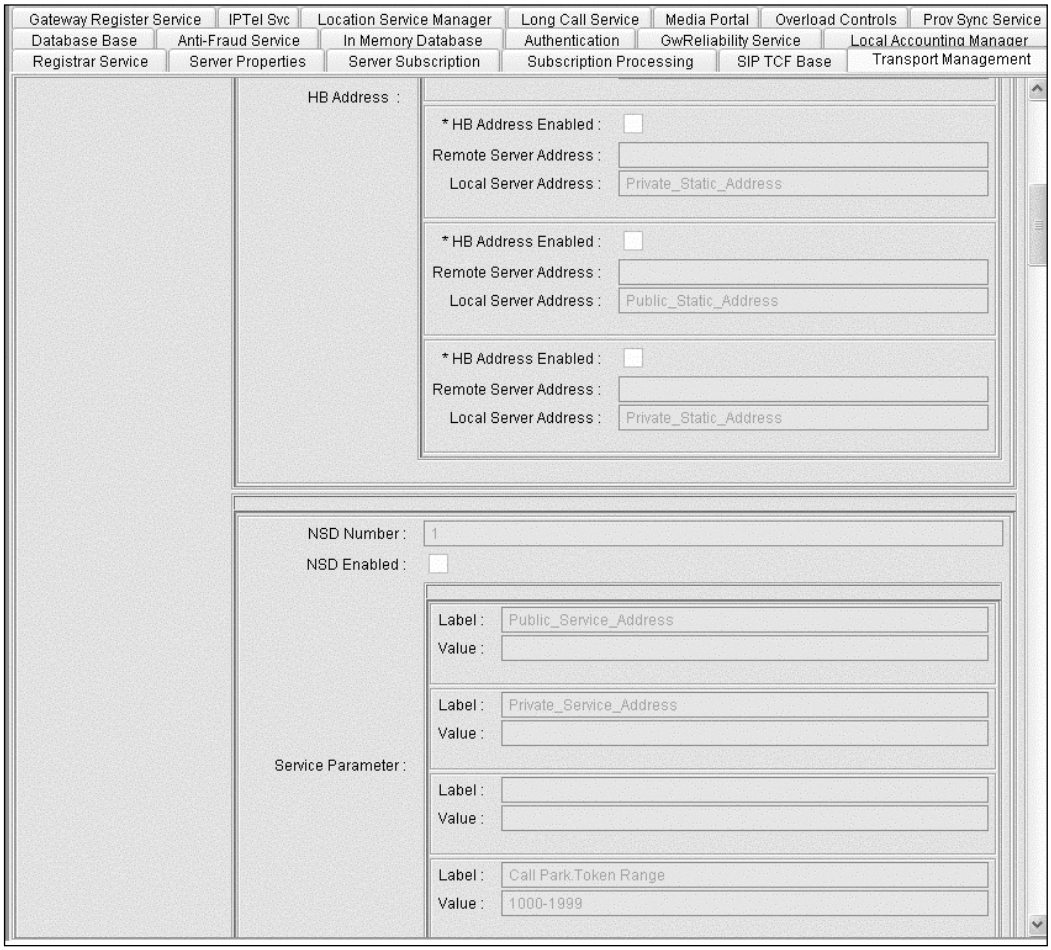


Figure 3.78 APP1 Transport Management Service

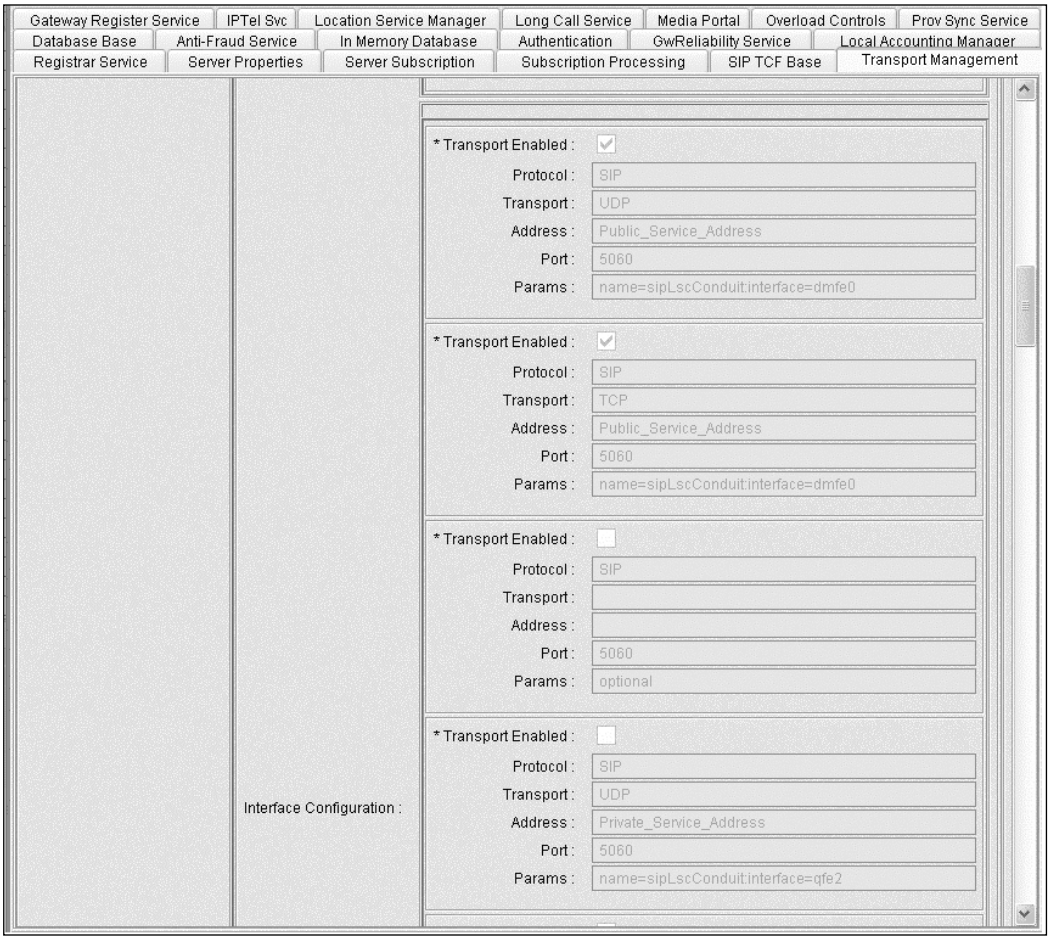


Figure 3.79 APP1 Transport Management Service

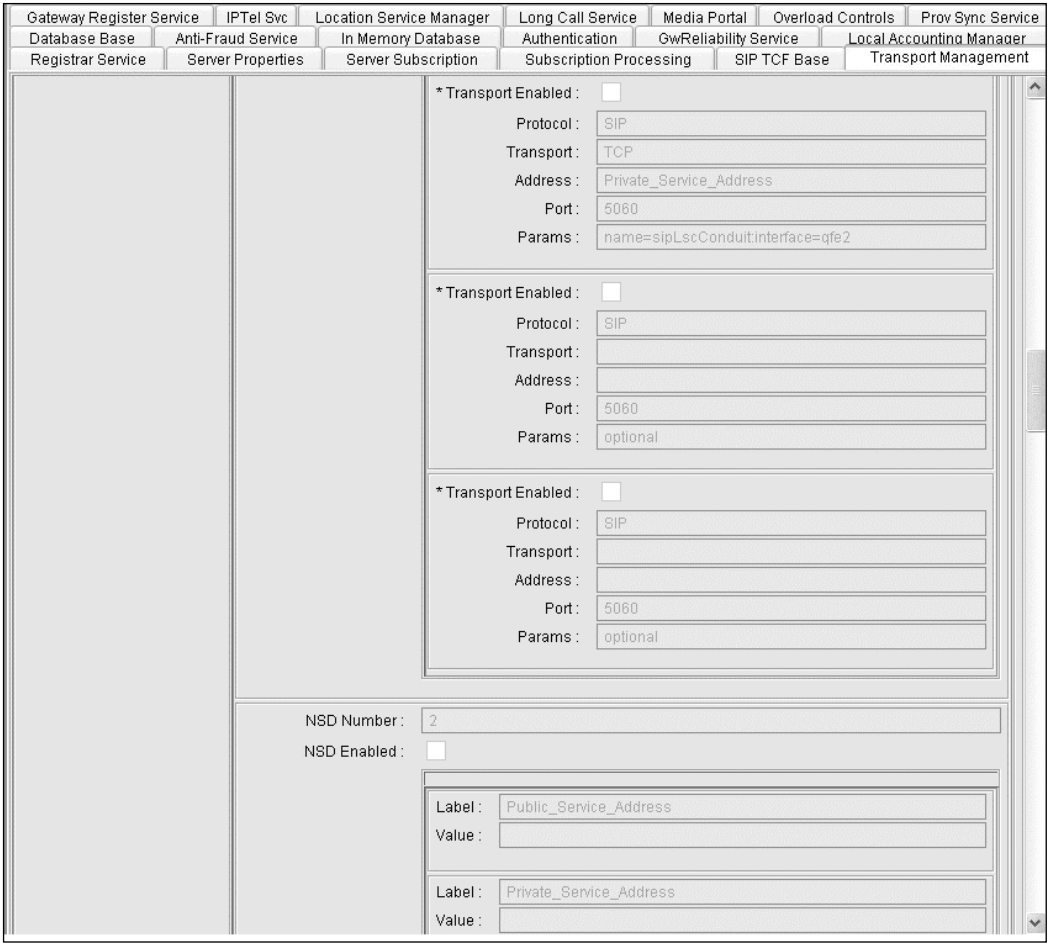


Figure 3.80 APP1 Transport Management Service

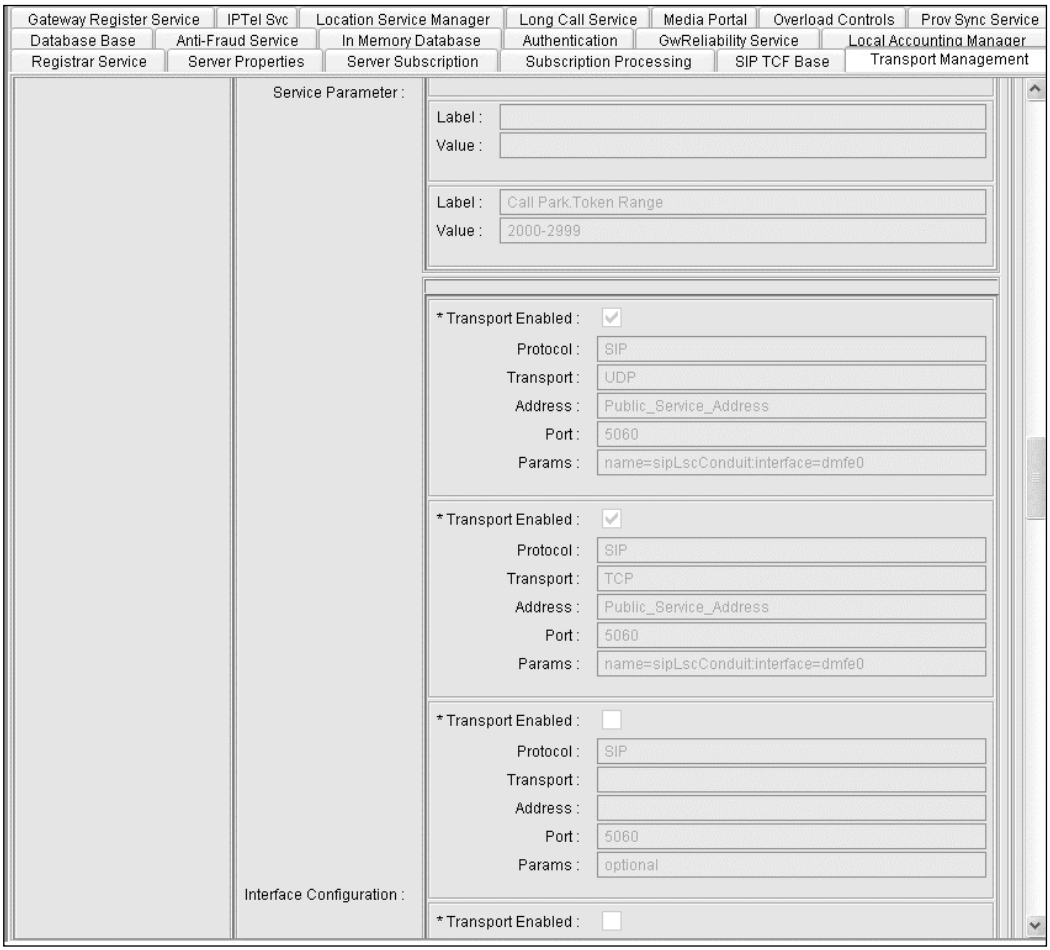


Figure 3.81 APP1 Transport Management Service

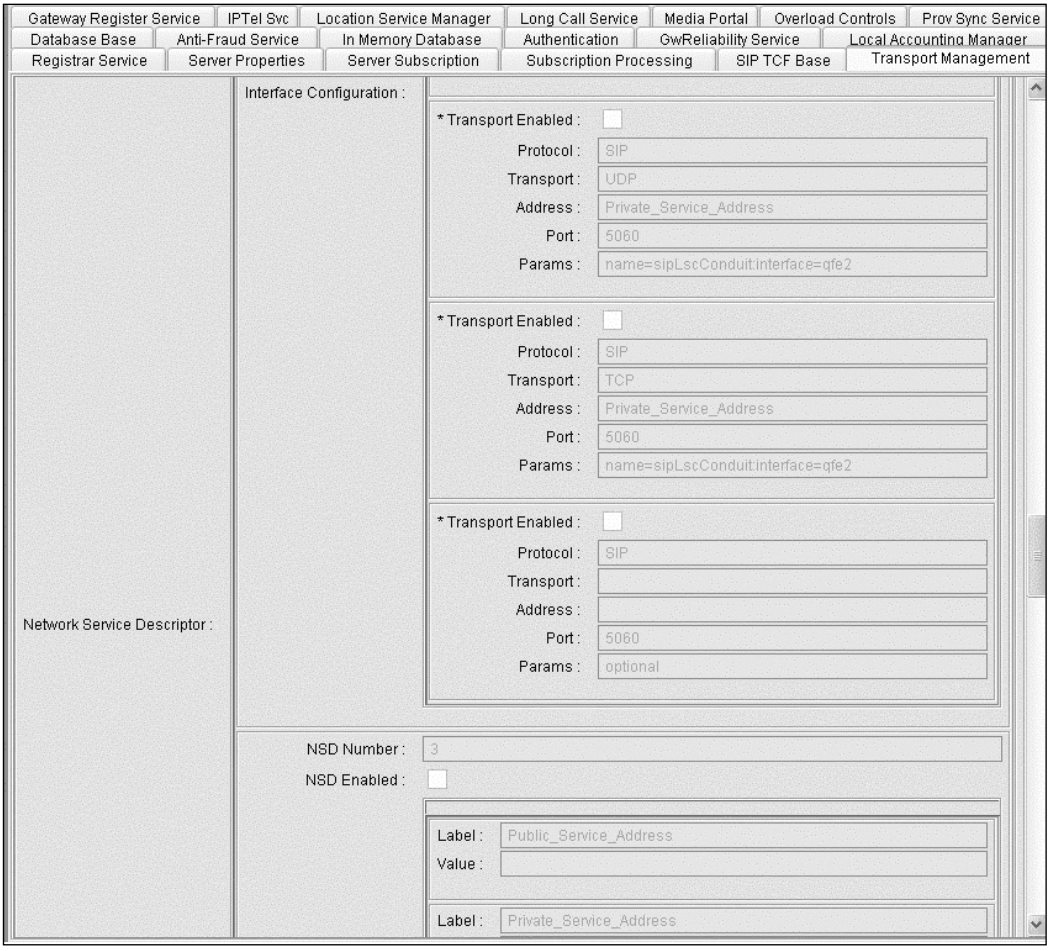


Figure 3.82 APP1 Transport Management Service

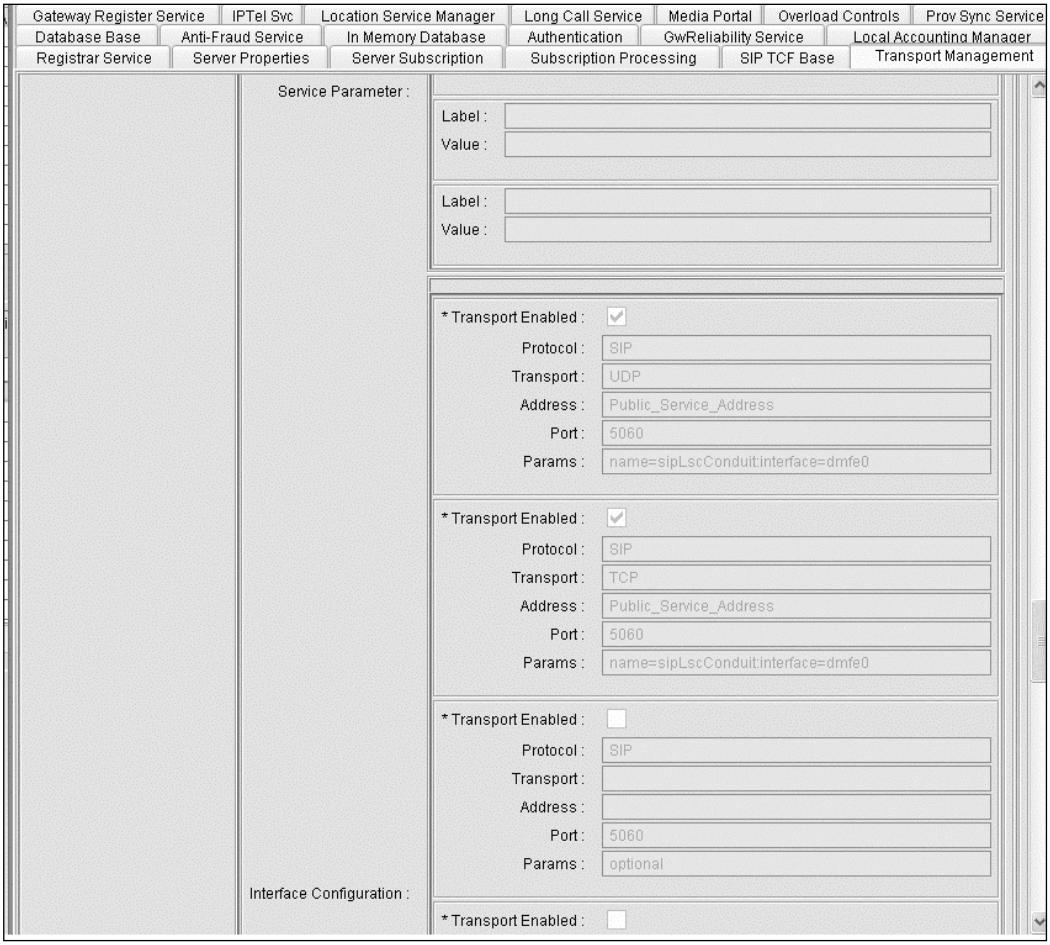


Figure 3.83 APP1 Transport Management Service

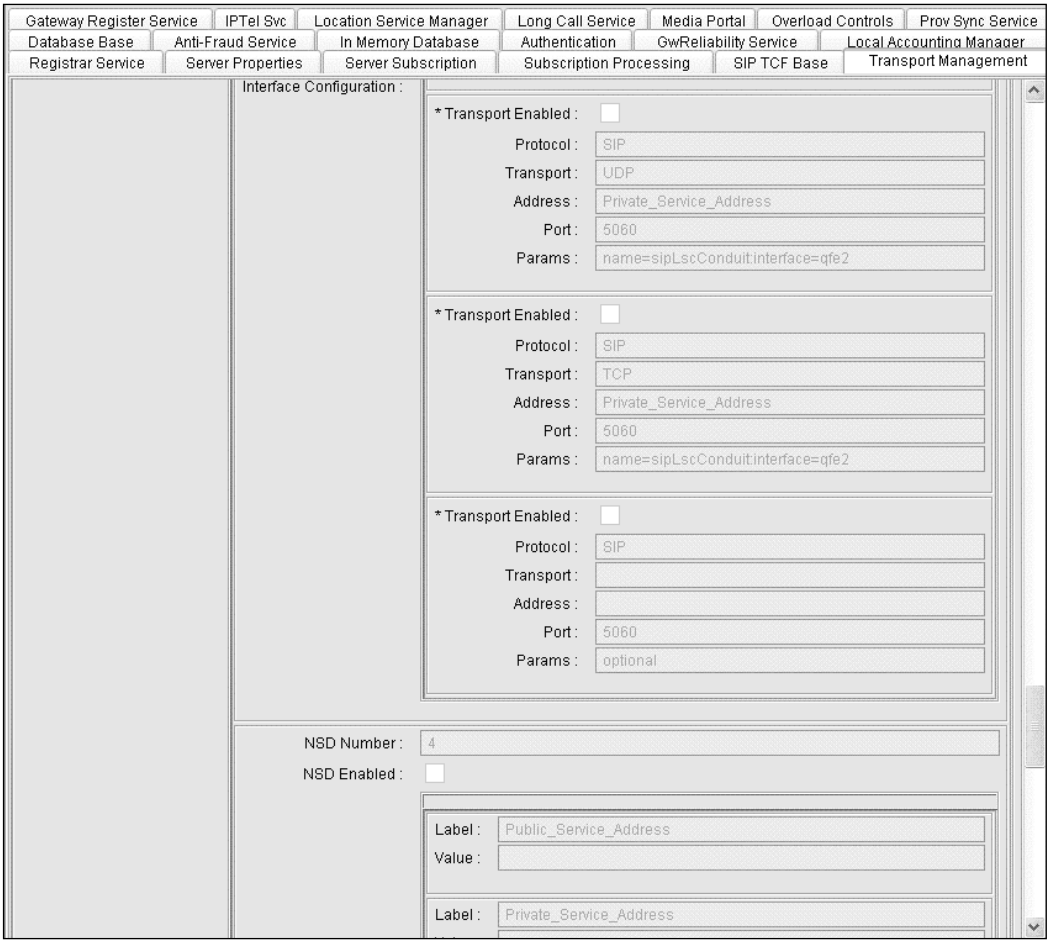
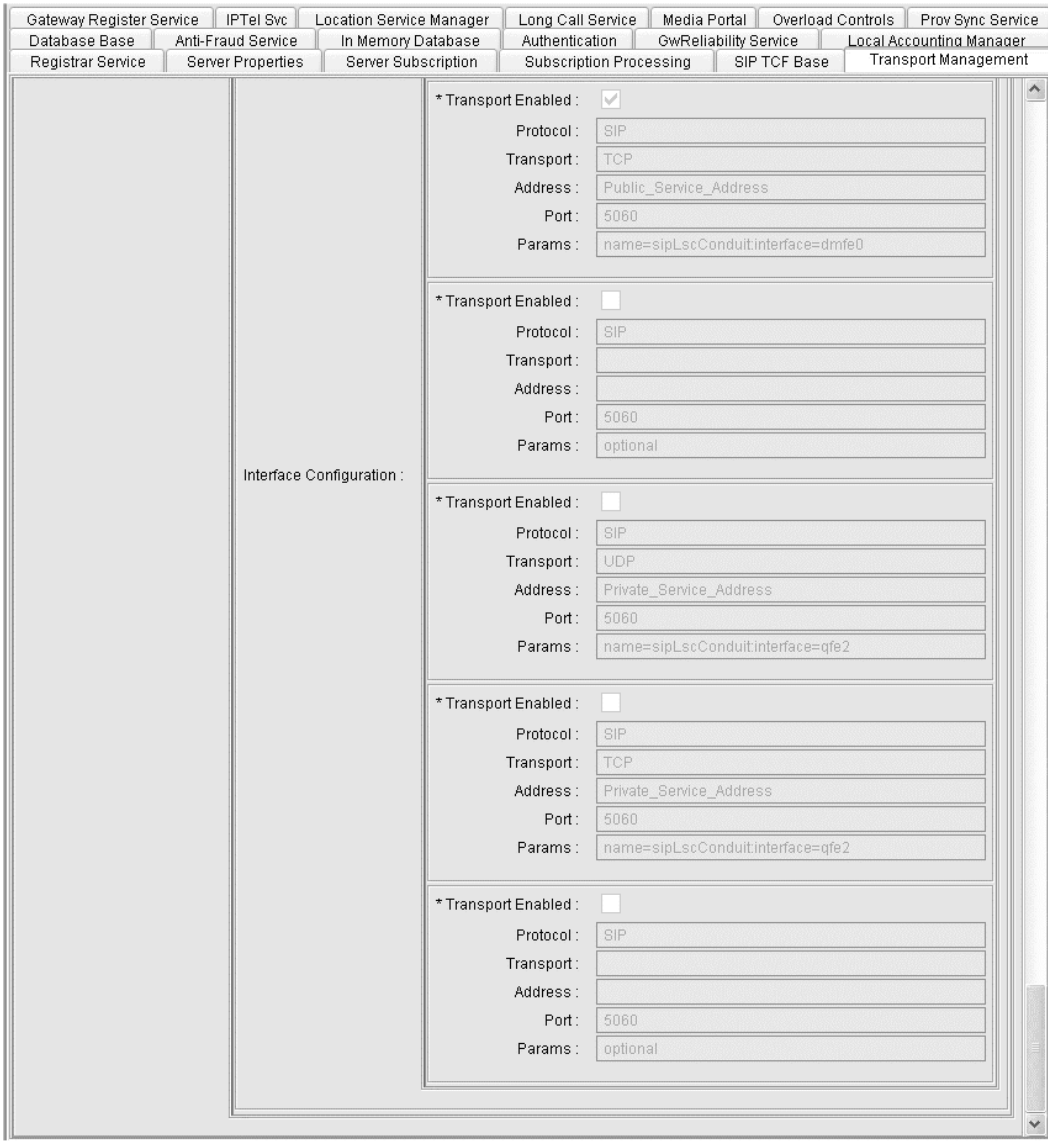


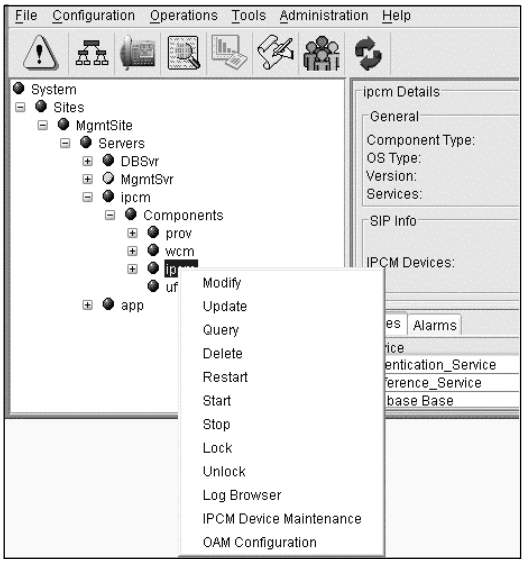
Figure 3.84 APP1 Transport Management Service



IPCM Device Maintenance

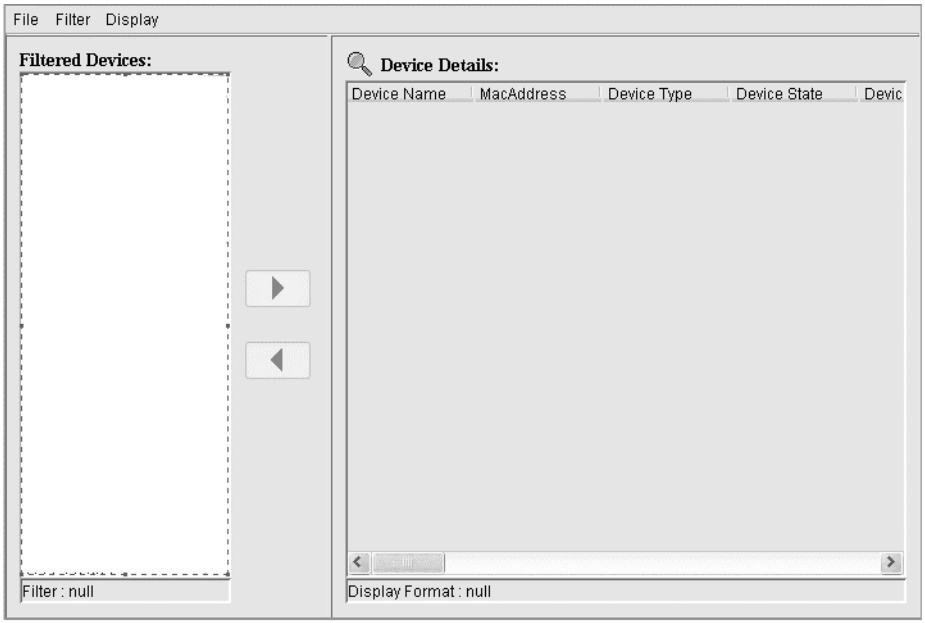
In this next section we are going to cover the IPCM Device Maintenance, which is located with in the IPCM Service under the IPCM Server. To get to this screen you will need to right-click the IPCM service, which produces the menu shown in Figure 3.85. Select the **IPCM Device Maintenance** in the menu. This area will allow the administrator to view, change options, and troubleshoot all IP Phones that are registered to the IPCM at that time. They can be in use, logged out, or not in service but they will still be shown.

Figure 3.85 IPCM Device Maintenance Menu



When the IPCM Device Maintenance is selected, a new GUI screen will appear like the one in Figure 3.86. If you have no IP Phones registered to the IPCM then the screen called Filtered Devices will be blank. In the top menu on the GUI, select Filter, which will allow you to change the menu listings shown in the Device Details on the right window of the GUI. The filtered device menu can be configured to show the devices in many different ways as we will see in a later figure. At this time there are now IP Phones registered to the IPCM; before going into detail, we will register one IP Phone for use in this book.

Figure 3.86 IPCM Device Maintenance Selected

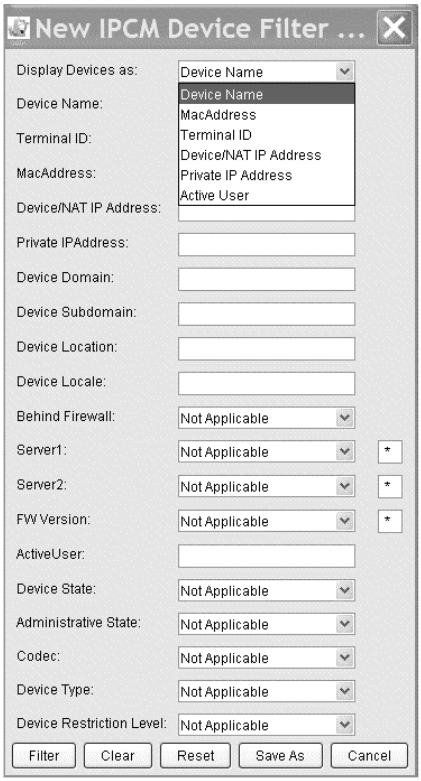


Once you have selected the word Filter in the menu, you can add, change, and delete configured filters. Figure 3.87 shows the options allowed when creating a new device filter or making changes to an existing device filter. All fields in the device detail may be changed or deleted if not used by the user. Also the fields within the filtered devices may be changed so that different device names may be used in the window.

The first field is Display Device as. This will allow the device to be displayed by the items in the drop-down box: Device Name, Mac Address, Terminal ID, Device Nat IP Address, Private IP Address, and Active User. You can select and make different filters for different uses when providing administration, monitoring, or troubleshooting to the IP Phones.

There are no drop-down boxes for some of the fields shown in Figure 3.87. This provides you with better filtering for specific fields that may be needed. Since these fields have different values it is not possible to provide drop-down boxes for them. These are single values and no more than one value may be added into these fields. If you need to add more than one value to a field, a new or different filter will need to be created.

Figure 3.87 Display Device Field



In Figures 3.88 through 3.95 we will show the options provided by the drop-down boxes. If the system is behind a firewall you would select True in the Behind Firewall option in Figure 3.88. You may also select False if there is no firewall or select Not Applicable if you are not sure. In Figure 3.89 it is a little confusing, but if you remember that not equal to means no, and equal to means yes, you will be just fine. If you are using one IPCM, just select the options from Server1; if using two IPCM Servers, select the options in Server2.

Figure 3.88 Behind Firewall Drop-Down Menu

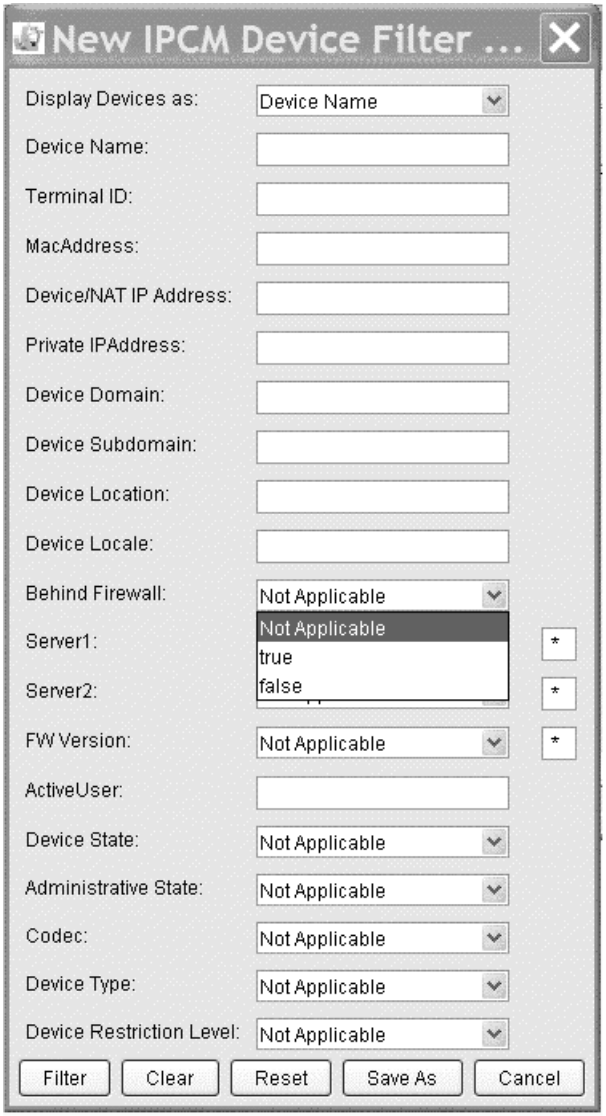
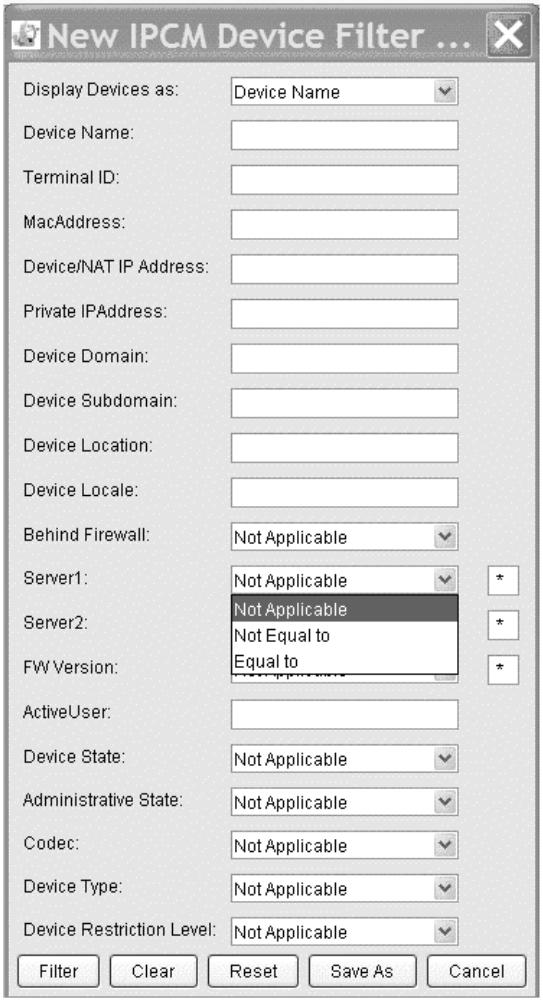


Figure 3.89 Server1 Drop-Down Menu



Figures 3.90 and 3.91 cover the firmware version and device status. In Figure 3.90, you can select whether you want to display the firmware version in the select filter. This is the same as described earlier for the servers. If you want to display the firmware select Equal to; if you do not, select Not Equal to. You may also select Not Applicable if you do not know or want to leave it blank. In Figure 3.91, the device state may be chosen, for each IP Phone. The user may select OFFL for offline, INSVC for in service, INSANE FIRMWARE for installing firmware, or User failed Registration.

Figure 3.90 FW Version Drop-Down Menu

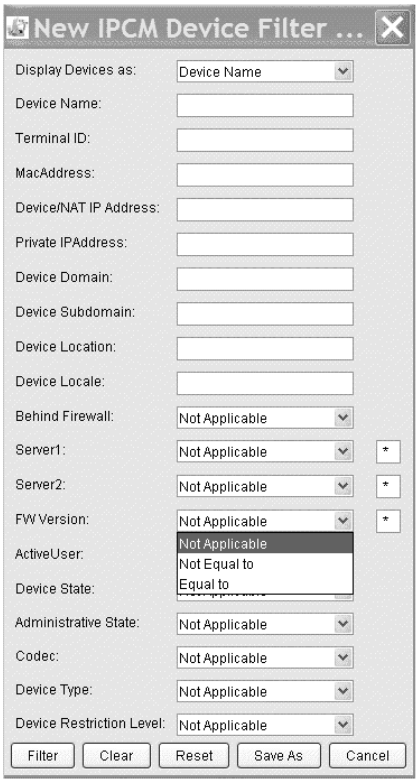
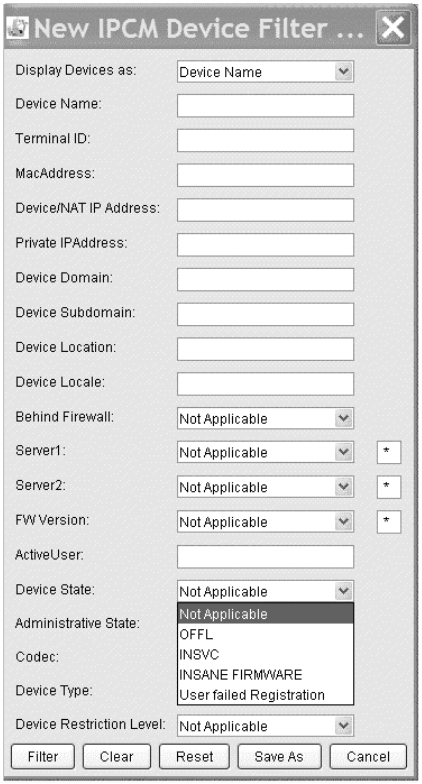


Figure 3.91 Device Status Drop-Down Menu



As shown in Figure 3.92, you can select how you would like to see the administrative state of the IP Phone. Three states may be selected: Locked, Unlocked and Shutting Down. In Figure 3.93, for the codec used on the MCS 5100, choose G711U, G723, G711A, L16, G729A, or Not Applicable. Even though there is a selection for Unknown Codec, most likely you will never use this on the system.

Figure 3.92 Administrative State Drop-Down Menu

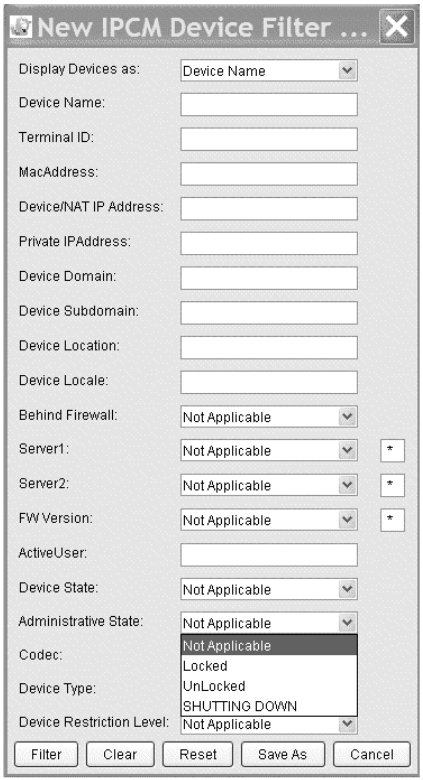
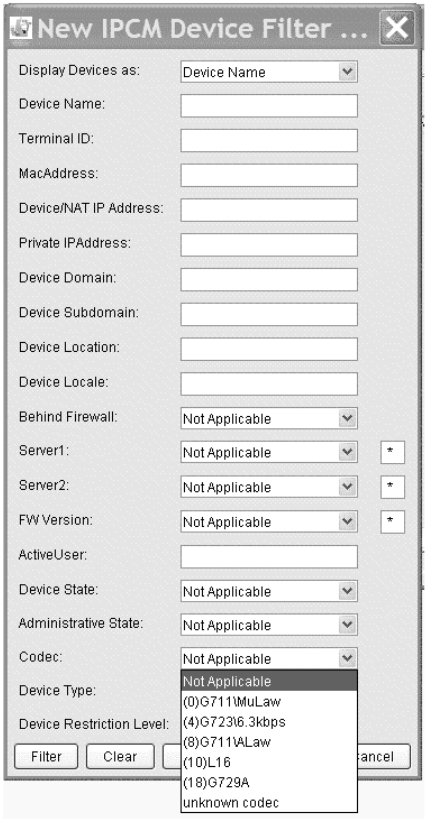


Figure 3.93 Codec Drop-Down Menu



The last two figures in the IPCM Device Filter are used for selecting the device type and the device restriction level. In Figure 3.94, the user may select the device type for the filter; as you can see in the drop-down menu these are Nortel IP Phones. If you are not sure what type of IP Phone you are looking for, select Not Applicable and all IP Phones will be displayed. If the IP Phones have been set up with restriction levels, then in the screen shown in Figure 3.95 you can choose either Full or Restricted access for the filter. Once again if you are unsure, select Not Applicable and all devices will be displayed regardless of restriction.

Figure 3.94 Device Type Drop-down Menu

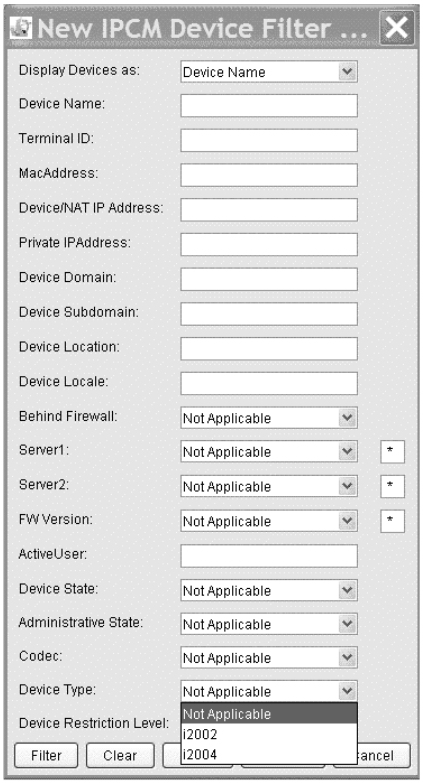
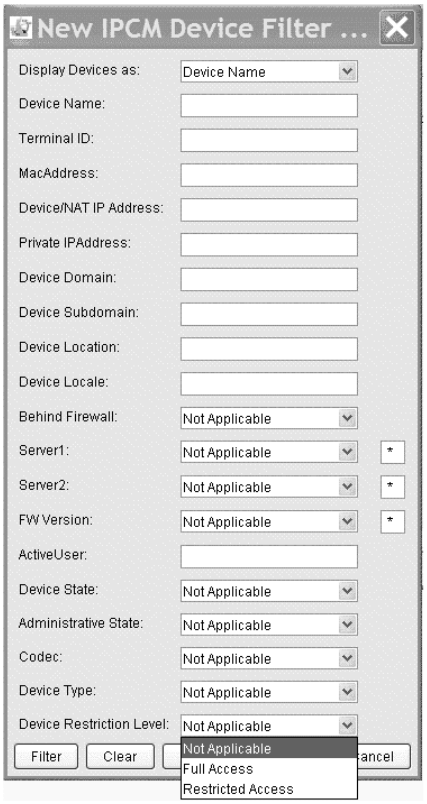


Figure 3.95 Device Restriction Level Drop-down Menu



Once the filter has been completed, select Save to save the filter to a file-name to be used again. After the filter has been saved, select filter and the IPCM Device Filter will then use your new filter to change the display in the right-hand side window. As shown in Figures 3.96 through 3.98, the device details have changed based on the new filter created. The menu list shown is scrolled from right to left to see all the fields, and the fields may be shortened or lengthened. This lets you see all of what is in the fields for the devices.

Figure 3.96 Device Details

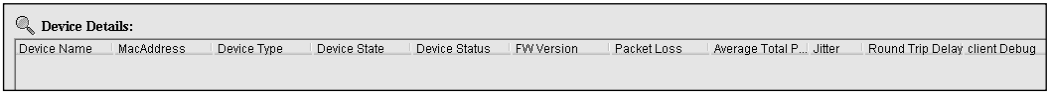
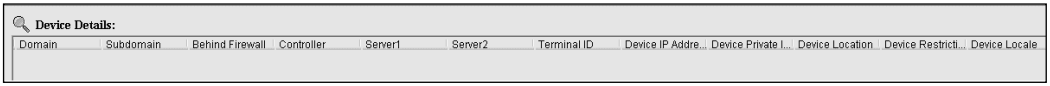


Figure 3.97 Device Details

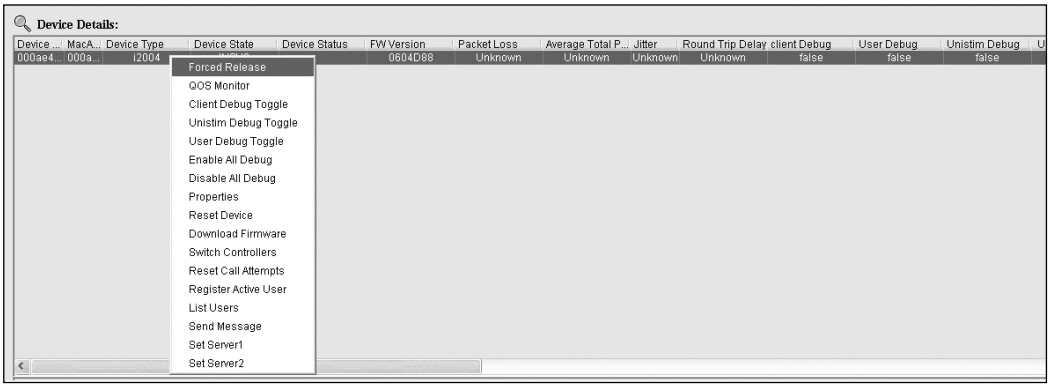
Figure 3.98 Device Details



We have added one IP Phone to our system for this book. Once we added the IP Phone it was displayed in filtered device name on the left side of the GUI. The IP phone was selected, and once selected, it was displayed on the right as shown in Figure 3.99. Now you can display all IP Phones or select IP Phones as needed. It is much easier to create filters as shown earlier to display numerous IP Phones rather than selecting them one by one out of the filtered device area.

Right-click the device to produce the menu shown in Figure 3.99. These are administrative and troubleshooting options that you can use on each IP phone. This is the only place within the MCP Client where this can be done with the IP Phones. It is recommended that you get to know this area and try each of the options shown so that if problems do happen, a remedy or some corrective action can be taken.

Figure 3.99 Device Drop-Down Menu



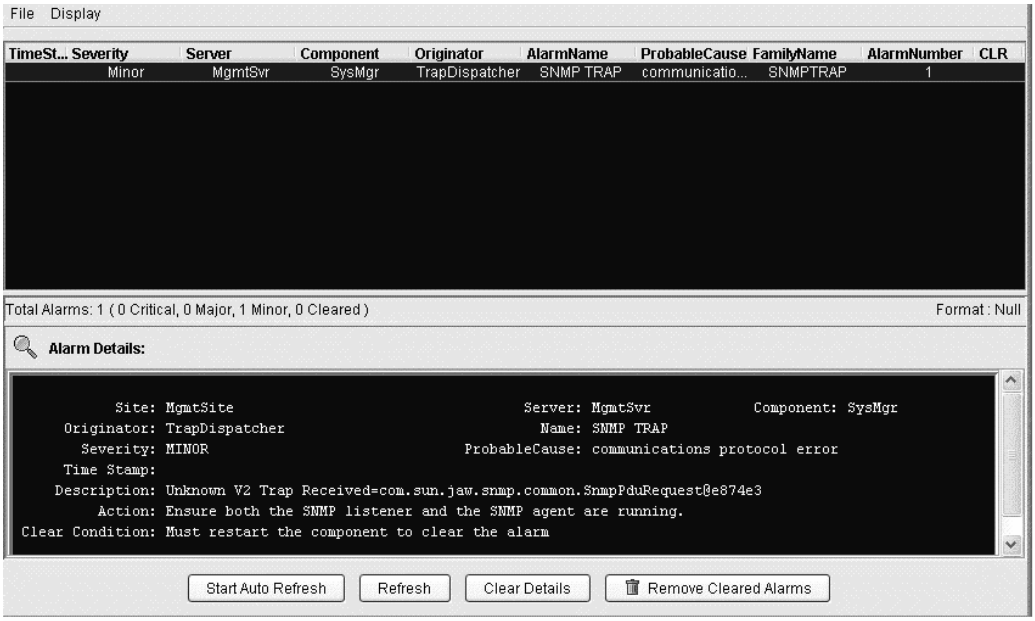
Troubleshooting Alarms

This section covers the alarm section of the MCP Client. As shown in this chapter, you may select the alarm browser from the main menu at any time. When looking at the alarms you may select a site, server, or component to view alarms. Alarms may also be viewed within the alarm tab of the MCP Client. This tab is on the right-hand side of the GUI when the site, server, or component is selected.

In Figure 3.100, you can see what the alarm browser looks like; right now we have created an alarm in the system to display. The alarm is displayed at the top of the browser at first and then when double-clicked the details are displayed below. In the details you may find the where the alarm is coming from all the way down to the service. In Figure 3.100 you can see the alarm is on the MgmtSite, on the MgmtSvr, within the SysMgr component. The originator of the alarm is the trap dispatcher and the problem is a communications protocol error.

The alarm detail will also give you the last time of the alarm and the date, a description, what action you should take, and what needs to be done to clear the alarm. You may remove the alarms from the browser only if they have been cleared or fixed; this is done by selecting Remove Cleared Alarms. If the user selects the auto refresh then the alarm browser will refresh itself with new and clear alarms. If this is not selected, you will need to select the refresh button on the bottom; the system does not auto refresh alarms by default.

Figure 3.100 The Alarm Browser



System Options

The last section of the chapter will cover the options with in the system sections of the options tree. We are looking at this by itself and not in the other sections because it deals with SNMP and licensing on the MCP Client. It is one section that you will need to know when adding more options to your system and more users to you system. When you have questions about how many licenses you have left for uses this is where you will look on your system for the information.

Configure OAM File Retention Period

In Figure 3.101 you see that right-clicking on the system area within the tree on the left will produce a menu of options. The first options we will look at will be the configure OAM file retention period. When selecting this it will produce another menu as shown in Figure 3.102. This will allows the administrator to change the period or time that the log files and OAM file retention stay or accumulate on the server. The settings in Figure 3.101 are default and may be changed by the user by choosing each option in the figure.

Figure 3.101 Configure OAM File Retention Period

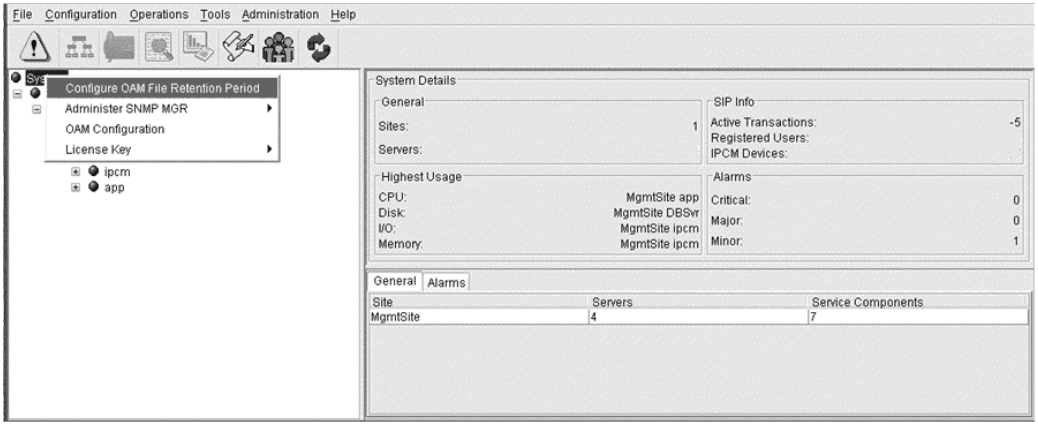
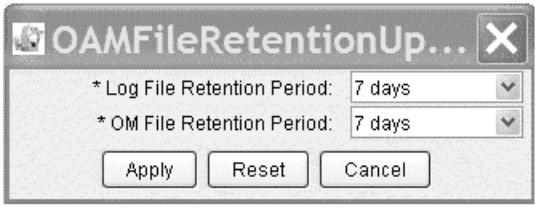


Figure 3.102 OAM File Retention Up



Administer SNMP MGR

Being able to have your network management retrieve alarms from any system is important. This may be done on the MCP Client by selecting the administer SNMP MGR options shown below in Figure 3.103. When you select this option on the menu in Figure 3.104, it will allow the administrator to input the IP address of the SNMP manager for the system. Then the administrator may change the SNMP community string, shown below is the default string used. Security concerns are important for the system so the author does recommend that the string be changes with upper, lower and numbers in the string.

In Figure 3.105 the administrator may change the port used for the SNMP traps on the system. While we are showing the default trap port the administrator may change this. It is not recommended by the author that this be changed.

Figure 3.103 Administer SNMP MGR

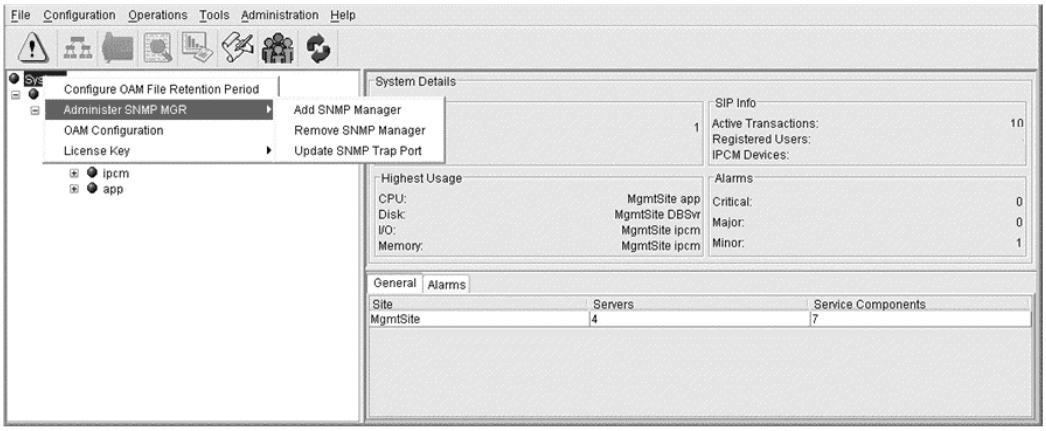


Figure 3.104 SNM MGR Config Add

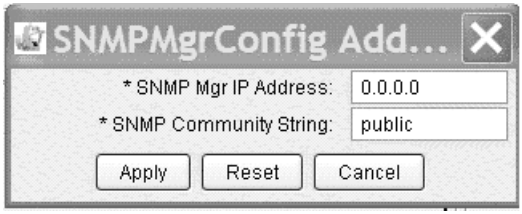
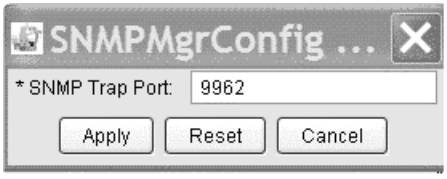


Figure 3.105 SNMP MGR Config



OAM Configuration

In the same menu we are going over in this section, the third options down on the menu shown in Figure 3.106 is the OAM configuration. When this is selected a menu will appear, as show in Figure 3.107. This will allow the administrator to change the options and times for the files used on the system. The settings are default and once again the administrator many change these. The author recommends that these be left at a default state.

Figure 3.106 System Tree Options

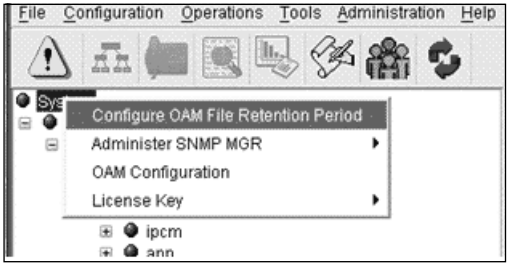
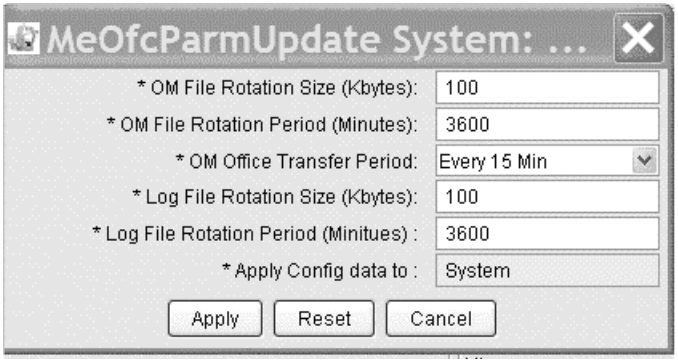


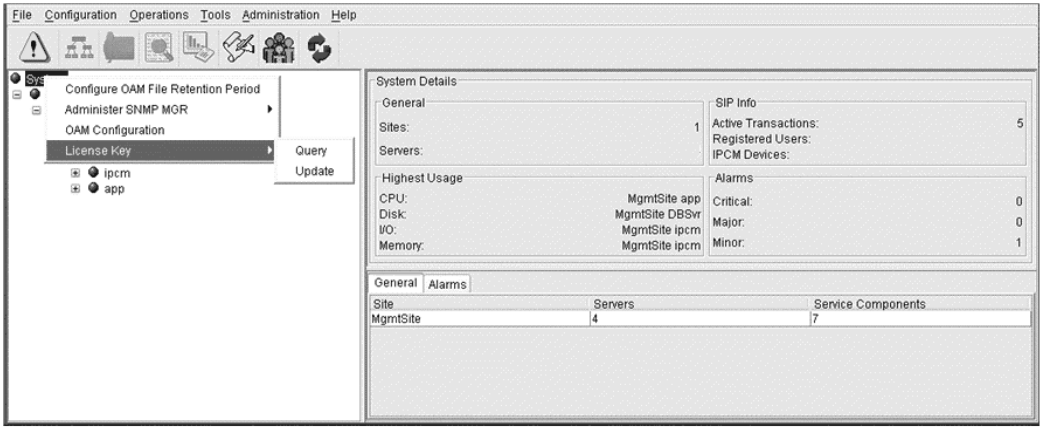
Figure 3.107 OAM Configuration



License Key

The last option as shown in the menu below in Figure 3.108 is for the license key. The figures in this section will show information on the license that has been uploaded to your system. It will provide the administrator with a way to gauge when they need to add more licenses, where to add licenses for new servers or equipment added to the system. In Figure 3.108 we have chose the first options in the sub menu for query. When query is selected it will produce a menu such as the one in Figure 3.109. There are five tabs for the administrator to query.

Figure 3.108 System Tree Options



Designing & Planning…

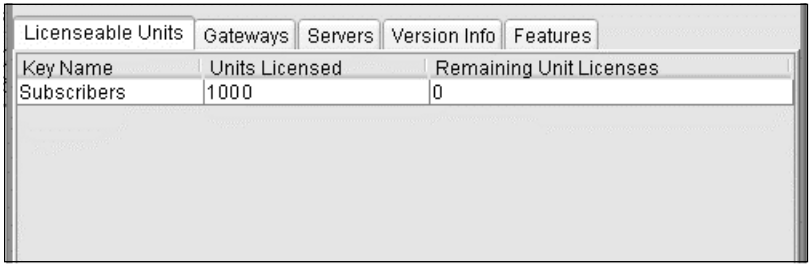
Adding Users

As an update we have seen where Nortel has sent the wrong license or the licenses and keys codes are not correct on the Web site when going to download keys. Nortel also uses this area to plan for future upgrades. There is nothing worse when going to add a user and you have run out of licenses for that user or even a new server.

Query

The first tab in Figure 3.109 is for licensable units allowed on the system. Each account created on the system for use is a subscriber on the system. In our system we have added a license for 100 subscribers and have put all 100 onto the system. This is why there are no licenses units remaining in the field. If there were units left they would be displayed in the system.

Figure 3.109 Licensable Units

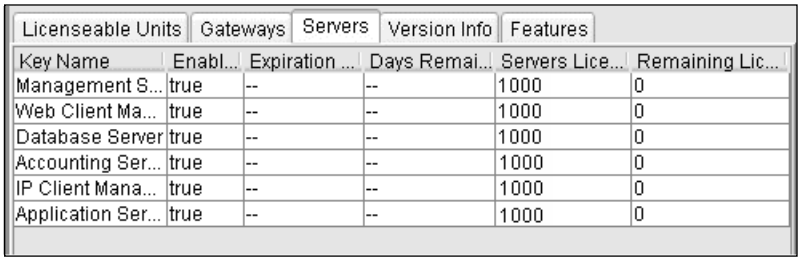


Gateway and server tabs in Figures 3.110 and 3.111 are the next two tabs we will talk about. When adding a gateway trunk to your system you will need to have a license for this, below you can see that a license has been added for this trunk. One this to remember to look at is that the enable is set to true, if it is set to false the license is not working correctly and needs to be redone in the system. In the servers tab you can see we have all of the servers that have been added to our system. For our display we have taken off all duplicate server licenses so that you can see we have a 1 in the server license field.

Now if we had purchased more than one license for our system but we were not using it on a server it would be show in the remaining license field on the far right. As you can see also all of our enable fields are set to true which means they are working correctly.

Figure 3.110 Gateways

Figure 3.111 Servers



Displayed in Figure 3.112 is the tab for the version info. This will display the information about your key, product name, version id, the generation date and who generated the keys for the system. This is always good to know in case you have to follow up on the key added to the system. In Figure 3.113 we can see we have the last tab in the menu and these are the features you have purchased for your system. Each feature that you would like to use on your system needs to have licenses purchased for it.

In our system we have added licenses for our display. You can see that they are all set to true, which means they are working and the mount of unit licenses we have for each key name. Also on this figure we did not add all of the units to the system so that you could see that we have remaining units left in Figure 3.113.

Figure 3.112 Version Info

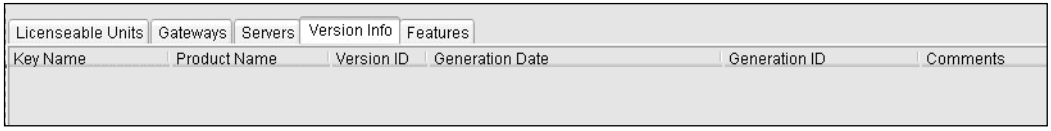
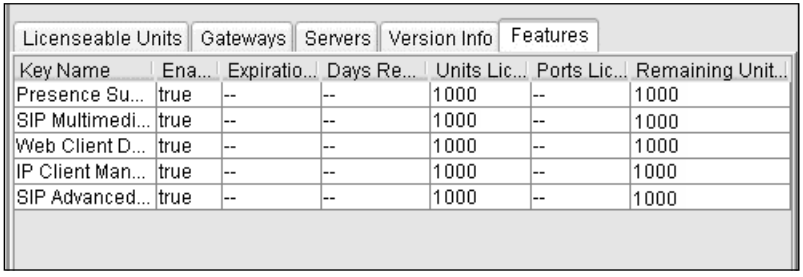


Figure 3.113 Features

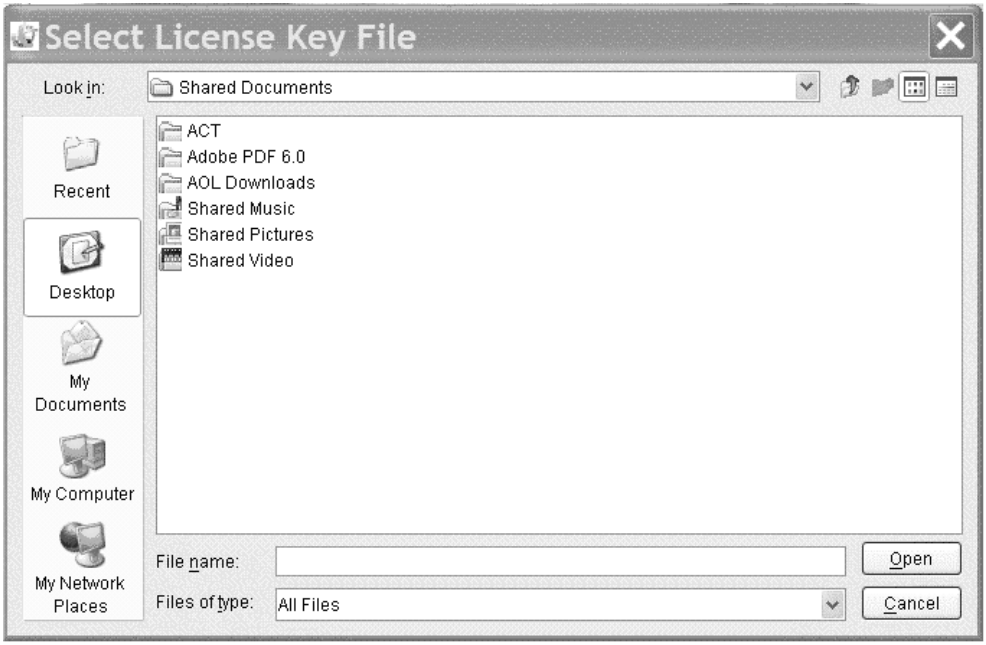


Update

When adding a key or updating a license, you will need to select the update options in the menu, as displayed in Figure 3.108. After you select this option from the menu, it will display the select license key file box, as shown in Figure 3.114. This is where you will select the key file that you have downloaded from the Nortel Key Web site. When you receive you license packet from Nortel all of your licenses will be separated.

The administrator will need to log on to the Nortel Web site, register, and then use the licenses given to receive your key codes off of the secure Web site. Then you will take those and add them to your system once you have downloaded and save them to you computer. It is not recommended that you try to write down the whole code; it is much safer to highlight the code then copy/paste into a notepad.

Figure 3.114 Select License Key File



Summary

The MCP Client is a vital part of the MCS 5100 system and proper configuration and training need to be taken into account when installing the system. As you can see by the size of this chapter there is a great deal to learn about the MCP Client and what it can and cannot do within your system. This chapter could have been well over three times the size it is now if we went into every kind of different configuration that could be used on the system. The configuration we used in our chapter will provide any user with the necessary information and options needed to get your system up and running.

Any changes in the MCP Client can be service impacting to the system and users; this is one thing to be very aware of when using the MCP Client. It is suggested that only users who have had the proper training and have had time using the MCP Client should be installing, administrating, or troubleshooting the system. This will provide your users and company with a system that will be well taken care of and provide great service.

Solutions Fast Track

Installing MCP Client

- ☑ When installing the MCP Client onto a computer, it is better to have more RAM. This is due to the amount of windows that you could have open at one time.
- ☑ The MCP Client can be installed on multiple computers since it pulls information from the MCS 5100 to the MCP Client.
- ☑ The correct version of MCP Client needs to be used for the correct version of software or firmware on the MCS 5100.

Configuration of MCP Client

- ☑ Remember what the differences are between your site, server, component, and services; this will help eliminate issues in configuration or troubleshooting.

- ☑ If you right-click certain items in the system tree a new menu will display for your use on those areas.
- ☑ To make changes you need to lock the component and then unlock the component to put it back into service.

IPCM Device Maintenance

- ☑ Before using the GUI, create a filter or multiple filters to pull information on the IP Phones.
- ☑ Once IP Phones have been selected and moved to the device detail, right-click on the IP Phone to produce a menu of options to be used.
- ☑ This is the only area in the MCP Client where you can perform services on the IP Phones at this level.

Alarm Browser

- ☑ You can select the site, server, or component that you want to see alarms on at that time. The higher you go into the system tree in the selections of alarms the more alarms you will see.
- ☑ After opening the alarm browser select the auto refresh to update the browser.
- ☑ Alarms can be deleted only if they have been cleared.

System Options

- ☑ System files and log options may be changed in this area along with the IP address and community string for the systems SNMP manager.
- ☑ Licenses and key codes are displayed for the uses of the administrator.
- ☑ All licenses and key codes for servers, gateway trunks and systems features are added and updated through the menus in these sections.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Is there a limit to the number of MCP Clients used on a given MCS 5100?

A: No there is not. But you do not want ten people on ten different computers making changes all at the same time.

Q: If there a Web version of this client to use?

A: No, this client comes in only one version at this time from Nortel.

Q: If I have more than one MCS 5100 in my network can I use just one MCP Client for both?

A: It can be done if it is a redundant system; if it is a separate system you will need to use a different client due to the different IP addresses that will be used for each system.

Q: When I am installing new software to my MCS 5100, do I need to install a new MCP Client?

A: You should check with your Nortel SE to check if your current version will work with the new software. You can always try to connect; if it does not work you need a new version of the MCP Client.

Q: Is there a time out feature on the MCP Client if left opened?

A: No, no default time out is set. The MCP Client can be left open so that you can use the alarm browser.

Q: Can I load new software to IP Phones from the Client?

A: Yes, you may select certain IP Phones to load software in the MCP Client, or you may push it out to IP Phones over the IPCM Device Maintenance GUI.

Q: Is there a menu I should look at when I open the MCP Client to get an overall look at the system?

A: Yes, select your site or severs and look at the details screen to the left for disk usage, alarms, and any other problems that could be taking place at that time.

Chapter 4

Provisioning Client

Solutions in this chapter:

- **Administration**
- **Domains**
- **Devices**
- **Gateways**
- **IPCM Cluster**
- **Voice Mail**
- **Services**
- **Media Portal**
- **System**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

The Provisioning Client is the heart of the MCS 5100 administration and where administrators will spend the majority of their time. This is a Web-based GUI used off the IPCM Server within the MCS 5100. The client itself is used to administer rolls and privileges, manage users and devices, define and update service packages for domains, and provision voice-mail servers—along with E911—for the system. It is also where all call routes to SIP devices, such as IP phones, gateways and network routing servers are provisioned.

In this chapter, we discuss the Provisioning Client and all the options necessary to configure the MCS 5100. We show how to add administrators and what they can do on the system. We also show how and where to add users, as well as options available to them via the package assigned by the administrator. You will learn how to give users different routes out of the MCS 5100 system for SIP gateways, network routing services, and more.

We also explore adding voice mail to your users and configuring IPCM clusters, as well as adding and subtracting users from a domain or subdomain, which is helpful to service providers. In the Provisioning Client, the administrator also has the ability to add a foreign domain to the system. In Table 4.1, we have put together a small table showing the steps needed for configuration of the Provisioning Client. In this chapter, we are not following this list, but rather starting at the top of the tree and work our way down. For first-time users this seems more helpful.

Table 4.1 Step-by-Step Provisioning Configuration

Step	Task
Define roles and rights and use to create new Administrators	Add role and assign rights Add Administrator
Define new domain or domains	Add domain Add subdomain
Define service parameters and assign to domain	Define service parameters Assign services to domain

Continued

Table 4.1 continued Step-by-Step Provisioning Configuration

Step	Task
Define domain service package	Create service package Assign service package to domain and subdomain. Assign services to subdomain
Define voice mail server and assign to domain	Add voice-mail server and assign to domain
Add IPCM and assign to domain	Add IPCM Assign IPCM to domain
Add domain status reason	Add status reason for domain
Add users to domain	Add users Add users to subdomain Add the i2002 and i2004 devices
If not auto provisioning, assign devices to domain	Add device Assign users to device
Define gateway, gateway routes, and trunk groups	Add gateway Add gateway route Add trunk group
Define domain telephony routes and parameters	Add routing Class of Service Add telephony routes: Private, SIP and Gateway Change routing parameters Add route list
Define banned users for domain	Ban user if needed

Administration

The first section of this chapter deals with administration or the *admin tab* in the provisioning tree. First, you need to know how to get into the provisioning client on the MCS 5100.

In a supported Web browser, type the IP address of the IPCM and add a /prov at the end of the Web address. This will produce the screen shown in Figure 4.1. Insert the same user name and password used in the last chapter

for the MCP Client. Once you have done this, click the **Log In Now** button on the bottom right. If you have logged on correctly, you will see a screen like the one in Figure 4.2.

Figure 4.1 Client Login Page

Figure 4.2 shows the layout of the Provisioning Client in the Web-based GUI. To the right is a provisioning tree that allows the administrator to drill down into the topics listed.

Figure 4.2 Welcome Page

NOTE

The author cannot stress enough to learn where everything is located within the provisioning client, what it does, and how it affects other items. Administrators will spend about 90 percent of their time in this GUI, and it is very important to learn as much as possible before putting live users on the system.

Before adding an administrator, you need to understand the roles of the three administrators and what they can do. In Table 4.2, we created a Provisioning Role example showing the three different administrators; user, device, and system. The system administrator is the only one preloaded into the system, and it cannot be deleted. It is also the highest level of administrator in the system. Giving proper roles to the correct people will help in implementation and troubleshooting of the system down the road. Giving incorrect roles can cause many problems, including if something is configured incorrectly or deleted by an administrator without proper training.

Table 4.2 Provisioning Role Examples

Provisioning Role Example	Rights Given	Allowed Tasks
User administrator	User management with read, write, and delete access Domain management with read access only	Can view domain details and add, delete, or modify users. Does not have access to other parts of the system; for example voice mail, service packages, and so forth.
Device administrator	Domain management with read access Device management with read, write, and delete access	Cannot add or modify users Allowed to add, modify, or delete devices

Continued

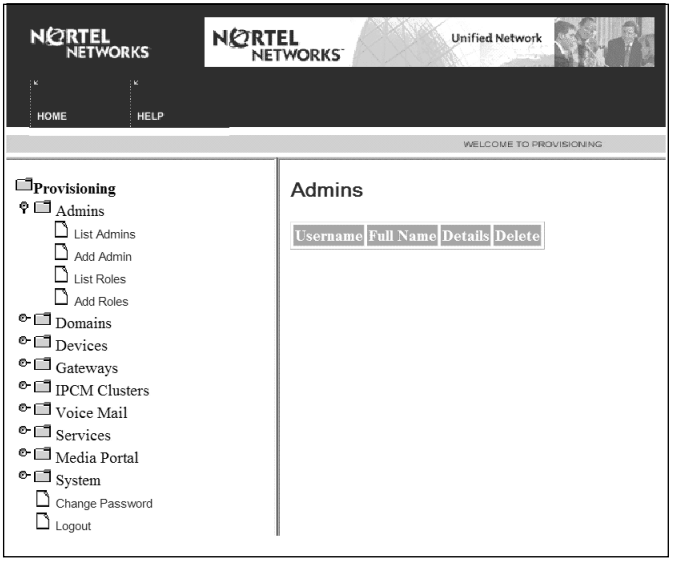
Table 4.2 continued Provisioning Role Examples

Provisioning Role Example	Rights Given	Allowed Tasks
System administrator	Full domain access	Can see all domains, regardless of who created the domain, or the list of domains provisioned against the administrator

List Admins

Next, we look at how to add administrators to the Provisioning Client. In Figure 4.3, we have clicked the **Admins** tab in the provisioning tree to the left of the GUI. There are four options under this tab—List Admins, Add Admins, List Roles and Add Roles. Figure 4.3 shows we have no admins listed in our system.

Figure 4.3 Admins



One point that will help when configuring new admins is that you should first make a chart of who will be doing what and who is responsible for what

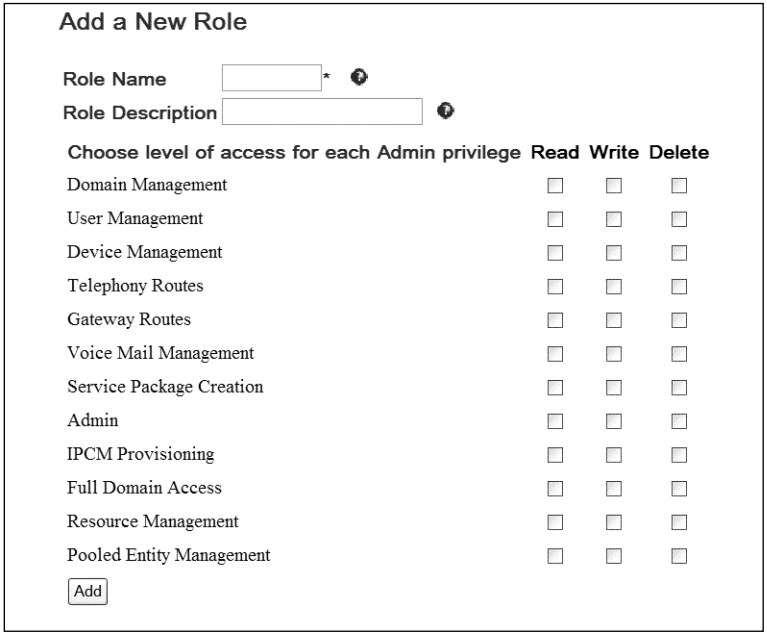
on the system. This will help you in the next part, which is adding the admin roles. Before you add a user, you need to add the roles of the users that will be on the system. You can add the administrators first, but you will have to go back and add the roles later.

Add Roles

In Figure 4.4, you can see that we have selected the tab for Add Roles. This is the section where your planning will pay off if you have done that for your new administrators. Based on rolls and privileges you want to assign to each administrator, you will fill out the screen in Figure 4.4. First insert a roles name and then assign a roles description in the screen. After that is complete, you may use the example we created in Table 4.1 or create your own names and based roles.

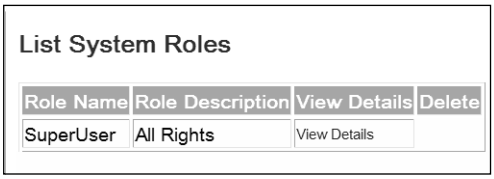
Remember when filling the levels of access out for each administrator to give them the proper read or write roles for the job they will be doing. You would not want to give write access to someone who has no training on the system. Once you have inserted the correct information, press the **Add** button, shown at the bottom right of Figure 4.4.

Figure 4.4 Add a New Role



After you have added the system roles, you will have a list similar to the one shown in Figure 4.5, List System Roles. This list shows the two user roles names we have added. You may view the information of these roles by selecting **View Details**. Once you have added your roles, you are ready to add your admins to the system. These users are the same admins we looked at earlier in this chapter.

Figure 4.5 List System Roles



Add Admins

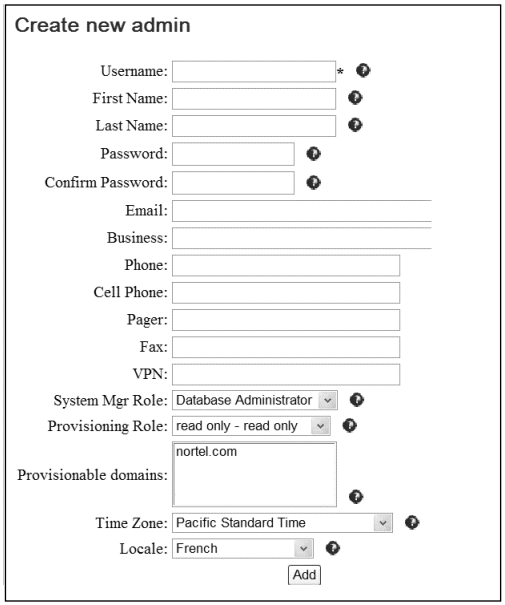
In the Figure 4.6, you can see the screen where you will create your different admin accounts. The first area you need to fill in is **Username**. The user will log in with the name and password you assign them on this page. You may fill out the other information for each user down to the System Mgr Role. This drop-down box shows the roles added in Figure 4.6. Choose the role for this admin System Mgr Role drop-down box.

Next, as shown in Figure 4.6, select if they have read or write access to the system in the Provisioning Role box, and then, choose the domain they can make changes to in Provisionable Domains. Finally, select the correct time zone and language. Click the **Add** button, and the admin is added to the system.

Domains

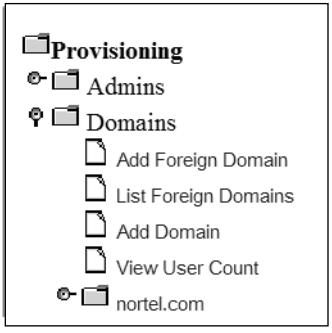
In Chapter Two, we discussed what domains were, as well as the architecture around the domain structure used in MCS 5100. Now it is time to use that information—the architectural plan you have laid out to add domains to the system. In Figure 4.7, we have moved down the system tree from Admins to Domains. Here are four different areas for us to look at: Add Foreign Domain, List Foreign Domains, Add Domain and View User Count.

Figure 4.6 Create New Admin



A foreign domain is one that is outside the IP addressing scheme of the MCS 5100. Only use this option to, maybe, connect endpoints to the MCS 5100 over such areas as a SIP trunk. In the Add Domain section, you will add your company domain to the system. For testing, in Figure 4.7, it is set to nortel.com. Planning is an essential part of the process and helps you later when you add other domains or subdomains.

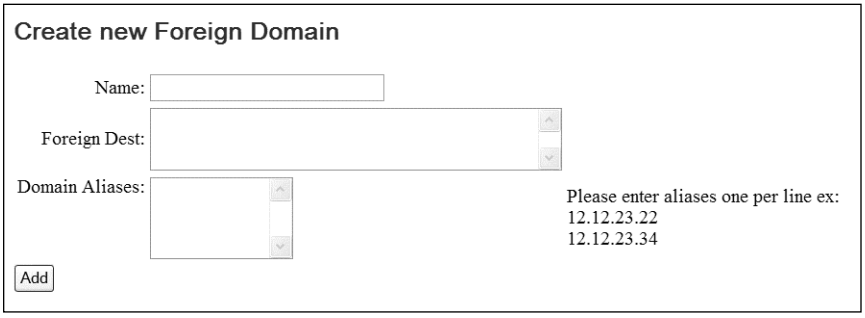
Figure 4.7 Domains



Add and List Foreign Domains

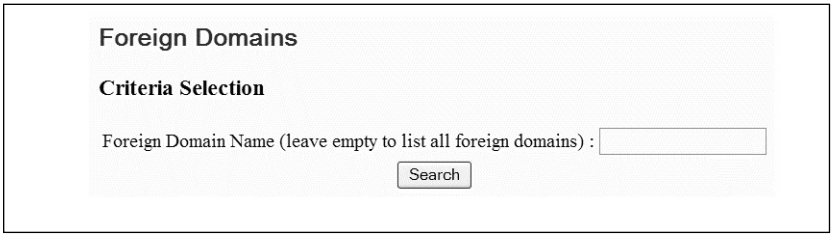
Figure 4.8 shows the first place where you can add a foreign domain. Although it says **Create New Foreign Domain**, they are both the same, so do not let this confuse you. Here you will add a name, foreign destination, and domain aliases. After you have added these entities, press **Add** to create your new foreign domains.

Figure 4.8 Create New Foreign Domain



Once you have added your foreign domains, you may go to the next area, Foreign Domains, as is shown in Figure 4.9. Input the name of the foreign domain and do a search, or just click, the Search button, and it will list all of the foreign domains.

Figure 4.9 Foreign Domains



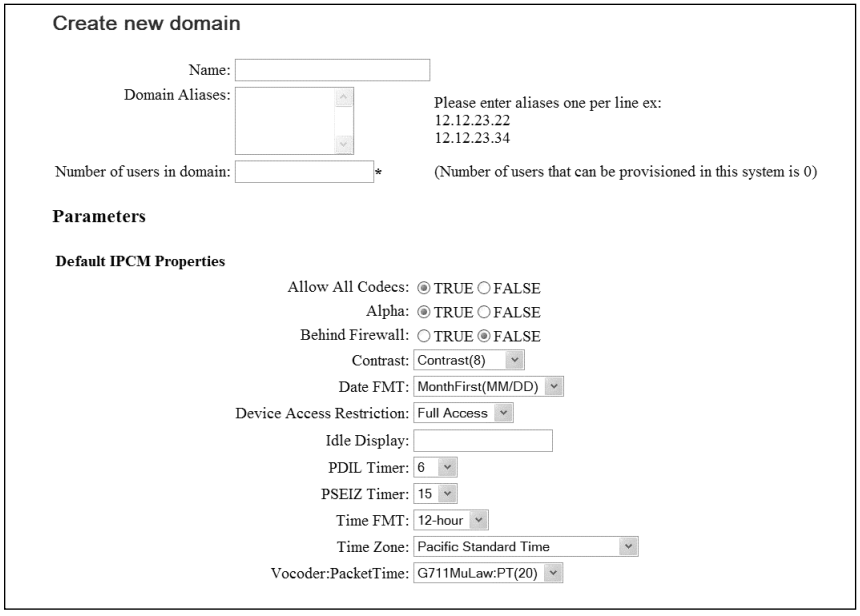
Add Domains

When adding a new domain, which will be your company domain, fill in Create New Domain, as shown in Figures 4.10 and 4.11. Here you will assign your domain a name, such as Nortel.com, and add the domain aliases for the

system. Then you will need to input the number of users in the domain and this should correspond to the licenses you have received and input into the MCP Client from the last chapter. Be sure of this number before inputting information into the section. Otherwise, if filled in incorrectly, this can cause you problems down the road.

For the other fields that need to be completed, we have created a chart showing you the name, information, defaults, and values for use in the properties (see Figures 4.10 and 4.11). This chart is handy when filling this in for the first time, or when you have to troubleshoot a problem in your system. I suggest you copy or print the chart and keep it handy.

Figure 4.10 Creating a New Domain: IPCM Properties



Tables 4.3 through 4.6 represent the information necessary to choose correct options and complete your system in Figures 4.10 and 4.11. Please make sure you read and understand the descriptions, defaults, and values allowed for those figures. These include Tables 4.3 for Default ICPM Properties, Table 4.4 for Default Meet Me Properties, Table 4.5 for Default UC Properties, and Table 4.6 for Miscellaneous. After you have added all your information, click the **Add** button as shown at the bottom of Figure 4.11.

Figure 4.11 Creating a New Domain: Meet Me, UC, and Micellaneous Properties

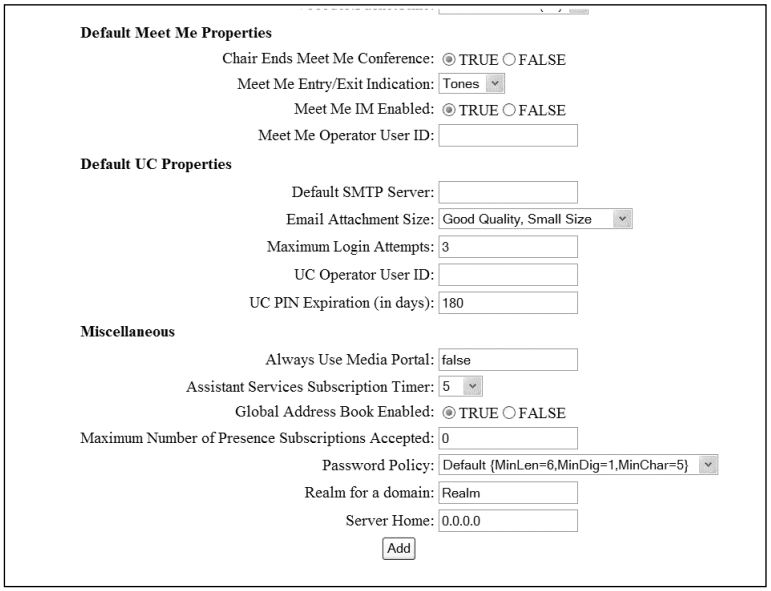


Table 4.3 Default IPCM Properties

Parameter	Range	Default	Description
Default IPCM Properties			
Allow All Codecs	True/False	FALSE	Allow all codecs (true) or only the selected codec (false). See the Vocoder parameter.
Alpha	True/False	FALSE	Enables alphanumeric dialing as the default dialing style. If False, the i2002 or i2004 Internet Telephone defaults dialing style to numeric.
Behind Firewall	True/False	True	Indicates whether there is a firewall between the IPCM and the i2002 or i2004 Internet Telephone

Table 4.3 continued Default IPCM Properties

Parameter	Range	Default	Description
Contrast	0 - 15;	8	The i2002 and i2004 Internet Telephone display contrast settings.
Date FMT	MonthFirst MM/DDFirst MonthDD/MM	2	2 standard, 3 inverse.
Device Access Restriction	Full Access Hands Free Disabled Restricted	na	Provides the ability to restrict functionality of an i2002 or i2004 Internet Telephone respective to the subscribed users who are registered on the device. If multiple people are logged in, they can all receive a call on that phone and can place calls from their account by selecting their line.
Idle Display	Max to 30 characters	na	Idle telephone display heading
PDIL Timer		4	Interdigit time-out (seconds)
PSEIZ Timer		15	Time-out for first dialed digit.
Time FMT	12 hours, French 24 hours	0	The time format of the proxy used as default for the i2002 or i2004
Time Zone	Max to 30 characters	na	Time zone
Vocoder: PacketTime	Select from drop down list: 0 – G711 Mu-law 4 – G723\6.3kbps 8 – G711\A-law 10 – L16 18 – G729A	na	Default Codec Setting.

Table 4.4 Default Meet Me Properties

Parameter	Range	Default	Description
Default Meet Me Properties			
Chair Ends Meet Me Conference	True/False	True	When set to True, the conference will end when the chairperson exits the conference. There are two places to set the Chair Ends Meet Me Conference property: At the root domain/subdomain level, you can set the default value for all users for that domain/subdomain. If you don't set it for an individual user, then each user receives the value set at its immediate domain or subdomain. You can change it for individual users using the Provisioning Client (Meet Me Properties link) or using the Personal Agent.
Meet Me Entry/Exit Indication	Tones/None	True	When set to True, a tone is heard whenever a person enters or exits the conference.
Meet Me IM Enabled	True/False	True	When set to True, IM displays each participant as they enter or exit the conference.
Meet Me Operator User ID	NA	NA	NA

Table 4.5 Default UC Properties

Parameter	Range	Default	Description
Default UC Properties			
Default SMTP Server	NA	NA	The hostname or IP address of the SMTP server that the Unified Communications service will use when sending e-mail
E-mail Attachment Size	NA	NA	This is how the Unified Communications service encodes the voice mail message attachment included in e-mail.
Maximum Login Attempts	NA	NA	The number of incorrect login attempts before the Unified Communications service locks the user's mailbox
UC Operator User ID	NA	NA	The username of the Unified Communications service operator. Example: uc_operator
UC PIN Expiration	NA	NA	The number of days that a user's mailbox password is valid

Table 4.6 Miscellaneous

Parameter	Range	Default	Description
Miscellaneous			
Always Use Media Portal	True/False	FALSE	This directs the Application Server to use the RTP Media Portal when set to True. The purpose is to use the RTP Media Portal function in dealing with special SIP scenarios. For example, a domain that straddles multiple sites contains users who do not have IP connectivity between them due to firewalls

Continued

Table 4.6 continued Miscellaneous

Parameter	Range	Default	Description
			at a different site. This domain requires the *Always Use Media Portal* to be set to *True* to negotiate between firewalls to set up SIP sessions.
Assistant Services	1 - 15	5 minutes	Specifies the amount of time Subscription Timer minutes that a client running as an Assistant Console will wait before re-subscribing to the services needed for an Assistant to provide assistant support for another user.
Maximum Number of Presence Subscriptions Accepted	0 - 100	0	Maximum number of inbound subscriptions to any given user in this domain. The Personal Agent, the Multimedia PC Client, and the Multimedia Web Client will use this limit when allowing a particular username to be added to a subscriber's list of friends.
Password Policy	Select from drop-down list	Default	Specifies the subscriber password
Server Home	Up to 60 characters	NA	Specifies the SIP Application Module that will host the users in this domain. This is used in an N+1 environment. All SIP Application Modules that are not the home SIP Application Module will forward requests for users in this domain to the specified address.

Continued

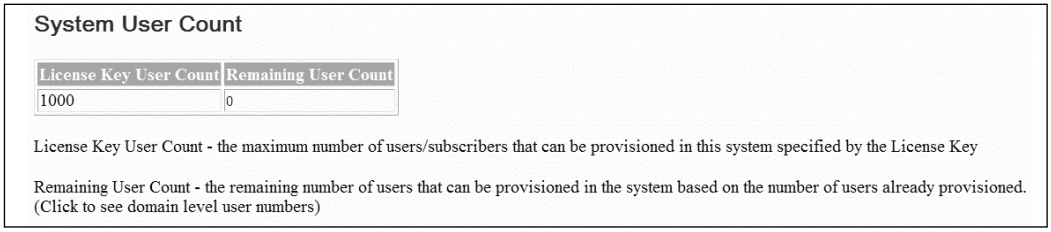
Table 4.6 continued Miscellaneous

Parameter	Range	Default	Description
Realm for a Domain	Up to 120 characters	Realm	Identifies the domain for subscribers when they are being authenticated. Subscribers may register in multiple domains. When they are required to enter a password during authentication, they need to know which domain it is so that they can enter the appropriate password.

View User Count

The last area you need to be familiar with under the Domain section of the tree is the View User Count shown in Figure 4.12. Here you may look at how many users you have on your system and how many users you have remaining in your count. As you can see in Figure 4.12, we have a license key for 100 users, and we have put all 100 users on the system to show a remaining count of 0.

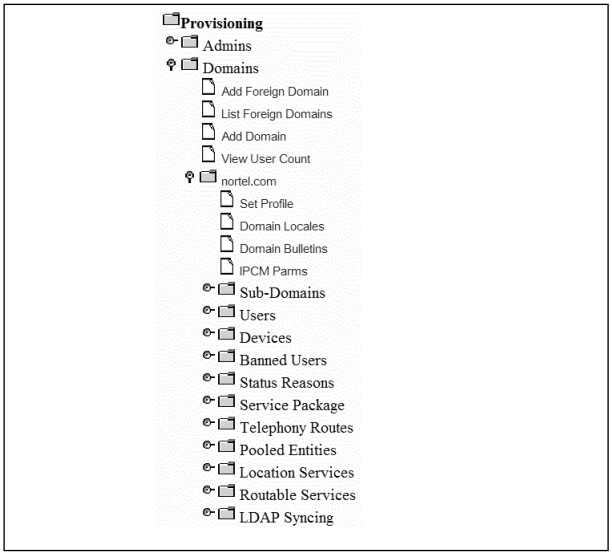
Figure 4.12 View User Count



Nortel.com

Now that we have added our domain to the system as nortel.com, we can now go in and look at what is saved. As you can see in the tree (Figure 4.13), many areas in the tree under Nortel.com need to be configured. We will go through and look at each area that needs to be configured. The darker folders you see in the tree mean there is more information to open; the blank-paper-like areas are just single areas that can clicked.

Figure 4.13 Nortel.com Domain



When you click **Nortel.com** you will get a screen showing you the details for the Nortel.com domain shown in Figures 4.14 and 4.15. In this area, you may make changes to the root domain. Remember to refer to Tables 4.2 to 4.5 for further explanation for each area.

Figure 4.14 Details for Domain

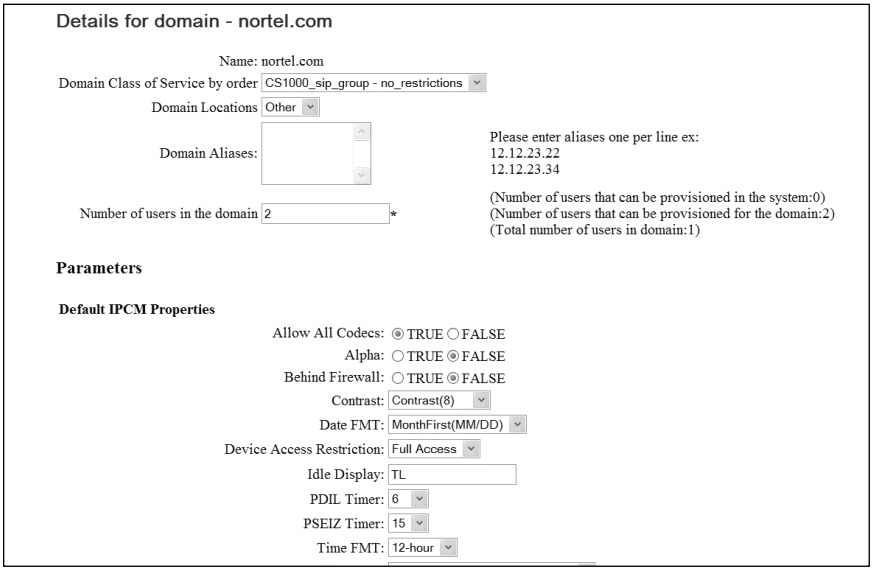
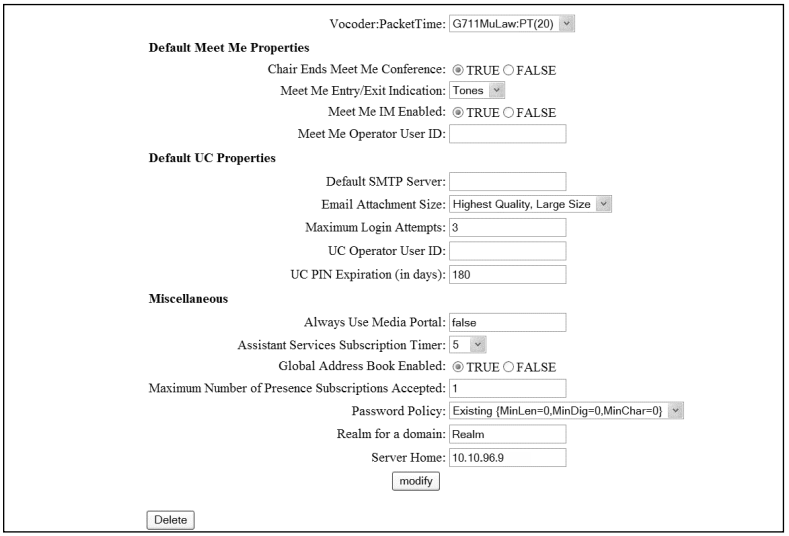


Figure 4.15 Details for Domain



Set Profile and Domain Locale

In the first area under Nortel.com, set your profile for the domain. As shown in Figure 4.16, enter a profile name. The domain and profile shown in Figure 4.16 is Nortel.com. Be sure and **Save**.

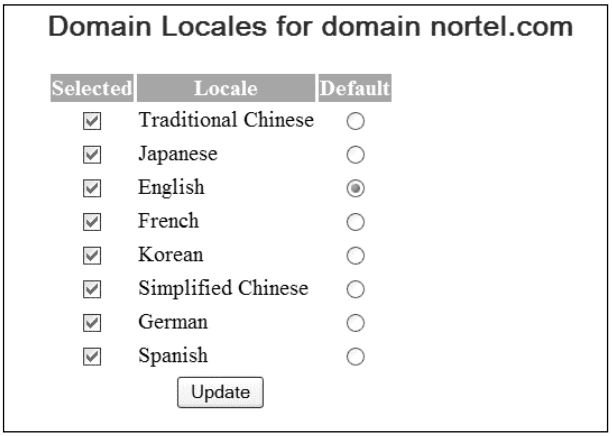
Figure 4.16 Set Profile

In Figure 4.17, select what you will allow from each locale. The word locale here means language—what you have selected and loaded into the system. You may also select a default language that everyone will use unless they change it on their IP Phone or PC Client.

Select all of the languages that you need for your system and then a default language. Hit **Update** at the bottom of the screen. You may at anytime come back into your domain and add, remove, or change the default

locale for your domain. Be aware that this is the root level domain when making changes.

Figure 4.17 Domain Locale



Domain Bulletins and IPCM

The next section to fill out is the domain bulletins (Figure 4.18) for the Nortel.com domain. This is a message that will be displayed on IP Phones that are connected to the system and are registered. Once you put in a message, you hit **Update** and add it to the system. You may also add more than one message, and move the order around for which message or bulletin for which to display first, second, third, or last. To remove a message, select the message, hit the **Remove** button, and then select **Update**.

The messages do not update instantly and they do not remove instantly. There is a time delay for these on the system. So be sure you know what you are adding to the system.

Configure the IPCM Parameters for Nortel.com as shown in Figure 4.19. To understand what changes can be made or added to the IPCM parameters, we have added Table 4.7 with information on what each area means and what values are allowed.

Figure 4.18 Domain Bulletins

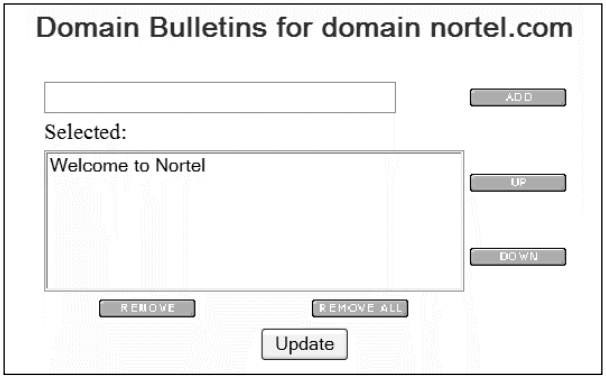
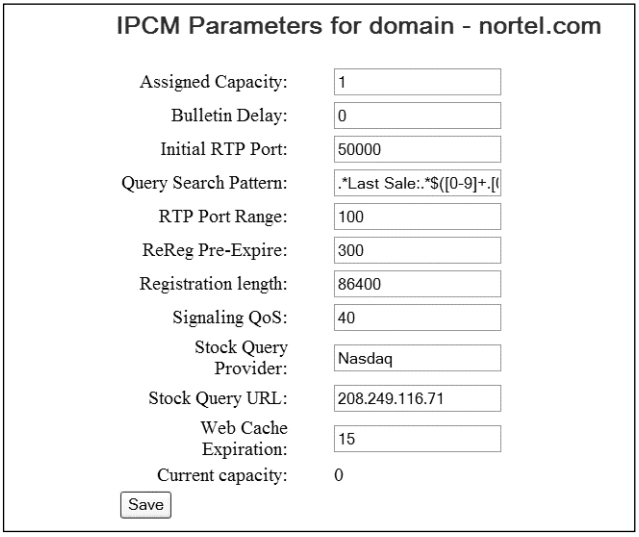


Figure 4.19 IPCM Parameters for Domain



NOTE

When you are adding the stock query URL to the IPCM parameters, the IPCM server itself may need to be reset for the changes to take effect. This is what we found on our system when adding or changing the value. The Nortel documentation does not mentioned this, so we are making our readers aware of the it.

Table 4.7 IPCM Parameter Options

Parameter	Range	Default	Description
Assigned Capacity	NA	0 for new domains; 200 for existing domains	The number of devices allowed provision for the domain
Bulletin Delay	0 – 525,600	10	The amount of time that the i2004 IDLE Display is displayed A value of 0 will cause Bulletins to never be sent to the i2004 Internet Telephone.
Initial RTP Port	0-65,535	50,000	The Initial port from which media is sent Ports in initial RTP Port through the next 'RTP Port Range' ports must be open on the network firewall.
Query Search Pattern	NA	NA	The regular query describing search pattern for stock query
RTP Port Range	2-200	100	The number of ports that the IPCM devices cycle through (using Initial RPT Port as the starting point on the system) when allocating media ports
ReReg Pre-Expire	Oct-00	300	The time interval in seconds prior to registration expiration when the IPCM starts attempting to renew the registration
Registration Length	3,600-86,400	86,400	Registration and subscription time in seconds
Signaling QoS	0-63	40	QoS DiffServ values used for Signaling Packets
Stock Query Provider	NASDAQ	NA	String describing provider of stock query info. Only NASDAQ is currently supported.

Continued

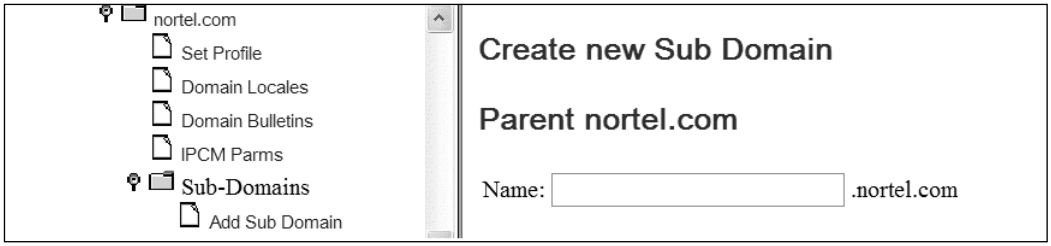
Table 4.7 continued IPCM Parameter Options

Parameter	Range	Default	Description
Stock Query URL	NA	NA	IP Address for NASDAQ
Web Cache Expiration	Jan-60	15	Length of time (in minutes) the IPCM will cache stock query information
Current Capacity	NA	NA	This is a display-only field of the number of devices currently provisioned for this domain. The Assigned Capacity parameter minus the Current Capacity parameter equals how many more devices you can provision in this domain.

Subdomains

In Chapter Two, we discussed what subdomains would be used for and why you would want to use them. In Figure 4.20, we selected the subdomain area under Nortel.com in the system tree. That produced the area to the right where you can add a new subdomain. As you can see the root domain of Nortel.com is already there and cannot be removed. All that needs to be added is a name for your subdomain in the space. Do not add a period at the end since it is already added to the right of the name area.

Figure 4.20 Create New Subdomain



Users

In Figure 4.21, we selected **Domains** and **Users** in the system tree. Add User, List users, List Aliases, List Converged Aliases, and Move Users are displayed for use. In these areas, you will need to configure each user who will have an IP phone or a PC Client for addition to this area.

All IP phones have to be logged in with a user account and password on the MCS 5100; this is unlike a CS1000 that can be set to a phone number or extension in the set up of the IP Phone based on a terminal number.

Configuring & Implementing…

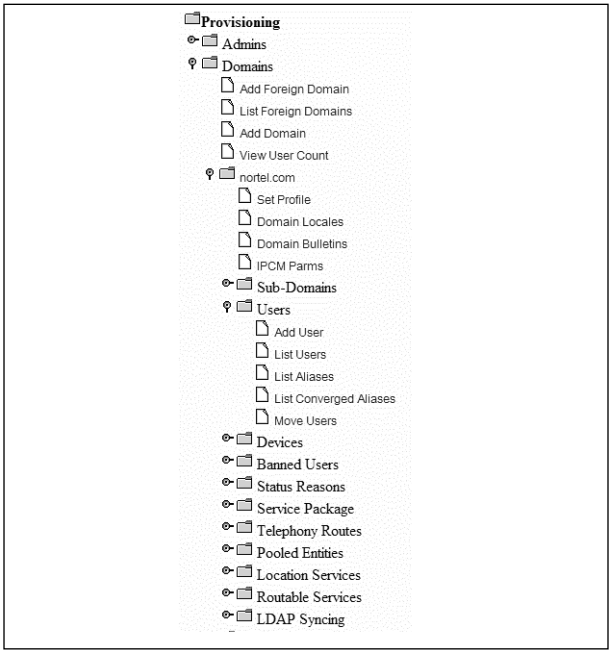
The Initial Configuration of the MCS 5100

Starting with this section we have decided to work this chapter from the top of the system tree to the bottom. Before you can configure certain areas in the user profile, you will have to configure service packages, telephone routes, pooled entries, locations services and routable services. When you configure the MCS 5100 for the first time, you can add your user, but you will have to go back and update areas after you configure the rest of the system in this chapter.

Users

Now it is time to configure a user in the fields shown in Figure 4.22. The user name is the name you decide to give user on the system, such as first initial, last name, or even last name and first initial. It can be what you want it to be, but if you have a Novel network, unlike the Microsoft networks around now, you could get some weird user names. It is always good to give a user name that will people will remember. This will make life easier on your network users if you do this right the first time.

Figure 4.21 Users



Next fill in the user's first and last name plus a temporary password. You will configure the drop-down box for the service package later in this chapter. This must be done before adding a user. In **Aliases,** insert the phone number or extension you will give to this user. Most of the time, you will put the 10-digit phone number for the aliases. You may insert more than one phone number or extension to this box.

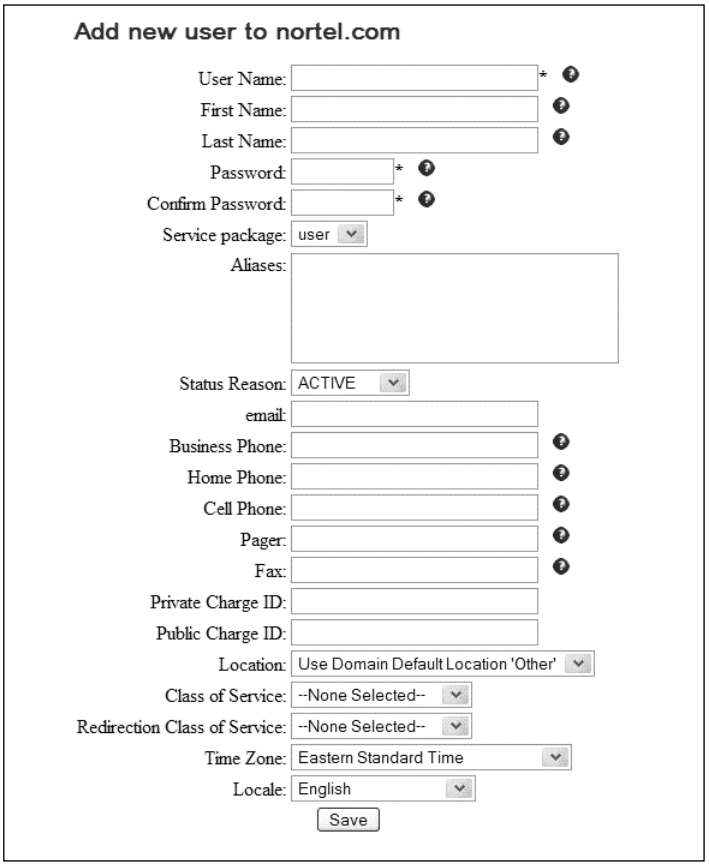
Set the next box to active for the user, and allow the user to fill out the personal boxes down through the fax number. This will save much time for the administrator. The boxes for private and public charge IDs are for users' aliases you listed, so just input their 10-digit phone number to make it easier. Next is the location drop- down box. By now, you have added your locations to the system, so choose the location for the user. You may also leave this at the default, and the users can pick their location each time they log into the IP phone or PC client.

In the **Class of Service** drop-down box, as well as the **Redirection Class of Service** , you need to choose the routes these users will use. Most of the time, you will have two classes of service for users to select: These are

primary and backup routes out of the system to the public switched telephone network (PSTN). In some small systems, you might only have one class of service or route, in which case you will use the same route for both class of services. It is best to try to have at least two for the system, even if you have to run the second class of service from a different SIP endpoint for connectivity.

The last item in adding a new user in Figure 4.22 is configuring the time zone and locale. To insure that you receive the proper alarms and messages from user, you need to select the correct time zone. Locale refers to the language for the system. Select from the languages listed in the drop-down box.

Figure 4.22 Add New User



Search User, Aliases, Converged Aliases and Move User in Domain

Figures 4.23 through 4.26 use information you used in Figure 4.21. The first three figures in this section search for users under the user area. Figure 4.23 gives you the option to insert the user name or alias in the blank area and press the **Search** button to produce your results.

Figure 4.23 Search Usernames

Figure 4.24 gives the same option as Figure 4.23, except you are searching for aliases.

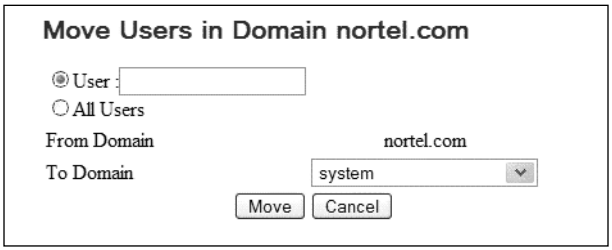
Figure 4.24 Search Aliases

Figure 4.25 gives you the option of searching for converged aliases. Search by entering the alias name and then press the Search button.

Finally, Figure 4.26 allows you to move users from one domain to another. Use this option when users move to a different location.

Figure 4.25 Search Converged Aliases

Figure 4.26 Move Users in Domain



User List

In Figure 4.27, we selected a user added to the domain and used the search feature to produce the results shown. This is what it would look like if you did a search by user name within the domain. It gives you some very basic information on the user, but you may click **Details** to find more information. If you need to delete a user from the domain, it is easy to accomplish. If you hit **Delete** by accident, don't worry. To delete a user from the domain, you must insert the admin password after hitting **Delete**.

Also in Figure 4.27, on the far right, notice *Logout Contact*. This option allows you to log the user out from the PC client and IP phone. This is good to know in case someone forgets to log out, or if you have some abuse on the system.

Figure 4.27 User List

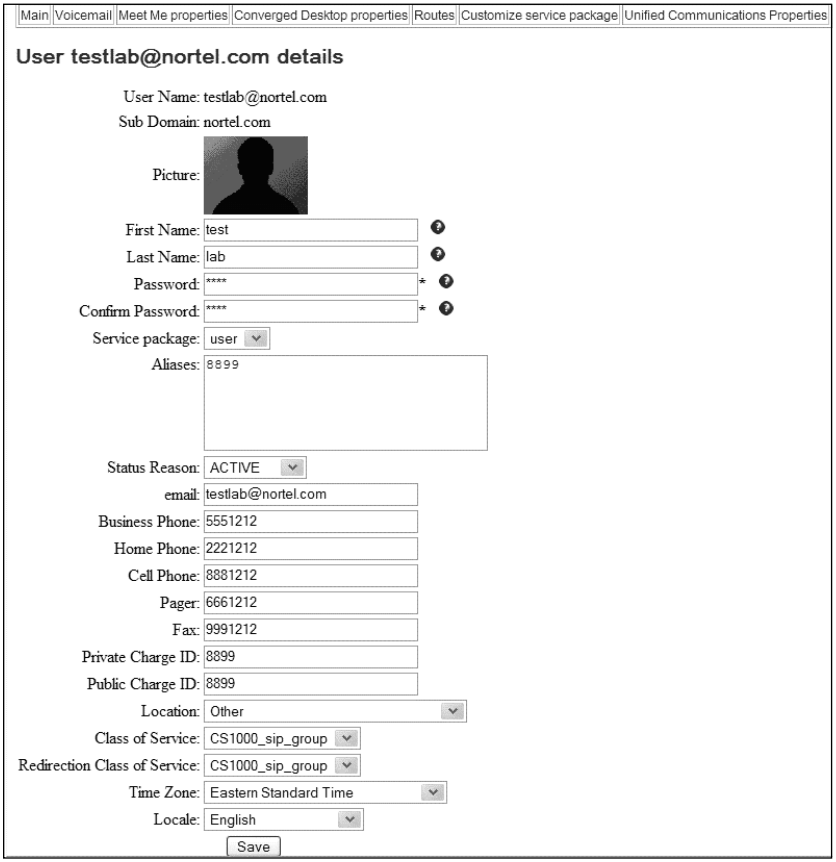
Users in nortel.com

Username	Domain	Name	Phone	Details	Delete	Logout Contacts
testlab	nortel.com	test lab	2221212	Details	Delete	Logout Contacts

User Detail

Figure 4.27 will produce the following details about the user if you have selected the user's details. Figure 4.28 shows how to make changes to this user information and save it to the system. As you can see, this is the test user and the information we have given him for the purposes of this book. In addition to the user details, notice other areas highlighted in blue on the menu. These are additional information areas you can select for user detail. We will go through each of these areas so you know what is available and how to configure the areas.

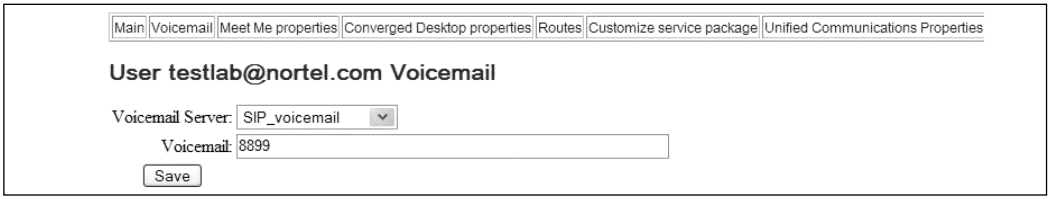
Figure 4.28 User Details



Voice Mail

We did not select voice mail from the top menu; this produced the screen shown in Figure 4.29, which is the voice-mail server we have created for connections to a Nortel Call Pilot. This is going through a CS 1000 via a SIP trunk since the Call Pilot does not support, as of yet, a direct SIP Trunk from any source. You may have more than one voice mail server, so please use the drop-down box to select the correct voice mail server. Then input the voice mail box of the user as it appears in the voice-mail server. Usually, it will be the same aliases you listed in user details.

Figure 4.29 Voice Mail

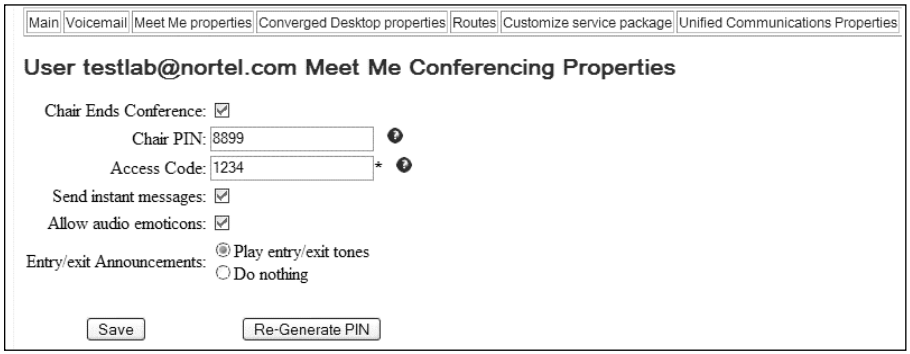


Meet Me Properties

In Figure 4.30 of the menu bar, we look at the *Meet Me* properties of the listed user. Meet Me services are the conferencing services for MCS 5100. In this section, you need to insert the **Chair PIN**, which is good to make the 7 or 10 digit phone numbers. A ping number is really a password that the user will use to open the conference call. *Send instant messages* and *Allow audio emoticons* are good to check since users will be using PC Clients off their PCs. By checking *Chair Ends Conference* at the top, the user controls the session. If he/she leaves, the call is ended.

This is good to use when trying to control the cost of your system and your telecom bills. *Entry/exit Announcements* allow tones to sound when people enter and exit the conference call. I suggest you always have this checked to play tones. After you have filled in or selected your choices as shown in Figure 4.30, be sure to press Save to save your preferences.

Figure 4.30 Meet Me Properties



Converged Desktop User

The converged desktop user (Figure 4.31) is a unique feature of the MCS 5100 since it allows the system to be used with a CS 1000. This happens by allowing the CS 1000 to handle voice call on a phone while the MCS 5100 acts as a desktop client for multimedia. You may wonder about the purpose of this since MCS 5100 does this already with the PC Client by allowing the PC Client to use the audio of the IP phone. That is true. However, this method allows two different PBX systems to work together; that is the benefit.

If you are just using the MCS 5100, you do not need to fill this in, and it will not be part of your service package for users. We show how to use the converged desktop for reference purposes. Before filling anything out in this section, it is best to consult with an experienced engineer on the CS 1000 side to make sure your settings are correct. After that, you may start to fill out the information needed in Figure 4.31. This is the same information you will use in the CS 1000.

Figure 4.31 Converged Desktop Data for User

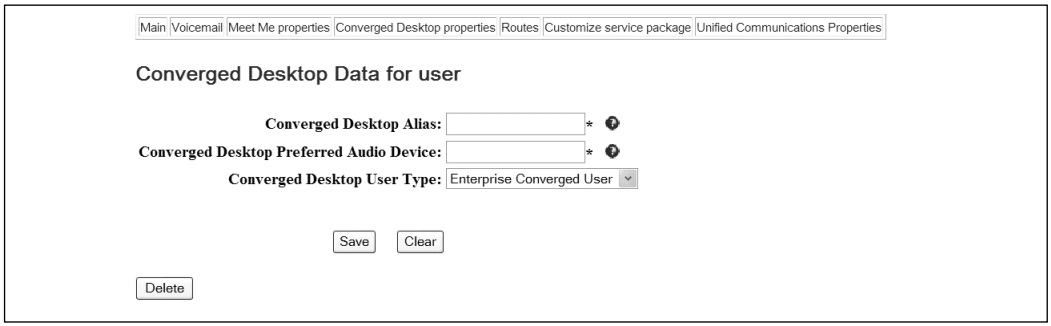
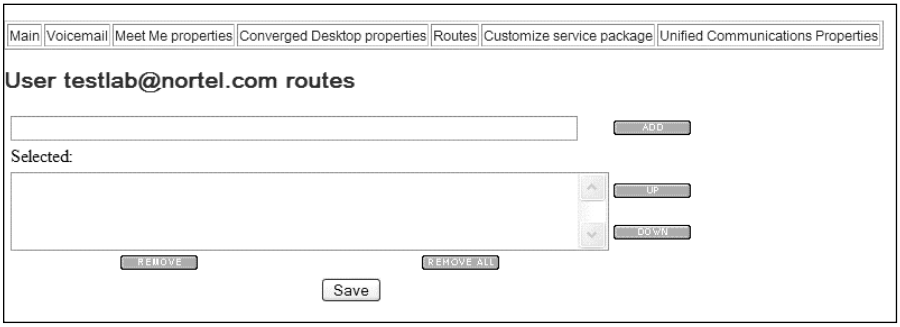


Figure 4.32 shows the routes options for users; when you need a specific route applied to a user, add it here. You may also remove and/or move the routes up and down within the field, depending on which route needs to go first in the order. The unified communications area is only available as an option on the MCS 5200.

Figure 4.32 Routes



Customize Service Package

Figure 4.33 shows a customized service package assigned to a user. In this example, the package is called *user*. Options are shown that are currently assigned to the package. You have the option to make further changes. If there is an option the user needs that is not displayed in the package in Figure 4.33, you may either add the option in the package or change the user's package entirely. However, remember that a package covers a number of people within the domain.

Therefore, it is a good practice to map out your service package strategy before making it available to the domain on which you will use it. We will cover this later in the chapter.

Devices

The next area we look at is the device area or folder within the system tree. This is shown in Figure 4.34 and has two pages shown at the bottom. These two pages are *Add Device* and *List Device*. When we refer to *device*, we are referring to an IP phone that will work on the MCS 5100 system. If you try to add other devices to the system through this area, it will not work.

Figure 4.33 Customize Service Package

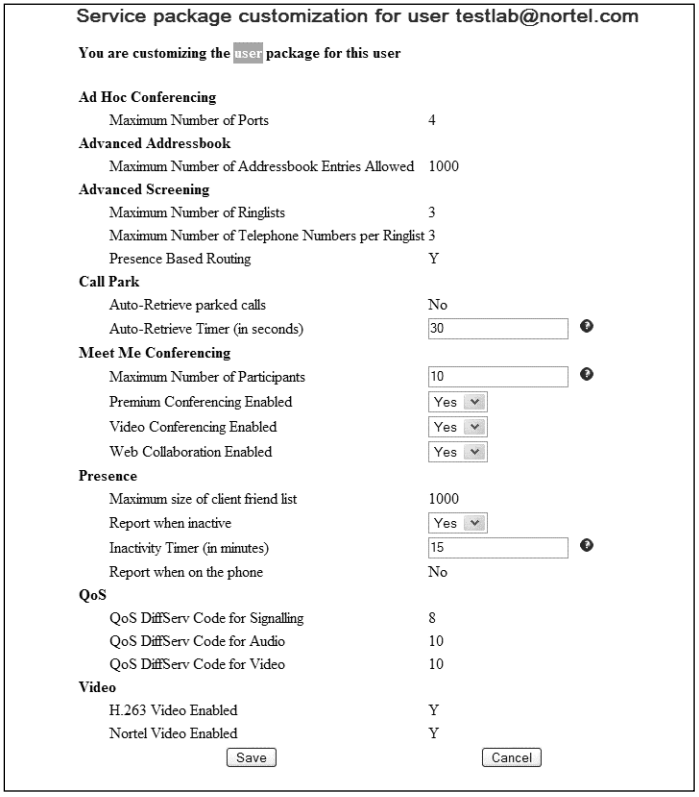
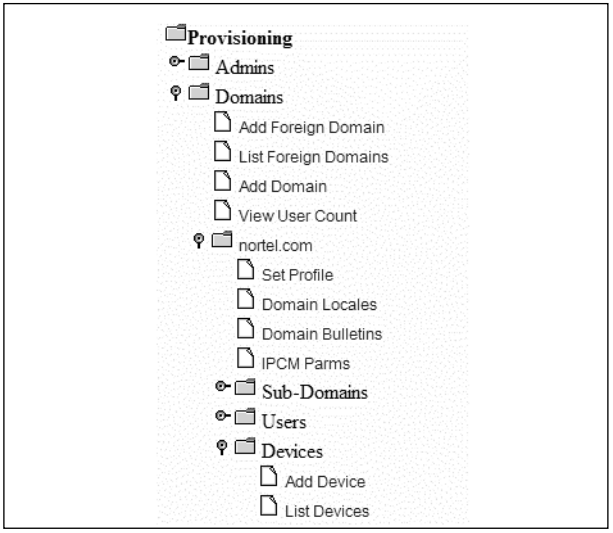


Figure 4.34 Devices

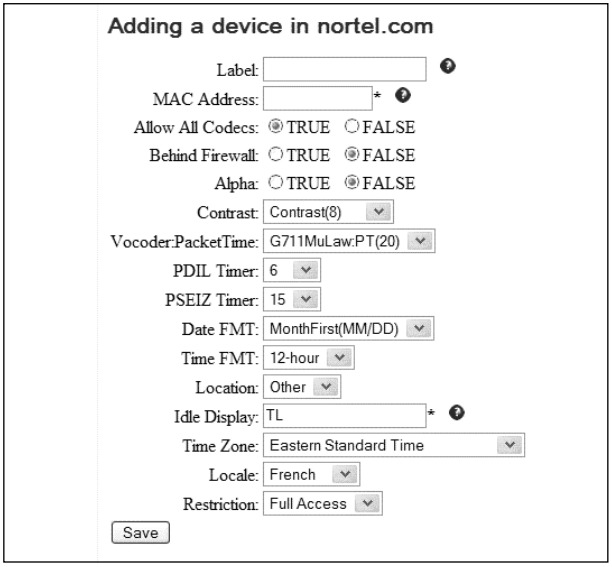


Add Device and List Devices

Figures 4.35 and 4.36 are the result of selecting the pages in the system tree under devices. If you select **Add Device**, you will get a menu that looks like the one shown in Figure 4.35. These settings should look familiar since we went over them in the first part of the chapter. The administrator may add each device, one by one, using this area, but I would not suggest this to anyone. This is not a good use of time.

It is much better just to let you IP phones register to the domain and use the defaults that you have established in the domain for the IP phone.

Figure 4.35 Add Device



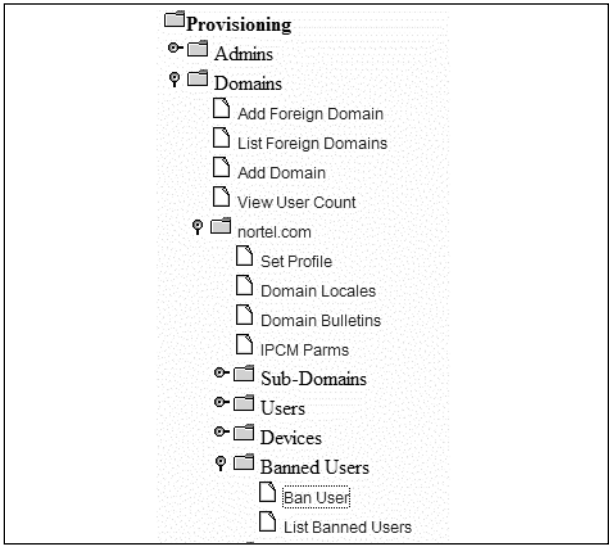
You may use Figure 4.36 to locate the IP phone and make changes to it as you feel they are necessary. This will make the administrator's job much easier, and, it will set a standard for all IP phones on the domain. A uniform look is better for all.

Figure 4.36 List Device

Banned Users

Figure 4.37 shows the banned user section on the system tree. In this area, you are able to ban users from the domain that you are in at that time. So, under each domain, you have a banned users area. You cannot ban users from other domains in this area; you need to go to that domain area and use the section under that domain.

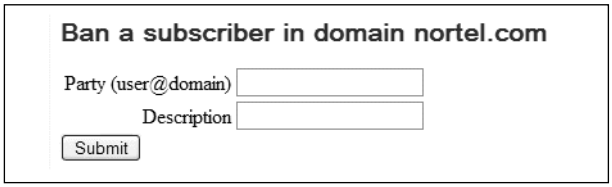
Figure 4.37 Banned Users



Ban User and List Banned Users

In Figure 4.38, the system shows banning a subscriber in domain Nortel.com. Therefore, only users in this domain are subject to the ban; if you try to use other domains or users not registered, the server will kick it back. Make sure you put the users name in and @.nortel.com, as an example. Then you may add a description of why the user is banned.

Figure 4.38 Ban User



If you need to look up the banned users or delete a banned user and put them back to active status, see Figure 4.39

Figure 4.39 List Banned Users

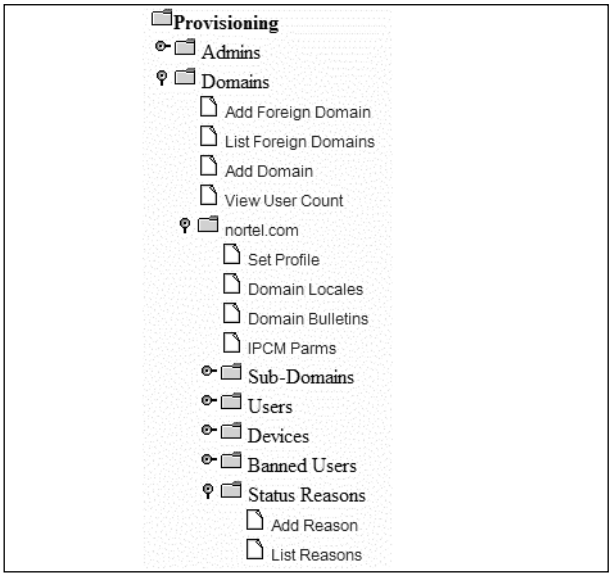
Status Reasons

The next area that you need to configure is the status reasons (see Figure 4.40) for the user on the domain. This is used to tell people why they cannot get to a call, what they are doing while on a call, or redirecting them, via a Web push, to a page when they cannot get to the phone. In this section, you may be creative for your users, but be aware that on the user personal assistant, they may create their own to use, also. So this might be an area where you just want to give some general reasons and give your user some hint on what to use.

Add Reason and List Reasons

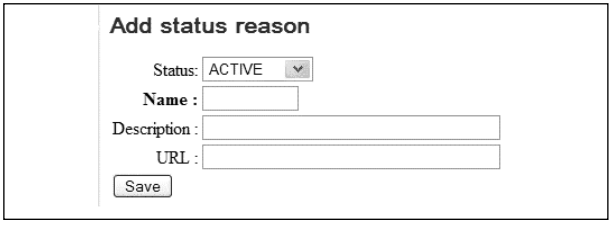
Figure 4.41 shows how to add a status reason and allows you to do just what it says. However, it also allows the administrator to make active or inactive the status reason. You will first make the reason active to use on the domain, and then give the status reason a name. You may also give it a description, and this is what will display to other users when they receive a status reason. As an example, you could put "on the phone" for the name, then, in the description add, "Sorry, but I am on the phone right now and will call you back." The second part is what the calling party gets from the user when this reason is

Figure 4.40 Status Reasons



The user may also use a URL to be pushed to the calling party's pc client and displayed on the system. Once you have configured the status reason, click the **Save** button, as shown in Figure 4.41, to save the status reason and changes made to the area.

Figure 4.41 Add Status Reason



If you need to look at all of your reasons, or delete or see the details, you may select the **List Reasons** page from the system tree. Once you do this, a page like the one in Figure 4.42 will display.

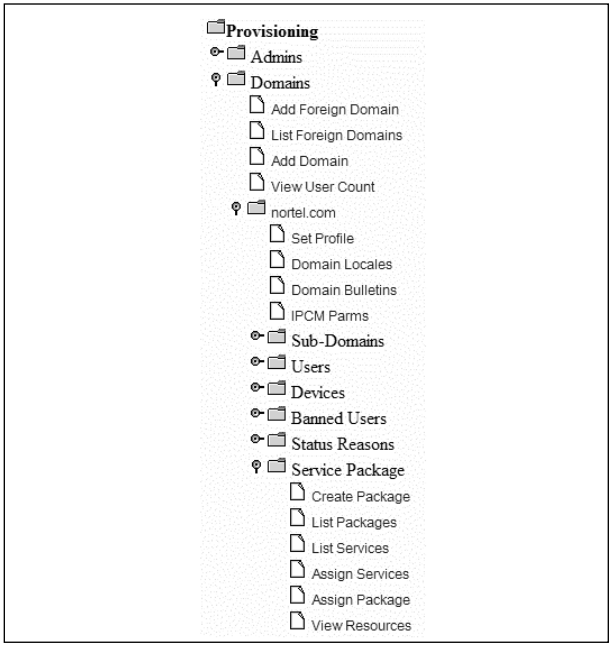
Figure 4.42 List Status Reason

Service Package

A service package section will be filled out for the domain that it is currently under. You may create more than one domain; this is for users who will have different options. You might have some users who do not need video, conferencing, or even chat. But it is best to determine this before you start this section of the domain.

It is recommended that the administrator map out who will have what options on the domain and then make the service packages. This will save your system resources and also your license when configuring your domain. In Figure 4.43, you see that the service package has many different options from which to choose . You will start with *View Resources*, which will tell you your resources for the domain you are in at that time.

Figure 4.43 Service Package



Create Package and Assign Services

Next, you create your service, and then add your service package (Figures 4.44 and 4.45). You do this by choosing the services first, after selecting your domain and clicking **Continue**. In our package, we chose the Web collaboration tool, or Blackberry client, to show that only services selected will be shown in your package. Choose a name and if this package is your default package for the domain. This means that when a user logs on, this will be the package that they receive, unless you chose another one for them. The administrator will then need to select the options needed for that service package.

Figure 4.44 Assign Services

Some of the services listed in Figure 4.45 allow the administrator to select options for more of a configuration for the service package. The options are selected when you create the services later in this chapter. After you have selected all of your services and options, hit the Save button at the bottom. Then you may start over to create another service package, if needed.

List Packages

As you can see in Figure 4.46, we have created a service package called *user* in our Nortel.com domain. You may select **Details-Modify** to go back into your service package to make changes. You may also delete the service package, if needed. Before doing this on a live system with user, remember that the user will not have any options after you delete the service package.

Figure 4.45 Add Service Package

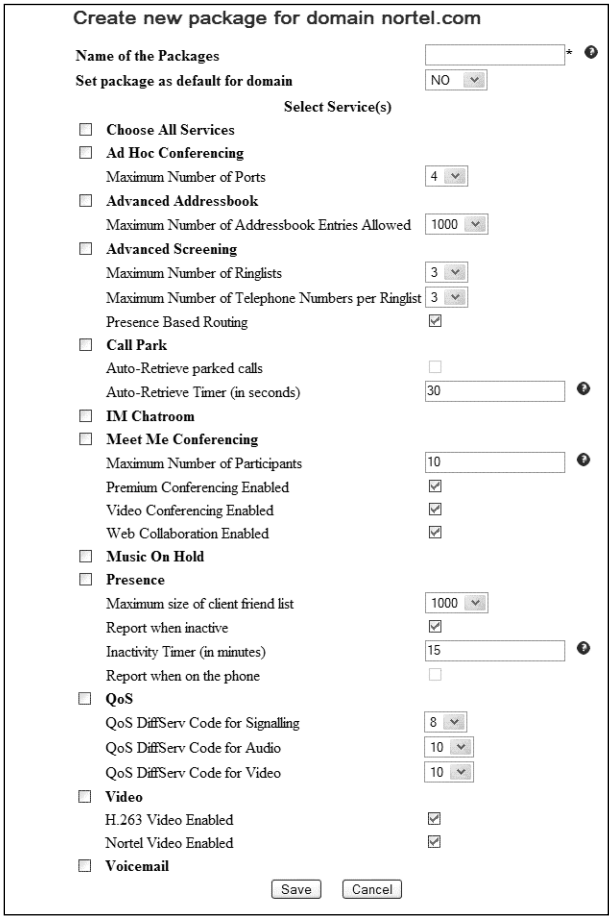


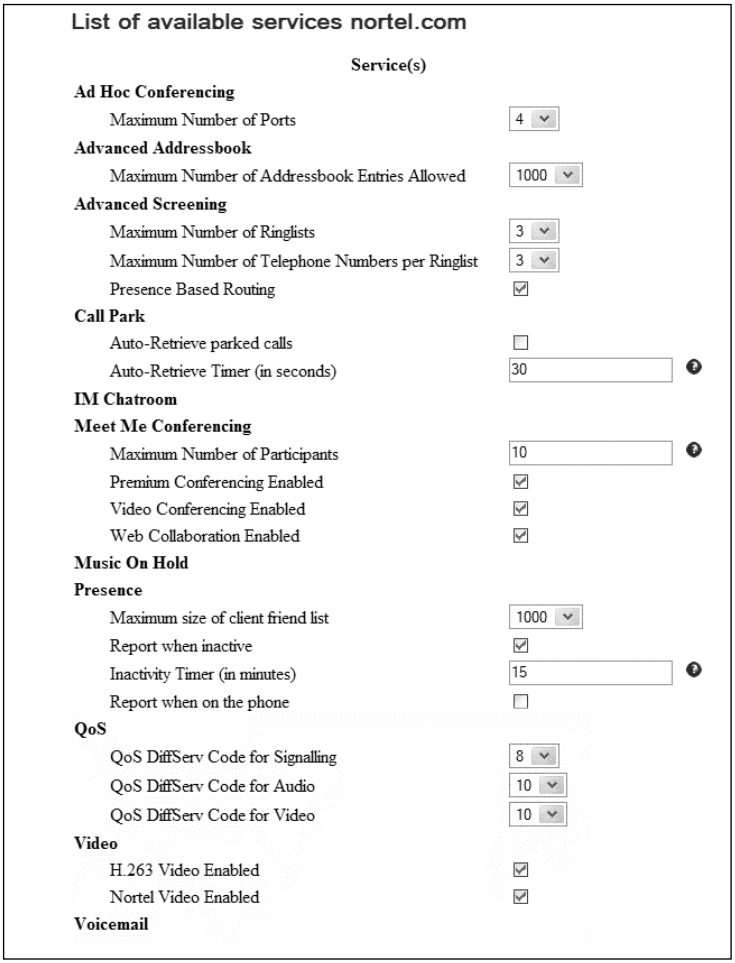
Figure 4.46 List Service Package

List Services

After you have created your service package, you may need to make changes to it. Click **Details-Modify**, as shown in Figure 4.46, and you will see the screen shown in Figure 4.47. Here is where you may make changes to the

service package. By using the buttons shown at the bottom of the illustration, you may select **Save and Enforce Now**, which means the user will get the update immediately, unless they are on a call. The administrator may then choose **Save and Enforce Later**. In that case, the changes will be saved, then the administrator can do an *enforce now* to update the users.

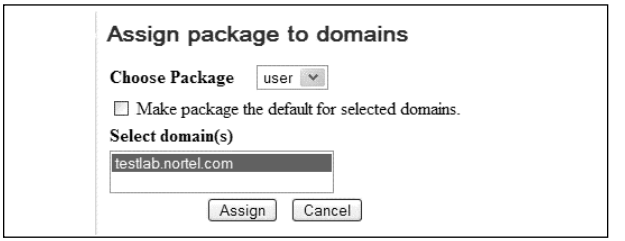
Figure 4.47 List Available Services



Assign Packages

Figure 4.48 shows how the administrator may assign service packages to a domain, and designate a default if needed. Only one service package may be the default. After you make your selections, click **Assign.**

Figure 4.48 Assign Package



View Resources

As we talked about before, this is where you view the resources you have available for the domain (see Figure 4.49). This allows the administrator to plan who will have what services based on the licenses added to the system. Remember the licenses are added in the MCP Client.

Figure 4.49 View Resources

Assigned Resources for domain nortel.com

Service Name	Assigned Resource Count	Current Resource Count	Remaining Resource Count
SIP Advanced Screening	2	1	1
Presence Subscribers	2	1	1
Subscribers	2	1	1

Assigned Resource Count - the maximum number of units allowed for the resource in the domain

Current Resource Count - the number of units of the resource currently used in the domain

Remaining Resource Count - the number of units of the resource available to be assigned or given out.

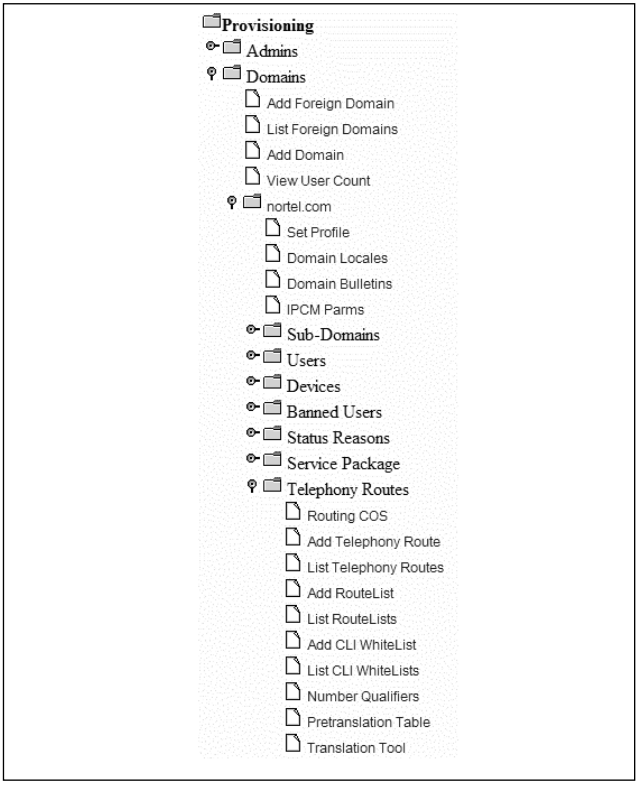
Telephone Routes

The telephone routes within the provisioning client can be the most confusing part of the process if you are not familiar with dialing plans. This is another one of those sections where you might need to search outside help if you just don't get it, because if you do it wrong you will have to start over. The administrator needs to take into account how and why each route and group will work. What are the short-term needs, and, most important, what are the long-term and growth needs for the system?

Some of the settings are a bit tricky to use and understand; also, if you are using a Nortel Call Pilot Voice Mail system, you will be using SIP trunks to a Nortel CS1000 or SIP PBX. In our example, we have set our system up with this architecture so you can understand and see how SIP trunks are added, as well as normal PSTN trunks to the gateway. There are many different routes for regular dialing, PSTN dialing, voice mail dialing, and SIP trunk dialing.

In Figure 4.50, we have opened the folder for the telephone routes; this figure shows all of the route options.

Figure 4.50 Telephone Routes



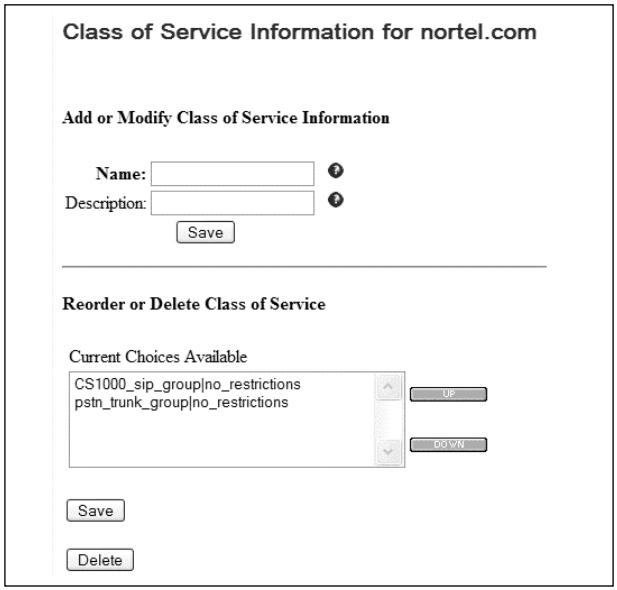
Routing COS

Each route that is made in the system may have a class of service or COS given to it (see Figure 4.51). This allows the administrator to place a restriction on certain routes. So let's say you have two routes like the ones we have created, we have added them to the system with a class of service set to *no*

restrictions. We could also change them to place restrictions on them, so we could create a new class of service that would restrict long distance to the CS1000 SIP Group. This would be added like the ones created now.

The administrator may add, modify, and save within this area. Also, once you have added all of your classes of service to this area, the administrator may put them in the order they will be used within the call sequence. This means that the first class of service that a call matches, it will take and use in the call. So it is important to place them in the right order; this will help eliminate call problems with users.

Figure 4.51 Routing COS



Add Telephone Route

The administrator will need to configure, add, remove, and modify all telephone routes in the system. Someone who knows a little about PSTN routes should do this part. However, as is often said, practice is the best way to learn. In Figure 4.52, we show the area for creating new telephone routes. The administrator will need to first put a name into the route. It is always suggested that the names be something that makes sense and will work for your system. Using long or obscure names will cause problems down the road.

I have fixed many systems that users misconfigured by giving names that made no sense to what the route was used for at the time. Then, they were guessing when using the routes farther down in the configuration. So pay special attention to the names given to the routes.

The next area is the description area; put something in this area that will help you in the system. The next line to configure will be from the digits and to the digits. This means you need to think about what digits this route will start with, if it is going to be a local route or a long distance route. It also could be an internal route, a callback route, and maybe an extension route.

Some companies say that all outbound calls start with 9, then the user may dial the 7, 10, or 11 number. This route can be used for both local and long distance calls. The next areas to be filled in are the minimum and maximum digits the route will support. This means different routes may be created for local and long distance, if the administrator wants to. This is good, since it give the administrator many options within the system.

So if you have a different route that you would like your long distance to go out from away from your local calls, you may do this with a new route. This works the same in reverse.

Next, the administrator chooses a route type; most of the time, it will be a gateway route, but it also could be a private route. We suggest the administrator stick with gateway route. The administrator next may choose a prefix to add to all calls, such as a 9 for users who forget to dial it for outbound calls that fail the other internal routes and get redirected to a default route.

Finally, the administrator will select either **Yes** or **No** from the recursive box menu. Most of the time, it will be no. Then, you have to associate a route list under you new telephone route. After this is done, the administrator will choose **Save** to add the route.

List Telephone Route

After the administrator has configured the new telephone route list shown in Figure 4.52, he or she may show a list of the telephone routes as shown in Figure 4.53. As you can see, text displayed in blue may be clicked on to bring up more information about the route list. The administrator may also delete the route list from the system using this screen.

Figure 4.52 Add Telephone Route

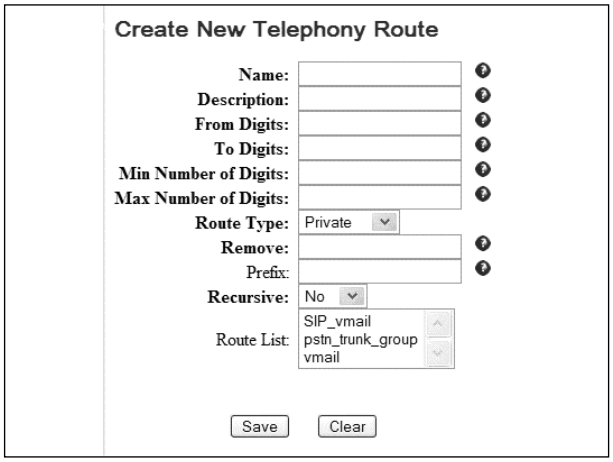
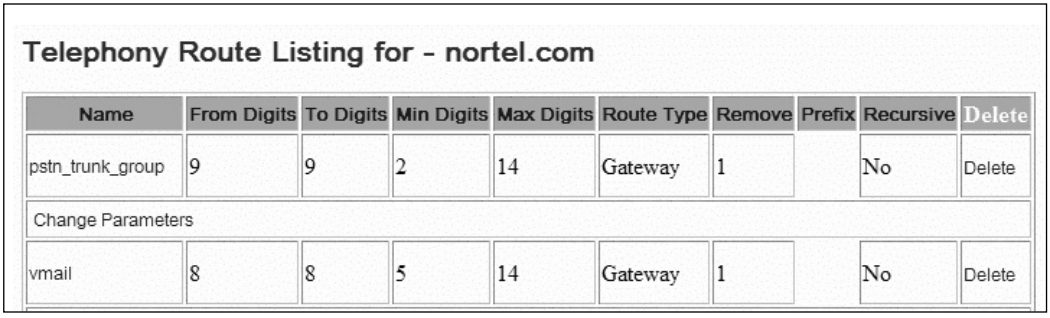


Figure 4.53 List Telephone Route



Telephony Route Listing for - nortel.com

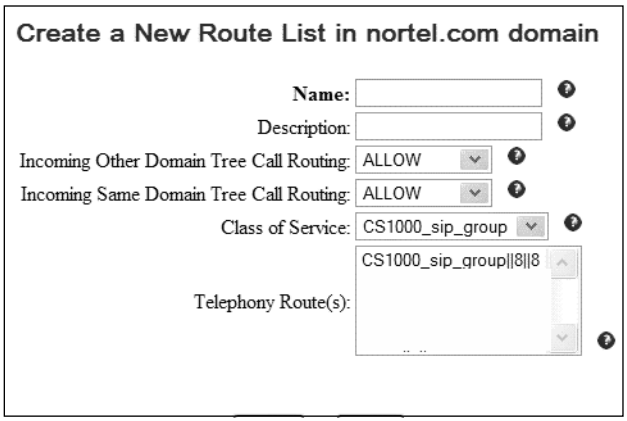
Name	From Digits	To Digits	Min Digits	Max Digits	Route Type	Remove	Prefix	Recursive	Delete
pstn_trunk_group	9	9	2	14	Gateway	1		No	Delete
Change Parameters									
vmail	8	8	5	14	Gateway	1		No	Delete

Add Route List

In Figure 4.54, we show how an administrator configures a new route list for the domain. This is different in that you will be taking the already-created telephone routes and putting them into overall route lists. After you give the route list a name, you will need to choose the class of service and the telephone routes to associate with the route list. You may make more than one

selection by holding the ctrl button on your computer and clicking on more than one telephone route. After you are finished, select the **Save** button.

Figure 4.54 Add Route List



List Route Lists

Now that the administrator has configured the routes list, you may go back in to look at the route lists created. This is done by selecting **List Route Lists** from the system tree. Then, as shown in Figure 4.55, the route lists will appear. The administrator may make changes to the route lists by clicking on the name of the route list. Also he or she may delete telephone routes, or even the whole route list, if needed.

Add CLI WhiteList and List CLI WhiteLists

The CLI (calling line ID) white list function of the MCS 5100 allows the administrator to screen incoming calls from another SIP gateway. This allows calls to be allowed in, denied, or even replaced with another phone number. Then you would apply the white list to your telephone route list. In Figure 4.56, we show the configuration screen that allows the administrator to add the CLI white list.

Figure 4.55 List Route Lists

Name	Description	Same Domain Action	Other Domain Action	Class of Service	Delete
vmail	vmail	ALLOW	ALLOW	CS1000_sip_group	Delete

Associated Telephony Routes

Route Name	From Digits	To Digits	Remove	Prefix	
pstn_trunk_group	9	9	1		Delete
vmail	8	8	1		Delete

pstn_trunk_group	pstn_trunk_group	ALLOW	ALLOW	CS1000_sip_group	Delete

Associated Telephony Routes

Route Name	From Digits	To Digits	Remove	Prefix	
pstn_trunk_group	9	9	1		Delete
vmail	8	8	1		Delete

Figure 4.56 Add CLI WhiteList

Add CLI WhiteList in nortel.com

Name

Add New Range

From Digits	To Digits	Min Digits	Max Digits	Add
				Add

Current Ranges

From Digits	To Digits	Min Digits	Max Digits	Delete

Save

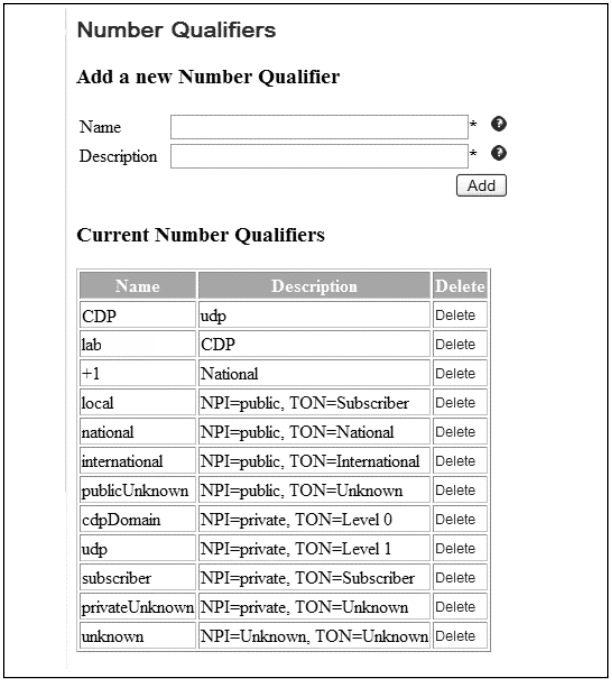
Once the WhiteList is complete, Figure 4.57 shows how they may be searched for and listed.

Figure 4.57 List CLI WhiteLists

Number Qualifiers and Pretranslations Table

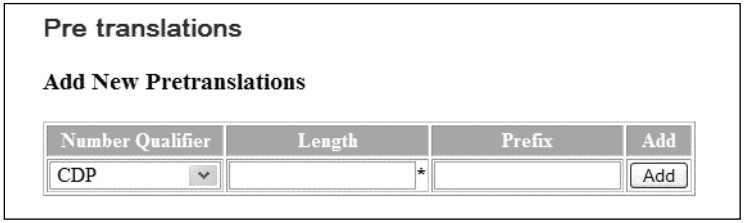
In Figure 4.58, there are a number of default number qualifiers already added to the system for your use. But, you may also use the *New Number Qualifier* to add new qualifiers. This is a great feature in case you are adding different equipment or an end point from an outside company. You may need to add a different number qualifier to be able to route calls correctly to that end point. Once you have added your new number qualifier, hit the **Add** button to add it to the list.

Figure 4.58 Add Number Qualifiers



For pretranslations within the number qualifiers, you will use the GUI in Figure 4.59. The administrator uses these to add length and a prefix to the number qualifier.

Figure 4.59 Pretranslations



Translations Tool

Figure 4.60 shows how the administrator uses the translation verification tool to test new and old lists and routes to see if they are working correctly. We took the requested URI, 6969, and then added lchaffin@pluto-networks.net in the **To** and **From** spaces. After hitting **Execute**, we see the page shown in Figure 4.61.

Figure 4.60 Translation Tool

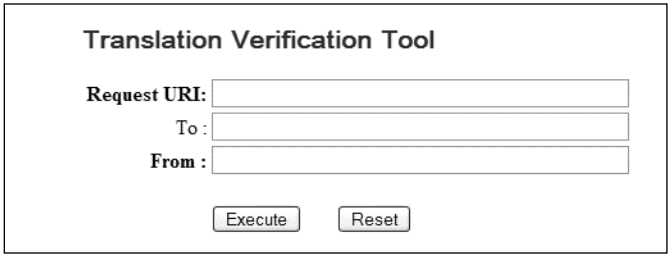


Figure 4.61 shows the route taken by the call, the route type, which route list it uses, and also the class of service for the call. Then it shows the domain for the route list, a public route list, if there is a CLI white list involved with the call, and at last, the destination taken for the call.

It is good to use this to test your routes and lists before putting them into production. It will save you many angry calls from users if they fail and you did not test them beforehand. In addition, if you have a problem with a caller saying they cannot call a number, you may use this to test their problems and

see where the issue lies. It could be that a new route or list needs to be created, or perhaps they are just dialing the number wrong.

Figure 4.61 Translation Tool Results

Route	Nortel SIP
RouteType	Gateway
RouteList	Pluto Networks Unified VMail
Class of Service	CS1000_sip_group
RouteList Domain	Pluto-Networks.net
Gateway Route Type	PUBLIC
OverRideCharge ID	N
OverRide Charge Value	No Override Value Was Found.
Destinations	sip:6969;phone-context=vmail@pluto-networks.net;gw;trusted;maddr=10.10.99.33;norteltrkgrp=CS1000_sip_trunk;user=phone

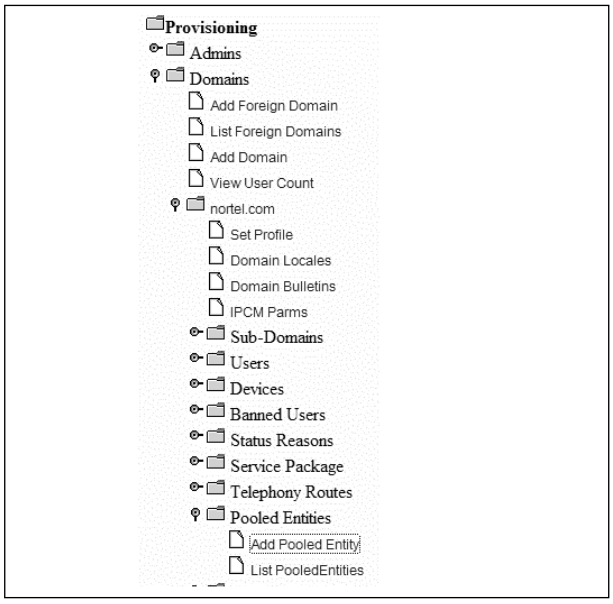
Pooled Entities

In Figure 4.62 we show the system tree and that we have now moved to pooled entities. This is where you may add different pools of services or different servers to one pool. Depending on your system and your user base, you could have one Meet Me Conferencing server, or you may have three for your user base. This all depends on the resources needed for your system. In other chapters of the book, we talk about how many users you can have on a server or licenses.

Add Pooled Entity

Figure 4.63 shows the GUI you see after selecting **Pooled Entity**. This has your routable services, which you would have already added to the system. You may choose a name now for your entity. After you select a name, which should be both an easy name to remember and have something to do with the routable service, you may select the weighted average. In addition, by now, you will have added your locations for the system, and you may assign these to the pooled entity.

Figure 4.62 Pooled Entities



Then you need to add a route. A route could look something like this SIP: 10.66.69.12; trusted. This means that your route is a SIP route going to this address, and it is trusted. Next, give a weight to the route. If you are only using one server for your pooled entity, the weight would be 1 for 100 percent. It could be that you have three servers—a, b, and c. Servers a and b receive a weight of 1, while server c receives a weight of 2. When the servers are used, server c is used twice as often as servers a and b. Once completed with your selections, click the **Add Resource** button.

Figure 4.63 Add Pooled Entity

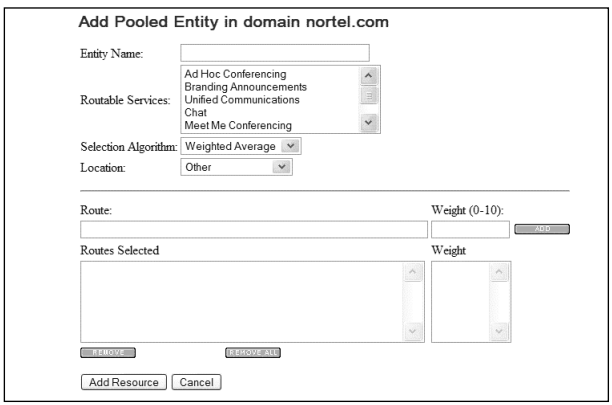
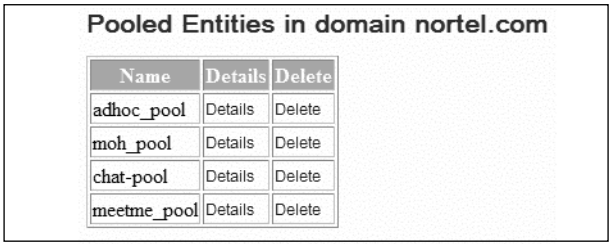


Figure 4.64 shows how you may list the pooled entities and select details of each to make changes to them. If need be, for some reason, you may also use the delete button in that same GUI.

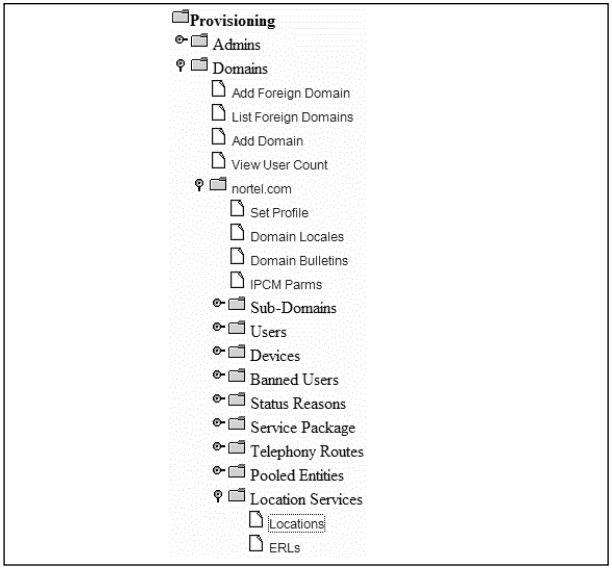
Figure 4.64 List of Pooled Entities



Location Services

Today, all VoIP providers are required to provide emergency services to the user. In this area, called location services, you can map out your user locations so they may choose the site where they are located. Since some users will use just a soft client, this is important so when they log into the system, they may select the correct location. So we will start with Figure 4.65, which shows the Location Services and the two areas below it in the system tree, *Locations* and *ERLs*.

Figure 4.65 Location Services



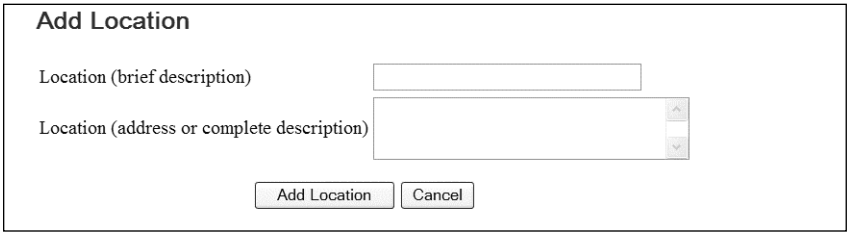
Locations

First, you need to create locations for your sites by selecting locations. After the locations are selected, you will see a GUI like the one in Figure 4.66. Here our GUI does not have a domain since we are just using it for testing. It would normally say "Pluto Networks.net."

Figure 4.66 Location Management

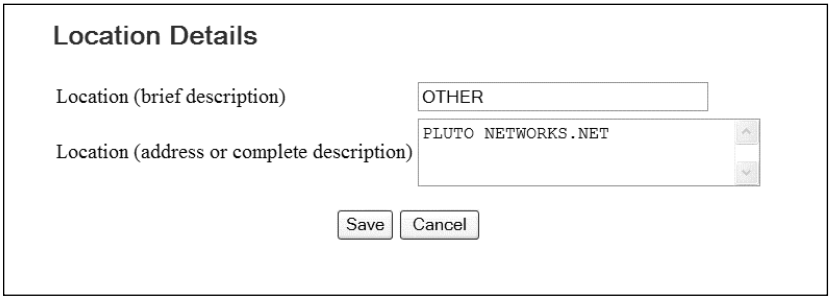
Next, select the **Add Location** tab, and that will produce the screen shown in Figure 4.67. Here you will add the location name and address of the site. You may also include the floor or area on the floor, to be more exact.

Figure 4.67 Add Location



In Figure 4.68, we have selected a site that we created, and it shows the information we have added. You may change or update the information, then click S**ave**.

Figure 4.68 Location Details



ERLs

The next tab to configure is the ERL. This is how calls get out in case of an emergency, or gives instruction on whom to call. It also tells what route it will take out of the domain and if it will provide an instant message to someone when this emergency happens. This is good to do if you have a security guard station. A PC Client can be noted on a computer or even an IP Phone, and they will receive a message when an emergency number is dialed. Figure 4.69 shows the locations for our domain. Click **Other** to select the location.

Figure 4.69 Emergency Response Location Management

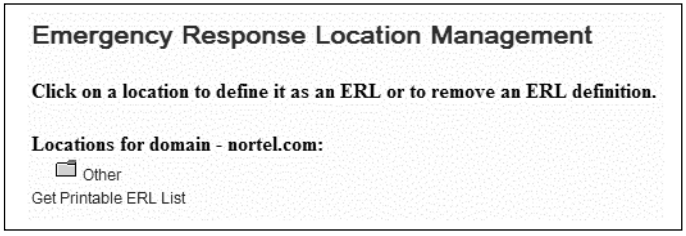
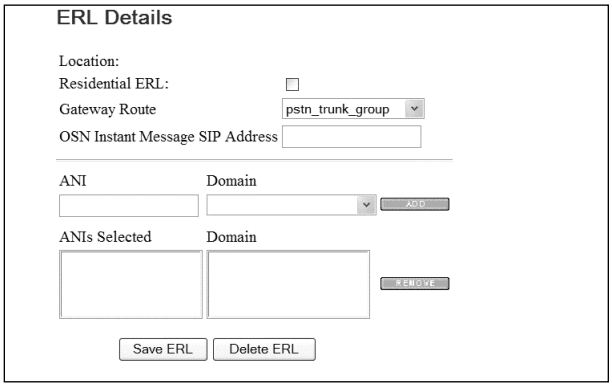


Figure 4.70 is where you configure your ERL information. Location is where you show your domain, for example, Pluto Networks.net. You can also choose whether this is a residential location or not by marking the Residential ERL box. Next, you need to select a gateway route for the ERL to take. It is always recommended that the ERL have its own telephone route or list to get to the outside. Next, you may input a SIP address on your system for an emergency instant message. Our system will be configured for security@pluto-networks.net.

Select a ANI that will dial when there is an emergency. Most of the time, it will be 9-1-1. While this can be directed to the outside PSTN, it can also be directed to the inside in case you need all calls to go to a security desk, and not 9-1-1. Once that is complete, select the domain to which the ANI will belong and click the **Add** button. Finally, select **Save ERL**.

Figure 4.70 ERL Details



Routable Services

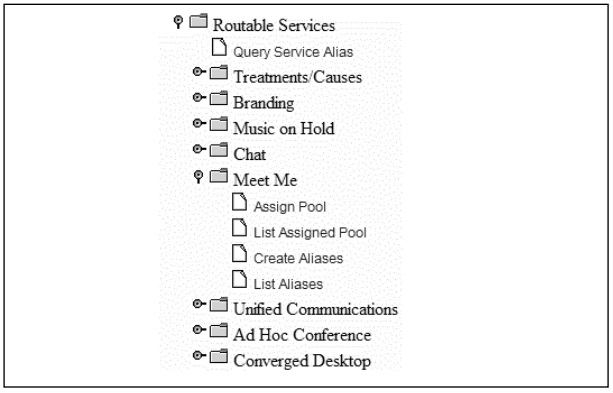
The next area in the system tree we want to configure is *Routable Services*. Figure 4.71 addresses these. A routable service has some type of route assigned to it for it to work on the MCS 5100. Each of the services that you see in Figure 4.71 is an option on the MCS 5100. If you will be using these services, you need to configure them within your domain. Since they are easy to configure, we are just going to configure one for paper purposes.

Figure 4.71 Routable Services

Meet Me

In Figure 4.72 you can see that we have selected the Meet Me service for our example. There are four different options under the service that need to be configured. Remember earlier, you gave some names to your pooled entities. Now you will use those in this area for the routable services.

Figure 4.72 Meet Me



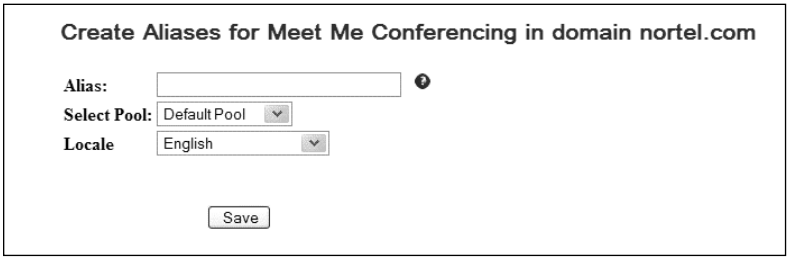
In the pooled entities, we gave the name *meetme_pool* to our pool on the system. Now we are going to make sure that the current pool is correct. When looking at Figure 4.73, be sure to have the correct pool selected for the service. Do this by selecting the drop-down box and then hitting the **Save** button.

Figure 4.73 Modify Meet Me Conferencing Pool

After that, you need to create aliases for the Meet Me Conferencing service, as shown in Figure 4.74. The aliases are the number that the user will dial on the service to reach it. In our example, we use a four-digit number, but you can use a regular seven- or 10-digit number.

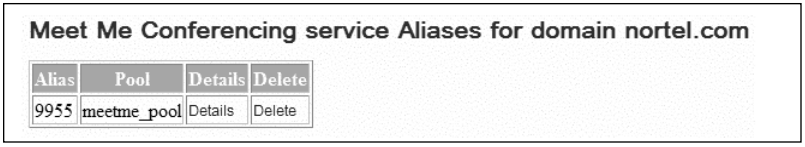
This is just for this service; all of the services will be different with the aliases and pools they use. Next, select the pool you would like. Most of the time, you will just use the default pool for the service since you have checked that already. Next select a locale and hit the **Save** button.

Figure 4.74 Create Aliases



Last, we will look at the list aliases under the Meet Me Service. Here you can list the aliases for the current domain (see Figure 4.75). You may select the **Details** button and make changes to the current aliases, or you may delete it altogether. Be aware that when you delete aliases, it will affect users of that service.

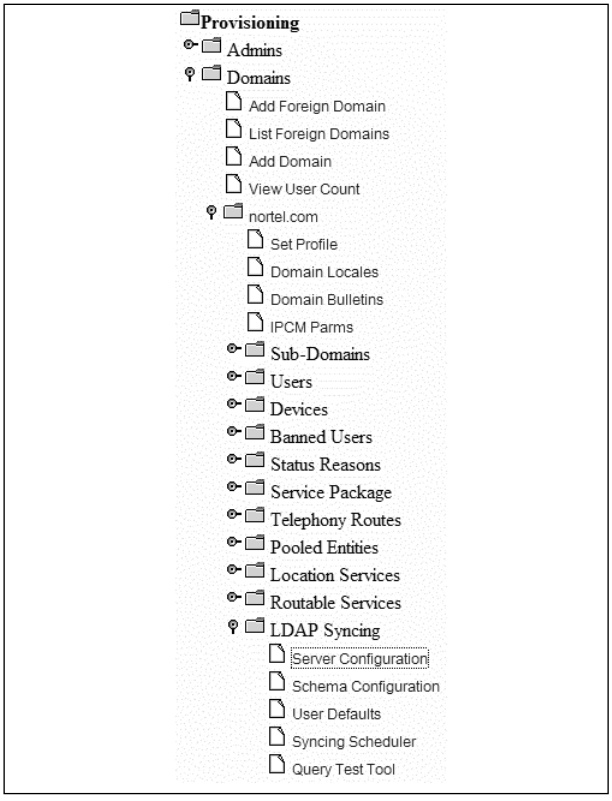
Figure 4.75 Alias List for Meet Me Conferencing



LDAP Syncing

In Figure 4.76, we have moved on to the last area in the system tree under the current domain, which is used for LDAP syncing. This is very straight foreword. Anyone who is an administrator on a system should be able to complete this section with no problems. This is a connection to your local company LDAP server that has e-mail information, address books, and contacts that your user will be able to sync with when this is configured.

Figure 4.76 LDAP Sync



Server Configuration and Schema Configuration

To configure your MCS 5100 to do a dip to your LDAP server, you need to configure the information shown in Figure 4.77. Select whether this LDAP server is the primary or back-up server for your company, and insert the IP address. Insert name of the server port, and check the box if the server requires a login. Most secure LDAP servers require logging in to receive information. So after you have placed a check in the box, type the **User Name** and **Password**. Ask your LDAP administrator whether this is a secure connection or not; sometimes on an internal network, it is not. After you are done, click **Save**.

Figure 4.77 LDAP Server Configuration

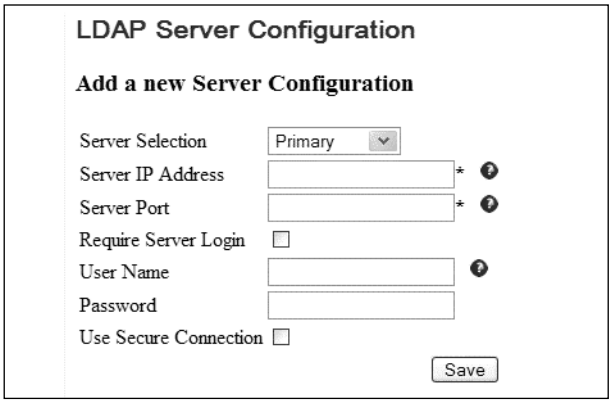
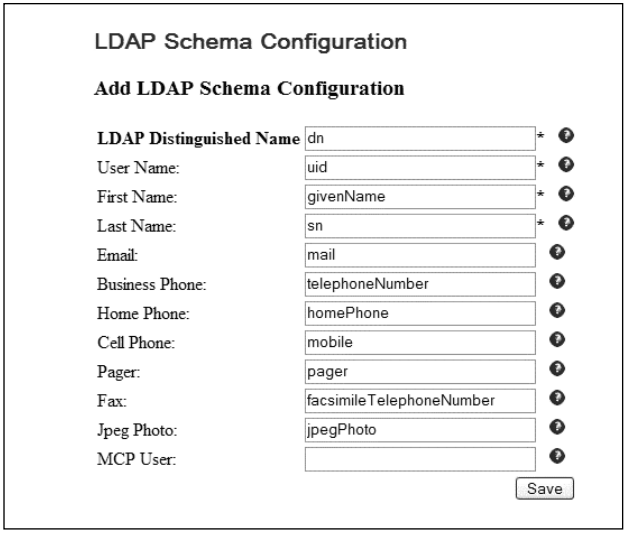


Figure 4.78 shows how to configure a scheme to pull correct information from your LDAP server. I suggest that you verify the information on the LDAP server, and use that same scheme in this area. If it is incorrect, it will not work.

Figure 4.78 LDAP Schema Configuration



User Defaults and LDAP Scheduler Configuration

We configure the MCP User defaults in Figure 4.79. First, configure your *Default User Password* and the *Default Service Package* and *Default Class of Service*

from the drop-down menus. The *Default Status Reason* is usually active, and last, the *Time Zone* and *Locale* need to be set from the drop-down menus. After the defaults are configured, save your work. You may configure more than one default, such as one default for each user package in the domain.

Figure 4.79 MCP User Defaults

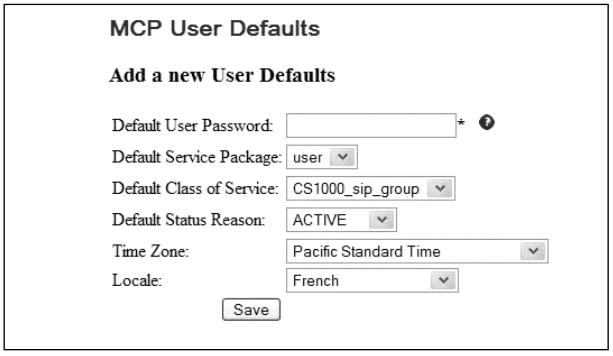
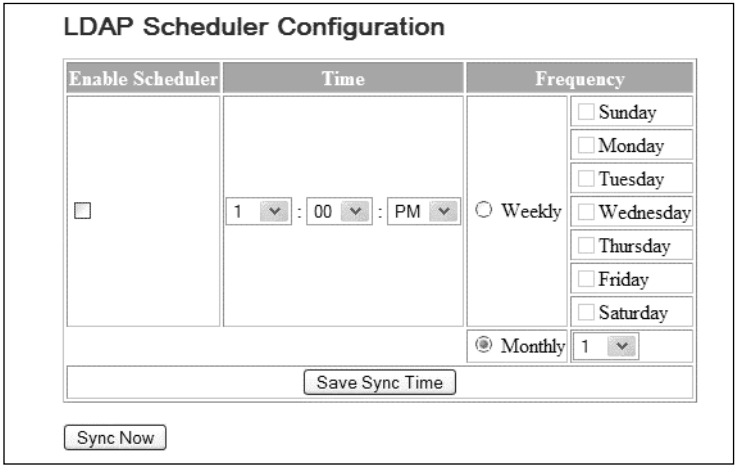


Figure 4.80 shows how to configure the LDAP Scheduler in the domain. This allows the administrator to determine when the MCS 5100 or domain will sync with the current LDAP server. Choose the box on the left under *Enable Scheduler*, and select a time and frequency. After you are finished, press **Save Sync Time** and **Sync Now**.

Figure 4.80 LDAP Scheduler Configuration



LDAP Query Test Tool

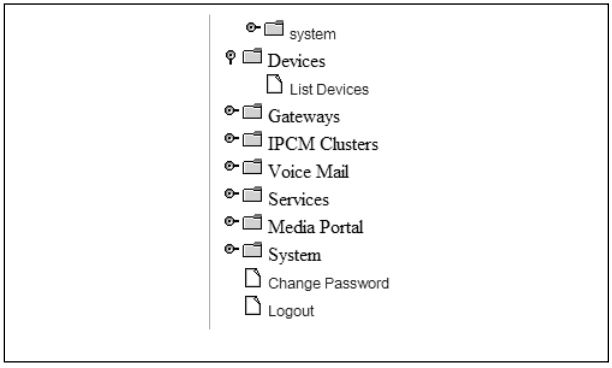
In Figure 4.81, we have the LDAP Query Test Tool, which allows you to test the settings you are adding before you do them. Also, it allows the administrator to troubleshoot problems if the LDAP server and the MCS 5100 do not sync up.

Figure 4.81 LDAP Query Test Tool

Devices

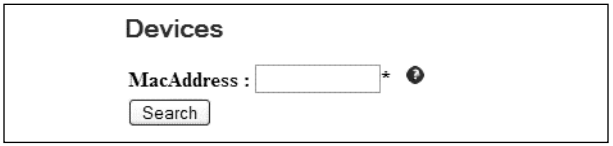
This section is very short, but we need to cover it. We are out of the domain and back to the main system tree. This is the same selection you can make within the domain to show the devices. In Figure 4.82, we have chosen the device area from the system tree.

Figure 4.82 Devices



Just as in the domain area, select the **List Device**s tab, which displays the screen shown in Figure 4.83. Then you will have to insert the Mac address of the device to find it on the network.

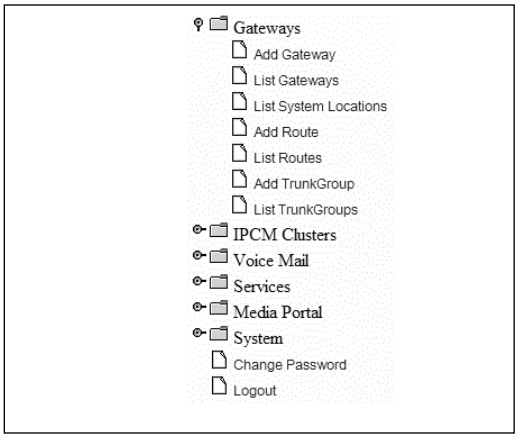
Figure 4.83 Devices Search



Gateways

For your MCS 5100 system to connect to other SIP devices, endpoints, or PSTN, the administrator needs to configure gateways with in the system. We selected the gateway folder in the system tree, and it has displayed the contents (see Figure 4.84).

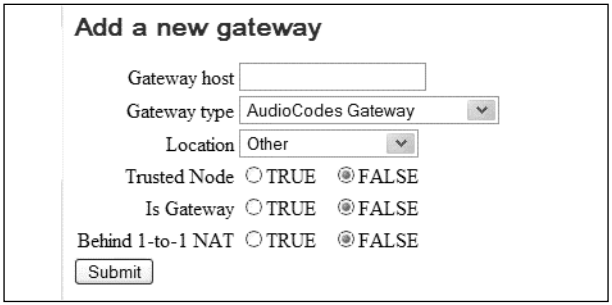
Figure 4.84 Gateways



Add Gateway and List Gateway

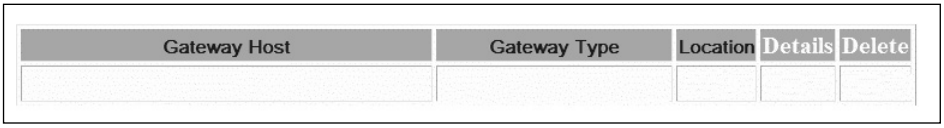
First the administrator needs to add a gateway by clicking on **Add Gateway** under gateway folder, as shown in Figure 4.84. Then the contents shown in Figure 4.85 are displayed. The *Gateway host* is the IP address of the gateway, and the *Gateway type* is selected from the drop-down box. The gateway host will have a name such as *Pluto-Networks.net;maddr=10.2.4.19*. The location is selected next, along with indicating if it is a trusted node, a gateway, and last, if the gateway is using NAT. Once that is all finished click the **Submit** button.

Figure 4.85 Add a New Gateway



The administrator needs to configure a gateway for each gateway in the system. It could be that there is a SIP gateway being used to a CS1000 and a gateway to the PSTN. In Figure 4.86, the list gateway GUI is displayed. As with other areas on the provisioning client, the administrator may click the **Detail** button to make changes to the gateway.

Figure 4.86 Gateway List



List System Locations

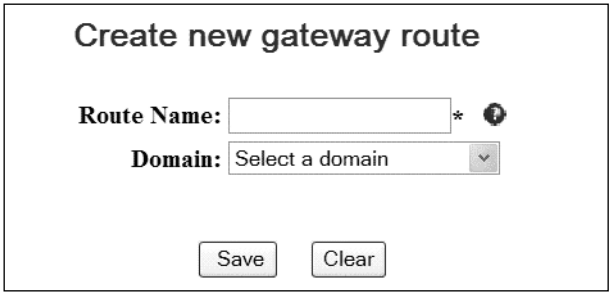
In Figure 4.87, the administrator can add or delete locations for the domain by selecting the **Add Location** folder.

Figure 4.87 Location Management

Add Route and List Routes

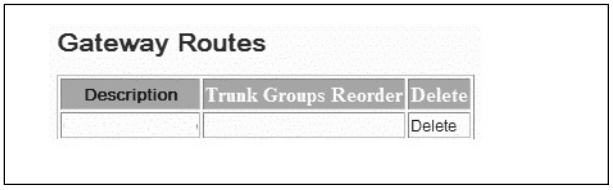
In Figure 4.88, the administrator may add a new gateway route for the system by selecting a route name and the domain where the route will be used, and saving the changes.

Figure 4.88 Create New Gateway Route



In Figure 4.89, if we had added a gateway route it would be listed here.

Figure 4.89 Gateway Routes



Add Trunk Group List Trunk Groups

To provision a trunk group for the gateway, the administrator will follow the steps shown in Figure 4.90. A gateway is selected from the drop-down menu, and a route is chosen from the ones already created. The administrator then gives the trunk group a name and clicks **Save**. The administrator may then see all of the trunk groups created by selecting the list trunk groups from the system tree.

Figure 4.90 Trunk Group Provisioning

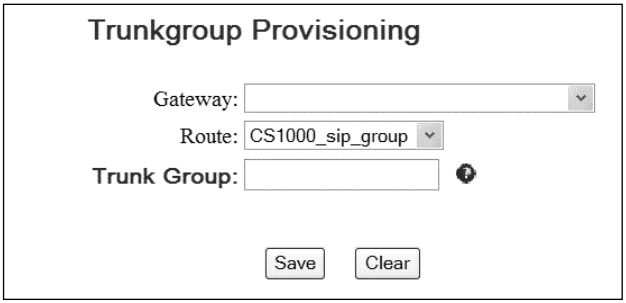
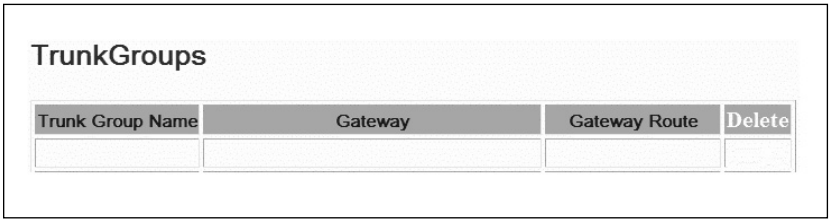


Figure 4.91 displays the information for all trunk groups configured.

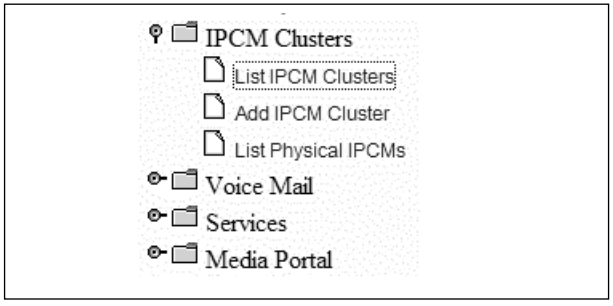
Figure 4.91 Trunk Group List



IPCM Clusters

Remember, the IPCM is what your IP Phone connects back to within the system. So the IPCM that was configured in prior chapters will need to be configured now. In Figure 4.92, we selected the IPCM Clusters from the system tree. There are only three areas that can be accessed with in this area.

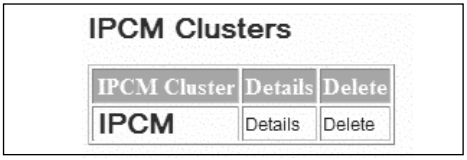
Figure 4.92 Selecting IPCM Clusters



List IPCM Cluster

Figure 4.93 shows an IPCM cluster when it has been configured on the system. The administrator may select the *Details* button on any of the ICPM clusters to allow changes to to the clusters.

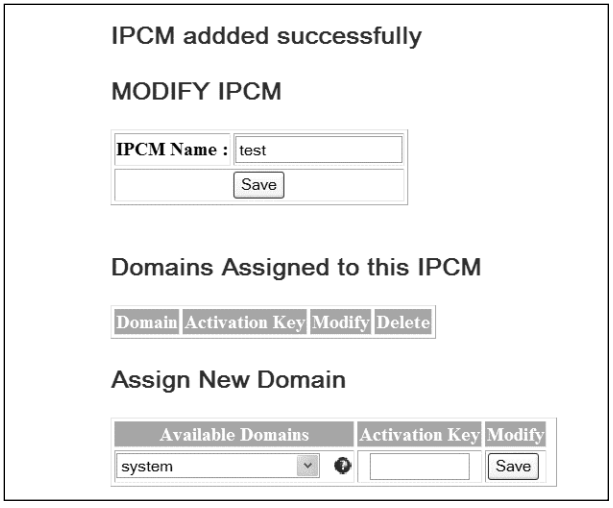
Figure 4.93 An IPCM Cluster Configured on a System



Add IPCM Cluster

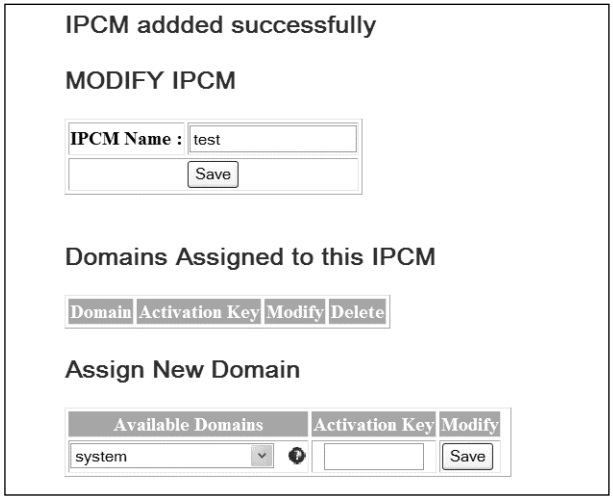
To create a new IPCM cluster, take the name you used in the prior chapter and add it here in Figure 4.94, which is *Create new IPCM*. After typing in the name, click **Add** and the message shown in Figure 4.95 will display. We added the IPCM cluster test for this figure.

Figure 4.94 Create New IPCM



In Figure 4.95, the administrator needs to select the domain to which this IPCM will be added and choose an *Activation Key*. This key is used to allow IP Phone onto the IPCM Cluster and register. This can be a simple 1234, or a harder key code. Each domain needs to be assigned to an IPCM cluster.

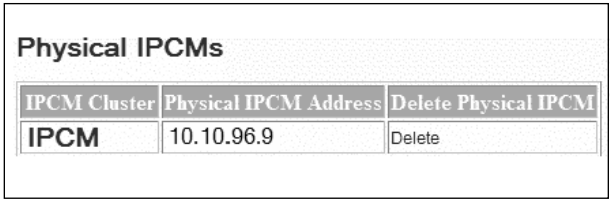
Figure 4.95 IPCM Added Successfully



List Physical IPCMs

After you have added all the information, you may choose **List Physical IPCMs** from the menu. After the selection, Figure 4.96 will display. Your IPCM cluster and physical address will be shown here.

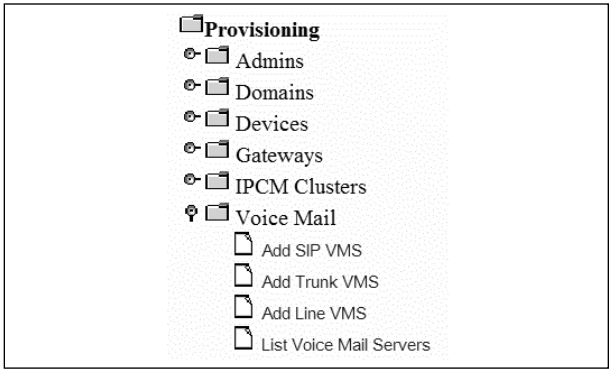
Figure 4.96 Physical IPCMs



Voice Mail

Earlier in this chapter, the user was directed to the correct voice-mail server where he or she configured the voice-mail server (see Figure 4.29). Remember to give the voice mail server a name that is be easy to use and shows the difference between it and others. Such names as sip_voicemail, cas_voicemail, pstn_voicemail, or line_voicemail work well. Figure 4.97 shows the selected voice-mail area from the system tree.

Figure 4.97 Voice Mail

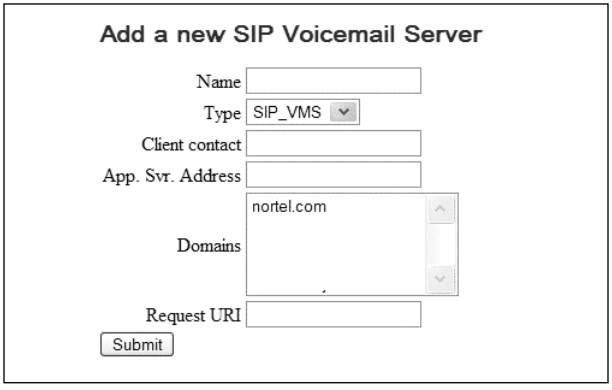


Add SIP, Trunk, and Line VMS

In this section, we have three figures that represent the different types of voice mail servers that can be added to the system. As you can see in Figure 4.98, the administrator can add a SIP voice mail server. After giving the server a name, fill in the *client contact* and *app server address*. This app server address is the IP address of your application server on the MCS 5100. Select the domain for which you will set this SIP voicemail server, and fill in the requested URI. This could be something like sip:8885551212@pluto-networks.net.

In most systems, you will use the SIP voice mail server to make a SIP connection to a CS1000 and then to a Call Pilot.

Figure 4.98 Add New SIP Voice-Mail Server



If you are using a CAS or a PSTN trunk to a voice-mail server, you need to fill in the information shown in Figure 4.99—the user name, password, port, address, and SMDI version for the trunk voice mail server. This also applies to Figure 4.100 for the Line Voice Mail Server. If you are connecting to an outside voice mail server, be sure you have the necessary information.

Figure 4.99 Add New Trunk Voice-Mail Server

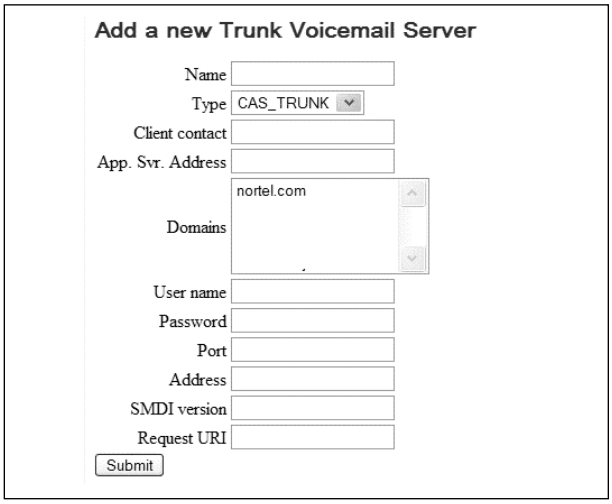


Figure 4.100 Add New Line Voice-Mail Server

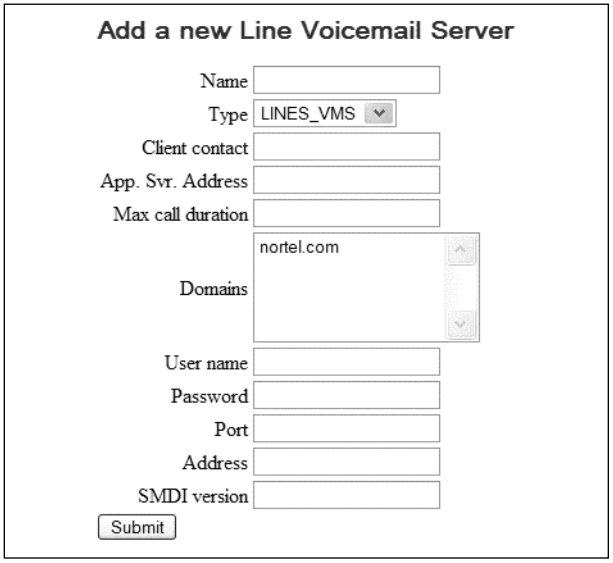
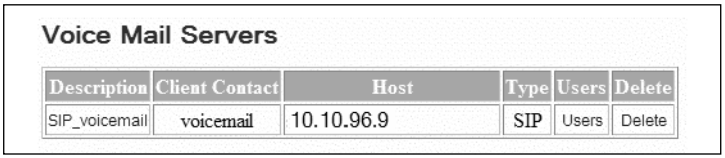


Figure 4.101 shows the GUI that is displayed when the administrator selects **List Voice Mail Servers** from the system tree. The administrator may select the description area to show the details of the voice mail server and make changes. Also, he may select the users area to show current users of the voice mail server.

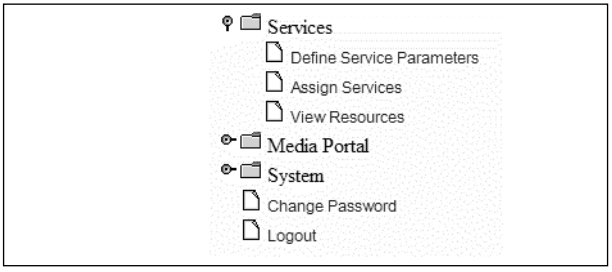
Figure 4.101 List Voice-Mail Servers



Services

As we talked about in the preceding sections in this chapter, the administrator needs to configure the service parameters for the domains. In this section, the administrator completes this task. Be aware that even though these services are shown, you need to have the key codes for them. With that said, in Figure 4.102, we selected the services parameters area in the system tree. This section is easy to understand and not that hard to configure.

Figure 4.102 Services

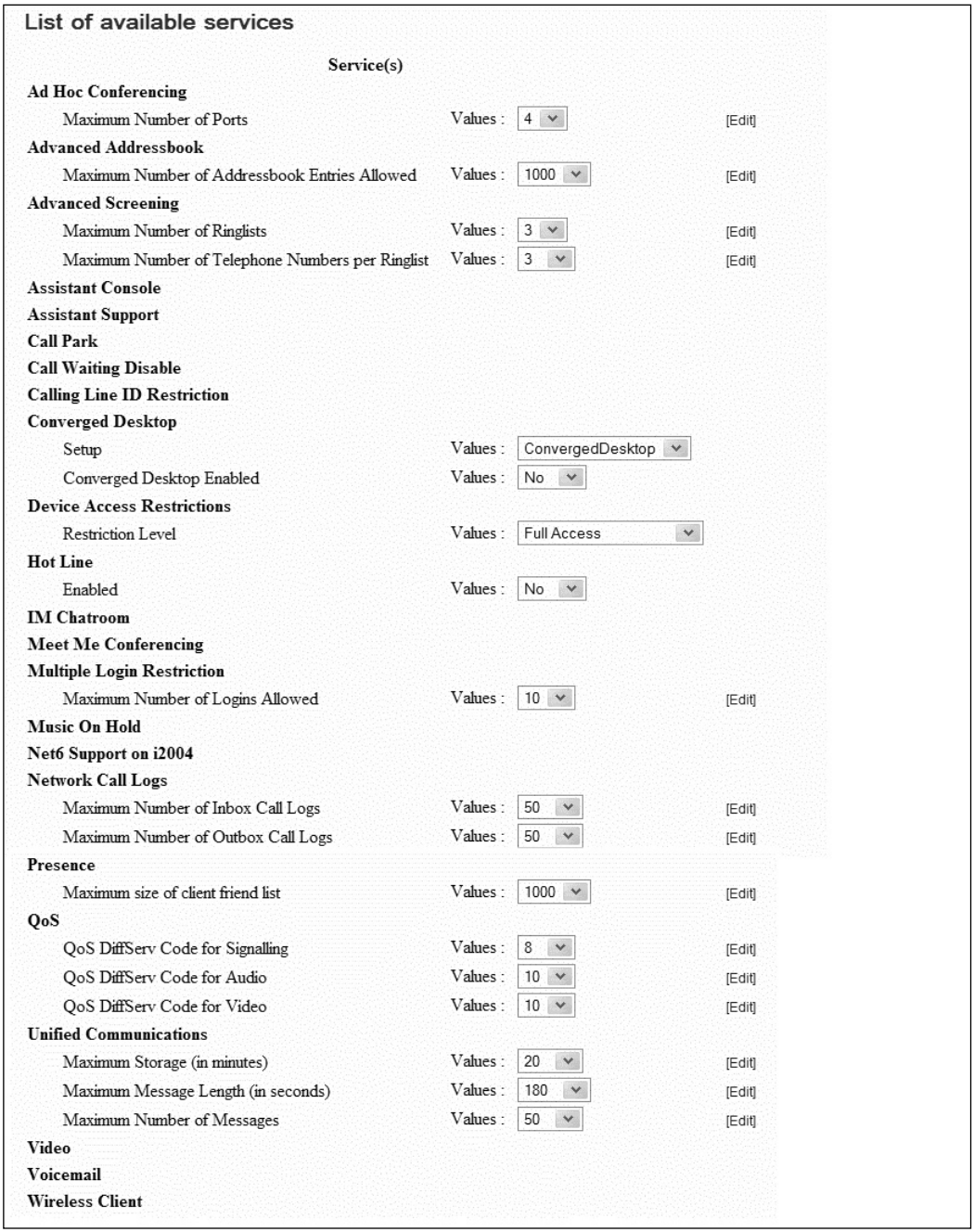


Define Service Parameters

In this section, we discuss a list of available services in Figure 4.103 for the domains that have been created. Not every service has a value that may be changed, but for the ones that do, you will see it to the right of the service. The administrator may choose from the drop-down menu in each value to select the value they wish to use for that service. If a value you would like to

use is not in the drop-down box, the administrator may select the edit button to the right. Then the administrator may add a value that is needed.

Figure 4.103 Define Service Parameters



Assign Services and Assigned Resources

After the administrator has chosen the values for the aforementioned services, he or she will need to assign the service to a domain.

Next, select **Assign Services** to produce the drop-down box shown in Figure 4.104. Here the administrator will select the domain to assign the services to. After the administrator selects the **continue button**, Figure 4.105 will be displayed. Use the drop-down box to select the domain to which the services will be assigned. The administrator will then put a check in each box for which he or she wants to assign to the domain. Also, the values on the right may be selected from the drop-down box. After all services are selected, click **Save**.

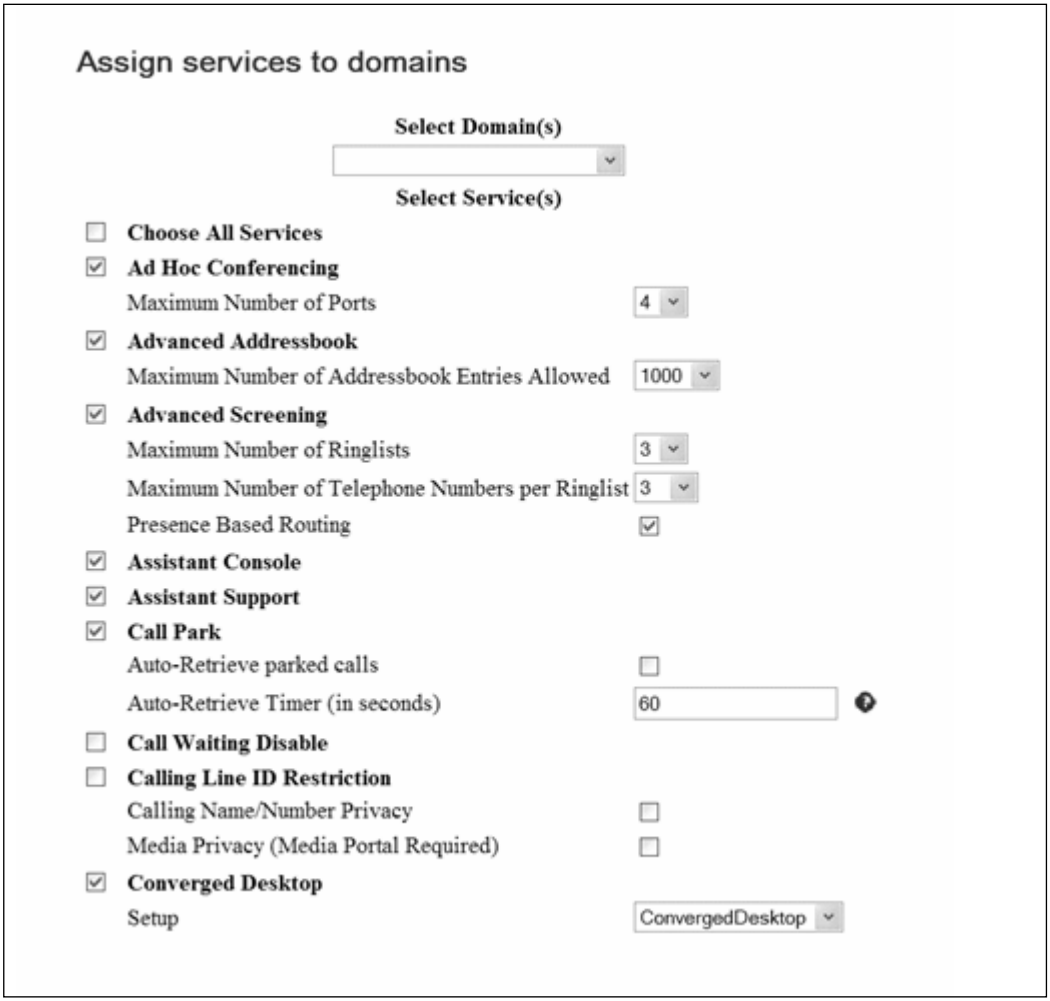
Configuring & Implementing…

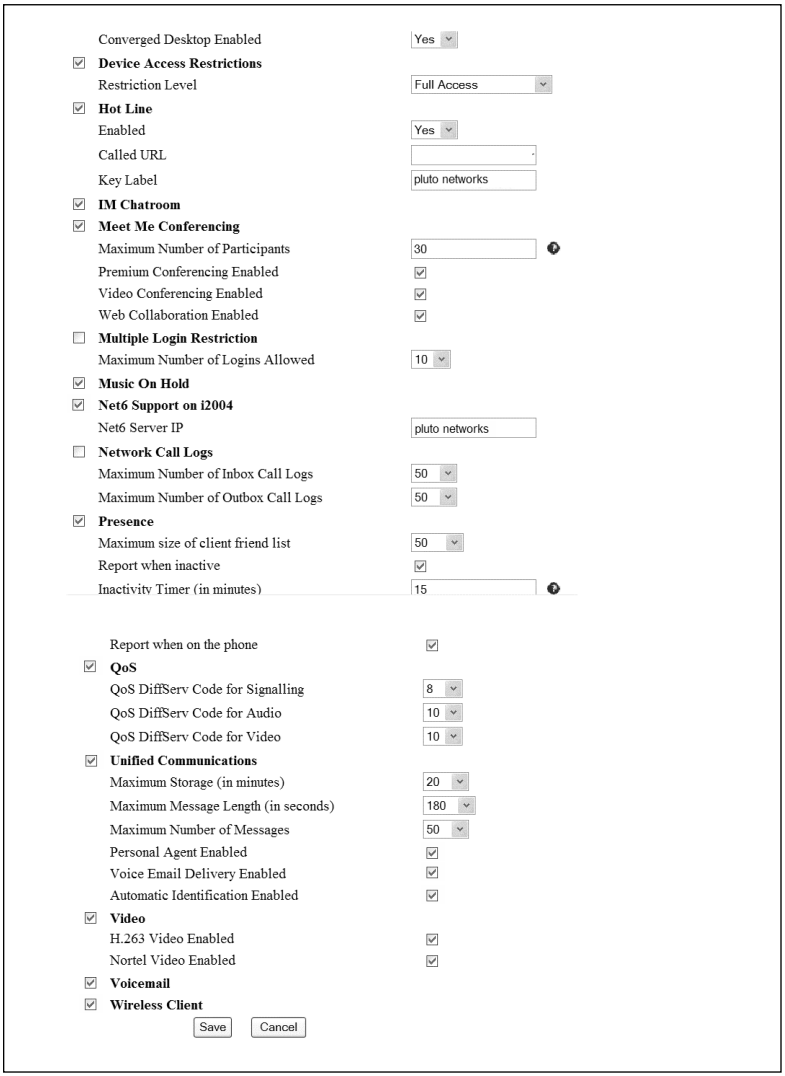
Services

When configuring the services, remember you may only assign the services for which you have licenses at that time. If you select a service for which you do not have license, you will receive an error message after clicking **Save**. The administrator will need to uncheck the box and click the **Save** button again for you to move to the next screen.

Figure 4.104 Assign Services

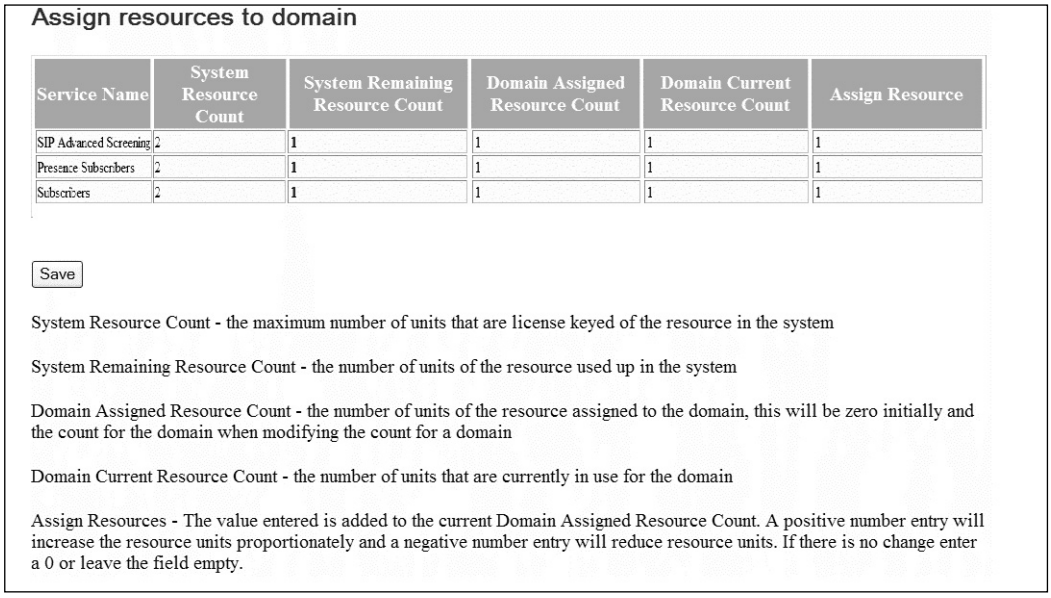
Figure 4.105 Assign Services to Domain





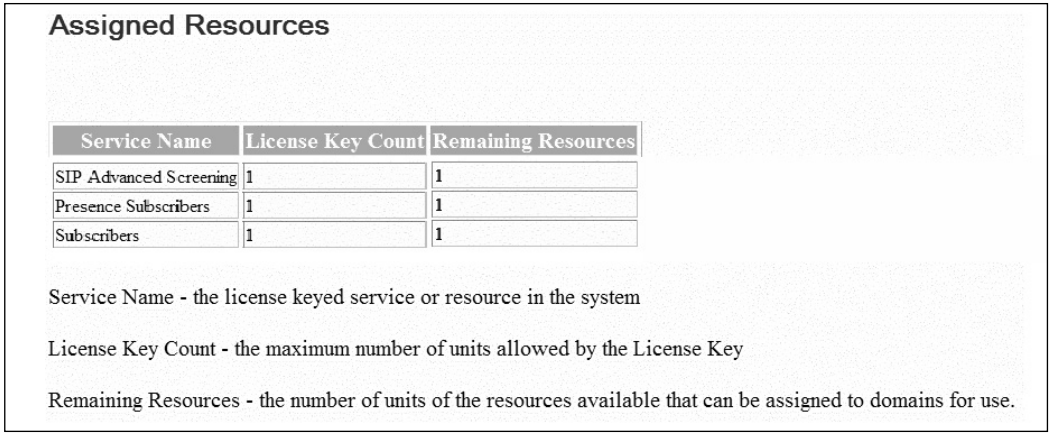
After you select **Save** in Figure 4.105, the screen in Figure 4.106 will display. Here is where the administrator will be able to assign resources to the service names. These resources are what you have licenses for on the system. So, if you have 200 presence licenses and need to split them up between different domains, you may do that in this area. Also, if you have assigned 100 users to the license and only 50 are being used, it will show the remaining count for the service. The administrator may also take resources away from a service name by adding a -2 to the *Assign Resource* box. This will take away two licenses or resources, and those may be used in another service name.

Figure 4.106 Assign Resources to Domain



When you select the assigned resources, the system will display Figure 4.107 showing the administrator what service name is being used on the system for licenses or resources. Next, it will show the current license key count and the remaining resources. This is a great area to look into when adding resources or planning for future user counts. Since the user will need service, the administrator will need to know what is available in the system.

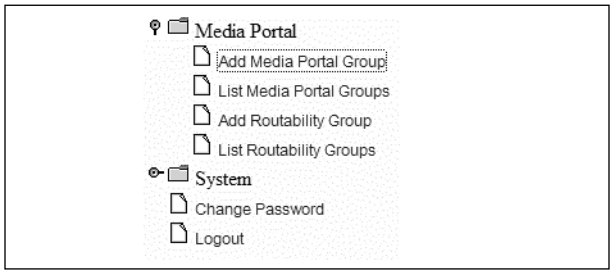
Figure 4.107 Assigned Resources



Media Portal

The Media Portal is a media proxy device that provides a variety of functions to overcome the obstacles to general deployment of MCS 5100. These functions enable the solution to extend its reach to include endpoints (to those clients that are behind a firewall or need a Network Address device). This is an option function of the MCS 5100 since most of the time you will not need this in the system. In Figure 4.108, we have selected the Media Portal Group from the system tree. There are four areas and only two need to be configured.

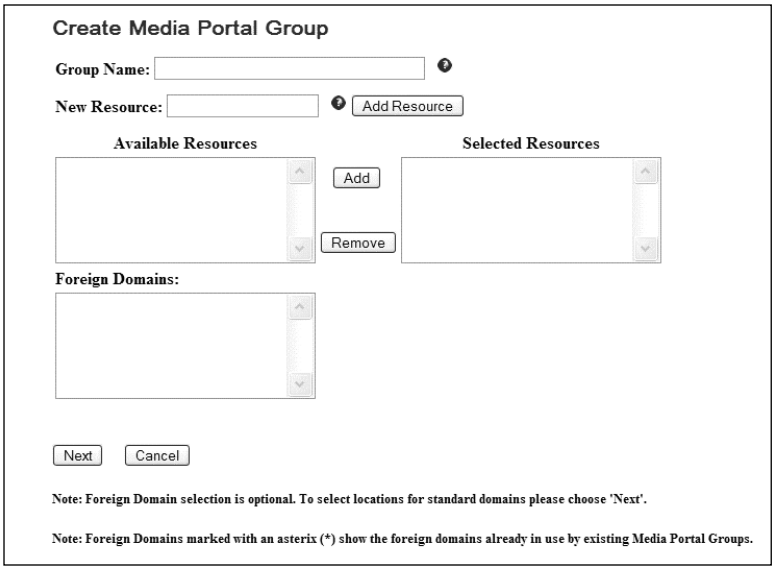
Figure 4.108 Media Portal



Create Media Portal Group

After selecting the **Add Media Portal Group**, add the new group name in the first box under Create Media Portal Group. Then you will need to add a new resource, which would be an IP address, and click **Add Resource**. The resource is added as a New Resource, shown in Figure 4.109. Next, you may highlight the IP address in **Available Resources** and select **Add** to move it over to the Selected Resources. The administrator may also select a foreign domain if one has already been added to the system. After you have completed your selections, click **Next.**

Figure 4.109 Add Media Portal Group



This will move you onto Figure 4.110, which allows the administrator to choose the domain in which to add the portal group. After selecting the domain, click **Next**. The administrator will move to Figure 4.111, which allows selection of the location for which the portal group will be used inside the domain. Click the **Save** at the bottom of the screen.

Figure 4.110 MP Portal Group Added

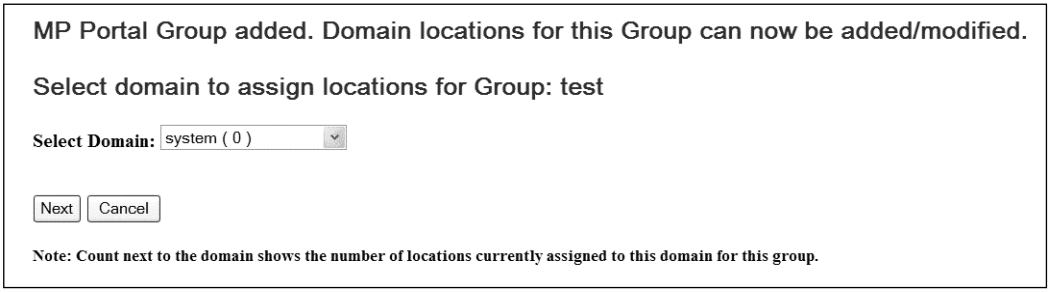
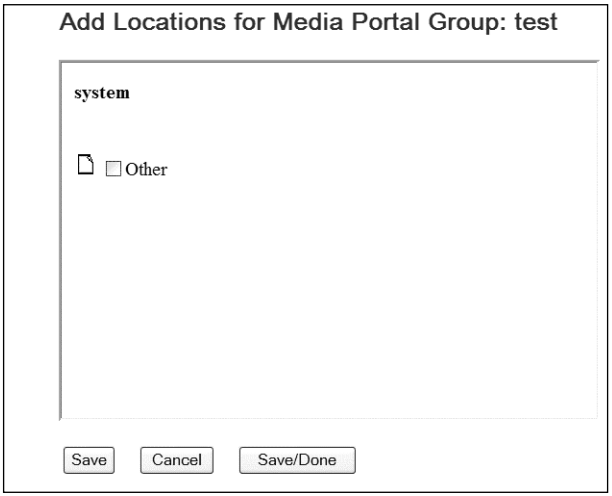


Figure 4.111 Add Locations for Media Portal Group



Once finished with the aforementioned tasks, the administrator may use the List Media Portal Groups to display the work done, as shown in Figure 4.112.

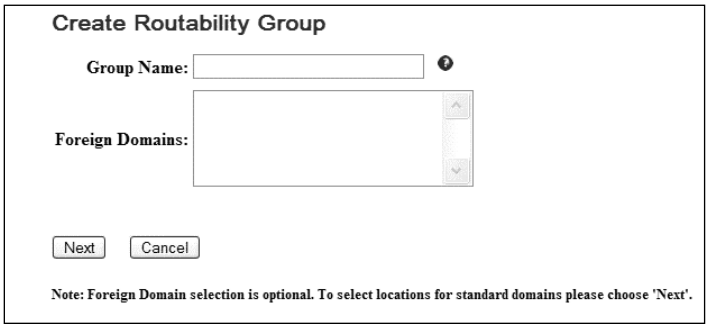
Figure 4.112 List Media Portal Group

Create Routability Groups

A routability group is the network topology of the customer's service area within the network. It consists of the locations that describe the geography that's served in the network and the network topology that connects them. This network will have firewalls and NAT devices spread throughout it, so some of those locations will be able to route clearly to others, and others will not. Those that can route clearly to each other could be placed in a routability group. That means that since they can route clearly, no portal is required. In Figure 4.113, we have selected the Create Routability Group. The administrators will need to select a name and the foreign domains to add to the group.

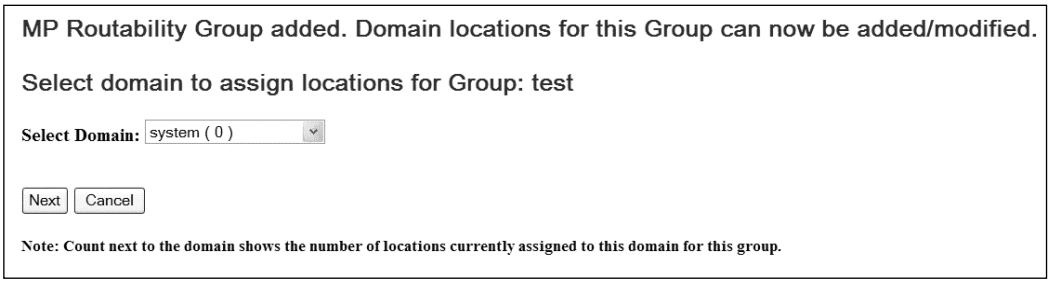
Once that is completed, they will need to select the **Next** button at the bottom.

Figure 4.113 Create Routability Group



As in the preceding section, the administrator will need to select the domain to which the routability group will belong, and click **Next,** as shown in Figure 4.114. Figure 4.115 will then be displayed, and the administrator will need to select the location for the routability group in the domain, and save the changes.

Figure 4.114 MP Routability Group Added



Once complete with the tasks, the administrator may use the list routability groups to display the work done, as shown in Figure 4.116.

Figure 4.115 Add Locations for Routability Group

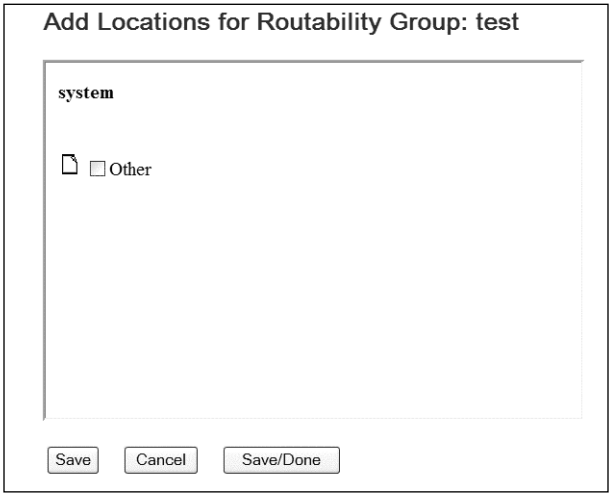
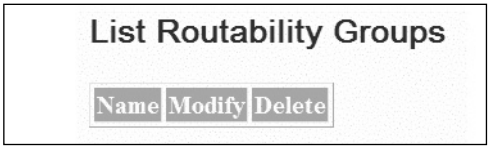


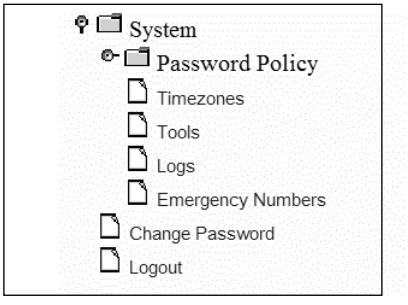
Figure 4.116 List Media Portal Group



System

In Figure 4.117, we have the last area we will cover, which are the system settings. These settings, as you can see, are general to the whole system and not just each domain. They are such areas as time zones, tools, logs, and emergency numbers. We will show these in detail for the administrator, but first, we must select the system area on the system tree to display the areas we just listed.

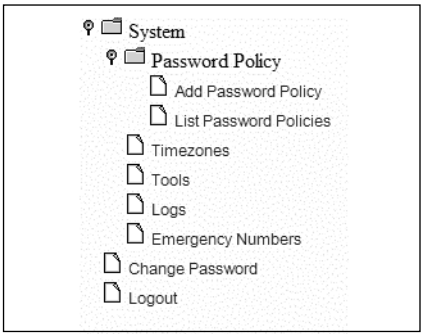
Figure 4.117 System



Password Policy

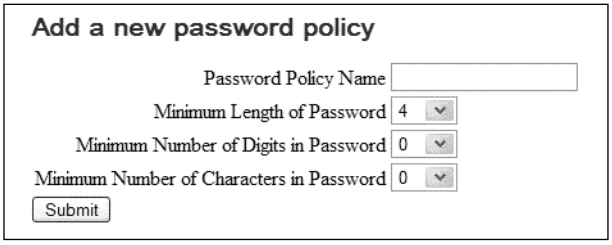
The first area shown in Figure 4.118 is for the password policy. This is a system setting and is how the administrators log into the system. After selecting the password policy, we have one area to configure—the *Add Password Policy*. Now the administrator may have many password policies, but we would recommend using one to keep a uniform look.

Figure 4.118 Password Policy



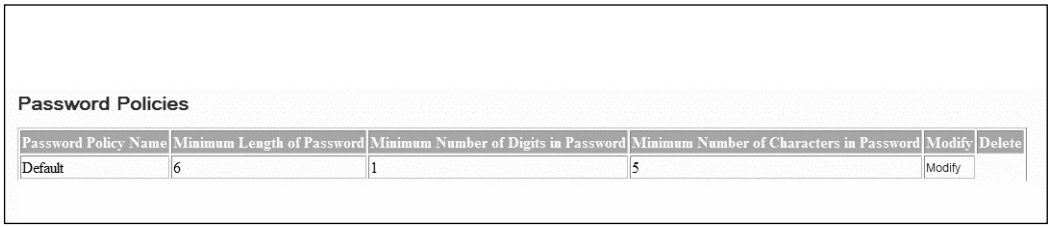
In Figure 4.119, we have selected **Add a New Password Policy**. The administrator needs to give a name to the password policy first. Then using the drop-down boxes, he will select the minimum length of the password and the minimum number of digits in the password. Last, he will select the minimum number of characters in the password, and click **Submit**.

Figure 4.119 Add New Password Policy



In Figure 4.120, we have selected List Password Policies from the system tree. As you can see, it will list all configured policies. The administrator may use the modify button at the far right to make changes to the password policy, if needed.

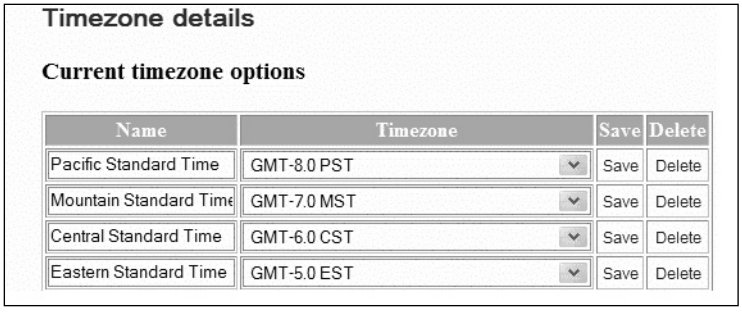
Figure 4.120 List Password Policy



Time Zone

Next the current time zones for the system need to be configured, as shown in Figure 4.121. Using the drop-down menu, the administrator may change the time zone associated with the current name to the left. After changes are made, click **Save**, to the right of each change.

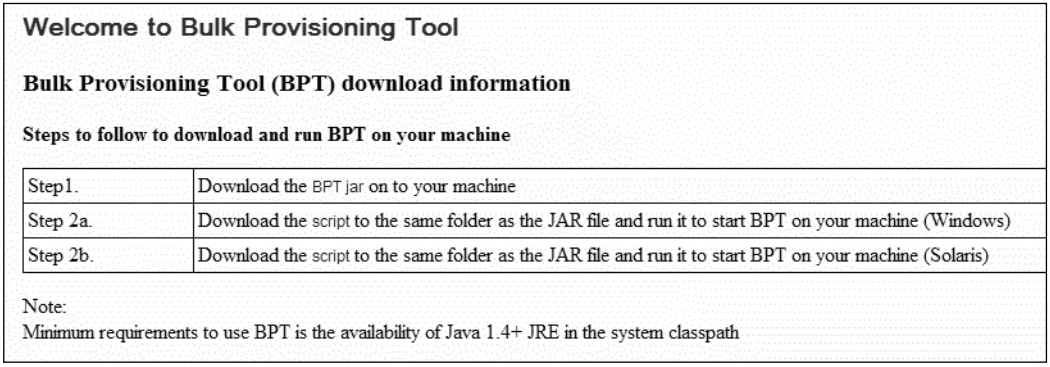
Figure 4.121 Timezone Details



Tools

The tools area in Figure 4.122 shows a bulk provisioning tool that can be downloaded to your machine, allowing the administrator to add a large group of users all at once, saving time. However, we recommend that you make a dummy or test domain to use this tool before trying it on your real domain. If you do something wrong, it could affect your domain.

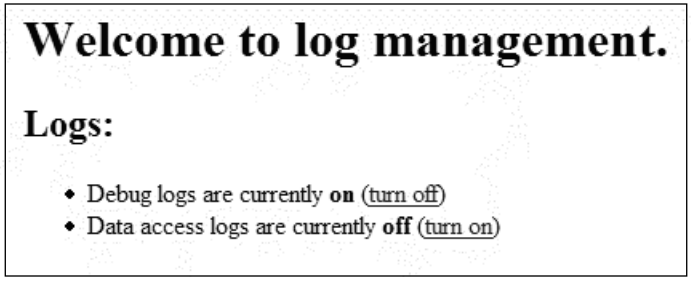
Figure 4.122 Bulk Provisioning Tool



Logs

Figure 4.123 depicts the small area that allows the administrator to turn on the debug and data access logs. Select the **Turn on** or **Turn off** to the right of each selection.

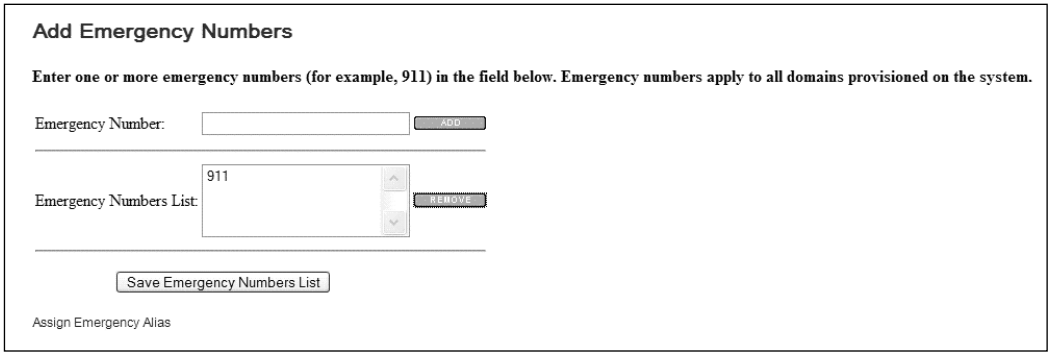
Figure 4.123 Log Management



Emergency Numbers

To add emergency number to the list, use the Add Emergency Numbers function, as shown in Figure 4.124. This is where you add 9-1-1. Click the **Add** button. This will put the 9-1-1 number in the Emergency Numbers List. After this is complete, click **Save Emergency Numbers List** at the bottom.

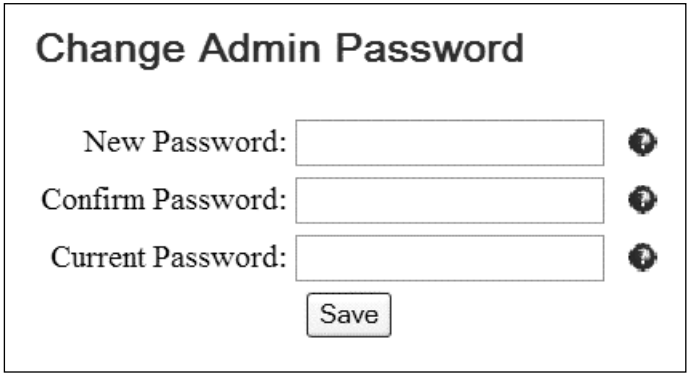
Figure 4.124 Add Emergency Numbers



Change Password

The last area to configure or change is Change Admin Password (see Figure 4.125). This is the root password for the MCS 5100 system. Please be careful when changing this. If you lose the password or make a mistake, it will be a long day. But you will need the current password for the system to make a change to a new password.

Figure 4.125 Change Admin Password



Summary

The provisioning client is the main administration part of the MCS 5100, and it is critical that the administrator know this client very well. Not understanding this section or how it works will hamper the system as a whole. Besides configuring users and options, the telephone routes and other options are configured on the client. The understanding of SIP routes is necessary to configure sections and options in the client. It is suggested that a dummy domain be created for the administrator to use in practice before making changes to the system. It is important to understand that options outside the domain and system-wide, and changes to those options will affect the whole system.

Solutions Fast Track

Administration

- ☑ It is suggested that the list of administrators to the system be kept to a minimum due to the nature of the system.
- ☑ Plan your roles for each administrator and what roles they will have in the system.
- ☑ Remember to delete administrators if they have no further use on the system; this is a good security tip.

Domains

- ☑ This section is the area where you will spend the most time in getting to know what a domain, sub domain, and foreign domain are. The more familiar you are with the system, the easier it is for the administrator to make the configuration.
- ☑ Changes made in this area affect the domain or sub domain you are in. Making changes to one domain will not affect another domain.

- ☑ All user changes are made in the domain or sub domain level. This includes adds, changes to users and service packages, and such things as password or number changes.

Devices

- ☑ To find a device on the system, just insert the Mac address.

Gateways

- ☑ Plan the type of gateways needed in the system to connect to the PSTN, and also a voice mail server.
- ☑ Changes to the gateway area are system-wide since the gateway is for the entire system and all domains.
- ☑ Create trunk group and routes names that make sense for the equipment and protocol used. This will help later, when making changes or troubleshooting.

IPCM Cluster

- ☑ The IPCM cluster will be the physical IP address of the IPCM Sun Server configured.
- ☑ Also, the application server may be added to the IPCM cluster.

Voice Mail

- ☑ Most systems will use a Call Pilot voice mail system, at which time you will configure a SIP voice mail route.
- ☑ Remember to use the application server physical IP address when filling out the add voice mail area.

Services

- ☑ This area is a systemwide area that affects the services and values assigned to the selected domain.
- ☑ After making changes, remember to assign the changes to the correct domain.
- ☑ Use the view resources area to plan for upgrades and added users. This will save time if new resources are needed before adding users.

Media Portal

- ☑ The media portal is an optional area to configure. Most systems will not need a media portal for the system to work properly.

System

- ☑ General settings for the system, such as password policy for administrators and configuration of time zones, are done here.
- ☑ You may download the Bulk Provisioning Tool from this area.
- ☑ Emergency numbers such as 9-1-1 will be added in this section, and you also have the ability to turn on and off logs in the system.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Is it necessary to have separate domains for all of the company's sites on the MCS 5100?

A: While you can do that, I suggest that there be one domain and that all of the sites not in the same city be sub domains. This will work better for E911 services and also telephone routes.

Q: Can a user belong to more than one domain?

A: No. The user is subject to only one domain, but you can create the user a new user name for another domain, if needed. It is not recommended in the system, though.

Q: Why does there need to be more than one service package for the domain?

A: While there does not have to be more than one if all of the users are going to have the same options on the system, if certain user will not be using services that have resources assigned to them, it is best to make separate service packages to save resources.

Q: Is it better to create status reason for users or allow them to create their own in the system?

A: As long as you have a policy, they can create their own. But sometimes people will add some improper messages in the system.

Q: Why is there a need to create different locations on the domain?

A: The biggest reason is E911, so that users may select the location where they are with a PC Client or IP Phone.

Q: Is LDAP a needed function of the MCS 5100?

A: It is not, and we have many customers who do not use it. However, it does save time if you can use it in the system.

Q: How many gateways will I need for the system? I see there were two listed in the section?

A: You can have as many as you would like, but the SIP gateway is a virtual gateway that connects to a server on something like a CS 1000.

Q: Can I use the Provisioning Client from anywhere, or just within the network?

A: As long as you have access to the IP address assigned to the Provisioning Client, you can use it.

Chapter 5

Ad Hoc and Meet Me Conferencing

Solutions in this chapter:

- **Ad Hoc Conferencing**
- **Meet Me Conferencing**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

In this chapter, we discuss the configuration of the Ad Hoc and Meet Me Conferencing Servers. To understand the difference, the installer needs to remember that these are located on separate IBM servers. Based on your system, you may have more than one server for each service. This will depend on the number of users you have on the system. It could also depend on the number of users you have given the service to within the service package.

In the MCS 5100, the Ad Hoc Conferencing Server is a required server for the system. The reason for this is to allow the user to place a caller on hold, call another person, and then conference in all three. The Meet Me Conferencing Server is an option server that is used to support conference call numbers. This is used when you are going to have a regular conference call that many users will dial into. Both of these servers support audioconference and videoconference calls.

Ad Hoc Conferencing

The Ad Hoc Conferencing Server is used for both audio and video calls. The service runs on the Nortel MAS (Media Applications Server). The server will provide audio mixing and transcoding for G711 and G729 audio codecs. Also, it will provide RTCP and QOS support for the service. The service will support multipoint videoconferencing using the DivX. The service should run on its own server with no other services added to the server (per Nortel documentation), but we have added other services with no problems. However, we recommend that Nortel documentation is followed and that all services have their own dedicated server.

The server will need to either be an IBM xSeries Server or an IBM eServer Blade Center. Windows 2000 Server runs on both of these pieces of hardware.

Configuring & Implementing…

Pooled Servers

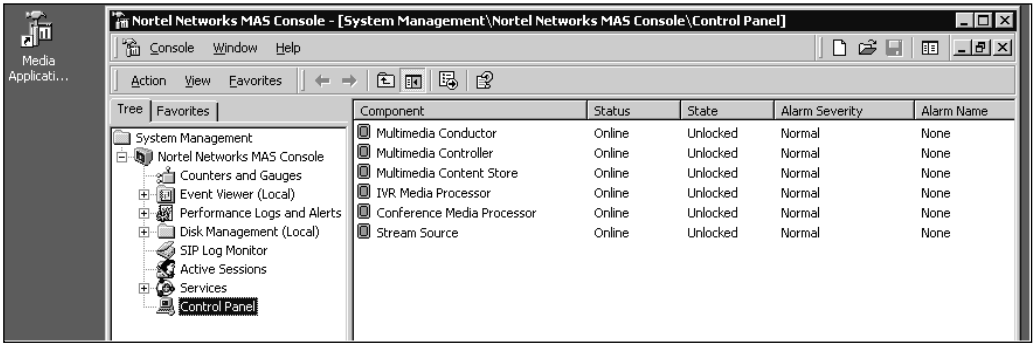
The systems that we are looking at in this chapter are single-server systems. They can be used in a pooled server configuration to add more resources to the MCS 5100. To understand how to do this, please reference the Nortel documentation on adding pooled servers for the Ad Hoc and Meet Me Conferencing Servers.

MAS Console

The Nortel MAS Console is the only piece of software that will be loaded onto the IBM server. After you click the **Media Application Server** icon on the desktop, the MAS console will appear, as in Figure 5.1. As you can see, it looks like any other window application under system management. But in the component window, you can see we have the MAS components. All of the components listed are shown in the status as online and unlocked. For the system to be operational, remember that these need to be unlocked. To make changes, as in the MCP Client, you would lock the component.

The alarm status is in a normal state with no alarms. If the component was in alarm, it would show it here and list the alarm. Also you would see it in the event viewer just like in windows. On the right is the Nortel MAS Console Tree. Under services, you see the services loaded and where to configure them. In the system tree, you also have a SIP Log Monitor where you can watch the logs while the service is being used. It also has an Active Sessions area that will display the user on the system from inside and outside the system.

Figure 5.1 Nortel MAS Console



Counter and Gauges

In the tree, the first area listed is the Counter and Gauges. This is where you can watch real-time statistics about the services running on the server. This area is good to use when you are having problems with the server and need to get information to refer to Nortel Technical Support. In Figure 5.2, we have clicked the counter and gauges in the system tree. It has a default number of counters and gauges that will display at first, but there are many more that you can use.

In Figure 5.3, we show the Add Counters window. In this window, you may add all of the counters available to the system or just selected ones from the window. From the drop-down window, select the **performance object**, and under that, in the counter window, select the **counter** you would like to display.

Event Viewer, Performance Logs, and Disk Management

Just as in Windows, you will have an event viewer, performance logs, and alerts on the system. Also, there will be an area for disk management, as shown in Figure 5.4. As in Windows, you use the same method to troubleshoot problems with the server and applications installed on the server. If you are having an issue on the server, the Event Viewer is the first place you should look to see what errors are listed on the server. It will also show the errors for the Nortel application installed on the server. This is a great help since most people are used to troubleshooting problems on Windows servers through the management tree.

Figure 5.2 Counter and Gauges

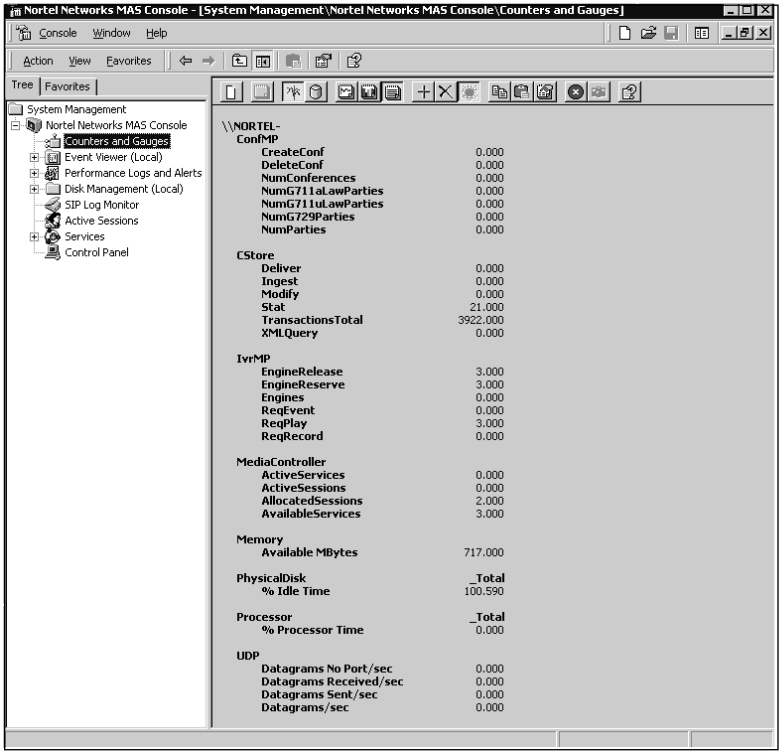
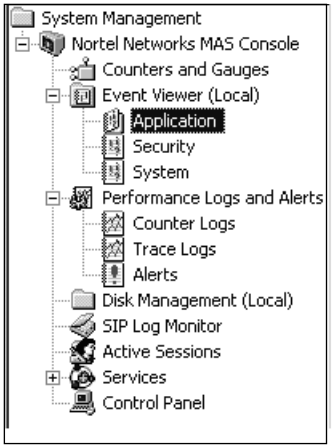


Figure 5.3 Add Counters

Figure 5.4 System Tree



System Configuration

In Figure 5.5, we have selected the services area from the tree, which has taken us to the system area and the configuration properties for the system. In the figure, the settings we have listed are default settings for the system, but you may change these based on your system. Within the content store server, local host name or IP address, and stream source destination servers, insert the IP address of the Ad Hoc Server. The SIP application server property, of course, has the IP address of the application server, but you need to add :5060 at the end of the IP address for it to work.

The license key that you have downloaded from the Nortel Web site will be pasted into the License Key property area. The preferred video frame size may be changed from larger to smaller based on your system limitations. If you are using an exterior alarm server, you will need to add your SNMP community string. Further, you will need to change the SNMP log traps from no to yes and input the SNMP management server IP address.

Ad Hoc Conferencing Configuration

The configuration for the Ad Hoc Conferencing is as easy at it seems in Figure 5.6. Both of the properties are required, and you want to select yes for *Send Accounting INFO* and then, enable the video either yes or no. If you have, the licenses for this, select **Yes**; if not, select **No**.

Figure 5.5 Services: System and Configuration

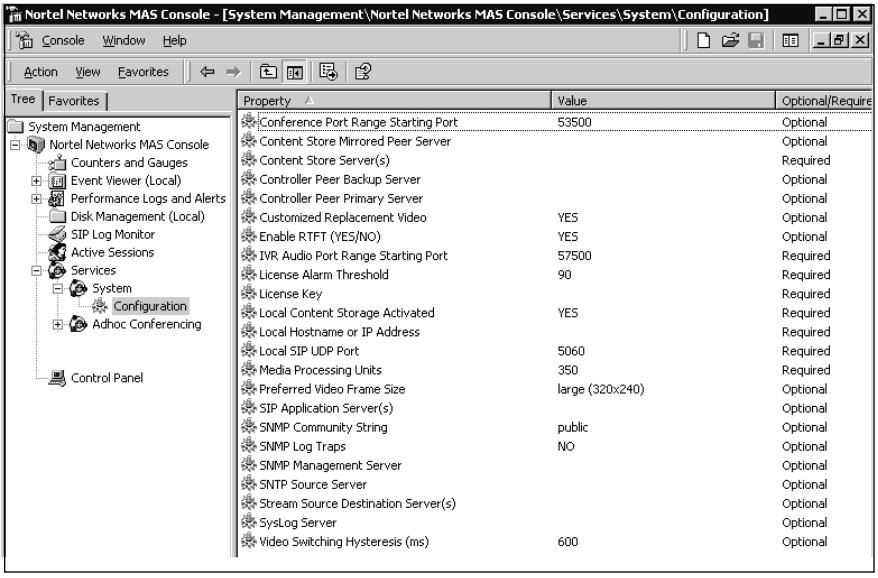
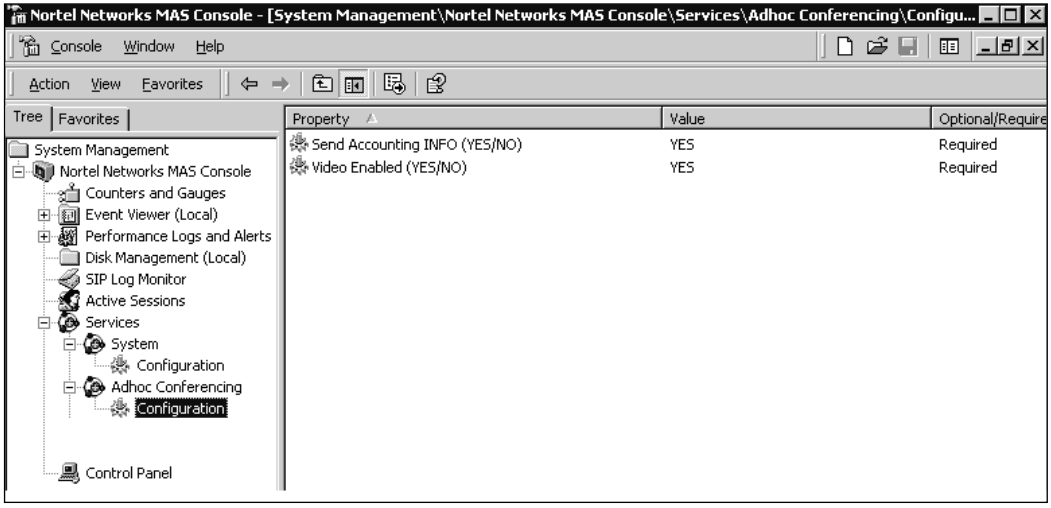


Figure 5.6 Services: Ad Hoc Conferencing and Configuration

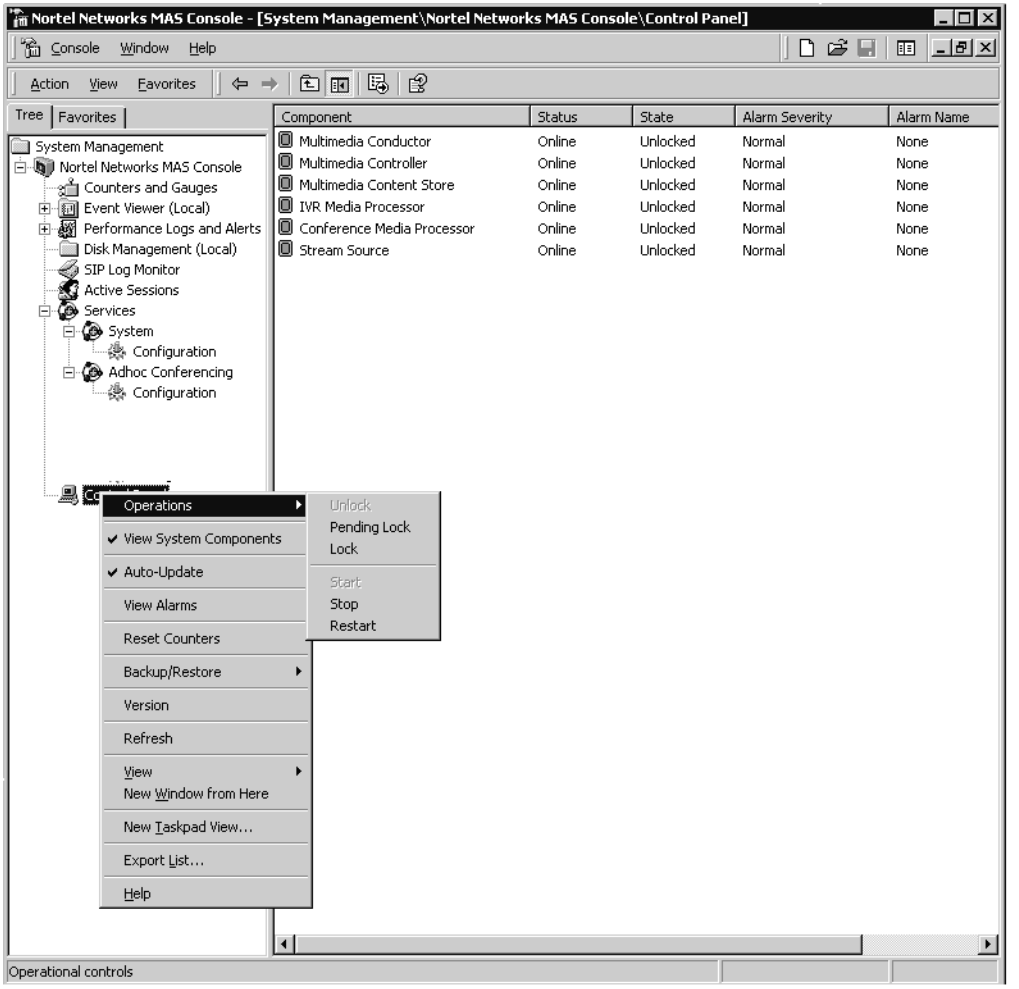


Control Panel

In Figure 5.7, if you right-click the control panel, it will display the menu shown. The Control Panel allows you to lock, unlock, pending lock, start stop, or restart the components on the server. You may also view the alarms, reset

the counters, back up or restore settings, and look at the version of software you have on the system.

Figure 5.7 The Control Panel

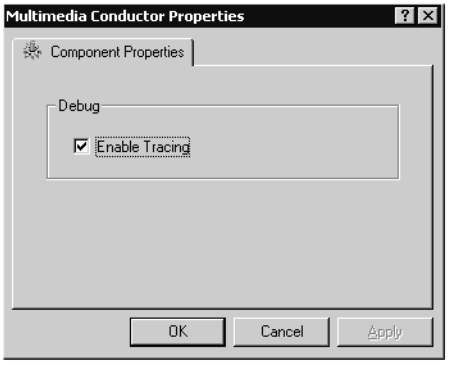


NOTE

Remember when you are looking for the version of software on the server, you need to look in the area under the Control Panel. Sometimes people forget it is there and waste time trying to find the information.

In Figure 5.8, we clicked on the component to get the screen that allows us to turn on debug tracing for the component. We recommend that you not have these enabled unless you have a problem with the system; it takes up space and resources on the server.

Figure 5.8 Conductor Properties



Meet Me Conferencing

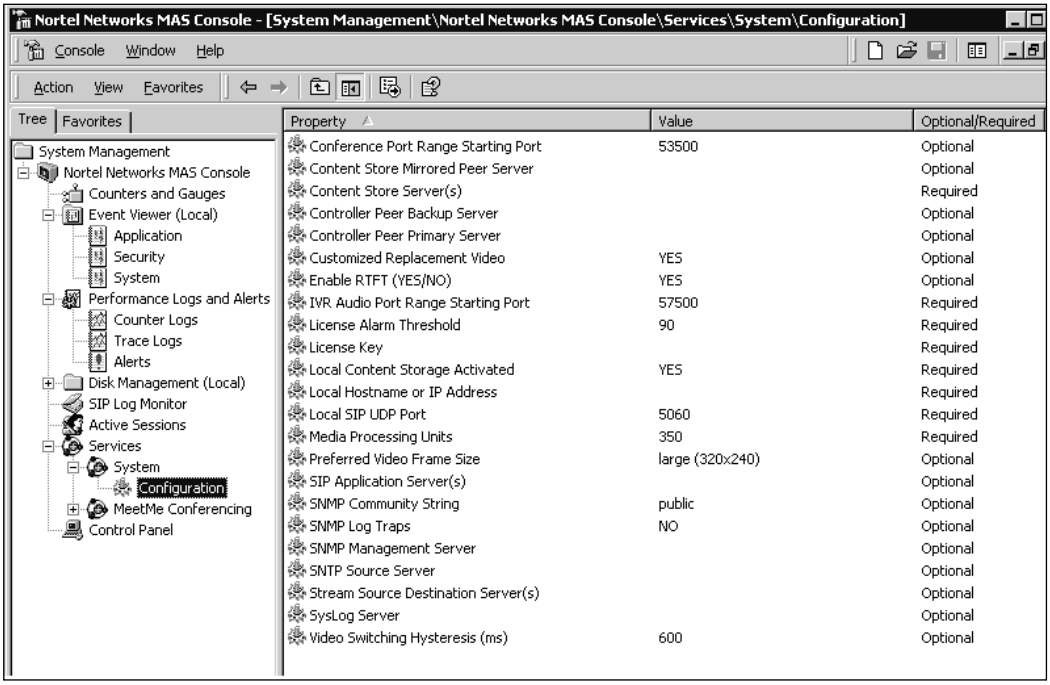
The Meet Me Conferencing resides on the same server as the Ad Hoc Conferencing. All areas other than system configuration and Meet Me configuration are different. In this section, we only cover these two configuration areas. The Meet Me Conferencing is different from the Ad Hoc in the way that people dial into a conferencing number, rather than being added in by putting a user on hold. We show two figures to of the configuration of the server.

System Configuration

As you can see in Figure 5.9, we have selected the services area from the tree, and that has taken us to the system area and then the configuration properties for the system. In the figure, the settings listed are default settings for the system, but these may change based on your system. In the content store server, local host name or IP address, and stream source destination servers, insert the IP address of the Meet Me Server. The SIP application server property, of course, has the IP address of the application server, but you need to add ":5060" at the end of the IP address for it to work.

Paste the license key that you downloaded from the Nortel Web site into the License Key property area. The preferred video frame size may be changed from larger to smaller based on your system limitations. If you are using an exterior alarm server, you need to add your SNMP community string. You will also need to change the SNMP log traps from no to yes, and then input the SNMP management server IP address.

Figure 5.9 Services, System, and Configuration

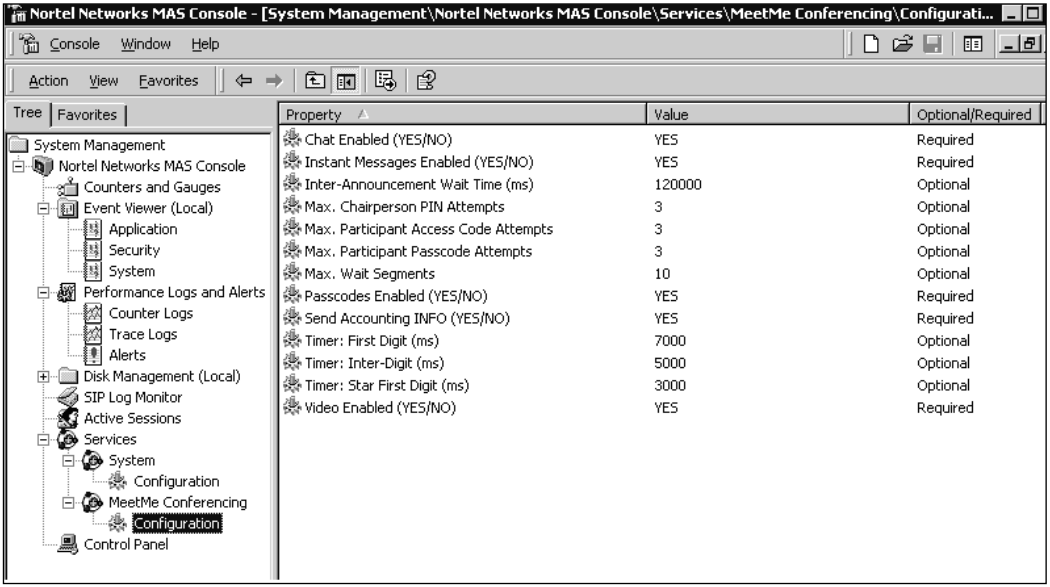


Meet Me Conferencing Configuration

Now we have made it to the configuration of the Meet Me Conferencing Service in Figure 5.10. All of the values for the properties that are options have been set to a default setting. These can be changed based on your system and preferences. If you would like to allow chat in the pc client or Web client while using the conference server, select **Yes**. This is the same for instant messaging during the conference call. As a best practice, you want to select **Yes** for the Passcodes Enabled and for Send Accounting INFO. This allows the administrator to select pass codes for all users to start or join a conference call.

If your system has the option *video license codes* on the system, then you want to select **Yes** in the last property. If you do not have the license code for this, be sure to select **No** for this property.

Figure 5.10 Services: Meet Me Conferencing and Configuration



WARNING

Turn off auto updates to the Windows 2000 Server; some new updates may not work correctly with your version of software on the server. This could cause the Nortel software to stop working or cause problems during the operation of the services.

Summary

As you can tell, there really is not too much to setting these up on the servers or to troubleshooting them. The things to remember are that the Ad Hoc server is a required server on the system and the Meet Me is optional. Both conferencing servers run on Windows 2000 Server so the administration is very straightforward, and troubleshooting is just like other programs installed on a Windows 2000 Server. Also remember that it is recommended that only one type of Nortel service be on a single server.

This means you would not want to put the Meet Me and Ad Hoc Conferencing service on the same server. For adding services such as Music on Hold, Chat, and Announcements, to the same server, because of port restrictions on the servers, always put these services on separate servers.

Solutions Fast Track

Ad Hoc Conferencing

- ☑ A required server on the MCS 5100 system to provide user with a way to place user on hold and do a three-way call.
- ☑ With the correct license code on the system, video can also be added to the audio conferencing. Audio is the default when installing the system.
- ☑ Although video is great to have, remember that there are bandwidth requirements that need to be met for the system to work correctly.

Meet Me Conferencing

- ☑ Provides a personal conference number for all users to use when they want. It is an on-demand system that is always there for the users to have access to.
- ☑ Always enable accounting and pass codes for the conferencing server; this will save your system from people outside the system using the resources.

☑ If conferencing is going to be a big part of your system, remember that you may use more than one server. This is called pooled servers and will make for more resources to be available to the system.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Why is the Ad Hoc Conferencing Server required on the MCS 5100?

A: Without this, you would not be able to do three-way calls or add more people onto a two-way call.

Q: Can this software run on Linux?

A: Right now, the Windows 2000 Server is the required software on both services.

Q: Why can I not just have one server to save money and add all of the options to it?

A: This is due to the amount of ports available to the server at one time. If other services are added, it takes away from the ports needed for just one of the services. Further, it is not supported by Nortel.

Q: Since this is on a Windows server, are there services that start for the Nortel software when the system is booted on?

A: Yes, there are services that start automatically when the system boots up to windows.

FAQ

Q: Since the Windows server updates should be turned off, when do I upgrade the windows server?

A: When Nortel sends information that new Windows server patches are approved for the version of software on your machine.

Q: How is the Nortel software upgraded on my server?

A: This is done by either downloading the software to the machine or using a CD to apply the software to the server. It will be a Windows-based *exe.* application.

Chapter 6

Multimedia PC Client

Solutions in this chapter:

- **Installing PC Client**
- **Logging On**
- **Preferences**
- **Make a Call and Video Call**
- **Instant Messaging**
- **Directory**
- **Call Logs**
- **Friends Online**
- **Retrieve Parked Call**
- **Change My Status**
- **Advanced User**
- **Capture Logs**

Introduction

The Nortel Multimedia PC Client is an application-based *soft phone* that provides many features that are not available on typical Internet Protocol (IP) phones. Some of those features include:

- A Do Not Disturb (DND) feature
- Instant Messaging chat rooms (IM Chat) for creating a chat room
- Advanced call handling to decline, redirect, or ignore incoming calls from internal and external clients
- Instant messaging for internal users to and from IP phones and PC clients
- Video and video conference calls using Meet ME and ad hoc servers
- Conference calls using Meet ME and ad hoc servers
- Collaboration tools (Web address push, shared whiteboards and clipboards)
- IP calls via Session Initiation Protocol (SIP) and UNIStim
- Advanced call logging for tracking incoming, outgoing, and missed calls via PC client
- A personal address book for internal and external clients
- A global address book for network clients
- Presence screening that shows who's online
- Controlling the Nortel IP phone via a Media Access Control (MAC) address
- The ability to place calls, use the call park/retrieve feature, and call transfer
- File transfers, which send and receive files to internal clients

This chapter examines the recommended computer requirements for the PC Client. The PC Client works best when there is a large amount of random access memory (RAM), which is needed when there are multiple

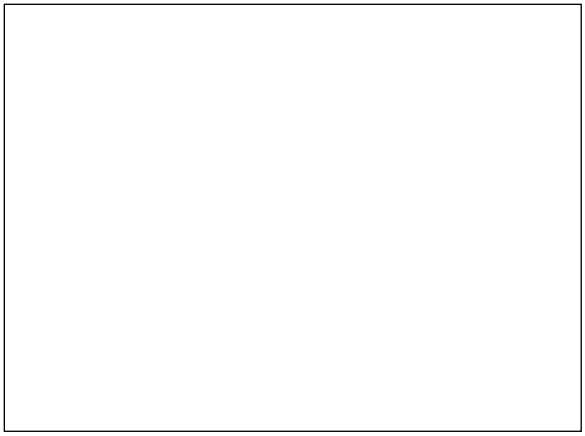
programs being used simultaneously. Following are the recommended computer requirements:

- At least a 1 Gigahertz (GHz) (or higher) Pentium-class or equivalent processor
- Microsoft supported versions Windows XP, Windows 2000, Windows 2002, Windows 98(SE), or Windows NT 4.x with Service Pack 5 (SP5)
- A 56-kilobit-per-second (Kbps) modem or faster network connection. (Network connections are recommended, due to the amount of data needed for the PC Client.)
- A full-duplex sound card with headset (microphone-headphone combination)
- A minimum of 64 megabytes (MB) of free RAM
- At least 75 MB of free hard disk space
- 800 x 600 or better video graphics card

Installing PC Client

This section covers installing a PC Client on a Windows-based machine, which is in *window.exe* format. Double-click the required file to start the InstallShield Wizard (see Figure 6.1).

Figure 6.1 InstallShield



Click the circle in the upper right-hand corner of the screen to open the software License Agreement (see Figure 6.2). The License Agreement indicates when the current software is set to expire, and forces the administrator to stay up-to-date on the newest versions of the PC Client (see Figure 6.3.) Click the **Next** button.

Figure 6.2 License Agreement

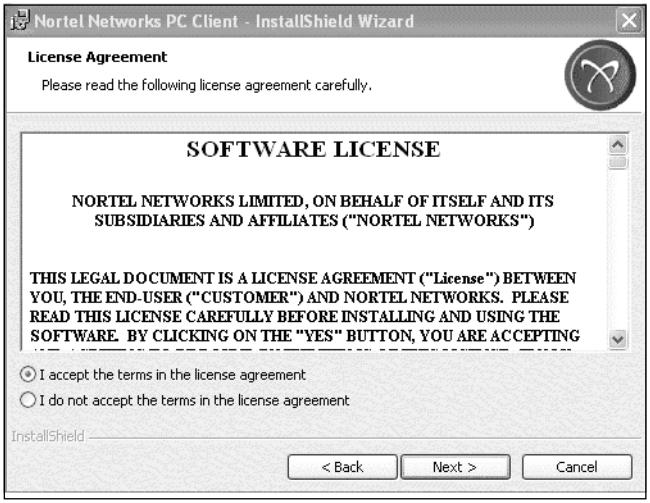
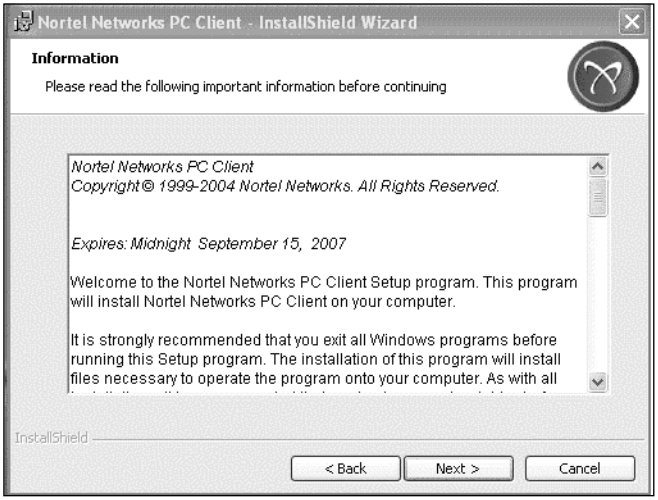
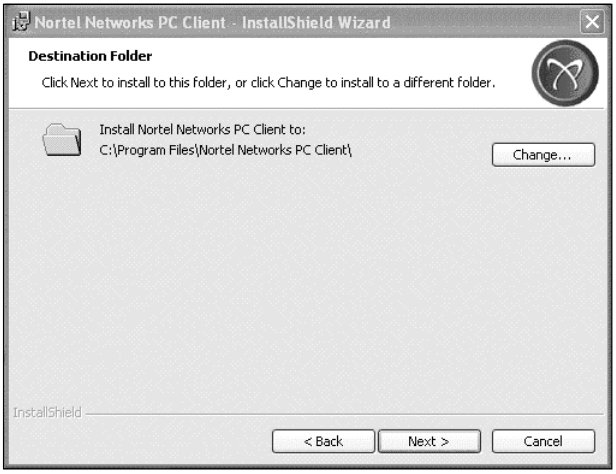


Figure 6.3 Information



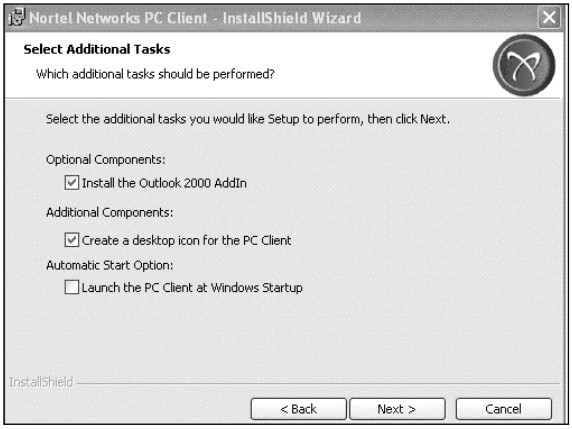
At the Information screen, choose where you want the file to be installed on the local PC. You can accept the default settings (recommended) or choose another location for the file installation (see Figure 6.4). When complete, click **Next**.

Figure 6.4 Destination Folder



At this point you can install the Outlook 2000 Add-in, which allows you to make calls to imported contacts from Outlook 2000 or 2002. You can also install a desktop shortcut to launch the PC Client when Windows is started. Place a checkmark in the box located next to each additional task you require and click **Next** (see Figure 6.5).

Figure 6.5 Select Additional Tasks



On the screen titled Ready to Install the Program (see Figure 6.6), use the Back button to double-check your work and correct any mistakes. When done, click the **Install** button. When the installation is complete, the Installation Completed screen confirms that the installation was successful (see Figure 6.7). Click **OK**.

Figure 6.6 Ready to Install the Program

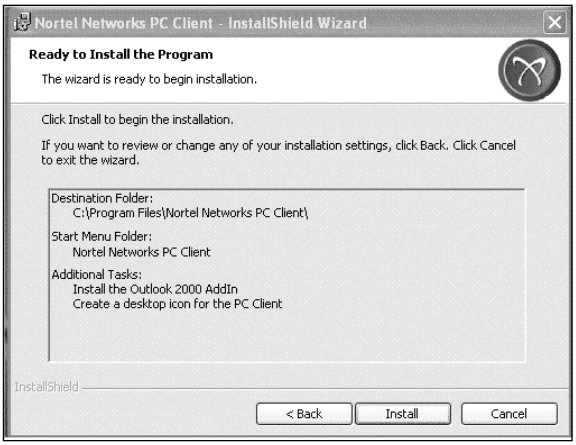
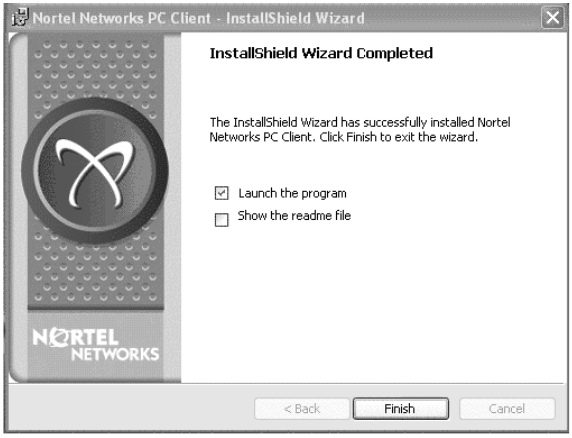


Figure 6.7 Installation Completed

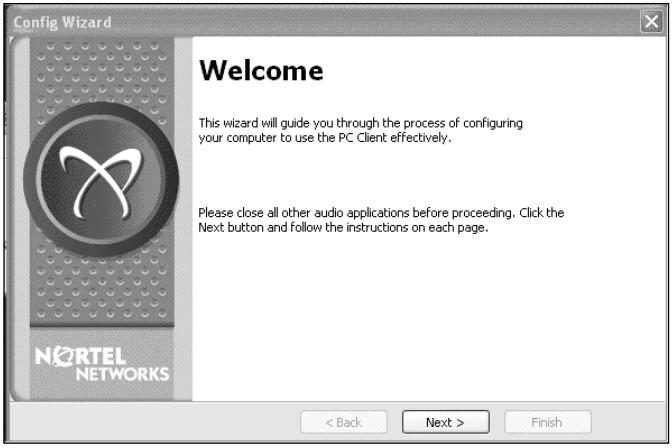
When the installation is complete, the InstallShield Wizard Completed screen appears, at which point you can choose to launch the program (see Figure 6.8). When done, click **Finish**, which will launch the PC Client on the desktop.

Figure 6.8 Installation Wizard



As part of the installation process, the Config Wizard will help configure the user and network settings (see Figure 6.9). Select the **Next** button to begin installation. Type in your username and then click **Next** (see Figure 6.10).

Figure 6.9 Welcome



Type in the **Proxy Address** and **Domain Name** and click **Next** (see Figure 6.11).

Figure 6.10 User Information

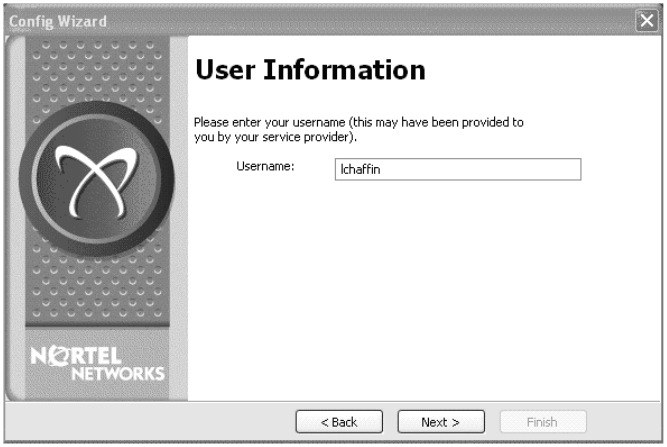
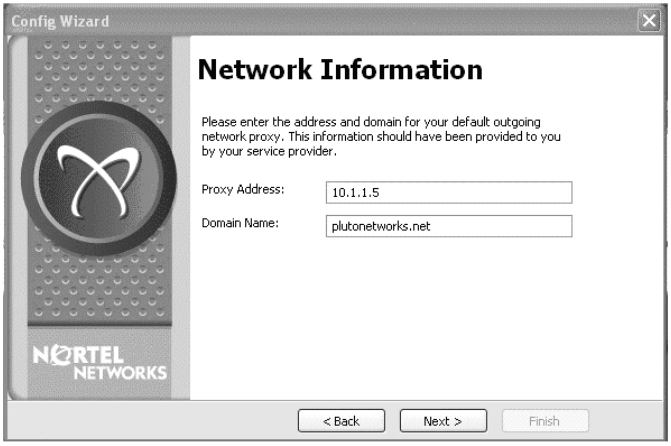


Figure 6.11 Network Information



At the Connection screen, type in the **current IP address** to be used for your PC Client and select the speed at which you will be connecting to the network. Click **Next** (see Figure 6.12).

If you are going to use headphones and microphones for the PC Client, you will need to test and configure the audio settings. With your audio equipment attached to your computer, click the **Start** button and speak into the microphone. You should be able to hear your voice coming out of the speakers. Click **Next** (see Figure 6.13).

Figure 6.12 Connection

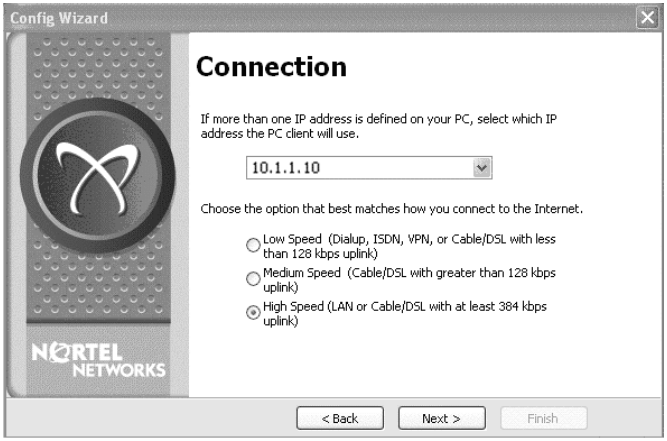
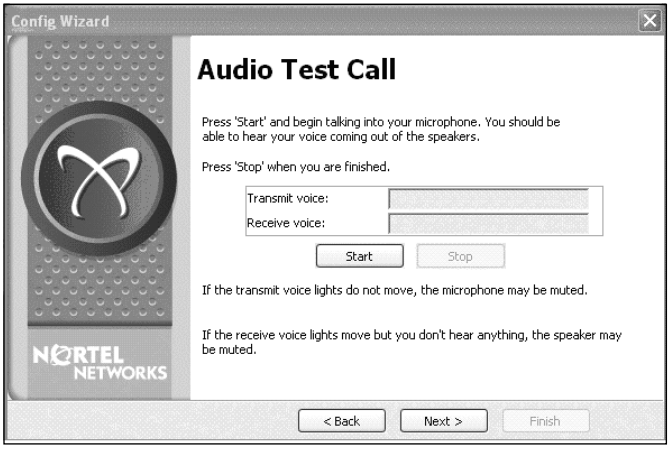


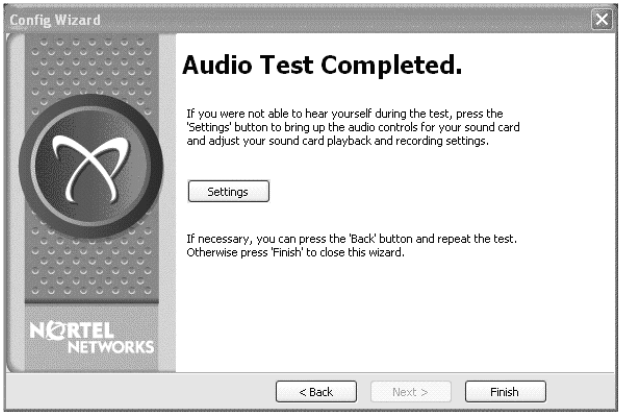
Figure 6.13 Audio Test Call



The Audio Test screen allows you to configure or fix the current settings for the audio section. To do so, go to Settings | Back, which will return you to the Audio Test screen where you can test your settings again. When you are done, click the **Next** button (see Figure 6.13) and then the **Finish** button (see Figure 6.14).

If you are not going to use a headset or microphone because you want to connect to IP Phone, click **Next** and fill in both figures.

Figure 6.14 Audio Test Completed

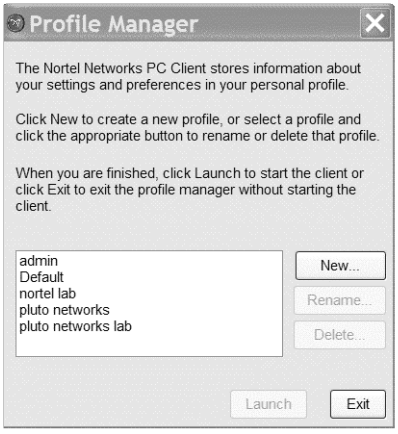


Logging On

After installation is complete, a PC Client and a Profile Manager are added to your programs list (see Figure 6.15). On the Profile Manager screen, you can see that more than one profile has been set up for testing. A PC Client can be installed on any computer and have many users; thus, those users must select their profile from the Profile Manager and then click the **Launch** button.

An administrator can create profiles on each PC for each user. Because a user can be set to different domains, the administrator must have the same information from the preceding configuration when adding new users to the Profile Manager.

Figure 6.15 Profile Manager



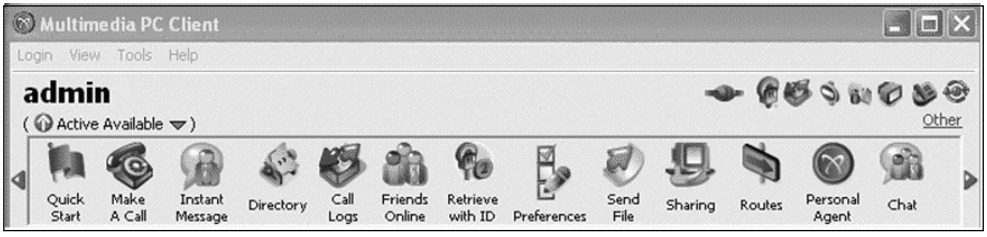
After a user has been selected, the PC Client launches and brings you to the Authorization Required screen (see Figure 6.16). This screen asks for the user's password and gives them two options to choose from: Remember my password, and sign me in automatically. It is recommended that you do not select either option, because it is would be too easy for an attacker to access your computer and use your PC Client. After inserting your password, click **OK**.

Figure 6.16 Authorization Required

Preferences

Once the PC Client is open, it can be configured based on a user's particular needs. After logging on to the system, you can see that there are many different icons to choose from (see Figure 6.17). Some were discussed in a previous chapter; therefore, this section only covers the Preferences, which can also be selected from the Tools menu. Clicking on the **Preferences icon** displays a new window called User Preferences (see Figure 6.18).

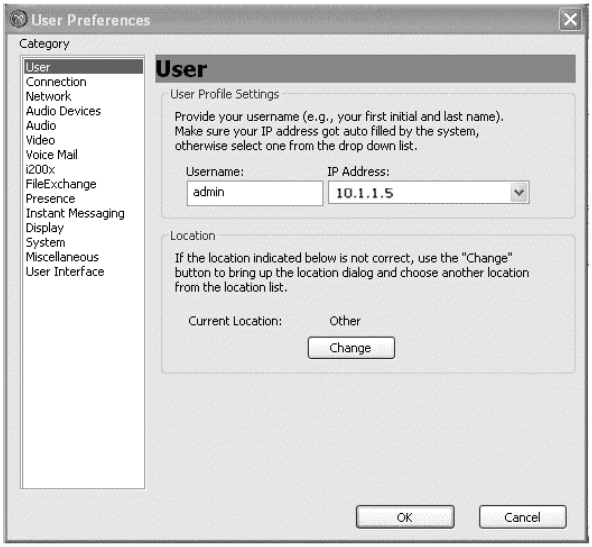
Figure 6.17 Preferences



User

At the User screen, you can make changes to the User Profile Settings, including the username and IP address of the computer currently being used on a virtual private network (VPN) in order to gain access to the proxy server (see Figure 6.18). When done, click **OK**.

Figure 6.18 User



Connection

Also under Preferences is the Connection screen where the network connection is chosen (see Figure 6.19). Although previously set up, you can change the settings on this screen based on any new requirements, using either a wireless card, a Digital Subscriber Line (DSL), or a cable modem from outside the office, or using the local area network (LAN) connection in the office.

Network

You won't have to change network settings unless your company has more than one proxy server or you have accounts on a different domain. Go to the Network screen and click the **Edit** button to edit the proxy, proxy port, domain name, and firewall timer. You can also set up different network

connections using the **Add** button (see Figure 6.20). There must be at least one active proxy. It is recommended that you not use Auto Sign In, because of security concerns in certain network environments.

Figure 6.19 Connection

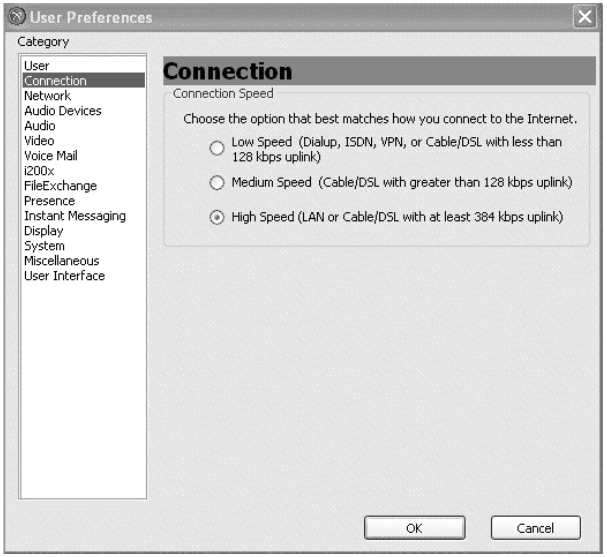
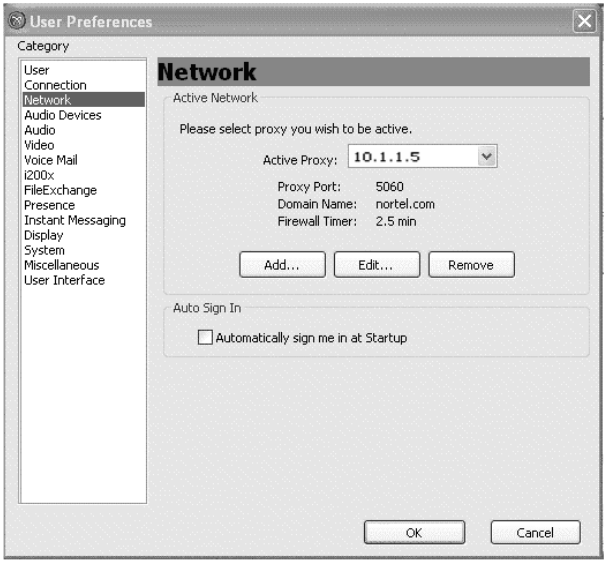


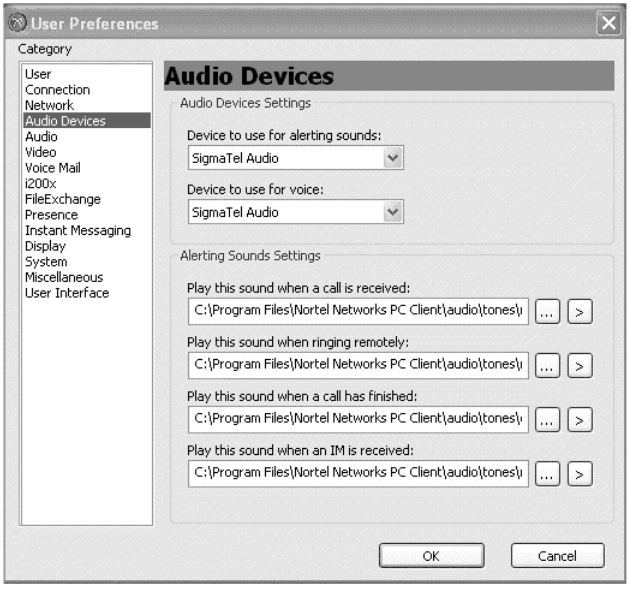
Figure 6.20 Network



Audio Devices

To add a new audio device or change the way sounds are played, go to the Audio Devices screen and select the device you want to use for alerting sounds and for voice (see Figure 6.21). You can also change the sounds of the ringer and instant messaging.

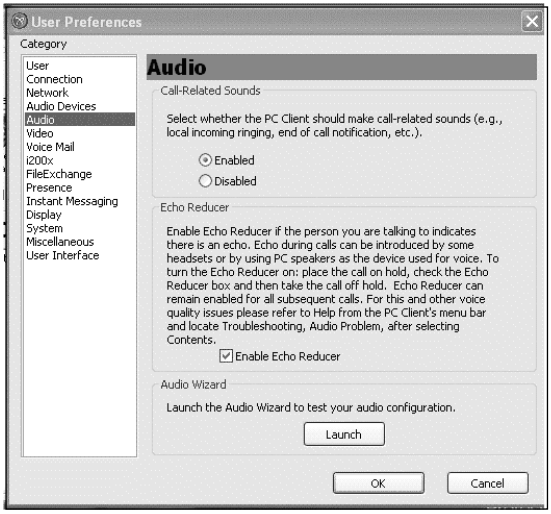
Figure 6.21 Audio Devices



Audio

In order for the PC Client to play the audio, select Enabled under Call-Related Sounds. It is also suggested that you select the Enable Echo Reducer. If you want to test or select new audio devices, select the Audio Wizard by clicking the **Launch** button. Adjust the volume on the microphone and headset and store the settings in the PC Client (see Figure 6.22).

Figure 6.22 Audio



Configuring & Implementing…

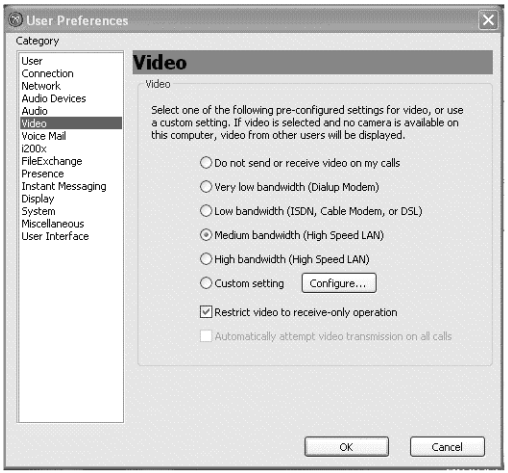
Web Cameras

If you are using a Web camera for video, remember that most of them have microphones that your system may select as the default device. Go to Audio Wizard and make sure the Web Camera is not selected as your default audio device for microphones.

Video

You have the ability to configure the video settings on the PC Client. Most users want to configure their PC Client to receive the most bandwidth possible for video; however, this will cause huge problems if it is set above what the network connection allows. On the Video screen choose whether or not you want to send or receive video, the speed of the video, to receive video only, or to automatically attempt video calls on all transmissions (see Figure 6.23).

Figure 6.23 Video



You can select the size of a video transmission at the Video Configuration screen (see Figure 6.24). You also have the ability to choose video camera and framing/speed options (see Figure 6.25).

Figure 6.24 Video Configuration

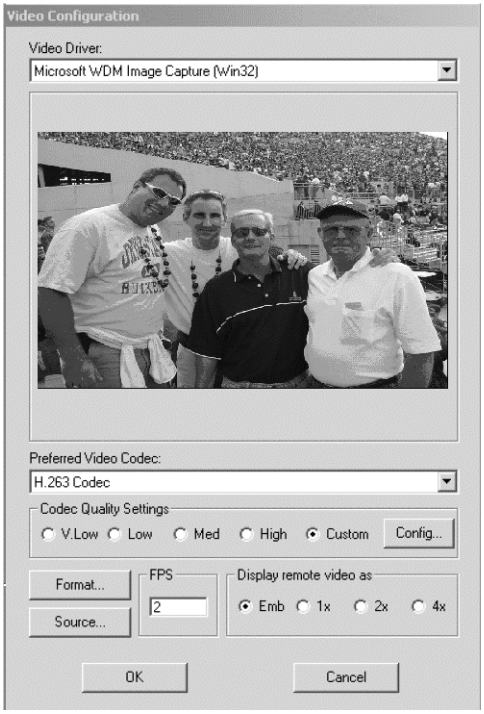
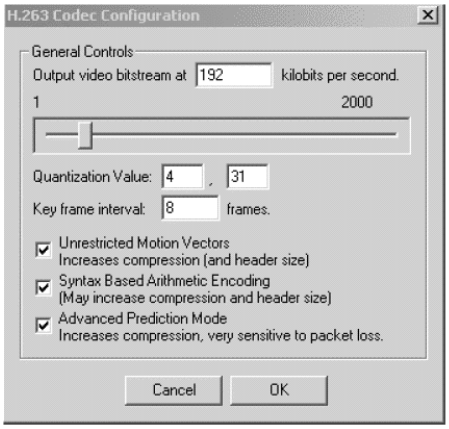


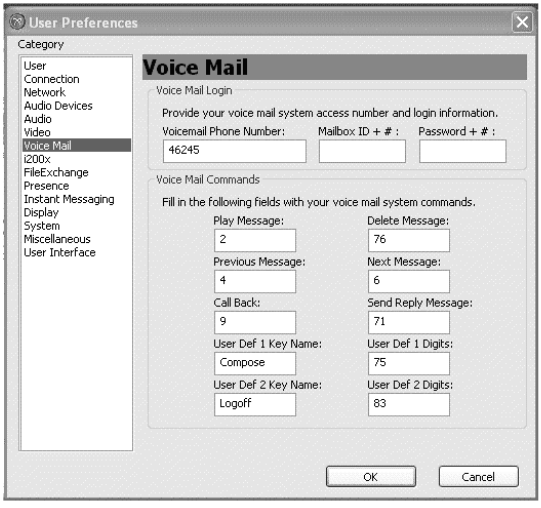
Figure 6.25 Codec Configuration



Voice Mail

If your system is connected to a Nortel voice-mail system, you can use the voice-mail default settings (see Figure 6.26). Otherwise, input the voice-mail number, the mailbox ID, and the password. Don't forget the # sign at the end of the mailbox and password, which allows the PC Client to automatically call voice mail when the voice-mail number is dialed. You can also program the PC Client to play messages, delete messages, and so forth, using preconfigured numbers.

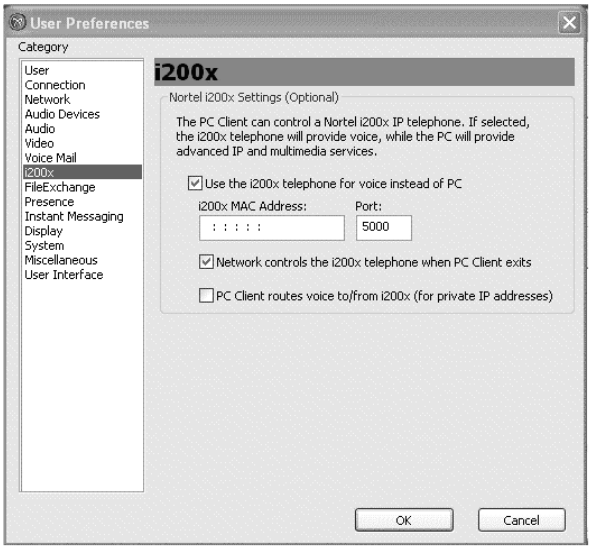
Figure 6.26 Voice Mail



i200x

You also have the ability to configure a Nortel IP phone to work with the PC Client. When this configuration is done, the audio part of the calls goes to the IP Phone, and the video and multimedia parts stay with the PC Client. To use the IP Phone, check the box titled Use the i200x telephone for voice instead of PC. Next, input the MAC address of the IP phone you want to use and the correct port number. (For this example, UNIStim was used to and from the IP Phone using port 5000. If you are using a new phase two IP Phone, you can use SIP on port 5060.) Next, check the box titled Network controls the i200x telephone when PC Client exits, which will allow the IP phone to work better when the computer is turned off (see Figure 6.27.)

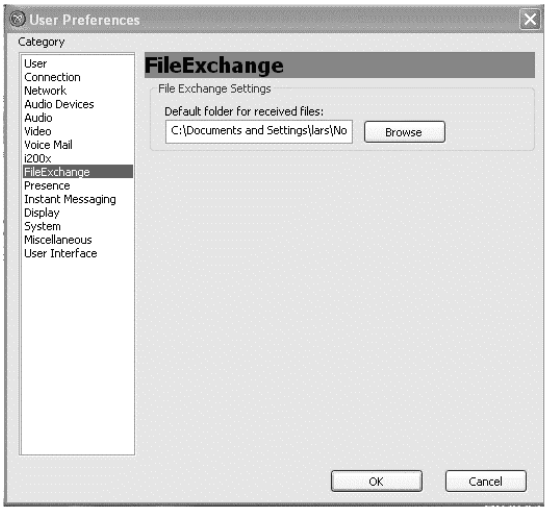
Figure 6.27 i200x



FileExchange

The File Exchange Settings on the FileExchange screen are set to the default settings. If you do a lot of profile exchanges, you might want to put FileExchange in a folder on your desktop for easy access. Use the **Browse** button to make a new folder (see Figure 6.28).

Figure 6.28 FileExchange



Presence

Presence is a big part of the MCS 5100, because it specifies whether other users can see when you're at your PC or using your phone. Check the boxes next to Report when inactive and Report when on the phone, and input the Inactivity Timer, to see when users are inactive, by how much time, and if they are on the phone. These can be changed by deselecting the boxes and changing the timer (see Figure 6.29).

Instant Messaging

If you use the MCS 5100 and PC Client you send instant messages to other users on the system. You can select if a sound is played when a new message is received, what timestamp was on the message, and if the window is a pop-up or stays on the taskbar. You can also select or deselect a timestamp when an instant message window is open (see Figure 6.30).

Figure 6.29 Presence

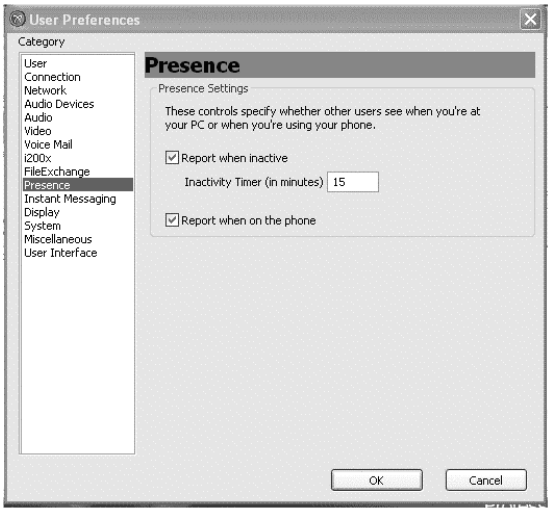
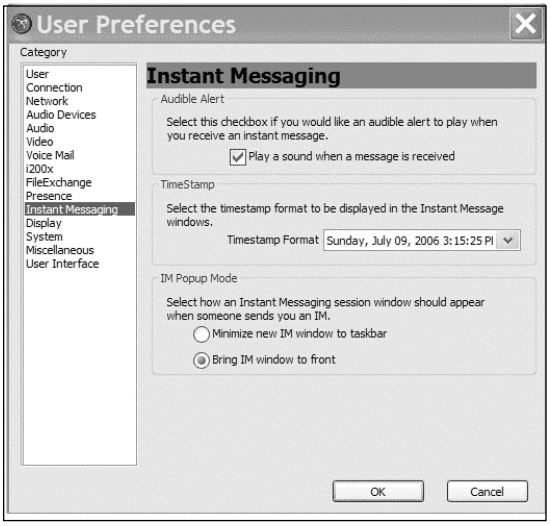


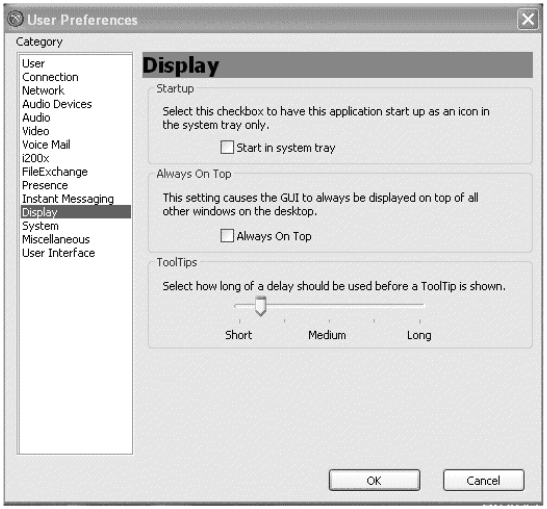
Figure 6.30 Instant Messaging



Display

It is recommended that you use the settings shown on the following Display screen (see Figure 6.31). Do not start the PC Client when Windows starts or when the GUI is on top of all of the other windows, because it can cause problems when using other programs in Windows.

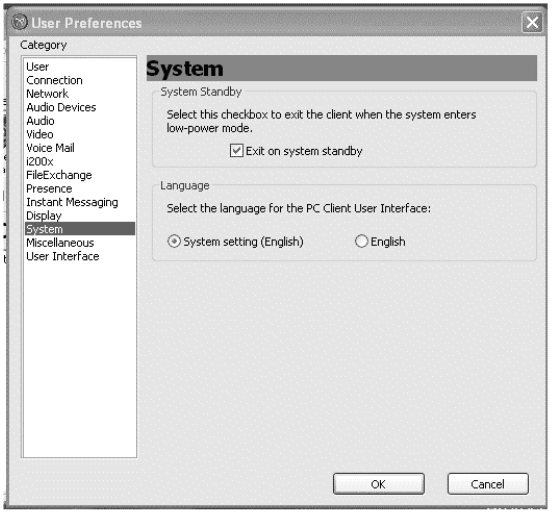
Figure 6.31 Display



System

To save system power while using a laptop, check the box next to Exit on system standby on the System screen (see Figure 6.32). You can also select the language for the PC Client.

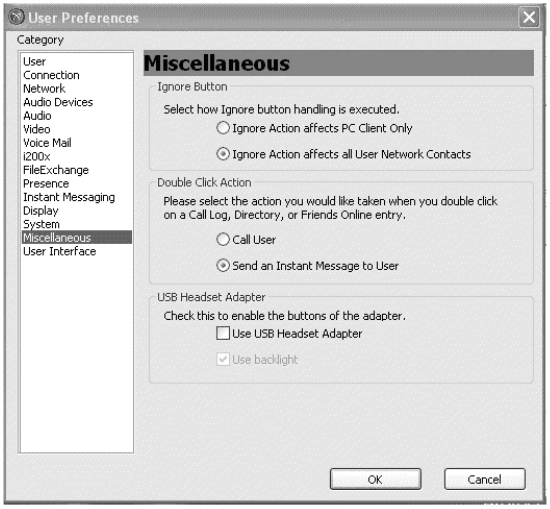
Figure 6.32 System



Miscellaneous

On the Miscellaneous screen under Ignore Button, select your preference for **Ignore** button handling. Next, select the action you want taken when you double-click on a Call Log, Directory, or Friends Online entry (see Figure 6.33).

Figure 6.33 Miscellaneous



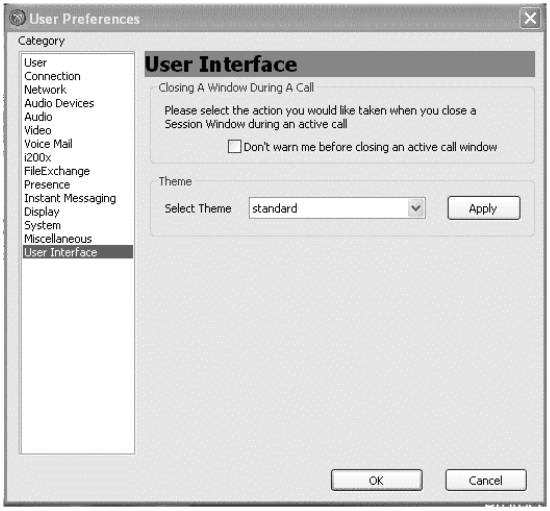
User Interface

When using PC Client, on the User Interface screen, select the option to warn user's before closing an active window. Also, select the appropriate theme for the PC Client within the user interface. When finished, click the **OK** button (see Figure 6.34).

Make a Call and Video Call

You can make regular phone calls to users inside the system and outside of the network within the PC Client. On the Make a Call screen, insert a number into the box above the dialing pad, or use the dialing pad to make the call. At the bottom of the screen, select a subject to display when a user calls someone on the network (see Figure 6.35).

Figure 6.34 User Interface



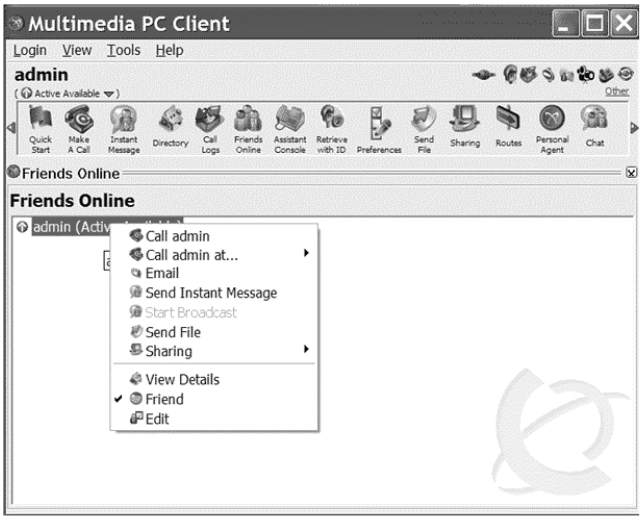
Choose the **Recent** button to obtain a list of calls in the call logs, your Personal Address Book, or your Enterprise directory (see Figure 6.35). You can also search for numbers using the Search option. Once you have entered a number or selected a user, select the buttons to make either a phone call or a video call.

Figure 6.35 Make a Call

Another way to make a call is to select a user from the Friends Online section within the PC Client. To do so, right-click on the user or friend that you wish to call and select the desired option (see Figure 6.36).

There is a checkmark beside Friend, which means that the user you've selected is on your Friends Online list. If you don't want that user on the list, click on **Friend** and the check mark will be removed, thereby deselecting the user. This can also be done from the Edit menu.

Figure 6.36 Friend Menu

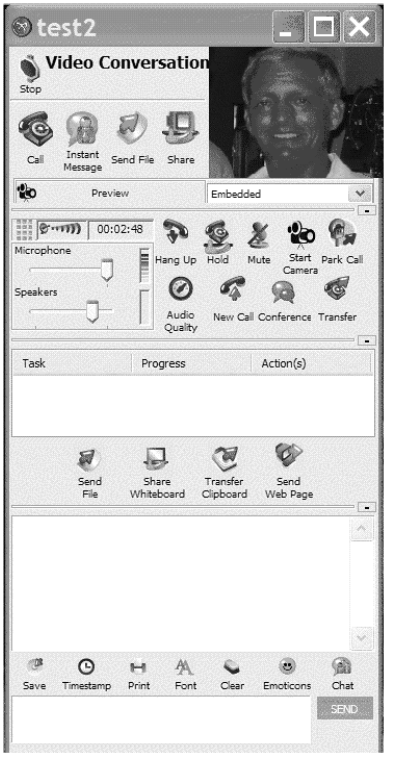


You have selected a user to call and the Voice Conversation window is displayed (see Figure 6.37). The top left of the window shows the status of the call. You can select Stop to end the call and use the volume controls for the speaker and microphone. Remember that if you are using a connected IP Phone, the volume controls will not work. All volume controls are handled by the IP Phone.

There are many different options to choose from when making a call. You can use the Preview button to view yourself camera to see what the called user is seeing. You can also put the caller on hold, make another call, conference the caller back in, and stop or start the video camera. You can mute the call, put the call in Call Park to be picked up by someone else, or transfer the call in either a blind transfer or an announced transfer (see Figure 6.38).

Figure 6.37 Making a Call

Figure 6.38 Video Call



Instant Messaging

Instant messaging can be used during a phone call or a video call (see Figure 6.39). As seen in the figure, an instant message was sent from the lchaffin account to the test2 account within the Nortel domain. Below the instant message are different options to choose from when sending an instant message. You can set the system up to either send the instant message by clicking the **SEND** button at the bottom of the screen, or by clicking the **Enter** button on the keyboard.

When sending or receiving an instant message, a new window opens up for each user. Depending on what you are doing, you can have as many windows open as you wish.

Figure 6.39 Instant Messaging

Directory

Phone directories can be selected from the menu bar (see Figure 6.40). As seen in the figure, the Global Address Book was automatically loaded. If desired, the drop-down menu can be used to select a different address book. Once you have chosen an address book, you can search by name or number. The system gives you a list either in name view or card view, which can be selected using the buttons below the search box.

On the right side of the window there are four icons: Adding Contacts, Deleting Contacts, Editing Groups, and Importing Contacts. In this example, Adding Contacts was selected and a phone number with a SIP ending has been entered into the SIP box. You can also choose a nickname that will appear in your Friends Online directory.

You can choose a specific ring tone for each user and also add them to your Friends Online list in the PC Client. Within this list you can assign Friends Online to certain groups. When you are finished, click **Save**.

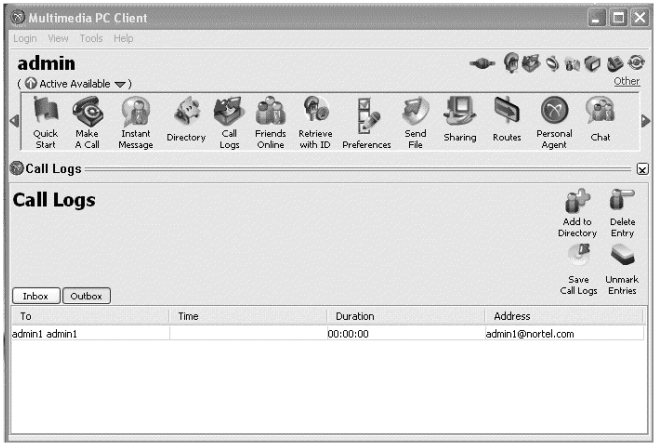
Figure 6.40 Directory Add Contact

Call Logs

Call Logs are logs of incoming and outgoing phone calls made from your account (see Figure 6.41). On the left-hand side of the screen are the Inbox

and the Outbox buttons. On the right-hand side of the screen, there are four icons: Add to Directory, Delete Entry, Save Call Logs, and Unmark Entries.

Figure 6.41 Call Logs



Friends Online

You may have Friends Online, a service that allows you to see what your friends' status is (e.g., are they free, busy, logged on). You can also make your status available for others to see by selecting **Active Available** (see Figure 6.42). You can also right-click **Friend** to produce a menu where you can choose the option to contact or edit settings for that friend (see Figure 6.43).

Figure 6.42 Friends Online

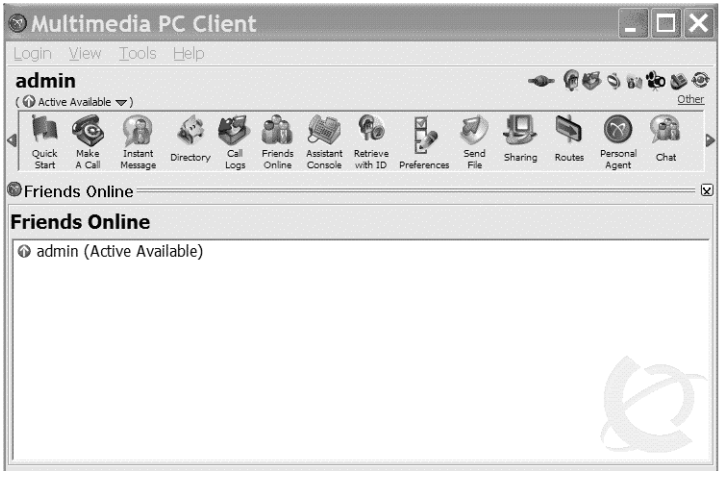
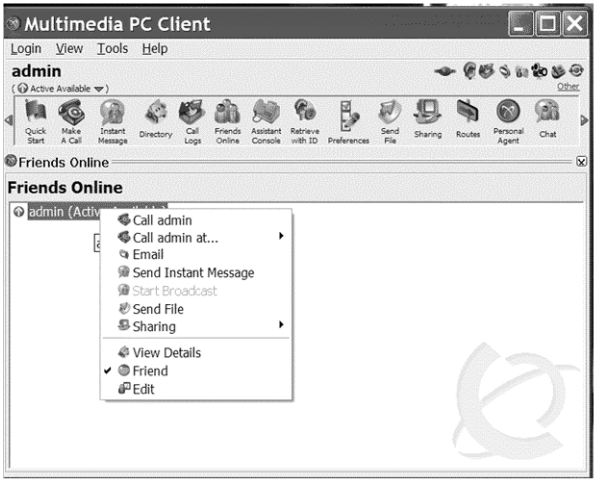


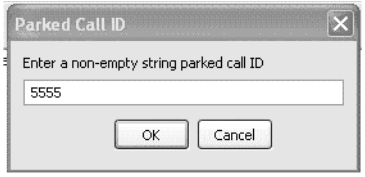
Figure 6.43 Friends Online Menu



Retrieve Parked Call IDs

The Parked Call ID feature is for both the PC Client and the IP Phones. When a call is parked to another user or to a general queue, a token is sent to notify you to retrieve the call. This allows you to answer the call on any IP phone or PC Client on the network (see Figure 6.44).

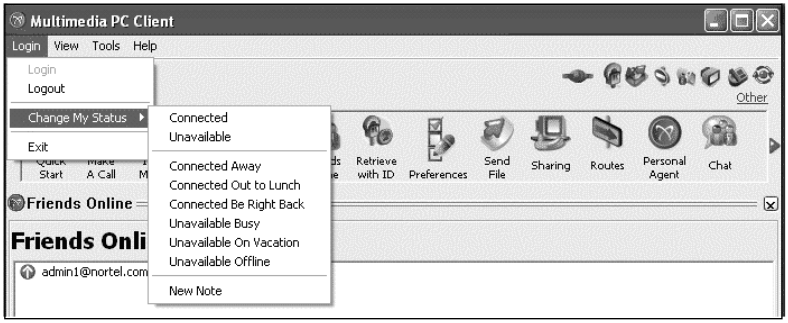
Figure 6.44 Parked Call ID



Change My Status

To change your status on the PC Client, go to Login on the Menu bar and select Change My Status, which brings up a list of options (see Figure 6.45). You can also create a New Note, which allows you to create a title that user's can see when checking their presence.

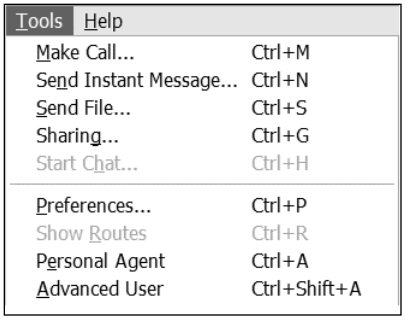
Figure 6.45 Change My Status



Advanced User

The Advanced User section is located on the Tools menu, which is where you can find useful information that will help you troubleshoot any problems within the PC Client. To get to this graphical user interface (GUI) go to **Tools | Advanced User** (see Figure 6.46). There are three options under Advanced User: Messages, Logs, and System Info, which can be used to stop a message for viewing (see Figure 6.47).

Figure 6.46 Tools Menu



Under **Advanced User - Debut Information | Logs** are logs from the PC Client (see Figure 6.48) and the system information is under **Advanced User - Debut Information | System Info** (see Figure 6.49). All of these logs can be stopped, saved, and cleared within the GUI, which allows you to clear information so that you can view new information. It also saves the logs to a file that is sent to Tech Support (See Figure 6.48).

Figure 6.47 Messages

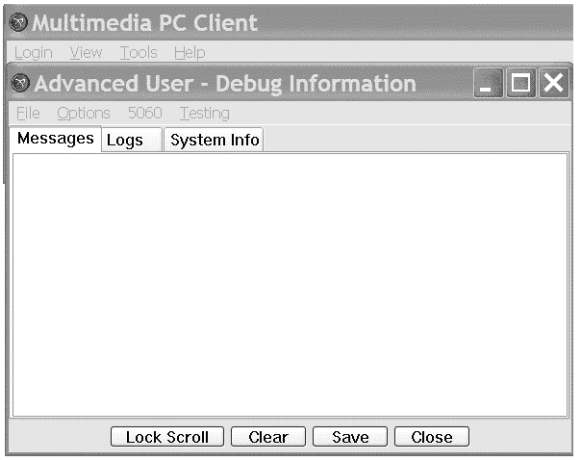
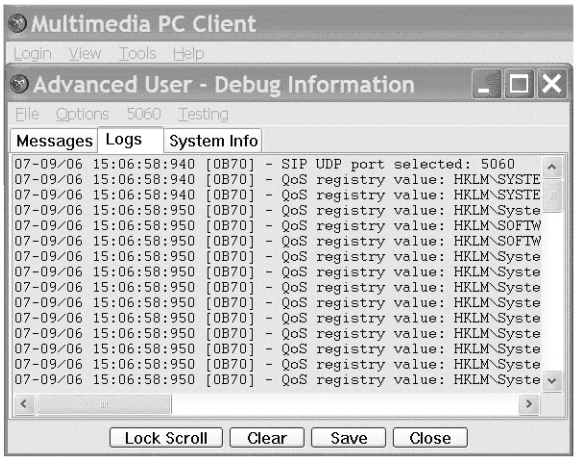


Figure 6.48 Logs



Capture Logs

If a Nortel tech support representative asks you for logs from the PC client, go to the Help menu and select **Capture Logs for Support** (see Figure 6.50). After selecting this, click the **OK** button (see Figure 6.50). Make sure you note where the logs are located on the system so that you can easily retrieve them (see Figure 6.51).

Figure 6.49 System Info

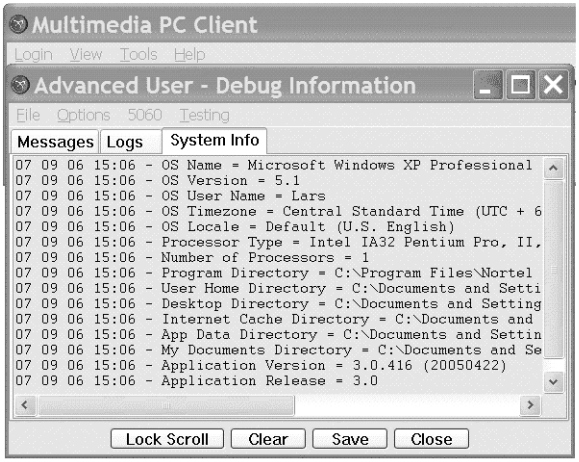


Figure 6.50 Help Menu

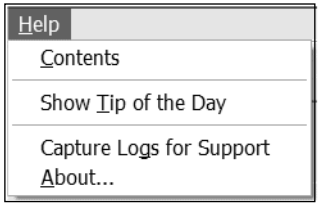
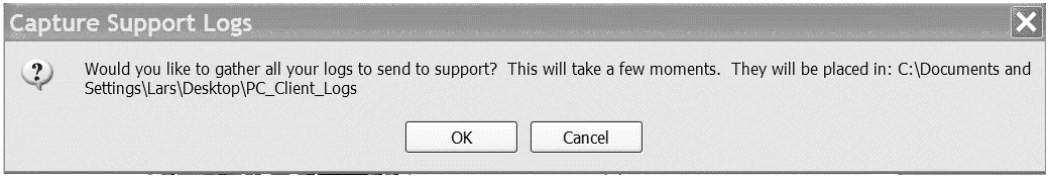


Figure 6.51 Capture Support Logs



Summary

The Nortel Multimedia PC Client is a highly advanced software client that brings the world of Voice over Internet Protocol (VOIP), video, and multimedia together, which allows you to be more responsive to the demands of work while maintaining the ability to be mobile. The PC Client provides a secure instant messaging platform. It also has the ability to provide out-of-network video via SIP connections to the PC Client, which helps eliminate travel expanses.

After the release of the PC Client in the MCS 5100 system, other companies (e.g., Avaya and Cisco) tried to build their own multimedia client. To date they have been unsuccessful. With all of its advanced features, PC Client is sure to be the leader for a long time.

Solutions Fast Track

Installing PC Client

- ☑ Remember to input the correct network address when installing the PC Client onto the user's PC.
- ☑ It is always a good idea to add Outlook AddIn to the PC, which allows you to import contacts to the PC Client.

Logging On

- ☑ We recommended that you do not sign in automatically or save passwords. This is a best practice in security.
- ☑ The login name used by the user is the same name that the administrator assigns when provisioning the PC Client.

Preferences

- ☑ The proxy, port ,and location can be changed in the GUI preferences.

- ☑ You can configure video under Preferences. Remember not to dial up the bandwidth, which will cause network problems and bad audio and video communications with the MCS 5100.
- ☑ Double-click on a friend to open the instant messaging window.

Make a Call and Video Call

- ☑ Making a call can be done from many different areas within the PC Client.
- ☑ To make a video call, you need a video camera set up on the PC Client. You also need the proper licenses.
- ☑ You can start and stop the video on a call at any time.

Instant Messaging

- ☑ Instant messaging is a secure communications application on the PC Client.
- ☑ Only users on the system or domain with a PC Client can use instant messaging.
- ☑ Logs are saved to folder on the PC for later use.

Directory

- ☑ Directories are used for both Enterprise and Personal Address Books.
- ☑ You can edit the friends in your Personal Address Books (e.g., insert them into groups and add different ring tones to each).

Call Logs

- ☑ Call Logs are kept for all inbound and outbound calls from the PC Client to the Inbox and Outbox.
- ☑ Callers can be added to the directory from the Call Logs by using the correct icons.
- ☑ All of the Call Logs can be deleted for privacy on the system.

Friends Online

- ☑ Users are limited to the number of online friends they can have.
- ☑ Friends can be added from the directory by right-clicking on the user.
- ☑ The status of friends is provided in real time via SIP.

Retrieve Parked Call

- ☑ User's can park calls to or retrieve a token to answer the call.
- ☑ A parked call can be picked up anywhere on the system via a PC Client or IP Phone.

Change My Status

- ☑ If the status has not changed, the user is inactive via the default settings within the preferences, unless they have deselected those options.
- ☑ User's can add their own status to be used on the system.
- ☑ To delete unused status, is must be deleted within the file placed on your computer by the PC Client. See your local administrator for help.

Advanced User

- ☑ Using Advanced User is an easy way to save logs and watch system information on a troubled PC Client.
- ☑ Remember that you can lock the scroll and clear the screen while using the system feature under the Advanced User tab.

Capture Logs

- ☑ Use Capture Logs only when asked by your administrator or a Nortel engineer.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I understand there are two versions of the PC Client; one is java-based and the other is C++ based. Is that correct?

A: Yes. The version used in this chapter was C++, but the java-based client can be launched from the personal assistant and has all of the same features and fields as C++.

Q: Can I use any IP phone with my PC Client?

A: Yes, as long as it is a Nortel IP Phone.

Q: My PC Client has an error that said it did not close correctly and now I have error logs on my desktop. Why?

A: You need to log off and exit the PC Client before turning off your PC.

Q: Why can't I use the volume control on the PC Client when I'm using the IP phone and PC Client together?

A: The audio stream is going to the IP Phone, not the PC Client.

Q: The video is very choppy on my PC Client. What is the fix?

A: Go into your preferences and video settings, lower the bandwidth for the video camera, and change your network settings.

Q: Can I have multiple users logged into my PC Client?

A: No. Only one user per PC Client is allowed. If you are doing SIP to an IP phone, you can only have one user.

Chapter 7

Personal Agent

Solutions in this chapter:

- Logging on to Personal Agent
- Routes
- Preferences
- Directory
- Click to Call
- Multimedia Web Client

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

The Personal Agent (PA) is an extension of the PC Client that allows the user to have more options. It lets you:

- Define how your incoming calls will be treated
- View and customize all your personal information and services
- Start the Multimedia Web Client from the Personal Agent
- Share files with other Personal Agent users or Multimedia Web Client users
- Manage and track and maintain contact information
- Establish a call between you and another user or contact

The PA is a Web-based GUI that works off of the IPCM much like the Provisioning Client that was covered in an earlier chapter. Since this is a Web-based GUI, you can connect from the PC Client tool bar, or you can bookmark the IP Address of the IPCM with the PA client ending to pull it up anytime from a Web browser. This is very helpful if your company has this set up on a SSL connection from the outside for authentications. In some places you might be able to get to your computer or have access to it.

If you have an outside IP address set up for your PA then you may go straight to it and log in; this will also let you log into a version of the PC Client that is for the Web. It has all the same features but allows you to use it anywhere you can get onto the Web page. It comes in very handy when you really need to send an IM, file, or make a quick change.

Logging on to Personal Agent

When logging in to the personal agent, you will need to either use the tool bar from the PC Client, as shown in Figure 7.1, or use a Web address within a Web browser, as shown in Figure 7.2. In Figure 7.1, to the far right on the icon tool bar you will see an icon for the Personal Agent. Selecting that icon will launch your local Web browser to the correct address and login to the PA. If you launch the PA from the PC Client, it will not require you to insert

your name and password since you are already logged into the system via the PC Client.

But if you go from a Web browser and insert an IP address or use a bookmark, it will ask you to log in to the system via the same information that you would use for the PC Client. It is your username and password for the system.

Figure 7.1 Nortel PC Client Tool Bar

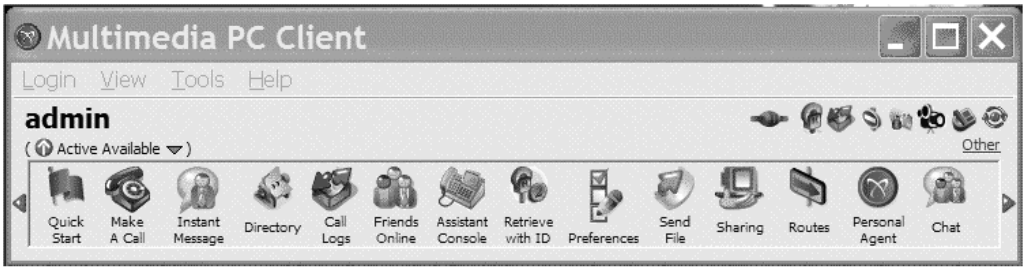
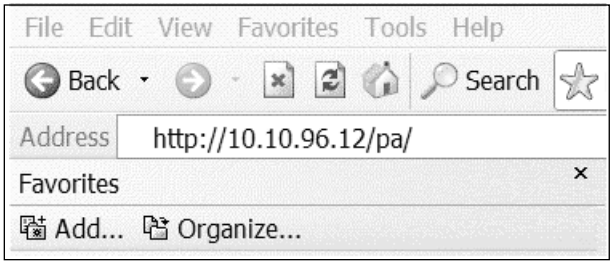
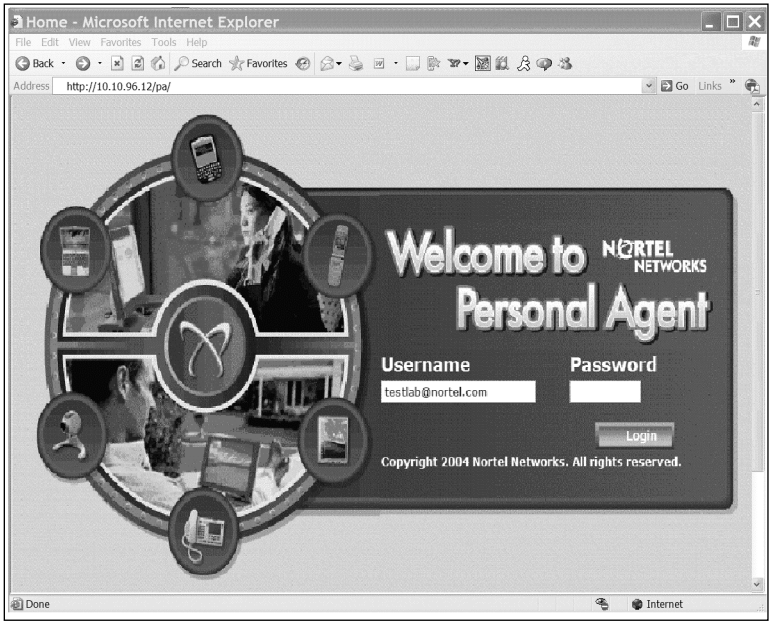


Figure 7.2 Web Browser



If you use the Web to go directly to the PA, you will first see the screen in Figure 7.3; this is what will be displayed in the Web browser after it launches from your local computer. Insert your username and password and click the login button. Remember that this is the same username and password used in the PC Client.

Figure 7.3 Nortel PA Login Screen



Designing & Planning…

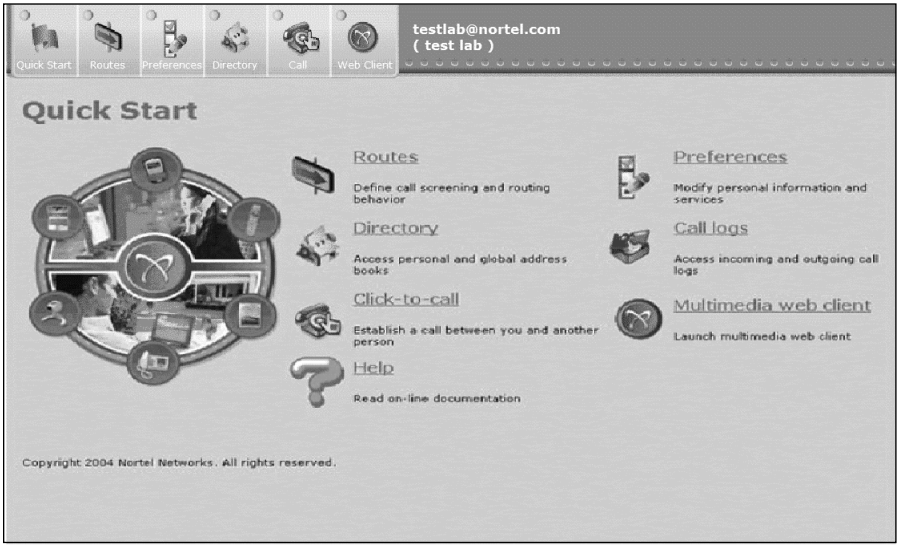
Choosing Clients

If your company has the ability to use an outside address and put this in a secure Web site using SSL, it is a great tool for people who travel or are on the go. Also there are some companies who do not want to add the C++ version of the PC Client and would rather use the Java-based Web client from the Personal Agent. It is best to work these details out before the installation, but it is really not hard to change once the system is installed, to go back and forth or just use both clients like we do now at Pluto Networks.

After a successful login, you'll see the PA main screen, the Quick Start screen shown in Figure 7.4. You can choose from five main areas while in the PA: Routes, Preferences, Directory, Call Logs, and Click to Call. Also listed is

the Web version of the PC Client and the Help or online documentation. These are also available from the tool bar at the top to make changing from one area to another much easier than using the back button on the Web browser.

Figure 7.4 Nortel PA Quick Start



Routes

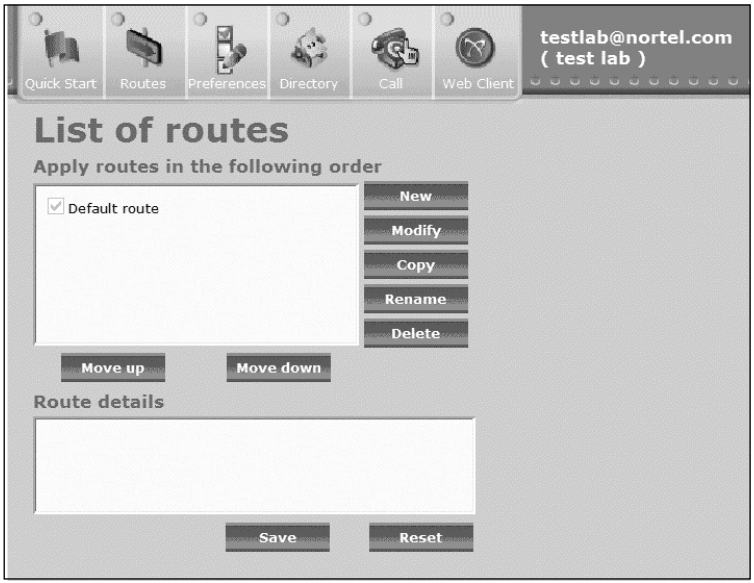
The Routes feature located in the PA is maybe one of the coolest features of the PC Client and the PA since it allows the user to manage from whom, how, and when they receive calls. You must have the advanced screening options within your service package for this to be able to work. The user can make routes for different groups or even different people who would be dialing into them. It allows treatment of callers who have no number displayed.

Also if you will be using the assistant console from the PC Client, the assistant will be using this Personal Assistant to make changes to the users account. Figure 7.5 is the first screen shown when selecting Routes. It is the List of Routes for the current user logged into the PA. Within this screen you may create a new route using the route wizard, modify an existing route, or

even delete the route if needed. The route may also be copied to create another similar route and renamed if a mistake or change is needed.

In the middle we have Move up and Move down buttons. These are used to move routes up and down within the list, since the calls coming in go by the list in order. So if a call comes in and a route at the top has the user or number in it, it will take precedence over a route below it in the list. It is just like an access list on a router or firewall. Once you have made your changes you can select the **Save** button, or if you need to start over, select the **Reset** button before using Save to start over.

Figure 7.5 Lists of Routes



Route Wizard

The first thing that we will need to explain is what the Route Wizard can provide to the user and how to understand the steps needed to make a route. Here is a short list of what the Route Wizard can provide:

- Help specify conditions as to how specific calls should be presented to you, also on what devices in a simultaneous or sequential fashion the calls are sent.

- Define personalized time blocks to further define your routes so that you are always in reach.
- Define routes for how your incoming calls and instant messages are handled.

The system will send an instant message when processing a ring list from the route wizard.

In Table 7.1 we have put together the steps that are needed to be taken when using the Route Wizard in the PA. There are only five steps that need to be taken to create a route for a user, number, or group; but there are many options within these steps that we will be taking a look at to make sure they are understood.

Table 7.1 Route Wizard Steps

Step	Specification
1. Initiate action	Main action or actions that initiate the processing of the route. There are two options listed here to select: (1) When a call is received, or (2) When an Instant Message is received. Select the desired option by clicking the appropriate check box.
2. Conditions	Filtering of conditions respective to the call originator and the time of day that must apply before the actions in step 3 can take place.
3. Actions	What action or actions are performed when a call is received. Actions are defined with respect to the services enabled in your service package.
4. Exceptions	Exceptions to the filtering conditions defined in step 2.
5. Finish	Name of the route and whether or not the route should be active or saved.

Step 1. Initiate Action

From Figure 7.5 we have selected the **New** button, which has taken us to Figure 7.6 for step one within the Route Wizard. As you can see, you may select either when a call is received or an instant message is received for your

route. Most users never think they can create a route for when an instant message comes in from a user, but with the system being highly usable with instant messages it makes for a great way to communicate. But we have selected When a call is received in step one, and put a check in the box, as shown in Figure 7.6. Then we have selected the **Next** button.

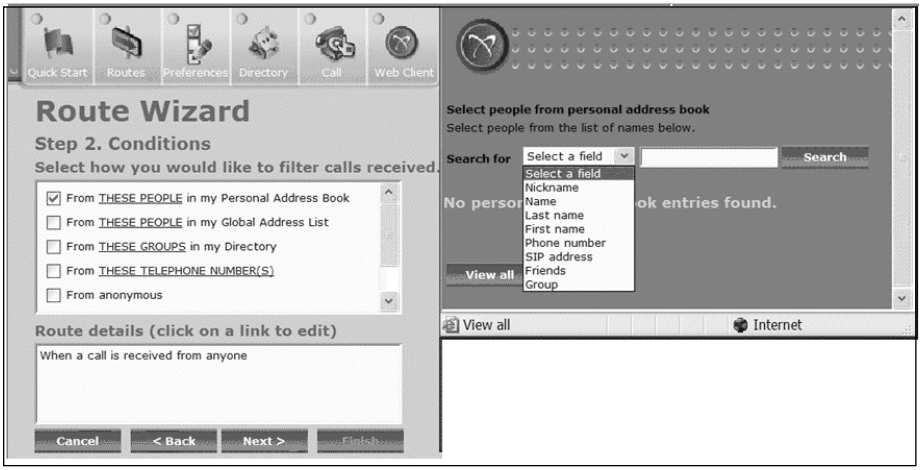
Figure 7.6 Route Wizard Step 1

Step 2. Conditions

After selecting **Next**, you will move on to step two in the Route Wizard, as shown in Figure 7.7. Here you can select a different way to filter the calls as shown on the left side of the figure. We have selected the personal address book in our first example and then clicked the blue hyperlink called **THESE PEOPLE**. This brings the window up to the right, which lets you select a user from your personal address book.

You can search by all the criteria we have pulled down from the drop-down box, then fill in the information to the right and select the **Search** button. Remember that this is just for the Personal Address Book and that the next filter down on the list is for the Global Address Book. You can follow the same steps in that filter as for the Personal Address Book to find the user you are looking for at that time. If there are no more filters, select **Next** or move onto other filters, as shown in Figure 7.7.

Figure 7.7 Route Wizard Step 2: THESE PEOPLE



In Figure 7.8 we have moved on and checked the next filter in the Route Wizard. This brought up the screen to the right, and shows that we have one group set up in our profile. These are the same groups that you would have set up within your PC Client under your personal and global address book. Just put a check in the box for the correct group and select **OK** at the bottom of the screen to the right. When finished, click **Next**.

Figure 7.8 Route Wizard Step 2: THESE GROUPS

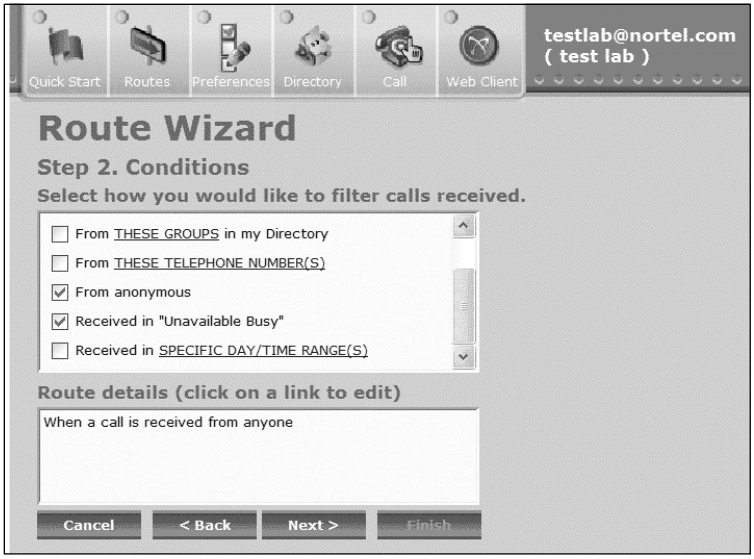
Now we have moved on to the step at which you can just add phone numbers to the filter; we have selected the filter in the Route Wizard, as shown in Figure 7.9. That produced the window to the right, at which time we added the number you see, and then selected **OK**. More than one number may be added at a time just by entering the number and pressing Enter to move down a line in the window. Do not use commas or periods; just stack the numbers one on each line from top to bottom in the window.

When you are finished, select **Next**.

Figure 7.9 Route Wizard Step 2: THESE TELEPHONE NUMBER(S)

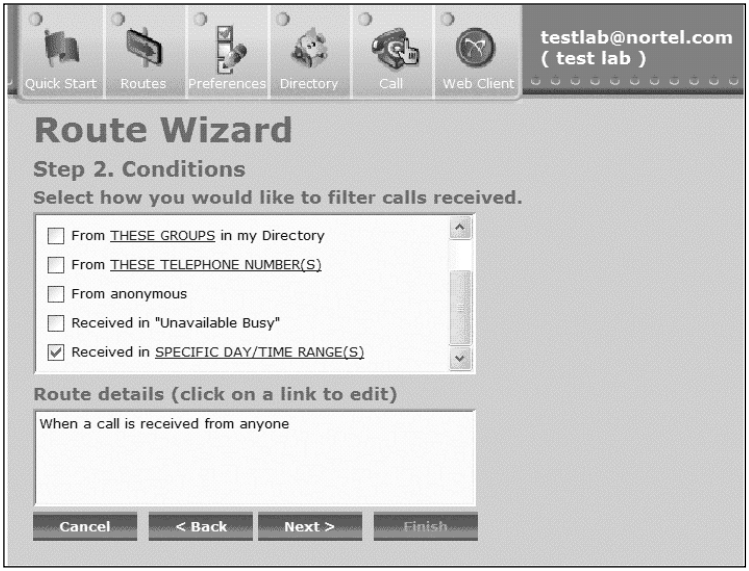
In Figure 7.10 we have selected **From Anonymous** and **Received in Unavailable Busy** for our next filters. These two do not have any other windows or options you can select. An Anonymous filter is used for people who block their phone numbers and have no digits to be received by the system. The Unavailable Busy filter is used for when you place your IP Phone or PC Client in that state, which means you cannot receive calls.

Figure 7.10 Route Wizard Step 2: From Anonymous



The last filter you may choose in step two is used for the specific time and date; once you have selected this by putting a check mark in the box you may select the blue hyperlink as you can see in Figure 7.11. This will produce a new window, which is displayed in Figure 7.12. You may use the day and time feature with any of the filters above it in the list.

Figure 7.11 Route Wizard Step 2: SPECIFIC DAY/TIME RANGE(S)



In the My Times window shown in Figure 7.12, you can create a new day and time filter for each route you create. So if you create ten new routes all with different filters, you can also create different My Times for each new route. This is done by selecting **Add** and creating a name, then selecting the day and times for the new My Times filter. Once finished you will have a filter like the one we have in Figure 7.12.

You can also from this screen and within each route modify, copy, rename, or delete the My Times filter you have created. When finished with all changes select the **Save** button.

Figure 7.12 Route Wizard Step 2: My Times

Step 3. Actions

In step three of the Route Wizard, we will select what numbers or clients from which the user will receive calls from the Route Wizard. Step three starts with the screen shown in Figure 7.13, where you can select **Ring my**

devices in the following ordered lists, or the option below it, **If no answer then send to voicemail**. After you select one of these two options, click **Next** to move to the next screen.

Figure 7.13 Route Wizard Step 3

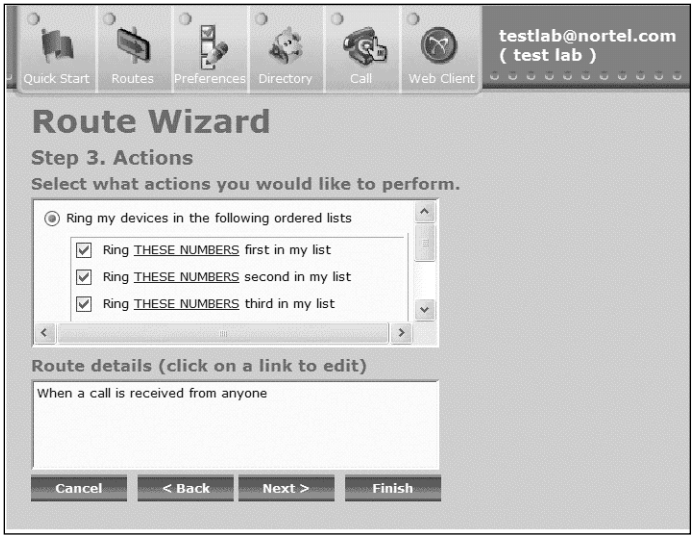
In the screen shown in Figure 7.13, we selected the first options, and in Figure 7.14, you can see the options it produced. We selected the option to **Ring THESE NUMBERS first in my list** and then selected the blue hyperlink called **THESE NUMBERS**, which produced the window to the right. In this window you can select which numbers to call, the instant message to send, and also the Web page to push. To start we are going to look at the telephone numbers to ring.

After you put a check mark in the box, select how many times the system will ring these phone numbers before it moves to the next type. In the boxes shown in Figure 7.14, you can select different types of phones like we have done already. Then add a phone number or address to the right of each. You also can elect to send an instant message to a user on the system or push a Web page instead. This works only for users on the system, but it is a great way to communicate with everyone. After you've finished, select **Save**.

Figure 7.14 Route Wizard Step 3: THESE NUMBERS

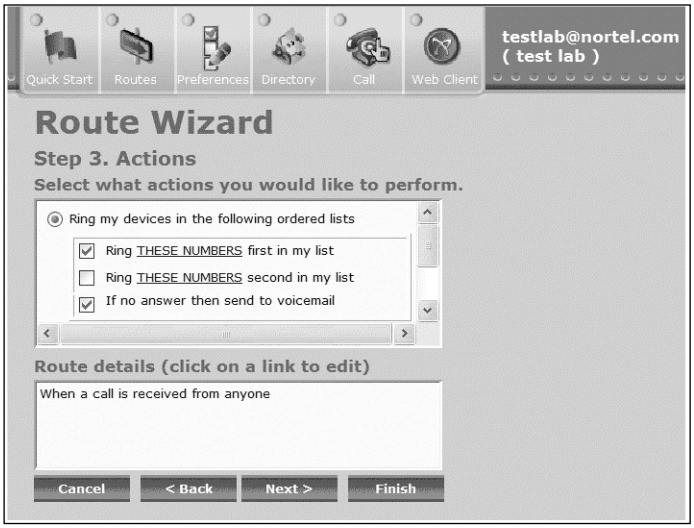
You can also select more than one set of numbers to ring first when a call comes in. As you can see in Figure 7.15, we have selected three different numbers to ring when a call comes in, so the system will go from one to another to another.

Figure 7.15 Route Wizard Step 3: THESE THREE NUMBERS



The one thing to remember, which we show in Figure 7.16, is that no matter how many routes you send the calls to, they must stop somewhere. That somewhere is in voicemail, and that should be the last place you will have the call go at the end of a route (unless the user is sending it to another voicemail that resides off the system or on a cell phone).

Figure 7.16 Route Wizard Step 3: THESE NUMBERS and Voicemail



NOTE

It is important to remember that all numbers that you send your calls to might be different, and you might have many different numbers to send the calls to. But some voicemails on systems pick up faster than others, so you will need to work on how many rights you use per number to get the call to cycle all the way to the end of the route like you have listed in the route options.

You can also set up a rejections message for certain users or spammers that might call. In Figure 7.17 we have selected the message hyperlink shown to produce the window to the right. Like the others, a new message may be listed or modified; then select **OK**. If all actions are complete, select **Next**.

Figure 7.17 Route Wizard Step 3: Select Rejection Messages

Step 4. Exceptions

In this step, you can list exceptions to the current route you are working on. This is the same as adding someone to the route by following the same example we have shown before in this chapter. When complete, select **Next**. In Figures 7.18 and 7.19, we show the different types of exceptions that you can select for this route. This means the selected users, people, numbers, and others will not be used in this route when it is enforced.

Figure 7.18 Route Wizard Step 4: Exceptions One

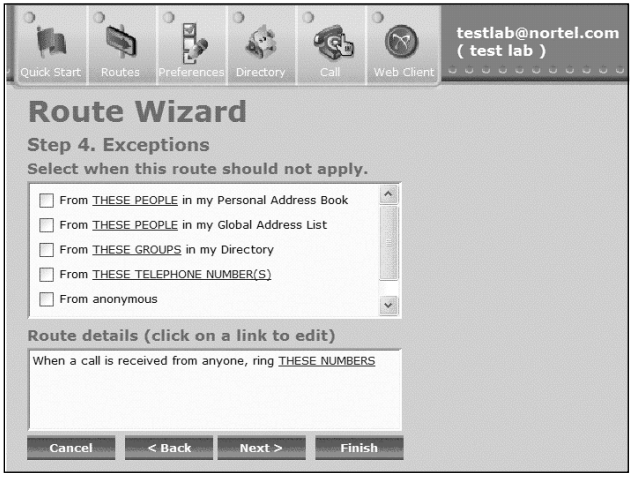
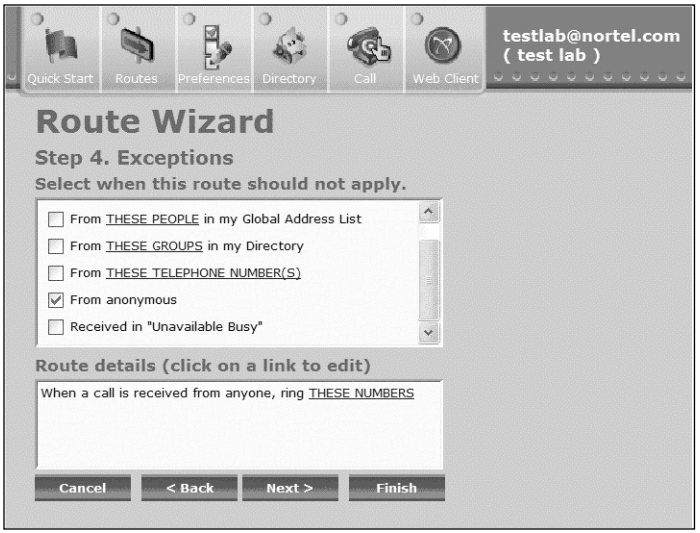


Figure 7.19 Route Wizard Step 4: Exceptions Two



Step 5. Finish

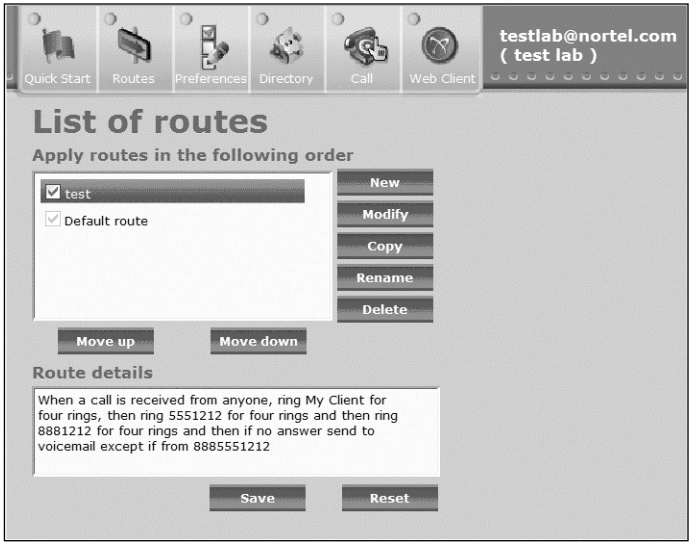
This last step takes all the information you have selected from the steps before and lists them as shown in Figure 7.20. While you are going over each step, it will add them into the route details for you to review. In the earlier steps, we chose not to do this to keep it a little cleaner, until we got to this final step to explain the route details. You may select the hyperlinks in the route details to change the information or list the information if needed.

Once you are finished with all changes, you can add a name to the route and select the box to make this route active. It the route is named and saved but not active it will not work; on the other hand, you can come back and either make it active or make it inactive if it is not needed. The route does not have to be deleted once saved, just made inactive or active will save you time in making another route.

Figure 7.20 Route Wizard Step Five Finish

After you select **Save** as shown in Figure 7.20, a list of routes showing which are active and inactive is displayed, as shown in Figure 7.21. If you highlight a route, the route details will display at the bottom. Select **Modify** if any changes are needed. You can also change the list of the routes by moving them up and down in the route list order and selecting **Save** when finished.

Figure 7.21 Route Wizard Step List Completed Routes



Preferences

The next areas we will look at in the Personal Assistant are the preference section located within the toolbar at the top and also the quick start menu. In the preferences you will be able to do many things such as update your personal information, add a picture, create new information for use on your PC Client or even your Web PC Client. As you can see in Figure 7.22, we have expanded the preferences tree to the left to show all the options that are available. Based on what you have on the system your tree could be smaller or bigger.

Personal

Within the personal area of the preference tree we have selected our first area to be filled in, which is shown in Figure 7.22. The contact info is meant for the user of the account; the first name, last name, and aliases will be filled in already and grayed out by the system. You cannot change these, only the administrator may change these settings. Fill in the information like we have in our test lab user example and select **Save**.

Figure 7.22 Contact Info

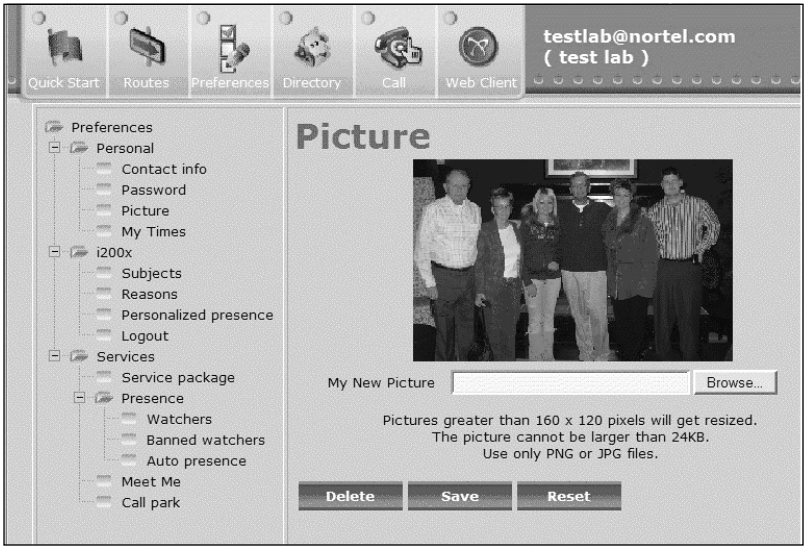
Figure 7.23 shows how you can change your password. This is the password that you use to log into the PC Client and the Personal Assistant, and is the same for logins to the IP Phones associated with the MCS 5100. Other than the administrator hanging the password for the user, this is the only place you may change your password on the system. This is done by adding a new password, then entering it again. The system will require you to insert the old password to confirm before changes are made. When you are done, select **Save**.

Figure 7.23 Password

As we showed within the PC Client, you can display a picture for all to see, as shown in Figure 7.24. However, you can use a picture only if it is on the computer you are logged into or can get to on the network. Sometimes, if you are on an Internet computer not on the network you might not be able to change the picture unless it is on a CD or USB stick. But once a picture is selected, just click **Save**.

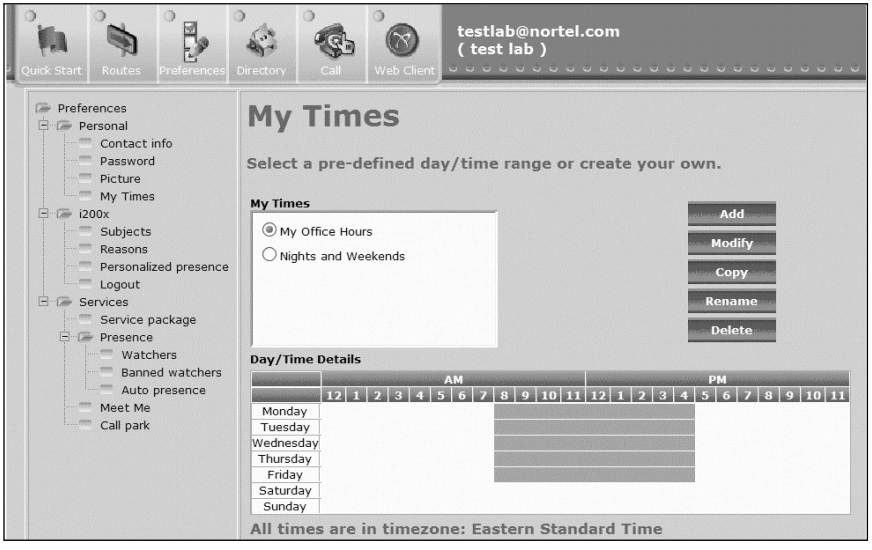
To change a picture, delete the current picture first, and then add the new picture. We have seen problems when trying to add a picture over an old picture.

Figure 7.24 Picture



Last within the personal area is the My Times section; this is just like the times you would have created in the routes area (see Figure 7.25). But here if you create them, they will be there when you get to the routes area. It is the same setup as far as adding, modifying, copying, deleting, or renaming a time that is in the system.

Figure 7.25 My Times

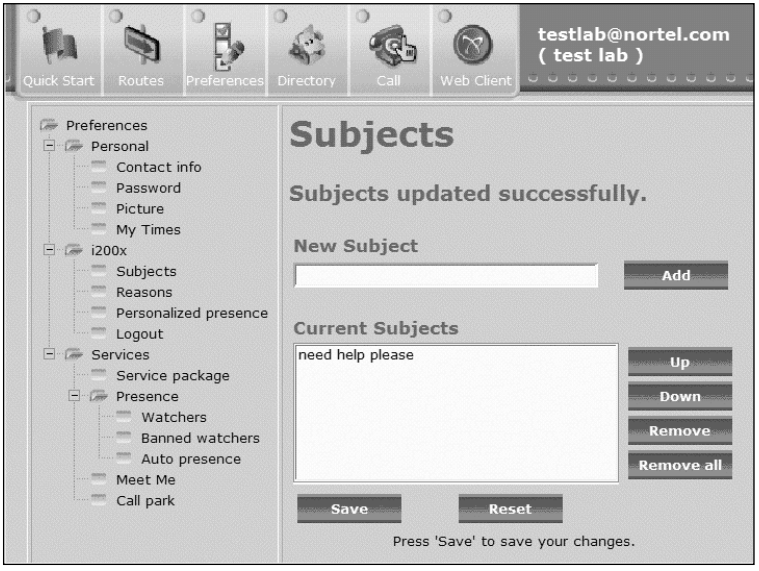


i200X

When receiving a call it would be nice to be able to send a message to someone before it goes to voicemail or let the person you are calling know what you need ahead of time. With MCS 5100, you can do all of that and more with the IP Phones and PC Client. Even though this section has a title of i200x, the same information can be used when using the PC Client. This is just another service of a multimedia system that you would not get with a normal VoIP PBX.

In Figure 7.26 we have selected the subject area under the i200x within the preference tree to the left. This has produced the window you see to the right, called Subjects. This identifies to the receiver what the call is about. You would add a subject in the new subject area, then select **Add**. The new subject is displayed at the bottom, where you can move it up or down, remove it, or reset it. Once complete, select **Save**.

Figure 7.26 Subjects



The section called Reasons shown in Figure 7.27 has the same set up as the Subject area shown in Figure 7.26. But this is used to tell users why you cannot get to a call. These are selectable on the IP Phones and PC Client

when calls come into the user. These are available only to users who are on the MCS 5100. Once complete, you must remember to select **Save**.

Figure 7.27 Reasons

As we had shown in the PC Client under Presence, you can add your own presence message instead of a system-provided message. This may be done within the PA; simply add a new note and select **Add**. When you are done, select **Save**. You can also remove notes if needed on the system, which is a good idea so you don't have a large drop-down menu for different notes within the PC Client. In Figure 7.28 we have added one note as an example for the section.

Sometimes a user will forget to log out of an IP phone or log into many IP phones and forget to log out of them when finished. This can cause phones to light all over an office, so the PA has this section, as shown in Figure 7.29, to fix that problem. This area will show all the IP phones that you are logged into at that time and will let you log out of the phones without going to each one. You just need to select the **Log me out** hyperlink to the right.

Figure 7.28 Personalized Presence

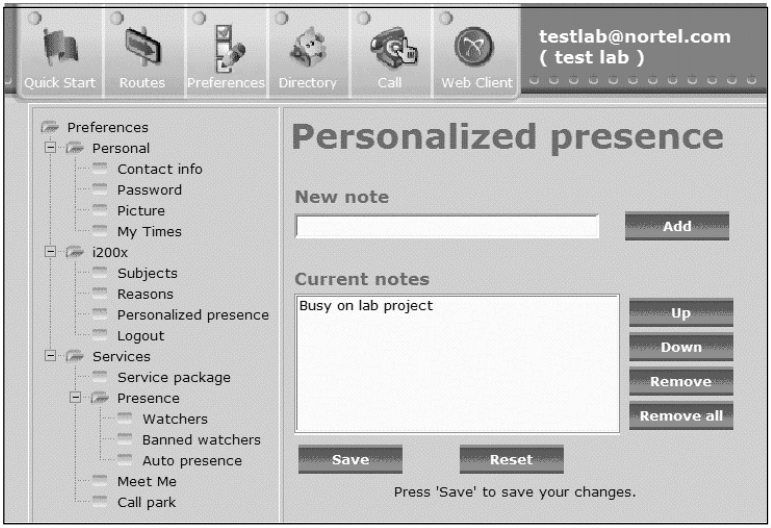
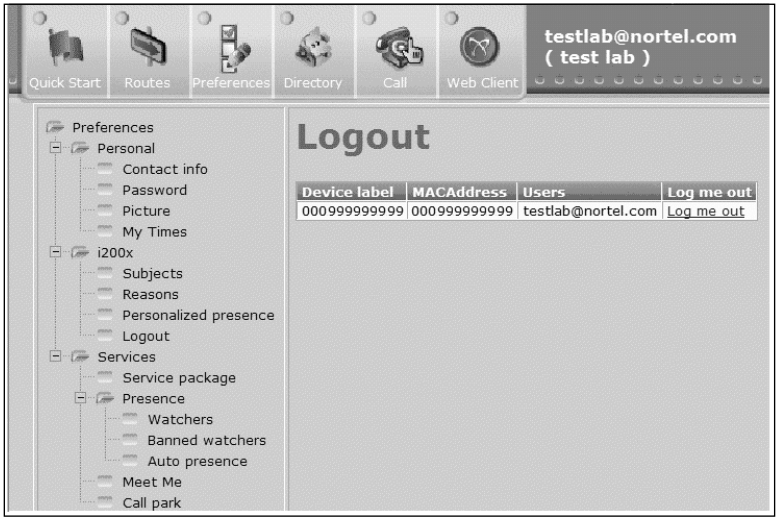


Figure 7.29 Logout

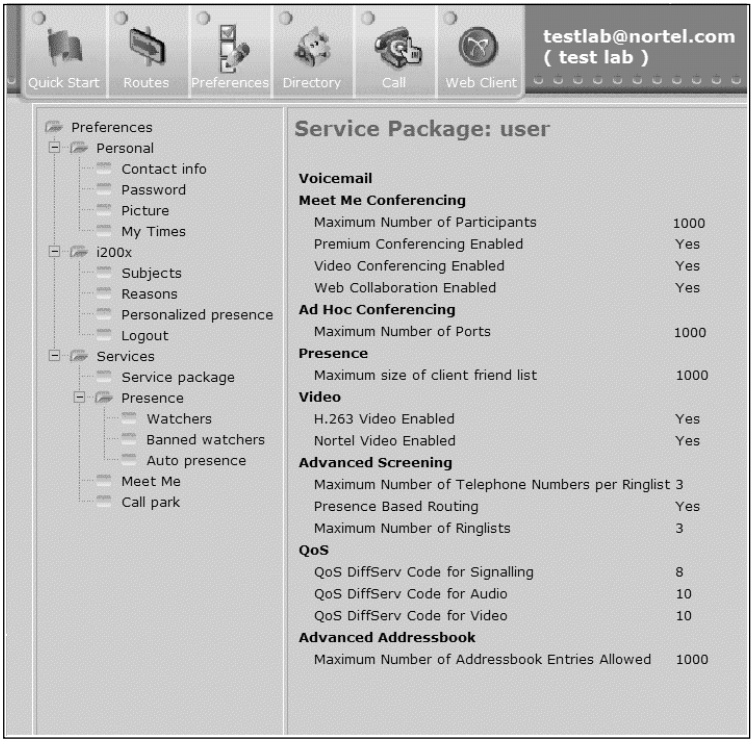


Services

The Service area shows what the administrator has assigned to you within the current service package. You cannot change these settings, but they can provide information so you are up to date on what options you do have on the system. Services such as address book, conference ports, and participants are

important to know so you don't invite too many people and not have enough room. Figure 7.30 shows current services available to our test user.

Figure 7.30 Service Package



In Figures 7.31 and 7.32 we have the Watchers list and the Banned watchers sections of the presence area. The watchers list contains people who have added you as a friend within the PC Client or IP Phone. This will give a full list of all users, their names, and how long they have been watching you, from the last time they have logged on to the system not from the first time they added you to the friends list. The hyperlink to the right lets you call the watcher from this screen if needed.

Also if you put a check in the box to the left of the name and then select the **ban watchers** button to the right, you will not see the real-time information about the current use in their friends list. Plus they will get an error saying that the user is no longer a friend when they log onto the PC Client.

Figure 7.32 shows the list of banned watchers you have selected, and allows you to delete them from the banned watcher list if needed.

Figure 7.31 Watchers List

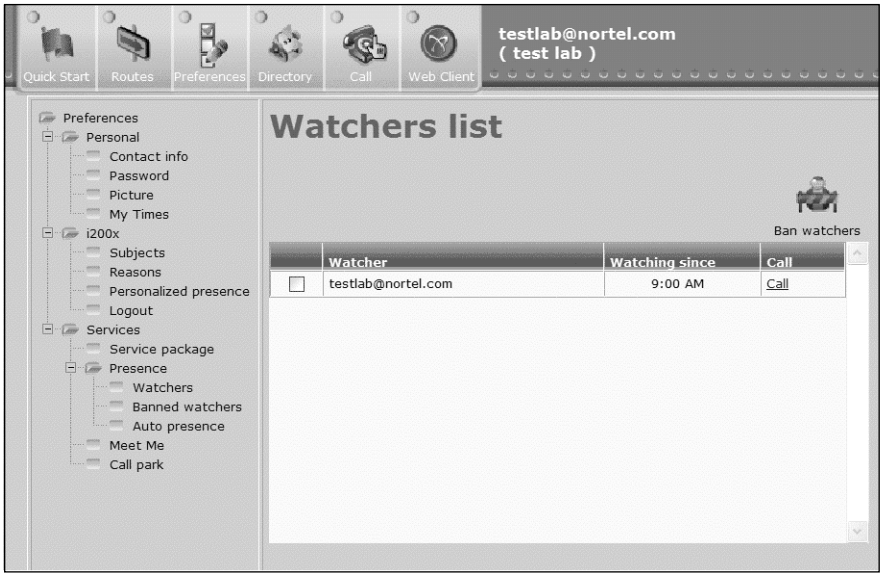


Figure 7.32 Banned Watchers

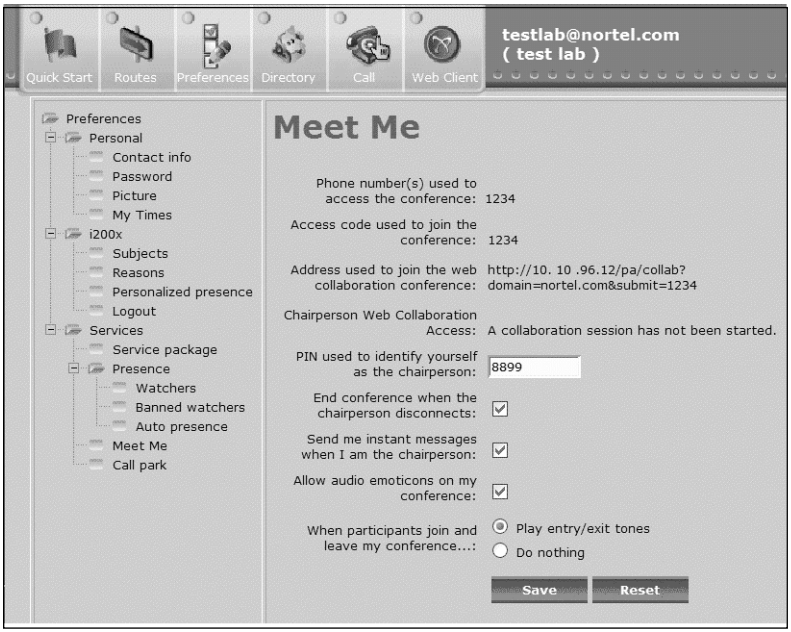
In Figure 7.33, you can select how other users on the system see you while on the IP phone or PC Client. You can change the inactivity timer; that is, change the report when inactive from yes to no. Once changes have been made, select **Save**.

Figure 7.33 Auto Presence

The Meet Me conferencing service of the MCS 5100 is one of the best features, and here within the PA you can see their options and make some changes to them. The system displays information you will need to have on hand such as the conference number, the user access code, and the address if you have the Web collaboration like we do on our system. It lets you change your user PIN to open the conference, and tell the system whether, when you leave, the conference ends or stays open.

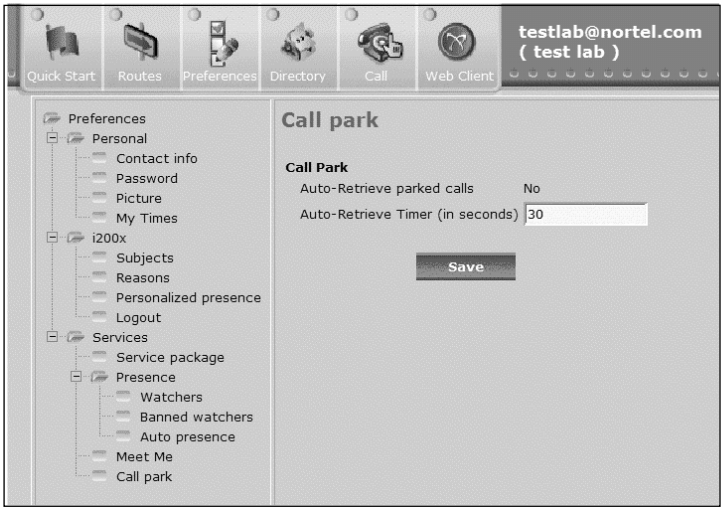
The system will also send instant messages about the conference to the user and play audio for the users when certain icons are used or when the users enter or leave a conference. You can check or uncheck these options in the boxes shown in Figure 7.34.

Figure 7.34 Meet Me



Call Park, as shown in Figure 7.35, is very simple and easy to configure. The administrator will have it configured for auto retrieval, and the only thing you can change is the timer of the auto retrieval on the call. When complete, select **Save**.

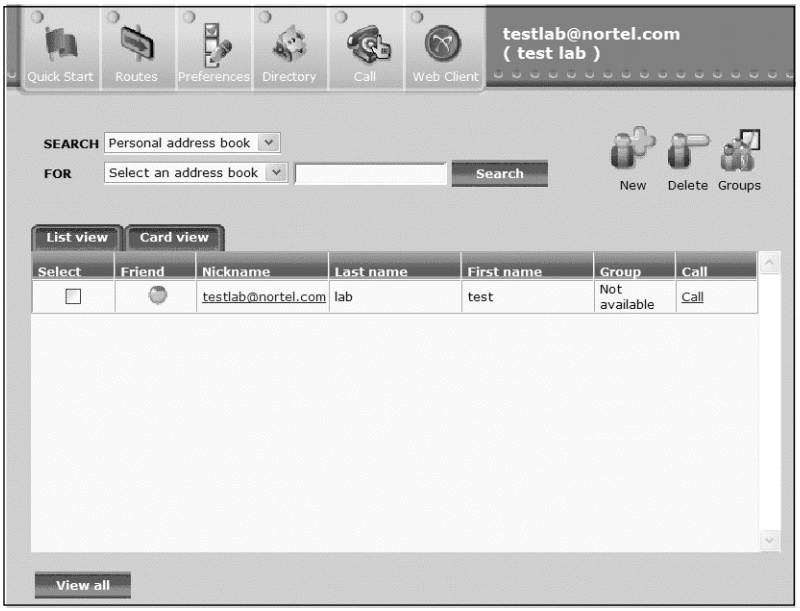
Figure 7.35 Call Park



Directory

The directory within the PA is the same as that seen within the PC Client. As shown in Figure 7.36, it lets you view the personal and global address books. You can add, delete, and make groups from users within these books, or add new users for outside users. In Figure 7.36 we show a list view for the personal address book, and then in Figure 7.37, we show a card view of the same user. Only in the card view can the user's picture be seen.

Figure 7.36 Directory List View



Click to Call

Click to Call lets you make a call if you are not using the PC Client or the Web Client. As shown in Figure 7.38, you can ring both parties. This may be done from the PC Client or from phones not on the system. This Click-to-Call feature is the same feature that is used when selecting a user to call within a call log on the system. Input the correct information to and from based on the current dialing plan and select the **Call** button.

Figure 7.37 Directory Card View

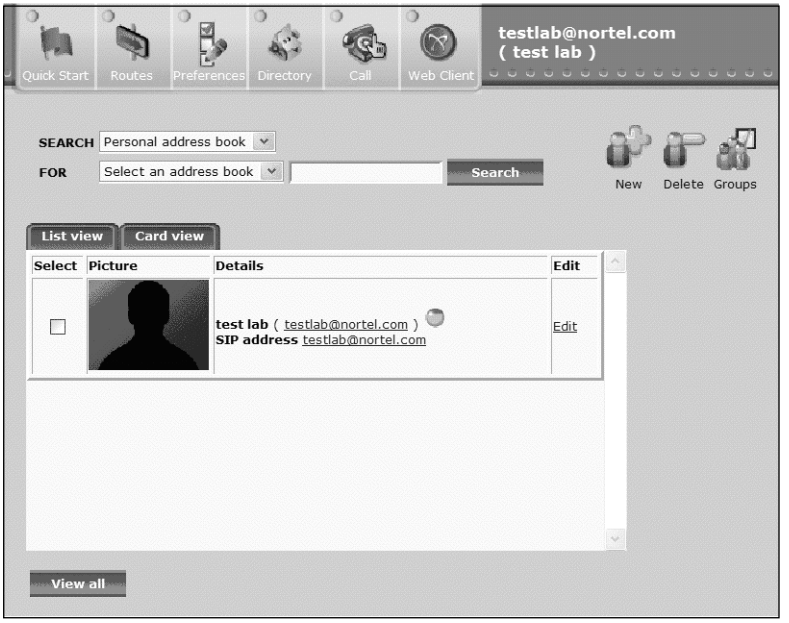
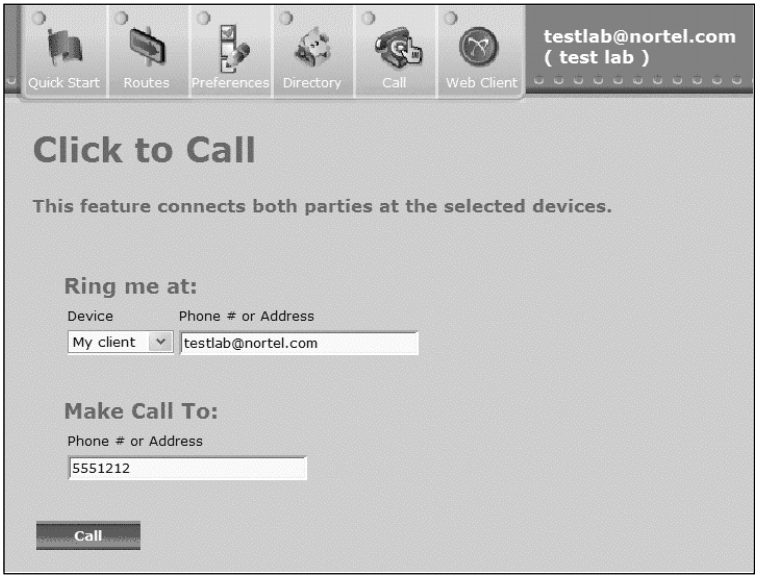


Figure 7.38 Click to Call



Web Client

We have talked about the Web Client that can be used from the PA and that it has all the same features as the PC Client. In Figure 7.39 we have selected the **Web Client** icon from the toolbar, and this has launched the Java-based client. Depending on how your computer is set up you could get the warning shown in the figure. Select either **Yes** or **Always** to move on to the next screen. In Figure 7.40 you can see that the client looks the same as the PC Client and the login is the same for both. Insert the username and password and click OK.

Figure 7.39 Web Client Warning

Figure 7.40 Web Client Sign In

Summary

The Personal Assistant is a tool that compliments the PC Client; it provides more features and service to the user who is either using the PC Client or an IP Phone. But the PA can be used as a standalone piece since it has the same client built into it—the Web Client. Since the Web Client has the same features as the PC Client, it is a company's decision on which they would like to use. If the company does not want to load new products or files onto the computer they can select the PA since it is available via a Web browser and only uses Java.

When users understand how they can use the PA to make day-to-day life even better while using its features, they will then understand the full capability of a Multimedia PBX. The Routes feature within the PA is the feature that will get the most use from each user. It is recommended that administrators pay attention to this and give plenty or training on this feature. It will help the users when they start to delve deeper into the PA client.

Solutions Fast Track

Logging on to Personal Agent

- ☑ User will use the same username and password as they do within the C++ PC Client.
- ☑ The PA does not work very well with Web browsers that are not Microsoft.
- ☑ Be sure to check settings and security features of the browser to make sure the client can be used to its fullest. This includes the deny pop-up feature.

Routes

- ☑ Provides real-time incoming call route transport for callers who are calling the user.

- ☑ Allows multiple routes to be made for users and groups based on numbers and nonnumbers.
- ☑ Users who are on the system can receive instant messages and push Web pages based on routes created by the user.

Preferences

- ☑ User may update information such as phone numbers, e-mail addresses, and other contact information to be shown within the address book.
- ☑ A picture may be up loaded by the user to be shown within the client and address book.
- ☑ User Times may be updated and created within the Preference area of the PA.

Directory

- ☑ Allows user to add other users either on or off the system to the personal address book.
- ☑ The user may create groups based on the users within the address book.
- ☑ Searches can be made in either the personal address book or global address book based on first, last, or nicknames.

Click to Call

- ☑ Users may use this to make calls from the call logs within the system.
- ☑ The feature connects the user and the person being called via the system; the user may be in the system or at a different number off the system.

Multimedia Web Client

- ☑ Multimedia Web Client is a Java-based client that has the same features as the C++ PC Client.
- ☑ Works best when used on a Microsoft Web browser.
- ☑ Can be used off the system for remote users who travel and have access only to a secure SLL Web page.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Based on the feature of the PA is there a reason to buy the C++ PC Client?

A: It is really a preference, since some companies do not like to be totally Web-based and like the hard client. But then some others use both since they have remote users.

Q: If I have the C++ Client will I still have the PA?

A: Yes, the Web Client is the other client that you will need licenses to use.

Q: How can I check the phone number assigned to me?

A: Look under the Preference area in Contact info; it will be listed under Aliases.

Q: Can I create more than one route for a user?

A: You could but it is not recommended; you should have one route per person or user. That will eliminate any problems when the routes are applied to the call.

Q: Can I change my services within the list of service packages?

A: No, this is just a list for the user. The administrator will need to make any changes needed.

Q: Do I have to show users what my status is while on my IP phone or Client?

A: No. Under auto presence you may select **No**, and this will just show you online and not if you are on the phone or inactive.

Chapter 8

SIP Architecture

Solutions in this chapter:

- **Understanding SIP**
- **SIP Functions and Features**
- **SIP Architecture**
- **Instant Messaging and SIMPLE**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

As the Internet became more popular in the 1990s, network programs that allowed communication with other Internet users also became more common. Over the years, a need was seen for a standard protocol that could allow participants in a chat, videoconference, interactive gaming, or other media to initiate user sessions with one another. In other words, a standard set of rules and services was needed that defined how computers would connect to one another so that they could share media and communicate. The Session Initiation Protocol (SIP) was developed to set up, maintain, and tear down these sessions between computers.

By working in conjunction with a variety of other protocols and specialized servers, SIP provides a number of important functions that are necessary in allowing communications between participants. SIP provides methods of sharing the location and availability of users and explains the capabilities of the software or device being used. SIP then makes it possible to set up and manage the session between the parties. Without these tasks being performed, communication over a large network like the Internet would be impossible. It would be like a message in a bottle being thrown in the ocean; you would have no way of knowing how to reach someone directly or whether the person even could receive the message.

Beyond communicating with voice and video, SIP has also been extended to support instant messaging and is becoming a popular choice that's incorporated in many of the instant messaging applications being produced. This extension, called SIMPLE, provides the means of setting up a session in much the same way as SIP. SIMPLE also provides information on the status of users, showing whether they are online, busy, or in some other state of presence. Because SIP is being used in these various methods of communications, it has become a widely used and important component of today's communications.

Understanding SIP

SIP was designed to initiate interactive sessions on an IP network. Programs that provide real-time communication between participants can use SIP to set up, modify, and terminate a connection between two or more computers,

allowing them to interact and exchange data. The programs that can use SIP include instant messaging, voice over IP (VoIP), video teleconferencing, virtual reality, multiplayer games, and other applications that employ single-media or multimedia. SIP doesn't provide all the functions that enable these programs to communicate, but it is an important component that facilitates communication between two or more endpoints.

You could compare SIP to a telephone switchboard operator, who uses other technology to connect you to another party, set up conference calls or other operations on your behalf, and disconnect you when you're done. SIP is a type of signaling protocol that is responsible for sending commands to start and stop transmissions or other operations used by a program. The commands sent between computers are codes that do such things as open a connection to make a phone call over the Internet or disconnect that call later on. SIP supports additional functions, such as call waiting, call transfer, and conference calling, by sending out the necessary signals to enable and disable these functions. Just as the telephone operator isn't concerned with how communication occurs, SIP works with a number of components and can run on top of several different transport protocols to transfer media between the participants.

Overview of SIP

One of the major reasons that SIP is necessary is found in the nature of programs that involve messaging, voice communication, and exchange of other media. The people who use these programs may change locations and use different computers, have several usernames or accounts, or communicate using a combination of voice, text, or other media (requiring different protocols). This creates a situation that's similar to trying to mail a letter to someone who has several aliases, speaks different languages, and could change addresses at any particular moment.

SIP works with various network components to identify and locate these endpoints. Information is passed through proxy servers, which are used to register and route requests to the user's location, invite another user(s) into a session, and make other requests to connect these endpoints. Because there are a number of different protocols available that may be used to transfer voice, text, or other media, SIP runs on top of other protocols that transport

data and perform other functions. By working with other components of the network, data can be exchanged between these user agents regardless of where they are at any given point.

It is the simplicity of SIP that makes it so versatile. SIP is an ASCII- or text-based protocol, similar to HTTP or SMTP, which makes it more lightweight and flexible than other signaling protocols (such as H.323). Like HTTP and SMTP, SIP is a request-response protocol, meaning that it makes a request of a server, and awaits a response. Once it has established a session, other protocols handle such tasks as negotiating the type of media to be exchanged, and transporting it between the endpoints. The reusing of existing protocols and their functions means that fewer resources are used, and minimizes the complexity of SIP. By keeping the functionality of SIP simple, it allows SIP to work with a wider variety of applications.

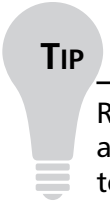
The similarities to HTTP and SMTP are no accident. SIP was modeled after these text-based protocols, which work in conjunction with other protocols to perform specific tasks. As we'll see later in this chapter, SIP is also similar to these other protocols in that it uses Universal Resource Identifiers (URIs) for identifying users. A URI identifies resources on the Internet, just as a Uniform Resource Locator (URL) is used to identify Web sites. The URI used by SIP incorporates a phone number or name, such as SIP: user@syngress.com, which makes reading SIP addresses easier. Rather than reinventing the wheel, the development of SIP incorporated familiar aspects of existing protocols that have long been used on IP networks. The modular design allows SIP to be easily incorporated into Internet and network applications, and its similarities to other protocols make it easier to use.

RFC 2543/RFC 3261

The Session Initiation Protocol is a standard that was developed by the Internet Engineering Task Force (IETF). The IETF is a body of network designers, researchers, and vendors that are members of the Internet Society Architecture Board for the purpose of developing Internet communication standards. The standards they create are important because they establish consistent methods and functionality. Unlike proprietary technology, which may or may not work outside of a specific program, standardization allows a protocol or other technology to function the same way in any application or

environment. In other words, because SIP is a standard, it can work on any system, regardless of the communication program, operating system, or infrastructure of the IP network.

The way that IETF develops a standard is through recommendations for rules that are made through Request for Comments (RFCs). The RFC starts as a draft that is examined by members of a Working Group, and during the review process, it is developed into a finalized document. The first proposed standard for SIP was produced in 1999 as RFC 2543, but in 2002, the standard was further defined in RFC 3261. Additional documents outlining extensions and specific issues related to the SIP standard have also been released, which make RFC 2543 obsolete and update RFC 3261. The reason for these changes is that as technology changes, the development of SIP also evolves. The IETF continues developing SIP and its extensions as new products are introduced and its applications expand.



TIP

Reviewing RFCs can provide you with additional insight and information, answering specific questions you may have about SIP. The RFCs related to SIP can be reviewed by visiting the IETF Web site at www.ietf.org. Additional materials related to the Session Initiation Protocol Working Group also can be found at www.softarmor.com/sipwg/.

SIP and Mbone

Although RFC 2543 and RFC 3261 define SIP as a protocol for setting up, managing, and tearing down sessions, the original version of SIP had no mechanism for tearing down sessions and was designed for the Multicast Backbone (Mbone). Mbone originated as a method of broadcasting audio and video over the Internet. The Mbone is a broadcast channel that is overlaid on the Internet, and allowed a method of providing Internet broadcasts of things like IETF meetings, space shuttle launches, live concerts, and other meetings, seminars, and events. The ability to communicate with several hosts simultaneously needed a way of inviting users into sessions; the Session Invitation Protocol (as it was originally called) was developed in 1996.

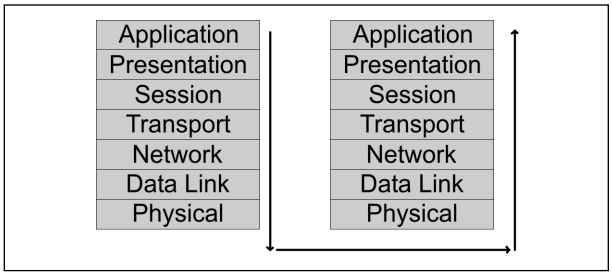
The Session Invitation Protocol was a precursor to SIP that was defined by the IETF MMUSIC Working group, and a primitive version of the Session Initiation Protocol used today. However, as VoIP and other methods of communications became more popular, SIP evolved into the Session Initiation Protocol. With added features like the ability to tear down a session, it was a still more lightweight than more complex protocols like H.323. In 1999, the Session Initiation Protocol was defined as RFC 2543, and has become a vital part of multimedia applications used today.

OSI

In designing the SIP standard, the IETF mapped the protocol to the OSI (Open Systems Interconnection) reference model. The OSI reference model is used to associate protocols to different layers, showing their function in transferring and receiving data across a network, and their relation to other existing protocols. A protocol at one layer uses only the functions of the layer below it, while exporting the information it processes to the layer above it. It is a conceptual model that originated to promote interoperability, so that a protocol or element of a network developed by one vendor would work with others.

As seen in Figure 8.1, the OSI model contains seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical. As seen in this figure, network communication starts at the Application layer and works its way down through the layers step by step to the Physical layer. The information then passes along the cable to the receiving computer, which starts the information at the Physical layer. From there it steps back up the OSI layers to the Application layer where the receiving computer finalizes the processing and sends back an acknowledgement if needed. Then the whole process starts over.

Figure 8.1 In the OSI Reference Model, Data is Transmitted down through the Layers, across the Medium, and Back up through the Layers



The layers of the OSI reference model have different functions that are necessary in transferring data across a network, and mapping protocols to these layers make it easier to understand how they interrelate to the network as a whole. Table 8.1 shows the seven layers of the OSI model, and briefly explains their functions.

Table 8.1 Layers of the OSI Model

Layer	Description
7: Application	The Application layer is used to identify communication partners, facilitate authentication (if necessary), and allows a program to communicate with lower layer protocols, so that in turn it can communicate across the network. Protocols that map to this layer include SIP, HTTP, and SMTP.
6: Presentation	The Presentation layer converts data from one format to another, such as converting a stream of text into a pop-up window, and handles encoding and encryption.
5: Session	The Session layer is responsible for coordinating sessions and connections.
4: Transport	The Transport layer is used to transparently transfer data between computers. Protocols that map to this layer include TCP, UDP, and RTP.
3: Network	The Network Layer is used to route and forward data so that it goes to the proper destination. The most common protocol that maps to this layer is IP.

Continued

Table 8.1 continued Layers of the OSI Model

Layer	Description
2: Data Link	The Data Link layer is used to provide error correction that may occur at the physical level, and provide physical addressing through the use of MAC addresses that are hard-coded into network cards.
1: Physical	The Physical layer defines electrical and physical specifications of network devices, and provides the means of allowing hardware to send and receive data on a particular type of media. At this level, data is passed as a bit stream across the network.

SIP and the Application Layer

Because SIP is the Session Initiation Protocol, and its purpose is to establish, modify, and terminate sessions, it would seem at face-value that this protocol maps to the Session layer of the OSI reference model. However, it is important to remember that the protocols at each layer interact only with the layers above and below it. Programs directly access the functions and supported features available through SIP, disassociating it from this layer. SIP is used to invite a user into an interactive session, and can also invite additional participants into existing sessions, such as conference calls or chats. It allows media to be added to or removed from a session, provides the ability to identify and locate a user, and also supports name mapping, redirection, and other services. When comparing these features to the OSI model, it becomes apparent that SIP is actually an Application-layer protocol.

The Application layer is used to identify communication partners, facilitate authentication (if necessary), and allows a program to communicate with lower layer protocols, so that in turn it can communicate across the network. In the case of SIP, it is setting up, maintaining, and ending interactive sessions, and providing a method of locating and inviting participants into these sessions. The software being used communicates through SIP, which passes the data down to lower layer protocols and sends it across the network.

SIP Functions and Features

When SIP was developed, it was designed to support five specific elements of setting up and tearing down communication sessions. These supported facets of the protocol are:

- User location, where the endpoint of a session can be identified and found, so that a session can be established
- User availability, where the participant that's being called has the opportunity and ability to indicate whether he or she wishes to engage in the communication
- User capabilities, where the media that will be used in the communication is established, and the parameters of that media are agreed upon
- Session setup, where the parameters of the session are negotiated and established
- Session management, where the parameters of the session are modified, data is transferred, services are invoked, and the session is terminated

Although these are only a few of the issues needed to connect parties together so they can communicate, they are important ones that SIP is designed to address. However, beyond these functions, SIP uses other protocols to perform tasks necessary that allow participants to communicate with each other, which we'll discuss later in this chapter.

User Location

The ability to find the location of a user requires being able to translate a participant's username to their current IP address of the computer being used. The reason this is so important is because the user may be using different computers, or (if DHCP is used) may have different IP addresses to identify the computer on the network. The program can use SIP to register the user with a server, providing a username and IP address to the server. Because a server now knows the current location of the user, other users can now find that user on the network. Requests are redirected through the proxy server to

the user's current location. By going through the server, other potential participants in a communication can find users, and establish a session after acquiring their IP addresses.

User Availability

The user availability function of SIP allows a user to control whether he or she can be contacted. The user can set themselves as being away or busy, or available for certain types of communication. If available, other users can then invite the user to join in a type of communication (e.g., voice or videoconference), depending on the capabilities of the program being used.

User Capabilities

Determining the user's capabilities involves determining what features are available on the programs being used by each of the parties, and then negotiating which can be used during the session. Because SIP can be used with different programs on different platforms, and can be used to establish a variety of single-media and multimedia communications, the type of communication and its parameters needs to be determined. For example, if you were to call a particular user, your computer might support video conferencing, but the person you're calling doesn't have a camera installed. Determining the user capabilities allows the participants to agree on which features, media types, and parameters will be used during a session.

Session Setup

Session setup is where the participants of the communication connect together. The user who is contacted to participate in a conversation will have their program "ring" or produce some other notification, and has the option of accepting or rejecting the communication. If accepted, the parameters of the session are agreed upon and established, and the two endpoints will have a session started, allowing them to communicate.

Session Management

Session management is the final function of SIP, and is used for modifying the session as it is in use. During the session, data will be transferred between the

participants, and the types of media used may change. For example, during a voice conversation, the participants may decide to invoke other services available through the program, and change to a video conferencing. During communication, they may also decide to add or drop other participants, place a call on hold, have the call transferred, and finally terminate the session by ending their conversation. These are all aspects of session management, which are performed through SIP.

SIP URIs

Because SIP was based on existing standards that had already been proven on the Internet, it uses established methods for identifying and connecting endpoints together. This is particularly seen in the addressing scheme that it uses to identify different SIP accounts. SIP uses addresses that are similar to e-mail addresses. The hierarchical URI shows the domain where a user's account is located, and a host name or phone number that serves as the user's account. For example, SIP: myaccount@madeupsip.com shows that the account *myaccount* is located at the domain *madeupsip.com*. Using this method makes it simple to connect someone to a particular phone number or username.

Because the addresses of those using SIP follow a *username@domainname* format, the usernames created for accounts must be unique within the namespace. Usernames and phone numbers must be unique as they identify which account belongs to a specific person, and used when someone attempts sending a message or placing a call to someone else. Because the usernames are stored on centralized servers, the server can determine whether a particular username is available or not when a person initially sets up an account.

URIs also can contain other information that allows it to connect to a particular user, such as a port number, password, or other parameters. In addition to this, although SIP URIs will generally begin with SIP:, others will begin with SIPS:, which indicates that the information must be sent over a secure transmission. In such cases, the data and messages transmitted are transported using the Transport Layer Security (TLS) protocol, which we'll discuss later in this chapter.

SIP Architecture

Though we've discussed a number of the elements of SIP, there are still a number of essential components that make up SIP's architecture that we need to address. SIP would not be able to function on a network without the use of various devices and protocols. The essential devices are those that you and other participants would use in a conversation, allowing you to communicate with one another, and various servers may also be required to allow the participants to connect together. In addition to this, there are a number of protocols that carry your voice and other data between these computers and devices. Together, they make up the overall architecture of SIP.

SIP Components

Although SIP works in conjunction with other technologies and protocols, there are two fundamental components that are used by the Session Initiation Protocol:

- User agents, which are endpoints of a call (i.e., each of the participants in a call)
- SIP servers, which are computers on the network that service requests from clients, and send back responses

User Agents

User agents are both the computer that is being used to make a call, and the target computer that is being called. These make the two endpoints of the communication session. There are two components to a user agent: a client and a server. When a user agent makes a request (such as initiating a session), it is the User Agent Client (UAC), and the user agent responding to the request is the User Agent Server (UAS). Because the user agent will send a message, and then respond to another, it will switch back and forth between these roles throughout a session.

Even though other devices that we'll discuss are optional to various degrees, User Agents must exist for a SIP session to be established. Without them, it would be like trying to make a phone call without having another

person to call. One UA will invite the other into a session, and SIP can then be used to manage and tear down the session when it is complete. During this time, the UAC will use SIP to send requests to the UAS, which will acknowledge the request and respond to it. Just as a conversation between two people on the phone consists of conveying a message or asking a question and then waiting for a response, the UAC and UAS will exchange messages and swap roles in a similar manner throughout the session. Without this interaction, communication couldn't exist.

Although a user agent is often a software application installed on a computer, it can also be a PDA, USB phone that connects to a computer, or a gateway that connects the network to the Public Switched Telephone Network. In any of these situations however, the user agent will continue to act as both a client and a server, as it sends and responds to messages.

SIP Server

The SIP server is used to resolve usernames to IP addresses, so that requests sent from one user agent to another can be directed properly. A user agent registers with the SIP server, providing it with their username and current IP address, thereby establishing their current location on the network. This also verifies that they are online, so that other user agents can see whether they're available and invite them into a session. Because the user agent probably wouldn't know the IP address of another user agent, a request is made to the SIP server to invite another user into a session. The SIP server then identifies whether the person is currently online, and if so, compares the username to their IP address to determine their location. If the user isn't part of that domain, and thereby uses a different SIP server, it will also pass on requests to other servers.

In performing these various tasks of serving client requests, the SIP server will act in any of several different roles:

- Registrar server
- Proxy server
- Redirect server

Registrar Server

Registrar servers are used to register the location of a user agent who has logged onto the network. It obtains the IP address of the user and associates it with their username on the system. This creates a directory of all those who are currently logged onto the network, and where they are located. When someone wishes to establish a session with one of these users, the Registrar server's information is referred to, thereby identifying the IP addresses of those involved in the session.

Proxy Server

Proxy servers are computers that are used to forward requests on behalf of other computers. If a SIP server receives a request from a client, it can forward the request onto another SIP server on the network. While functioning as a proxy server, the SIP server can provide such functions as network access control, security, authentication, and authorization.

Redirect Server

The Redirect servers are used by SIP to redirect clients to the user agent they are attempting to contact. If a user agent makes a request, the Redirect server can respond with the IP address of the user agent being contacted. This is different from a Proxy server, which forwards the request on your behalf, as the Redirect server essentially tells you to contact them yourself.

The Redirect server also has the ability to "fork" a call, by splitting the call to several locations. If a call was made to a particular user, it could be split to a number of different locations, so that it rang at all of them at the same time. The first of these locations to answer the call would receive it, and the other locations would stop ringing.

NOTE

RFC 3261 defines the different types of SIP servers as logical devices, meaning that they can be implemented as separate servers or as part of a single application that resides on a single physical server. In other words, a single physical server may act in all or one of these roles.

In addition to this, the SIP servers can interact with other servers and applications on your network to provide additional services, such as authentication or billing. The SIP servers could access Lightweight Directory Access Protocol (LDAP) servers, database applications, or other applications to access back-end services.

Stateful versus Stateless

The servers used by SIP can run in one of two modes: stateful or stateless. When a server runs in stateful mode, it will keep track of all requests and responses it sends and receives. A server that operates in a stateless mode won't remember this information, but will instead forget about what it has done once it has processed a request. A server running in stateful mode generally is found in a domain where the user agents resides, whereas stateless servers are often found as part of the backbone, receiving so many requests that it would be difficult to keep track of them.

Location Service

The location service is used to keep a database of those who have registered through a SIP server, and where they are located. When a user agent registers with a Registrar server, a REGISTER request is made (which we'll discuss in the later section). If the Registrar accepts the request, it will obtain the SIP-address and IP address of the user agent, and add it to the location service for its domain. This database provides an up-to-date catalog of everyone who is online, and where they are located, which Redirect servers and Proxy servers can then use to acquire information about user agents. This allows the servers to connect user agents together or forward requests to the proper location.

Client/Server versus Peer-to-Peer Architecture

In looking at the components of SIP, you can see that requests are processed in different ways. When user agents communicate with one another, they send requests and responses to one another. In doing so, one acts as a User Agent Client, and the other fulfills the request acts as a User Agent Server. When dealing with SIP servers however, they simply send requests that are

processed by a specific server. This reflects two different types of architectures used in network communications:

- Client/Server
- Peer-to-peer

Client/Server

In a client/server architecture, the relationship of the computers are separated into two roles:

- The client, which requests specific services or resources
- The server, which is dedicated to fulfilling requests by responding (or attempting to respond) with requested services or resources

An easy-to-understand example of a client/server relationship is seen when using the Internet. When using an Internet browser to access a Web site, the client would be the computer running the browser software, which would request a Web page from a Web server. The Web server receives this request and then responds to it by sending the Web page to the client computer. In VoIP, this same relationship can be seen when a client sends a request to register with a Registrar server, or makes a request to a Proxy Server or Redirect Server that allows it to connect with another user agent. In all these cases, the client's role is to request services and resources, and the server's role is to listen to the network and await requests that it can process or pass onto other servers.

The servers that are used on a network acquire their abilities to service requests by the programs installed on it. Because a server may run a number of services or have multiple server applications installed on it, a computer dedicated to the role of being a server may provide several functions on a network. For example, a Web server might also act as an e-mail server. In the same way, SIP servers also may provide different services. A Registrar can register clients and also run the location service that allows clients and other servers to locate other users who have registered on the network. In this way, a single server may provide diverse functionality to a network that would otherwise be unavailable.

Another important function of the server is that, unlike clients that may be disconnected from the Internet or shutdown on a network when the person using it is done, a server is generally active and awaiting client requests. Problems and maintenance aside, a dedicated server is up and running, so that it is accessible. The IP address of the server generally doesn't change, meaning that clients can always find it on a network, making it important for such functions as finding other computers on the network.

Peer to Peer

A peer-to-peer (P2P) architecture is different from the client/server model, as the computers involved have similar capabilities, and can initiate sessions with one another to make and service requests from one another. Each computer provides services and resources, so if one becomes unavailable, another can be contacted to exchange messages or access resources. In this way, the user agents act as both client and server, and are considered peers.

Once a user agent is able to establish a communication session with another user agent, a P2P architecture is established where each machine makes requests and responds to the other. One machine acting as the User Agent client will make a request, while the other acting as the User Agent server will respond to it. Each machine can then swap roles, allowing them to interact as equals on the network. For example, if the applications being used allowed file sharing, a UAC could request a specific file from the UAS and download it. During this time, the peers could also be exchanging messages or talking using VoIP, and once these activities are completed, one could send a request to terminate the session to end the communications between them. As seen by this, the computers act in the roles of both client and server, but are always peers by having the same functionality of making and responding to requests.

SIP Requests and Responses

Because SIP is a text-based protocol like HTTP, it is used to send information between clients and servers, and User Agent clients and User Agent servers, as a series of requests and responses. When requests are made, there are a number of possible signaling commands that might be used:

- **REGISTER** Used when a user agent first goes online and registers their SIP address and IP address with a Registrar server.
- **INVITE** Used to invite another User agent to communicate, and then establish a SIP session between them.
- **ACK** Used to accept a session and confirm reliable message exchanges.
- **OPTIONS** Used to obtain information on the capabilities of another user agent, so that a session can be established between them. When this information is provided a session isn't automatically created as a result.
- **SUBSCRIBE** Used to request updated presence information on another user agent's status. This is used to acquire updated information on whether a User agent is online, busy, offline, and so on.
- **NOTIFY** Used to send updated information on a User agent's current status. This sends presence information on whether a User agent is online, busy, offline, and so on.
- **CANCEL** Used to cancel a pending request without terminating the session.
- **BYE** Used to terminate the session. Either the user agent who initiated the session, or the one being called can use the BYE command at any time to terminate the session.

When a request is made to a SIP server or another user agent, one of a number of possible responses may be sent back. These responses are grouped into six different categories, with a three-digit numerical response code that begins with a number relating to one of these categories. The various categories and their response code prefixes are as follows:

- **Informational (1xx)** The request has been received and is being processed.
- **Success (2xx)** The request was acknowledged and accepted.

- **Redirection (3xx)** The request can't be completed and additional steps are required (such as redirecting the user agent to another IP address).
- **Client error (4xx)** The request contained errors, so the server can't process the request
- **Server error (5xx)** The request was received, but the server can't process it. Errors of this type refer to the server itself, and doesn't indicate that another server won't be able to process the request.
- **Global failure (6xx)** The request was received and the server is unable to process it. Errors of this type refer to errors that would occur on any server, so the request wouldn't be forwarded to another server for processing.

There are a wide variety of responses that apply to each of the categories. The different responses, their categories, and codes are shown in Table 8.2.

Table 8.2 Listing of Responses, Response Codes, and Their Meanings

Response Code	Response Category	Response Description
100	Informational	Trying
180	Informational	Ringing
181	Informational	Call is being forwarded
182	Informational	Queued
200	Success	OK
300	Redirection	Multiple choices
301	Redirection	Moved permanently
302	Redirection	Moved temporarily
303	Redirection	See other
305	Redirection	Use proxy
380	Redirection	Alternative service
400	Client Error	Bad request
401	Client Error	Unauthorized
402	Client Error	Payment required

Continued

Table 8.2 continued Listing of Responses, Response Codes, and Their Meanings

Response Code	Response Category	Response Description
403	Client Error	Forbidden
404	Client Error	Not found
405	Client Error	Method not allowed
406	Client Error	Not acceptable
407	Client Error	Proxy authentication required
408	Client Error	Request timeout
409	Client Error	Conflict
410	Client Error	Gone
411	Client Error	Length required
413	Client Error	Request entity too large
414	Client Error	Request-URI too large
415	Client Error	Unsupported media type
420	Client Error	Bad extension
480	Client Error	Temporarily not available
481	Client Error	Call leg/transaction does not exist
482	Client Error	Loop detected
483	Client Error	Too many hops
484	Client Error	Address incomplete
485	Client Error	Ambiguous
486	Client Error	Busy here
500	Server Error	Internal server error
501	Server Error	Not implemented
502	Server Error	Bad gateway
503	Server Error	Service unavailable
504	Server Error	Gateway time-out
505	Server Error	SIP version not supported
600	Global Failures	Busy everywhere

Table 8.2 continued Listing of Responses, Response Codes, and Their Meanings

Response Code	Response Category	Response Description
603	Global Failures	Decline
604	Global Failures	Does not exist anywhere
606	Global Failures	Not acceptable

Protocols Used with SIP

Although SIP is a protocol in itself, it still needs to work with different protocols at different stages of communication to pass data between servers, devices, and participants. Without the use of these protocols, communication and the transport of certain types of media would either be impossible or insecure. In the sections that follow, we'll discuss a number of the common protocols that are used with SIP, and the functions they provide during a session.

UDP

The User Datagram Protocol (UDP) is part of the TCP/IP suite of protocols, and is used to transport units of data called *datagrams* over an IP network. It is similar to the Transmission Control Protocol (TCP), except that it doesn't divide messages into packets and reassembles them at the end. Because the datagrams don't support sequencing of the packets as the data arrives at the endpoint, it is up to the application to ensure that the data has arrived in the right order and has arrived completely. This may sound less beneficial than using TCP for transporting data, but it makes UDP faster because there is less processing of data. It often is used when messages with small amounts of data (which requires less reassembling) are being sent across the network, or with data that will be unaffected overall by a few units of missing data.

Although an application may have features that ensure that datagrams haven't gone missing or arrived out of order, many simply accept the potential of data loss, duplication, or errors. In the case of Voice over IP, streaming video, or interactive games, a minor loss of data or error will be a minor glitch that generally won't affect the overall quality or performance. In these

cases, it is more important that the data is passed quickly from one endpoint to another. If reliability were a major issue, then the use of TCP as a transport protocol would be a better choice over hindering the application with features that check for the reliability of the data it receives.

Notes from the Underground…

UDP Denial-of-Service Attacks

Although denial-of-service (DoS) attacks are less common using UDP, data sent over this protocol can be used to bog down or even shut down a system that's victim to it. Because UDP is a connectionless protocol, it doesn't need to have a connection with another system before it transfers data. In a UDP Flood Attack, the attacker will send UDP packets to random ports on another system. When the remote host receives the UDP packets, it will do the following:

1. Determine which application is listening to the port.
2. Find that no application is waiting on that port.
3. Reply to the sender of the data (which may be a forged source address) with an ICMP packet of DESTINATION UNREACHABLE.

Although this may be a minor issue if the remote host has to send only a few of these ICMP packets, it will cause major problems if enough UDP packets are sent to the host's ports. A large number of UDP packets sent to the victim will cause the remote host to repeat these steps over and over. The victim's ports are monopolized by receiving data that isn't used by any application on the system, and ICMP packets are sent out to relay this fact to the attacker. Although other clients will find the remote host unreachable, eventually the system could even go down if enough UDP packets are sent.

To reduce the chances of falling victim to this type of attack, a number of measures can be taken. Proxy servers and firewalls can be implemented on a network to prevent UDP from being used maliciously and filter unwanted traffic. For example, if an attack appeared to come from one source previously, you could set up a rule on the firewall that blocks UDP traffic from that IP address. In addition to this, chargen and

Continued

echo services, as well as other unused UDP services, could be either disabled or filtered. Once these measures are taken, however, you should determine which applications on your network are using UDP, and monitor for signs of a UDP Flood Attack or other signs of misuse.

Transport Layer Security

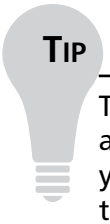
Transport Layer Security (TLS) is a protocol that can be used with other protocols like UDP to provide security between applications communicating over an IP network. TLS uses encryption to ensure privacy, so that other parties can't eavesdrop or tamper with the messages being sent. Using TLS, a secure connection is established by authenticating the client and server, or User Agent Client and User Agent Server, and then encrypting the connection between them.

Transport Layer Security is a successor to Secure Sockets Layer (SSL), which was developed by Netscape. Even though it is based on SSL 3.0, TLS is a standard that has been defined in RFC 2246, and is designed to be its replacement. In this standard, TLS is designed as a multilayer protocol that consists of:

- TLS Handshake Protocol
- TLS Record Protocol

The TLS Handshake Protocol is used to authenticate the participants of the communication and negotiate an encryption algorithm. This allows the client and server to agree upon an encryption method and prove who they are using cryptographic keys before any data is sent between them. Once this has been done successfully, a secure channel is established between them.

After the TLS Handshake Protocol is used, the TLS Record Protocol ensures that the data exchanged between the parties isn't altered en route. This protocol can be used with or without encryption, but TLS Record Protocol provides enhanced security using encryption methods like the Data Encryption Standard (DES). In doing so, it provides the security of ensuring data isn't modified, and others can't access the data while in transit.



TIP

The Transport Layer Security Protocol isn't a requirement for using SIP, and generally isn't needed for standard communications. For example, if you're using VoIP or other communication software to trade recipes or talk about movies with a friend, then using encryption might be overkill. However, in the case of companies that use VoIP for business calls or to exchange information that requires privacy, then using TLS is a viable solution for ensuring that information and data files exchanged over the Internet are secure.

Tools & Traps…

Encryption versus Nonencrypted Data

When sessions are initiated using SIP, the data passed between the servers and other users is sent using UDP. As it is sent across the Internet, it can go through a number of servers and routers, and may be passed through a local network on your end or the other participant's end. During any point in this trip, it is possible that the data may be intercepted by a third party, meaning that any confidential information you transmit may be less private than you expected.

One method that third parties might use to access this data is with a *packet sniffer*. A packet sniffer is a tool that intercepts the traffic passed across a network. They are also known as *network analyzers* and *Ethernet sniffers*, and can be either software or hardware that captures the packets of data so they can be analyzed. It is a tool that can be used to identify network problems, but it is also used to eavesdrop on network users, and view the data sent to and from a specific source. This allows someone to grab the data you're sending, decode it, and view what you've sent and received.

To avoid this problem, sensitive communications should always be encrypted. When data is encrypted, the data becomes unreadable to anyone who isn't intended to receive it. If a person accessed encrypted packets of data with a packet sniffer, it would be seen as gibberish and completely unusable to them. It makes the transmission secure, preventing the wrong people from viewing what you've sent.

Other Protocols Used by SIP

As mentioned, SIP does not provide the functionality required for sending single-media or multimedia across a network, or many of the services that are found in communications programs. Instead, it is a component that works with other protocols to transport data, control streaming media, and access various services like caller-ID or connecting to the Public Switched Telephone Network (PSTN). These protocols include:

- Session Description Protocol, which sends information to effectively transmit data
- Real-time Transport Protocol, which is used to transport data
- Media Gateway Control Protocol, which is used to connect to the PSTN
- Real-time Streaming Protocol, which controls the delivery of streaming media

The Session Description Protocol (SDP) and Real-time Transport Protocol (RTP) are protocols that commonly are used by SIP during a session. SDP is required to send information needed during a session where multimedia is exchanged between user agents, and RTP is to transport this data. The Media Gateway Control Protocol (MGCP) and Real-time Streaming Protocol (RTSP) commonly are used by systems that support SIP, and are discussed later for that reason.

Session Description Protocol

The Session Description Protocol (SDP) is used to send description information that is necessary when sending multimedia data across the network. During the initiation of a session, SDP provides information on what multimedia a user agent is requesting to be used, and other information that is necessary in setting up the transfer of this data.

SDP is a text-based protocol that provides information in messages that are sent in UDP packets. The text information sent in these packets is the session description, and contains such information as:

- The name and purpose of the session
- The time that the session is active
- A description of the media exchanged during the session
- Connection information (such as addresses, phone number, etc.) required to receive media

NOTE

SDP is a standard that was designed by the IETF under RFC 2327.

Real-Time Transport Protocol

The Real-time Transport Protocol (RTP) is used to transport real-time data across a network. It manages the transmission of multimedia over an IP network, such as when it is used for audio communication or videoconferencing with SIP. Information in the header of the packets sent over RTP tells the receiving user agent how the data should be reconstructed and also provides information on the codec bit streams.

Although RTP runs on top of UDP, which doesn't ensure reliability of data, RTP does provide some reliability in the data sent between user agents. The protocol uses the Real-time Control Protocol to monitor the delivery of data that's sent between participants. This allows the user agent receiving the data to detect if there is packet loss, and allows it to compensate for any delays that might occur as data is transported across the network.

NOTE

RTP was designed by the IETF Audio-Video Transport Working Group, and originally was specified as a standard under RFC 1889. Since then, this RFC has become obsolete, but RTP remains a standard and is defined under RFC 3550. In RFC 2509, Compressed Real-time Transport Protocol (CRTP) was specified as a standard, allowing the data sent between participants to be compressed, so that the size was smaller and

data could be transferred quicker. However, since CRTP doesn't function well in situations without reliable, fast connections, RTP is still commonly used for communications like VoIP applications.

Media Gateway Control Protocol

The Media Gateway Control Protocol (MGCP) is used to control gateways that provide access to the Public Switched Telephone Network (PSTN), and vice versa. In doing so, this protocol provides a method for communication on a network to go out onto a normal telephone system, and for communications from the PSTN to reach computers and other devices on IP networks. A media gateway is used to convert the data from a format that's used on PSTN to one that's used by IP networks that use packets to transport data; MGCP is used to set up, manage, and tear down the calls between these endpoints.

NOTE

MGCP was defined in RFC 2705 as an Internet standard by the IETF. However, the Media Gateway Control Protocol is also known as H.248 and Megaco. The IETF defined Megaco as a standard in RFC 3015, and the Telecommunication Standardization Sector of the International Telecommunications Union endorsed the standard as Recommendation H.248.

Real-Time Streaming Protocol

The Real-Time Streaming Protocol (RTSP) is used to control the delivery of streaming media across the network. RTSP provides the ability to control streaming media much as you would control video running on a VCR or DVD player. Through this protocol, an application can issue commands to play, pause, or perform other actions that effect the playing of media being transferred to the application.

NOTE

IETF defined RTSP as a standard in RFC 2326, allowing clients to control streaming media sent to them over protocols like RTP.

Understanding SIP's Architecture

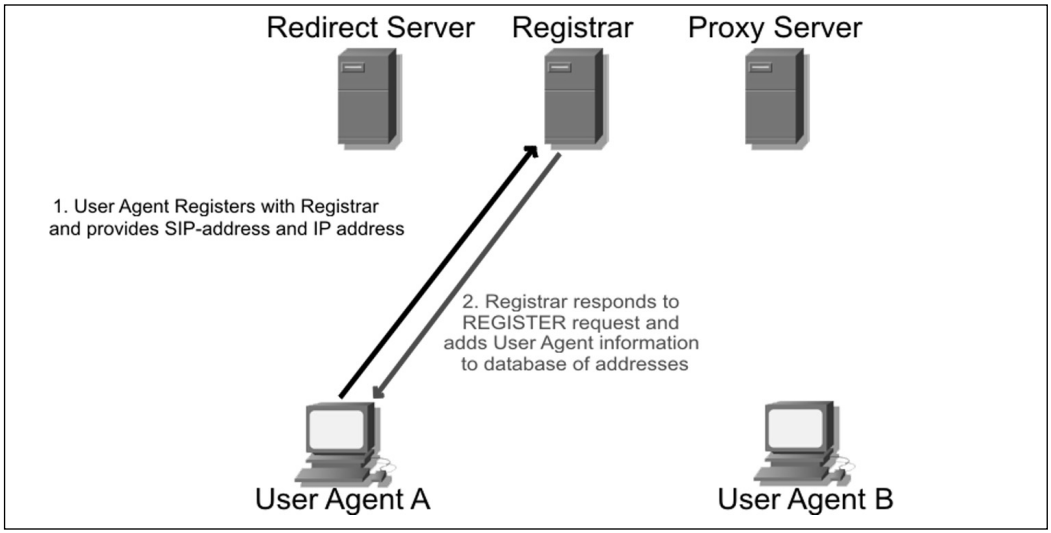
Now that we've looked at the various components that allow SIP to function on an IP network, let's look at how they work together to provide communication between two endpoints on a system. In doing so, we can see how the various elements come together to allow single and multimedia to be exchanged over a local network or the Internet.

The User agents begin by communicating with various servers to find other User agents to exchange data with. Until they can establish a session with one another, they must work in a client/server architecture, and make requests of servers and wait for these requests to be serviced. Once a session is established between the User agents, the architecture changes. Because a User agent can act as either a client or a server in a session with another User agent, these components are part of what is called a peer-to-peer (P2P) architecture. In this architecture, the computers are equal to one another, and both make and service requests made by other machines. To understand how this occurs, let's look at several actions that a User agent may make to establish such a session with another machine.

SIP Registration

Before a User agent can even make a request to start communication with another client, each participant must register with a Registrar server. As seen in Figure 8.2, the User agent sends a REGISTER request to the SIP server in the Registrar role. Once the request is accepted, the Registrar adds the SIP-address and IP address that the User agent provides to the location service. The location service can then use this information to provide SIP-address to IP-address mappings for name resolution.

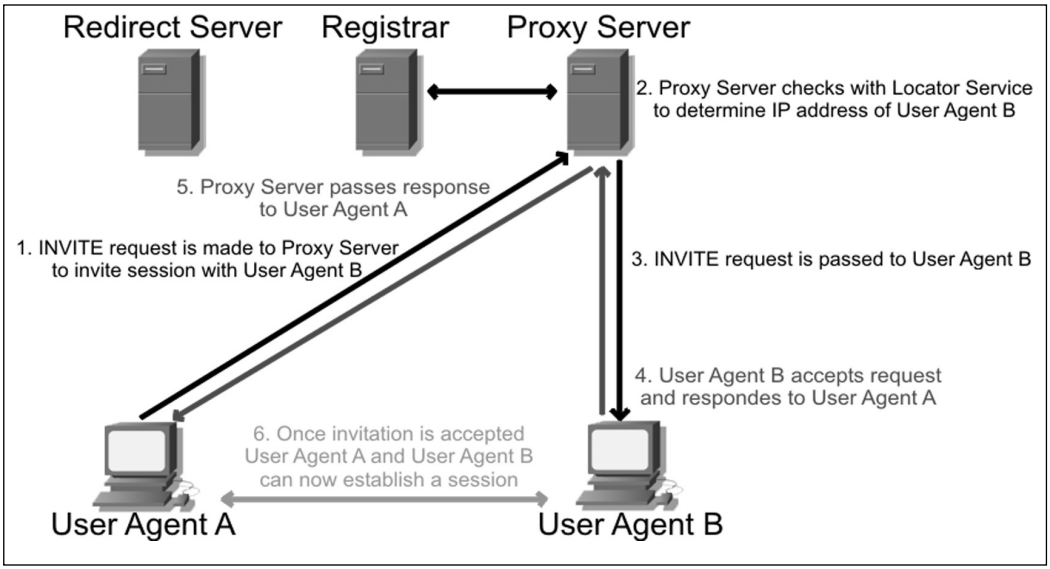
Figure 8.2 Registering with a SIP Registrar



Requests through Proxy Servers

When a Proxy Server is used, requests and responses from user agents initially are made through the Proxy server. As seen in Figure 8.3, User Agent A is attempting to invite User Agent B into a session. User Agent A begins by sending an INVITE request to User Agent B through a Proxy server, which checks with the location service to determine the IP address of the client being invited. The Proxy server then passes this request to User Agent B, who answers the request by sending its response back to the Proxy server, who in turn passes this response back to User Agent A. During this time, the two User agents and the Proxy server exchange these requests and responses using SDP. However, once these steps have been completed and the Proxy server sends acknowledgements to both clients, a session can be created between the two User agents. At this point, the two User agents can use RTP to transfer media between them and communicate directly.

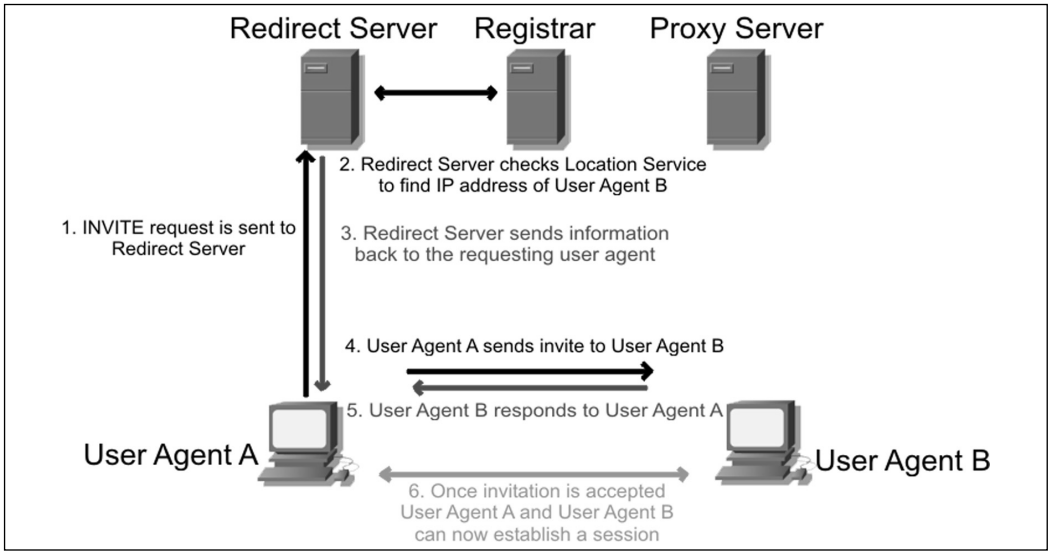
Figure 8.3 Request and Response Made through Proxy Server



Requests through Redirect Servers

When a Redirect server is used, a request is made to the Redirect server, which returns the IP address of the User agent being contacted. As seen in Figure 8.4, User Agent A sends an INVITE request for User Agent B to the Redirect server, which checks the location service for the IP address of the client being invited. The Redirect server then returns this information to User Agent A. Now that User Agent A has this information, it can now contact User Agent B directly. The INVITE request is now sent to User Agent B, which responds directly to User Agent A. Until this point, SDP is used to exchange information. If the invitation is accepted, then the two User agents would begin communicating and exchanging media using RTP.

Figure 8.4 Request Made through Redirect Server



Peer to Peer

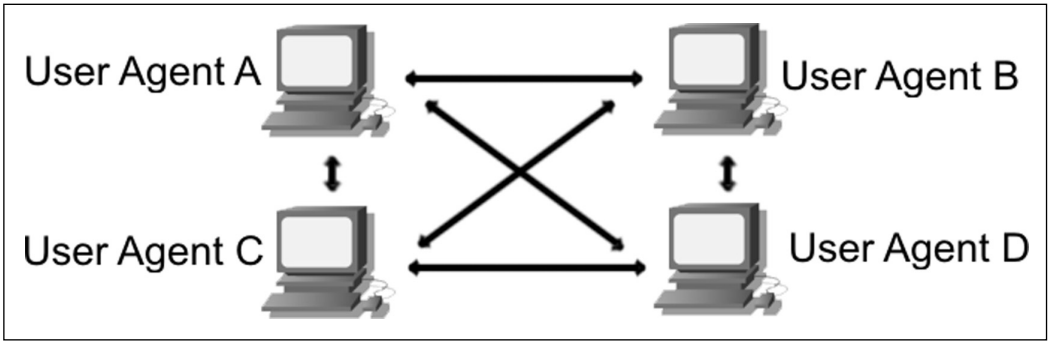
Once the user agents have completed registering themselves, and making requests and receiving responses on the location of the user agent they wish to contact, the architecture changes from one of client/server to that of peer-to-peer (P2P). In a P2P architecture, user agents act as both clients who request resources, and servers that respond to those requests and provide resources. Because resources aren't located on a single machine or a small group of machines acting as network servers, this type of network is also referred to as being *decentralized*.

When a network is decentralized P2P, it doesn't rely on costly servers to provide resources. Each computer in the network is used to provide resources, meaning that if one becomes unavailable, the ability to access files or send messages to others in the network is unaffected. For example, if one person's computer at an advertising firm crashed, you could use SIP to communicate with another person at that company, and talk to them and have files transferred to you. If one computer goes down, there are always others that can be accessed and the network remains stable.

In the same way, when user agents have initiated a session with one another, they become User agent clients and User agent servers to one

another, and have the ability to invite additional participants into the session. As seen in Figure 8.5, each of these User agents can communicate with one another in an audio or videoconference. If one of these participants ends the session, or is using a device that fails during the communication, the other participants can continue as if nothing happened. This architecture makes communication between User agents stable, without having to worry about the network failing if one computer or device suddenly becomes unavailable.

Figure 8.5 Once SIP Has Initiated a Session, a Peer-to-Peer Architecture Is Used



Instant Messaging and SIMPLE

Instant messaging (IM) has long been one of the most common and popular methods of communicating over IP networks. Whereas VoIP uses voice communication and videoconferencing uses live images and sound, IM simply uses text messages to allow participants to converse. These text messages are sent in real-time between the users who use the same IM application, and allows an individual to essentially create a private chat room with another individual where they can send text messages to one another. Many applications will even provide the ability to add additional participants to the chat, creating a text-based conference room of multiple users.

To manage the messages and identify whether specific users are online, an extension of SIP for Instant messaging has been developed. SIMPLE is an acronym that stands for the *Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions*. Although the name is ironically less than simple to remember, it is being developed as an open standard for how individuals

can determine the status of a person (i.e., whether they are online, busy, etc.), and for managing the messages that go back and forth between the participants in a chat.

Instant Messaging

In different variations, Instant messaging has been around longer than the Internet has been popular. In the 1970s, the TALK command was implemented on UNIX machines, which invoked a split screen that allowed users of the system to see the messages they typed in individual screens. In the 1980s, Bulletin Board Systems (BBSs) became popular, where people would use a modem to dial into another person's computer to access various resources, such as message boards, games, and file downloads. On BBSs, the system operator (SYSOP) could invoke a chat feature that allowed the SYSOP to send messages back and forth with the caller on a similar split-screen. If the BBS had multiple phone lines, then the callers could Instant message with each other while they were online. As the Internet gained popularity, the ability to exchange messages with other users became a feature that was desired and expected.

Today there are a large number of IM applications that can be used to exchange text messages over the Internet and other IP networks. Although this is nowhere near a complete list, some of the more popular ones include:

- AIM, America Online Instant Messenger
- ICQ
- Yahoo Messenger
- MSN Messenger

In addition to these, there are also applications that allow communication using VoIP or other multimedia that also provide the ability to communicate using text messages. As seen in Figure 8.6, Skype provides a chat feature that allows two or more users to communicate in a private chat room. Each message between the participants appears on a different line, indicating who submitted which line of text and optionally the time that each message was sent. This allows participants to scroll back in the conversation to identify previously mentioned statements or topics of discussion. Although the figure

depicts Instant messaging in Skype, it is a common format that is used in modern IM software.

Figure 8.6 Instant Messaging through Skype

One of the important features of any IM application is the ability to keep a contact list of those with whom you routinely communicate. In many programs the contact list is also known as a *Buddy List*. However, even with this listing, it would be impossible to contact anyone if you didn't know when each contact was available. If a person had a high-speed connection and was always connected to the Internet, then they might always appear online. As such, they would need a way of indicating that they were online but not available, or whether the person was available for one form of communication but not another. The ability to display each contact's availability in a Buddy List when someone opens an IM application is called *presence*.

SIMPLE

SIMPLE is an extension of SIP, which is used for maintaining presence information and managing the messages that are exchanged between the participants using Instant messaging. Just as SIP registers users with a SIP server

before they can begin a session, SIMPLE registers presence information. When a user registers through SIMPLE, those with this user in their Buddy List can access information that the user is online. When the people who have the user in their lists are alerted that the user is online, they can initiate a chat. If the user needs to do some work and changes their status to busy, or goes away from their desk and changes their status to being away, then this information is updated in the IM applications that have this person as a contact. Generally, the presence of a user is indicated in these programs through icons that change based on the user's status.

Because SIMPLE is an extension of SIP, it has the same features and methods of routing messages. The users are registered, and then send text-based requests to initiate a session. The messages are sent between user agents as individual requests between User agent clients and User agent servers. Because the messages are small, they can move between the two User agents quickly with minimal time lag even during peak Internet hours.

Although the IETF IM and Presence Protocol Working Group are still developing SIMPLE as a standard, it has been implemented by a number of IM applications. Windows XP was the first operating system to include SIMPLE, and is used by Microsoft Windows Messenger, and numerous other IM applications also are using SIMPLE as a standardized method for Instant messaging.

Are You 0wned?

Compromising Security with Instant Messaging

Instant messaging has become a tool that not only is used by the public for pleasure, but also one that is used by companies for business. IM software can be used as an alternative method of communicating with salespeople, customers, suppliers, and others who need to be contacted quickly. Because it is an effective communication tool, businesses have found benefits implementing it as part of their communications systems.

Unfortunately, a drawback of IM applications is that it provides a potential gap in security. Although companies will monitor outgoing

Continued

e-mail for illegal or inappropriate content, IM applications available to the public don't provide a centralized method of logging conversations that can be locked down. IM applications routinely offer a method of logging conversations, but these settings can be toggled on and off by the person using the program. This means that someone could inadvertently or maliciously provide sensitive information in Instant messages without anyone at the company every realizing it.

Added to this problem is the fact that IM applications provide the ability to transfer other forms of media between participants. IM applications can be used for file sharing, where one person sends a file to another through the program. This can result in activities like sharing music files at work, which albeit illegal is relatively harmless, but it could also cause major issues if sensitive corporate files were being sent. Imagine an employee at a hospital or doctor's office sending patient files, or a disgruntled employee sending out a secret formula to the public or competition, and its impact becomes more apparent.

Because files may contain more than you bargained for, the possibility of spyware or viruses being disseminated through Instant messaging must also be considered. Some applications that have supported Instant messaging include additional software that is spyware, which can obtain information about your system or track activities on your system. Even if the IM software used on a machine doesn't include spyware, the files sent between participants of a communication session can contain viruses or other malicious code. By opening these files, the person puts their computer and possibly their local network at risk.

If a company wishes to allow IM software installed on their machines, and doesn't want to block IM communications to the Internet, they need to educate users and install additional software on the computers. Just as employees should know what information should not be discussed on a telephone or sent by mail, they should know these same facts, and files should be off-limits in other communications. In addition to this, anti-virus software should be installed, and regularly updated and run. To determine if spyware is installed on the machines, they should either invest in anti-virus software that also looks for these programs or install additional software that searches for and removes them from the computer. In performing these steps, the risks associated with IM applications in a business can be decreased, making it safer for both the user and the company.

Summary

SIP works in conjunction with a variety of other protocols and specialized servers to provide communication between participants. Through SIP, a User agent is able to find the location and availability of other users, the capabilities of the software or device they're using, and then provides the functions necessary to set up, manage, and tear down sessions between participants. This allows participants to communicate directly with one another, so that data can be exchanged effectively and (if necessary) securely.

SIP is a standard of the Internet Engineering Task Force (IETF) under RFC 3261, and maps to the application layer of the OSI reference model. Because it isn't a proprietary technology, implementations of it can be used on any platform or device, and can be used on any IP network. In addition to this, SIP also makes use of other standards, such as URIs, which are used to identify the accounts used in SIP.

SIP's architecture is made up of a number of different protocols and components that allow it to function. Its architecture begins as a client/server architecture, in which requests are made to SIP servers. As the servers service these requests, they allow the participants to eventually communicate directly with one another, changing the architecture to a distributed peer-to-peer. As information is passed between these machines, a variety of different protocols are used, allowing data to be passed quickly between the computers, and securely if needed.

Instant messaging is another technology where SIP is being used. An extension of SIP called SIMPLE is used to maintain presence information and manage messages that are exchanged between the participants. Because SIMPLE provides the same features as SIP and is also an open standard, it is being used increasingly in IM software, making SIP and SIMPLE a staple in communications on IP networks.

Solutions Fast Track

Understanding SIP

- ☑ The Session Initiation Protocol is a signaling, application-layer protocol that is used to initiate interactive sessions on an IP network. Its purpose is to establish, maintain, and terminate sessions between two or more endpoints.
- ☑ SIP is a standard that was developed by the Internet Engineering Task Force (IETF). RFC 3261 is the finalized document that makes SIP a standard.
- ☑ SIP maps to the application layer of the OSI reference model. It is accessed by programs, to which it exports information. To make requests and access additional services, SIP uses other lower-layer protocols.

SIP Functions and Features

- ☑ SIP is used to determine location, availability, and capabilities of a user, and is used to set up and manage sessions.
- ☑ SIP's addressing system uses hierarchical URIs that are similar to e-mail addresses.
- ☑ SIP URIs generally begin with SIP:, but if secure transmission using the Transport Layer Security (TLS) protocol is required, then the URI will begin with SIPS:.

SIP Architecture

- ☑ A User agent can act in the role of a User agent client that makes requests (such as initiating a session) or a User agent server that services requests.
- ☑ A client/server architecture is used when the User agent communicates with various servers that may be used when

establishing a session. In this architecture, the client makes requests from dedicated servers that provide specific services on the network. Such servers include Registrar servers, Proxy servers, and Redirect servers.

- ☑ A peer-to-peer (P2P) architecture is used when the User agents establish a session. In this architecture, the computers act as equals, and make and respond to each other's requests. In doing so, their roles change from that of User agent client to User agent server.
- ☑ Registrar servers are used to register the location of a User agent who has logged onto the network.
- ☑ Proxy servers are computers that are used to forward requests on behalf of other computers. They can also provide such functions as network access control, security, authentication, and authorization.
- ☑ The Redirect servers are used by SIP to redirect clients to the User agent they are attempting to contact. They also have the ability to fork a call by splitting it to several locations.
- ☑ User Datagram Protocol (UDP) is used to transport units of data over an IP network. It is more lightweight than TCP, requiring less processing of data and allowing data to be transported quickly.
- ☑ Real-time Streaming Protocol (RTSP) controls the delivery of streaming media across the network.
- ☑ Media Gateway Control Protocol (MGCP) controls gateways that provide access to the Public Switched Telephone Network.
- ☑ Real-time Transport Protocol (RTP) transports real-time data across a network.
- ☑ Session Description Protocol (SDP) sends description information that is necessary when sending multimedia data across the network.

Instant Messaging and SIMPLE

- ☑ SIMPLE is short for *Session Initiation Protocol for Instant Messaging and Presence* Leveraging *Extensions*. It is an extension of SIP, and used to

determine the presence of individuals on an IP network and manage messages exchanged between participants.

- ☑ Instant messaging (IM) is used to communicate using text messages in a private chat room environment. IM applications can also be used to transfer files, video, and other media and data between participants.
- ☑ Presence technology is used to display the availability of contacts in a Buddy List.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I am used to seeing users that follow the scheme *SIP: username@domain.com*, but I've also seen them with the scheme *SIPS: username@domain.com*. What's the difference?

A: SIP uses Universal Resource Identifiers (URIs) for identifying users. A URI identifies resources on the Internet, and those used by SIP incorporate phone numbers or names in the username. At the beginning of this is SIP:, which indicates the protocol being used. This is similar to Web site addresses, which begin with HTTP: to indicate the protocol to use when accessing the site. When SIP: is at the beginning of the address, the transmission is not encrypted. Those beginning with SIPS: require encryption for the session.

Q: Why do all responses to a request in SIP begin with the numbers 1 through 6?

A: This indicates the category to which the response belongs. There are six categories of responses that may be returned from a request: Informational, Success, Redirection, Client Error, Server Error, and Global Failure.

Q: I received a response that my request was met with a server error. Does this mean I can't use this feature of my VoIP program?

A: Not necessarily. When a request receives a Server Error response, it means that the server it was sent to met with the error. The request could still be forwarded to other servers. A Global Error meanns that it wouldn't be forwarded because every other server would also have the same error.

Q: I need to use a different computer for VoIP. The software is the same as the one on my computer, but I'm concerned that others won't be able to see that I'm online because I'm using a different machine.

A: When you start the program and log onto your VoIP account, SIP makes a REGISTER request that provides your SIP address and IP address to a Registrar server. This allows multiple people to use multiple computers. No matter what your location, SIP allows others to find you with this mapping of your SIP-address to the current IP address.

Q: Should I always use encryption to protect the data that I'm transmitting over the Internet?

A: Unless you expect to be discussing information or transferring files that require privacy, it shouldn't matter whether your transmission is encrypted or not. After all, if someone did eavesdrop on an average conversation, would you really care that they heard your opinion on the last movie you watched? If, however, you were concerned that the content of your conversation or other data that was transmitted might be viewed by a third party, then encryption would be a viable solution to protecting your interests. As of this writing however, there are no interoperable, nonproprietary implementations of SIP that use encrypted signaling and media, so you will need to refer to the documentation of the application(s) being used to determine if this is available.

Appendix A

Regulatory Compliance

Solutions in this appendix:

- **SOX: Sarbanes-Oxley Act**
- **GLBA: Gramm-Leach-Bliley Act**
- **HIPAA: Health Insurance Portability and Accountability Act**
- **CALEA: Communications Assistance for Law Enforcement Act**
- **E911: Enhanced 911 and Related Regulations**
- **EU and EU Member States' eCommunications Regulations**

☑ **Summary**

☑ **Solutions Fast Track**

☑ **Frequently Asked Questions**

Introduction

The past decade has seen an explosion of government regulation that will directly or indirectly affect VoIP implementation security. Some of these regulations can be addressed by selecting and implementing compliant equipment, but the vast majority of these are *operational* in nature, meaning that to ensure compliance you'll need to pay more attention to (1) how your IP communications systems are designed and (2) how your organization's business and IT operations groups are using the equipment once it's live.

For this appendix, each applicable set of regulations will be discussed separately. What you'll want to ask yourself in each section is:

- Does this regulation apply to me and my organization (or my client's organization)?
- Who in my organization has responsibility for overall compliance with this regulation? In some cases, the answer may be you if there isn't already someone designated, but for many of these regulations your organization is likely to have a person or group specifically designated as the lead for addressing compliance, particularly with regulations for which security is only an ancillary component of the overall regulation.
- Is it likely that my systems and/or operations are not compliant with this regulation today? If you suspect that remediation is necessary, it's important to raise the concern to the appropriate level of management in a way that allows the issue to be corrected and reduce the risk of fines, negative publicity, or worse.

WARNING

Always consult experienced legal counsel (or your organization's audit or compliance department) for legal advice with regulatory issues that could materially affect your organization. Although this appendix highlights the most common regulatory concerns surrounding VoIP, it cannot provide complete guidance for every situation or jurisdiction. For instance, VoIP itself is considered illegal in certain countries when it

bypasses national carriers (sometimes known as PTTs) who may have a telecommunications monopoly. And new data privacy laws around the world seem to appear monthly.

NOTE

Despite the aforementioned caveat, you may find that the compliance experts available to you are not familiar with VoIP and how to apply broad regulations like GLBA or HIPAA to voice and other real-time communications systems. To help with these situations, pay special attention to the "Tools & Traps" sidebars in this appendix. They will provide specific guidance for you to share with a specialized compliance expert in that area of regulation.

Don't be surprised, however, if your expert chooses to ignore the additional information. Many experts prefer to apply these regulations narrowly and don't want to open the door to unanticipated compliance costs (common concern for internal experts) or expand the scope of compliance work without having the billable expertise to address it (typical for external experts). If that happens to you, just make sure to complete your due diligence by advising your organization's responsible executive (corporate counsel or chief compliance office) of your concerns in writing and leaving the matter in their hands.

In the next six sections, we'll review regulations that may affect you or your organization. You may safely skip some of them, so here's a quick way to tell which sections won't apply to you and your organization:

- If your organization is not public (listed on any U.S. stock exchange), then you can skip SOX.
- If your organization isn't involved with banking, consumer finance, securities, or insurance, then you can skip GLBA.
- If your organization doesn't handle any medical records (don't forget your HR department and any health insurance-related records when considering this question), you can skip HIPAA.

- If you're not a telecommunications carrier (or effectively replace one, like a university does for on-campus students, for example), then you can skip CALEA.
- If you don't have any physical locations in the United States or provide phone service there, you can skip E911.
- If you don't operate equipment within the United States, then you can sip the FCC section.
- If you don't have any customers, suppliers, or operations in an EU country, then you can skip the EU section, though if you operate in a state or country with data privacy regulations then this section might still be relevant.

SOX: Sarbanes-Oxley Act

Enacted in response to corporate scandals at Enron, Tyco, and Worldcom during 2001, the Sarbanes-Oxley Act of 2002 was designed to bolster confidence in the financial reporting of publicly traded corporations in the United States. When he signed the Act into law, President Bush hailed it as "the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt." Since that time, an estimated $5 billion has been spent by U.S.-listed corporations to comply with the act.

SOX Regulatory Basics

Let's take a few minutes to go through the Sarbanes-Oxley Act and what it requires, starting with what the regulations themselves explicitly require. Then we'll look at related recommendations that SOX consultants and auditors are likely to recommend above and beyond the explicit legal requirements.

Direct from the Regulations

When it comes to VoIP or any other IP application, Section 404 is the only part of SOX that even remotely applies. Section 404 isn't long but since it's been the basis for hundreds (perhaps thousands) of costly IT reporting and process changes ultimately attributed to Sarbanes-Oxley over the past few

years, I'm going to reproduce it in its entirety—but first here's the simple version:

- 404(a) requires an annual report from management regarding the effectiveness of internal controls.
- 404(b) requires an independent auditor to report on (and attest to) management's annual report.

So we're really just talking about two reports here: one that's signed by the officers of a company, and another that's signed by their independent auditor (typically from a large accounting and consulting firm). However, since a negative report could have huge consequences in the stock market, being able to produce an acceptable report supported by your auditor is a big deal

Here's the actual text of Section 404 of the Sarbanes-Oxley Act of 2002:

Section 404 Management Assessment Of Internal Controls

(a) RULES REQUIRED- The Commission shall prescribe rules requiring each annual report required by section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING- With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engage-

> ments issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

Now, if you've been part of an internal "SOX audit" you may be saying to yourself, "So where does it say I need to have complex passwords and encrypted links and quarterly user reviews and vulnerability testing and so forth?" And that's an excellent question because, of course, it doesn't say that at all. In fact, even the new internal controls audit standard ("Auditing Standard No. 2" or AS2) created by the Public Company Accounting Oversight Board (an organization created by the Act) addresses information technology only in terms of internal controls.

However, since Section 404 clearly states that the independent auditor must validate management's internal controls report, this gives management a strong incentive to defer to the auditor. As many large public companies found out in 2004 and 2005, a "disclaimer opinion" from an auditor suggesting that a company's internal controls are inadequate tends to push down its stock price. Thus, the security best-practices advice given by an auditor or SOX consultant is very likely to be driven down through an organization as if the law itself required it when that's not strictly true.

Nevertheless, since Section 404 speaks in terms of "internal controls," it only makes sense to ask what an internal control really is. The commonly accepted definition comes from the Committee of Sponsoring Organizations of the Treadway Commission (COSO):

> Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations.
> - Reliability of financial reporting.
> - Compliance with applicable laws and regulations.

What's most important to note about this definition is that it's *not* made in terms of technology (although organizations routinely use information technology as a *part* of the implementation of many internal controls). It's

not just a report, or a policy, or a line of code by itself; rather it's an entire operational process. Given that definition, it's easy to see that SOX really doesn't care if you're using VoIP or telepathy for your business communications so long as any associated internal controls (such as those for billing) are adequate. The critical standard to be met in designing a control is "reasonable assurance"—not absolute assurance. According to COSO, adequate controls should provide visibility and focus but cannot be expected to take the place of effective management:

> The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs.

In other words, design with the assumption that management can make appropriate executive decisions given the necessary background and context. If your control provides that level of input to decision-makers, it is adequate.

What a SOX Consultant Will Tell You

External auditors and other SOX consultants hired by your company have many incentives to provide broad, conservative guidance regarding SOX best practices. Why? First, given Arthur Anderson's collapse in the wake of the Enron debacle, one lesson learned by the large audit firms was the importance of giving conservative guidance even if management might take issue with the cost/benefit ratio. Keep in mind, however, that your company's independent auditor is prevented by SOX from offering nonaudit (consulting) services, so these recommendations may force another consulting firm to join the process.

For these additional consultants, comprehensive recommendations on their part tend to increase the length and scope of their billable engagements. And they don't have to worry about jeopardizing a long-term audit relationship

through a failed project. So with your management more concerned about passing the next SOX audit than the business value being derived from SOX-related work, a SOX consultant is much more likely to recommend embarking on a comprehensive security strategy in the name of SOX compliance. And the independent auditor has no good reason to suggest to management that the extra work is unnecessary, as that could only increase their liability in the post-Enron world.

If you're involved with security, that dynamic is a double-edged sword. On the plus side, some security best practices that you may have unsuccessfully lobbied for in the past are suddenly now the new law of the land in your company, with the full support of your CIO and CFO arriving in the name of SOX compliance. On the other hand, all sense of perspective when it comes to risk management seems to have been lost in the process. Millions of dollars are spent to implement solutions like enterprise role definition (ERD), single sign-on (SSO), and identity and access management (IAM). At the same time, labor-intensive tasks like a quarterly user review that cannot be outsourced to consultants are taking large chunks of time from the operational resources that you need in order to address risks not tied to SOX at all. And good security practices not tied to SOX may fall off the management's radar screen entirely.

So what specific recommendations are you likely to get from a SOX consultant for a VOIP system? Primarily, these are security best practices you may already be familiar with. Here's what you might expect in a thorough SOX examination of a VoIP system that is deemed to have internal financial controls (because of external billing or internal chargebacks, for example):

- **Logging and audit trails** Does your VoIP system log administrative changes and provide basic usage logs (in this case, Call Detail Records (CDRs) or something equivalent)? If a billing process requires those logs then what is protecting them? More broadly, are the associated internal controls around that billing system adequate? Are lists of authorized administrators and users reviewed for accuracy on a periodic basis (at least annually)?
- **Password complexity** Does your organization enforce consistent requirements for password complexity across applications, including

the VoIP system? For example, a password must be at least eight characters with at least one uppercase letter and one non-alpha character. Also, are default administrative passwords changed to comply (or default users removed)?

- **Password expiration** Does your organization enforce consistent expiration timeframes (example: 90 day expiration, 10 day warning) for passwords across all applications, including the VoIP system? Also, are accounts with expired passwords removed after a set timeframe?
- **Database user management** Do associated databases enforce password complexity and expiration rules? Are default database users removed or assigned new passwords that comply?
- **Server (and database) vulnerability management** Do associated servers/databases receive regular vulnerability scans, virus scans with regular updates, and security patches as part of a vulnerability and patch management system?
- **Server hardening** Are unnecessary services, packages, and tools removed from the VoIP system? Are all VoIP processes running as a nonprivileged user?
- **Encrypted IP communications** Do all administrative and operational links prevent user data, passwords, and any other sensitive information from being seen in the clear? This means that Telnet and ftp have been replace with their TLS-based equivalents (like ssh, sftp), external database connectivity runs over TLS, and (on a VoIP system) that signaling and media encryption are used.
- **Role-Based Access Control (RBAC)** Do you have a fine-grained authorization scheme that allows you to grant access to each administrative and functional capability independently? For VoIP systems, that means that there are separately granted administrative permissions for each major area of configuration (such as networking, PSTN integration, user administration, etc.) and user-level permissions for different classes of features, calling restrictions, and so on.

- **Segregation of Duties (SoD)** Have you separated administrative, operational, and audit roles within your VoIP system so that, for instance, an auditor can gain access to system logs without having the ability to change settings? To properly implement SoD, you will need to support RBAC.
- **Identity and Access Management (IAM) with Provisioning** Have you tied the VoIP system's user and administrative identities back to enterprisewide directories and authentication schemes? In other words, do users and administrators accessing the VoIP system use the same IDs and passwords on the VoIP system as they would on other enterprise applications? Do directory attributes like groups enable automatic assignment of roles in the VoIP system's RBAC scheme? Does VoIP system deprovisioning (or disablement) happen automatically for a user that has been removed from the enterprisewide directory upon termination? Optional: Are new employees able to be provisioned automatically to the VoIP system as part of the on-boarding process?
- **Enterprise Role Definition (ERD)** Has your organization identified across its business applications the employee roles and access required by those roles to be able to map the VoIP system's roles into that enterprise scheme? Have those roles been screened for Segregation of Duties conflicts with the VoIP system included? Note that RBAC and IAM with Provisioning typically are required for an ERD system to work smoothly in practice.

Tools & Traps…

Core SOX Compliance Issues for IP Communications Systems

The only direct SOX impacts to VoIP and other communications systems are likely to be billing related if your VoIP system is part of a service billed to others or if your SOX controls team considers it to be part of an internal control around PSTN usage costs being billed back to your company. Of course, indirect impacts through IT security policies around user, password, logging, systems, and database management are all likely since the VoIP system is a part of the overall IT infrastructure of your organization.

The SOX issue most likely to be ignored by your SOX team: internal controls for controlling VoIP calls that route through the PSTN create financial obligations (i.e., long-distance charges) so long as your long distance isn't fixed-cost (or free), since abuse of IP communications systems could have a material financial impact on your organization. In SOX terms, that means that the same controls used with critical financial systems should be evaluated for applicability to IP communications systems as well.

SOX Compliance and Enforcement

It may surprise you to know that most of the Act itself is focused on new practices and penalties for independent auditors, not public companies. The Sarbanes-Oxley Act created the Public Company Accounting Oversight Board (PCAOB) to address the audit processes used for public companies. The Act gives the PCAOB the authority to register, investigate, and discipline public accounting firms and auditors. Oversight of the PCAOB falls to the Securities and Exchange Commission (SEC). Penalties for certain white-collar crime were increased and the SEC has some additional civil enforcement tools as part of the Act, but in general all nonaudit compliance and enforcement for SOX remains within the enforcement frameworks previously established at the SEC.

Certification

Compliance is evaluated on an annual basis by two groups: the management of the public company itself (typically through your internal audit or compliance group) for the management report asserting that internal controls are adequate (i.e., compliant with Sarbanes-Oxley requirements); and the company's independent auditor for their attestation—either unqualified support of management's report or a "disclaimer opinion" that raises concerns about the adequacy of internal controls. Just to complete the attestation process each year, large companies can be charged up to $1 million or more by their independent auditor—over and above the fees paid for basic corporate audit work. These costs (and potential conflicts the process can create with EU Data Protection directives) have prompted a number of European firms to de-list from American stock exchanges.

SOX has no notion of "product certification" like some of the other regulations in this appendix.

Enforcement Process and Penalties

Auditors and auditing organizations are investigated and sanctioned by the Public Company Accounting Oversight Board (PCAOB), and corporate officers and corporations are investigated and sanctioned by the SEC. For the PCAOB, the maximum penalty for "violations committed in the preparation and issuance of audit reports," was $110,000 in 2005 for an individual and $2.1 million for an entity. And the SEC maximum penalty in 2005 for "intentional or knowing conduct, including reckless conduct, or repeated instances of negligent conduct" was $800,000 for an individual and $15.825 million for an entity.

The Act itself increased the maximum penalty for mail, securities, and wire fraud to up to 25 years imprisonment, and established maximum penalties for CEOs and CFOs that made willful and knowing violations of financial statement and disclosure rules punishable by a fine of not more than $500,000 and/or imprisonment of up to five years. The latter garnered a lot of press at the time and resulted in increased attention to SOX by corporate chiefs.

Both the SEC and PCAOB have processes in place to accept both anonymous tips and formal complaints. For the SEC, tips can be sent to enforcement@sec.gov and online forms can be found at www.sec.gov. The PCAOB can accept tips at tips@pcaobus.org or online at www.pcaobus.org.

GLBA: Gramm-Leach-Bliley Act

The US Gramm-Leach-Bliley Act of 1999—commonly referred to as GLBA—is landmark legislation that completely reorganized the statutory and legislative framework in place since the 1930s for the banking and financial services market. Of particular note is Title V, Subtitle A, Section 501, which requires that banking, consumer finance, securities, and insurance companies develop and meet new standards for protection of consumer privacy and safeguarding of financial institution infrastructure. Although VoIP systems were not specifically called out in the Act itself, the Federal Deposit Insurance Corporation (FDIC) and other financial regulatory agencies subsequently have issued VoIP-specific guidance to be used by regulated entities.

GLBA Regulatory Basics

Because the regulatory scope of GLBA is extensive and we really are interested only in the privacy and security effects of the legislation (and specifically, how they interact with VoIP systems), we will limit our discussion to Title V–PRIVACY. For those in the security community, every security reference to GLBA that you've seen is tied back to Title V, and we will review its contents later in this appendix. In addition, we will discuss supplementary guidance from consultants and regulators (including the FDIC VoIP recommendation) to help you understand what your organization will need for your VoIP system to operate in compliance with GLBA.

Direct from the Regulations

Title V is broken out into two subtitles. Subtitle A, "Disclosure of Nonpublic Personal Information," is where we will center most of our attention, particularly in Section 501. Subtitle B, "Fraudulent Access to Financial Information" criminalizes the act of using false pretenses to obtain financial information from an institution except under certain law-enforcement and investigative

exclusions. We won't spend any more time with Subtitle B, but if you ever find yourself investigating someone's financial information you would be wise to familiarize yourself with its contents.

Of the 10 sections in subtitle A, I am only going to reproduce section 501 in its entirety, since it is the basis for all of the GLBA security recommendations I encounter. The other nine talk through privacy definitions, enforcement, and the creation of detailed regulations from the GLBA. In any case, Section 501 is what we want to be most familiar with, and it is fairly straightforward:

> **SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.**
>
> (a) PRIVACY OBLIGATION POLICY- It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
>
> (b) FINANCIAL INSTITUTIONS SAFEGUARDS- In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

From this point onward, I'll use the commonly accepted terminology for the rules created by this section. 501(a) and subsequent joint regulations are

collectively known as the *privacy rule* and 501(b) with its joint regulations is called the *safeguarding rule*. Later in this appendix, you'll notice that HIPAA regulations follow a similar model, except the latter is called "security" instead of "safeguarding." (That's the way I think about GLBA as well: privacy + security.)

After the GLBA was signed, the Secretary of the Treasury, the National Credit Union Administration (NCUA), the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC) were required to create appropriate regulations as part of Title V. The resulting documents can be found at the FTC at www.ftc.gov/os/2000/05/glb000512.pdf and the Office of the Comptroller of the Currency (OCC) at www.occ.treas.gov/ftp/release/0509fin.pdf. Detailed requirements for the privacy disclosures and opt-out procedures are spelled out in detail within these two documents (and if you're like me, you receive the annual privacy disclosures they require in droves from financial institutions). In general, there are no VoIP considerations within the privacy rule that aren't more directly addressed by the safeguarding rule, so we're going to spend the rest of this section on the safeguarding rule.

Detailed regulations for the safeguarding were finalized in 2001 as the "Interagency Guidelines Establishing Information Security Standards" (see www.fdic.gov/regulations/laws/rules/2000-8660.html or www.ots.treas.gov/docs/2/25231.pdf for a typical copy), and it is these rules that you will want to become most familiar with, in particular, part III:

> **III. Development and Implementation of Information Security Program**
>
> A. **Involve the Board of Directors**. The board of directors or an appropriate committee of the board of each bank holding company shall:
>
> 1. Approve the bank holding company's written information security program; and
>
> 2. Oversee the development, implementation, and maintenance of the bank holding company's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank holding company shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

C. Manage and Control Risk. Each bank holding company shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank holding company's activities. Each bank holding company must consider whether the following security measures are appropriate for the bank holding company and, if so, adopt those measures the bank holding company concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that customer information system modifications are consistent with the bank holding company's information security program;

e. Dual control procedures, segregation of duties, and

employee background checks for employees with responsibilities for or access or customer information;
{{4-29-05 p.6120.37}}

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

g. Response programs that specify actions to be taken when the bank holding company suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

2. Train staff to implement the bank holding company's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank holding company's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

D. Oversee Service Provider Arrangements. Each bank holding company shall:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

3. Where indicated by the bank holding company's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank holding company should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. Adjust the Program. Each bank holding company shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank holding company's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. Report to the Board. Each bank holding company shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank holding company's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. Implement the Standards.

1. Effective date. Each bank holding company must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. Two-year grandfathering of agreements with service providers. Until July 1, 2003, a contract that a bank holding company has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information, as long as the bank holding company entered into the contract on or before March 5, 2001.

These are the standards against which financial regulators will evaluate your organization if it falls under the GLBA. For VoIP systems, the primary concern will be to ensure that risk management and security processes for

compliance include the VoIP infrastructure and that your organization's security standards developed for GLBA compliance will be applied to your IP communications systems as well.

What a Financial Regulator or GLBA Consultant Will Tell You

Until July 2005, when the FDIC provided very specific and detailed VoIP guidance, it was not uncommon for GLBA experts to consider voice communications systems to be outside the scope of GLBA's safeguarding rule. In what's known as a Financial Institution Letter or FIL (in this case FIL-69-2005—see www.fdic.gov/news/news/financial/2005/fil6905.html for a complete copy); the FDIC made it clear that VoIP systems must be included in GLBA risk assessment reports and processes. In their highlights, the FDIC noted:

- VoIP is susceptible to the same security risks as data networks if security policies and configurations are inadequate.
- The risks associated with VoIP should be evaluated as part of a financial institution's periodic risk assessment, with status reports submitted to the board of directors as mandated by section 501(b) of the Gramm-Leach—Bliley Act (GLBA). Any identified weaknesses should be corrected during the normal course of business.

This effectively told regulators and institutions that they will be expected to include IP communications systems in their GLBA compliance planning and reporting going forward. The FDIC VoIP security recommendation follows:

> Financial institutions can access various publicly available sources to develop VoIP security policies and practices. Widely accepted best practices are published by the National Institute of Standards and Technology (NIST), the agency responsible for developing information security standards for federal agencies (Special NIST Publication 800-58, Security Considerations for Voice over IP Systems, can be found at http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf.

Financial institutions contemplating the use of VoIP technology should consider the following best practices. Details of these best practices are further discussed in the attached "Voice over Internet Protocol Informational Supplement."

- Ensure that the institution has examined and can acceptably manage and mitigate the risks to information, systems operations and continuity of essential operations when implementing VoIP systems.

- Assess the level of concern about security and privacy. If warranted and practical, do not use "softphone" systems, which implement VoIP using an ordinary PC with a headset and special software.

- Carefully review statutory requirements for privacy and record retention with competent legal advisors.

- Develop appropriate network architecture.

- Use VoIP-ready firewalls and other appropriate protection mechanisms. Financial institutions should enable, use and routinely test security features included in VoIP systems.

- Properly implement physical controls in a VoIP environment.

- Evaluate costs for additional backup systems that may be required to ensure continued operation during power outages.

- Consider the need to integrate mobile telephone units with the VoIP system. If the need exists, consider using products implementing WiFi Protected Access (WPA), rather than Wired Equivalent Privacy (WEP).

- Give special consideration to emergency service communications. Automatic location services are not always as

available with VoIP as they are with phone calls made through the PSTN.

When a financial institution decides to invest in VoIP technology, the associated risks should be evaluated as part of a financial institution's periodic risk assessment and discussed in status reports submitted to the board of directors as mandated by section 501(b) of the Gramm-Leach-Bliley Act. Any identified weaknesses should be corrected during the normal course of business.

The aforementioned FDIC VoIP Informational Supplement can be downloaded at www.fdic.gov/news/news/financial/2005/fil6905a.html if you'd like to get more detail on the points covered in the previous section of this appendix. Since it rehashes points covered in detail elsewhere in this book, I will leave this as an exercise for you, dear reader.

Tools & Traps…

Core GLBA-Compliance Issues for IP Communications Systems

Although GLBA does not have specific rules for VoIP, its integration with the rest of your organization's data network clearly puts it in scope of GLBA safeguarding provisions. This was reinforced by FDIC FIL-69-2005, which suggests nine specific GLBA risk management activities for VoIP systems:

- Include VoIP systems into general risk management and continuity planning
- Avoid softphone systems (where warranted and practical)
- Review privacy and records retention approach within VoIP system
- Review VoIP network architecture as part of overall network architecture
- Enable and test VoIP security features; use VoIP-ready firewalls

- Implement appropriate physical controls on VoIP systems
- Consider costs of additional backup systems required during power outages
- Avoid WEP on wireless VoIP; use WPA instead
- Consider E911 location service implications

In addition to the items highlighted by the FDIC, the same user, password, log, and database management policies used for data applications should also be applied to IP communications systems.

GLBA Compliance and Enforcement

Enforcement of Title V of the GLBA falls to 57 different regulators in three classes: federal functional regulators, state insurance authorities, and the Federal Trade Commission as follows:

- **State insurance authorities in each state** Insurance providers
- **Securities and Exchange Commission (SEC)** Brokers, dealers, investment advisors and investment companies
- **Office of the Comptroller of the Currency (OCC)** National banks
- **National Credit Union Administration (NCUA)** Federally insured credit unions
- **Board of Governors of the Federal Reserve System (FRB)** Member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (except federal branches, federal agencies, and insured state branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act, and bank holding companies and their nonbank subsidiaries or affiliates not subject to the SEC or state authorities
- **Board of Directors of the Federal Deposit Insurance Corporation (FDIC)** Banks insured by the FDIC (except Federal Reserve System members), insured state branches of foreign banks,

and their nonbank subsidiaries or affiliates not subject to the SEC or state authorities

- **Director of the Office of Thrift Supervision (OTC)** Savings associations insured by the FDIC and their nonbank subsidiaries or affiliates not subject to the SEC or state authorities
- **Federal Trade Commission (FTC)** All others

No Certification

GLBA has no concept of certification, either for institutions, individuals, or products.

Enforcement Process and Penalties

The FDIC, NCUA, OTS, OCC, and FRB use uniform principles, standards, and report forms created by the Federal Financial Institutions Examination Council (FFIEC). The FFEIC has gathered together a broad set of IT-related presentations, examination booklets, and other resources (www.ffiec.gov/ffiecinfobase/index.html) that provide an excellent guide to what their examiners will be looking for in an information security examination. For the banks and other financial institutions that fall under these agencies, GLBA enforcement is part of the overall enforcement regime that is standardized by the FFIEC.

Each of the 57 possible regulators has discretion over sanctions and penalties for privacy or safeguarding rule violations (for Subtitle B there are criminal penalties but these don't apply to the privacy or safeguarding rules, only to criminal access to financial data under fraudulent pretenses), so penalties may vary. Also, civil suits can be brought against financial institutions that violate the GLBA privacy rule.

HIPAA: Health Insurance Portability and Accountability Act

Within the U.S. Health Insurance Portability and Accountability Act of 1996, Congress adopted a broad range of reforms and standards designed to improve healthcare and health insurance and move toward electronic transaction pro-

cessing and recordkeeping. As part of the 1996 Act, Congress acknowledged the need for privacy standards, but it failed to produce them in time to meet its own deadline; that job fell to the Department of Health and Human Services (HHS), which issued the final rule for privacy in December 2000. The final security rule was issued by HHS in February 2003.

HIPAA Regulatory Basics

The privacy and security mandates that can affect VoIP systems are found in Title II, Subtitle F, Part C – Administrative Simplification. There are three aspects to Title II: Privacy, Code Sets, and Security. HHS has issued detailed regulations for all three, but the only two that can apply to VoIP systems are Privacy and Security.

Critical to understanding HIPAA is the concept of Protected Health Information (PHI) or Individually Identifiable Health Information (IIHI). Think of IIHI or PHI as any set of information that contains health-related data for an individual that can be traced back to that person. In order to share health-related information with other individuals or groups that participate in a patient's care, a Covered Entity (organization subject to HIPAA) must first receive the patient's consent to share that PHI with those participants (insurance, billing, physicians, hospitals, pharmacies, and so forth). Protection of PHI by a Covered Entity is the objective of the HIPAA Privacy Rule and Security Rule.

Direct from the Regulations

Privacy in HIPAA is addressed in Section 264 (of Title II, Subtitle F, Part C). The HHS Privacy Rule is based on this text in the Act:

> The recommendations under subsection (a) shall address at least the following: (1) The rights that an individual who is a subject of individually identifiable health information should have. (2) The procedures that should be established for the exercise of such rights. (3) The uses and disclosures of such information that should be authorized or required.

Three years and over 52,000 comments later, the first HHS Final Rule for Privacy was published, and after four more amendments (the last of which

was in April 2003) the "Standards for Privacy of Individually Identifiable Health Information" had reached its present form (for a copy of the combined Privacy and Security regulations along with enforcement and penalty information, go to www.hhs.gov/ocr/combinedregtext.pdf). In general, the Policy Rule applies more to an organization's procedures independent of technology, so it makes more sense to dig into HHS Security Rule, "Security Standards for the Protection of Electronic Protected Health Information," which is based on this text in Section 1173 of the Act:

> (1) SECURITY STANDARDS.—The Secretary shall adopt security standards that—
>
> (A) take into account—(i) the technical capabilities of record systems used to maintain health information; (ii) the costs of security measures; (iii) the need for training persons who have access to health information;(iv) the value of audit trails in computerized record systems; and (v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and
>
> (B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.
>
> (2) SAFEGUARDS.—Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—
>
> (A) to ensure the integrity and confidentiality of the information;

> (B) to protect against any reasonably anticipated—(i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and
>
> (C) otherwise to ensure compliance with this part by the officers and employees of such person.

Notice the way that security is broken out in the Act—this structure is carried forward into the HHS Security Rule (and believe me, without that knowledge it's hard to make sense of the Rule).

The Security Rule

Within the Security Rule, there are general requirements that outline what a covered entity is required to document for compliance overall. Specific requirements then follow in four main categories: Administrative, Physical, and Technical Safeguards, plus Organizational Requirements. Understanding the difference between the first three is crucial to following the Security Rule:

> **Administrative safeguards** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
>
> **Physical safeguards** are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
>
> **Technical safeguards** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

With this in mind, let's start with the general requirements and objectives for the security rule, and the flexibility allowed in implementing and documenting standards in each of the four categories:

(a) General requirements. Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach.

(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

This flexibility is key to making your compliance document less painful to write. When you find that a vendor's equipment or solution does not provide a technical solution to a given standard, you can usually assemble an adminis-

trative solution that provides an acceptable workaround. And for those items that are not required (marked as Addressable in the Security Rule), you can still be compliant if you document why implementation of that item isn't reasonable or appropriate. Specifically,

> (d) Implementation specifications. In this subpart:
>
> (1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.
>
> (2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.
>
> (3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must—
>
> (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and
>
> (ii) As applicable to the entity—
>
> (A) Implement the implementation specification if reasonable and appropriate; or
>
> (B) If implementing the implementation specification is not reasonable and appropriate—
>
> (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

With this in mind, I want to skip ahead to the documentation standard so that you understand why documentation is so critical for HIPAA compliance:

(b)(1) Standard: Documentation.

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) Implementation specifications:

(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

You may never need to produce that documentation, but if your organization is subject to an investigation or a compliance review and you don't have it ready, you and your organization could face significant penalties.

WARNING

It's tempting to think of HIPAA documentation as something you can ask the VoIP (or other product) vendor to take care of for you, but there are two reasons why I don't recommend it. First, the vendor is not on the hook for your HIPPA processes; suppose they agreed to document a process for you, but it's one that you can't reasonably implement—it's your organization that will be held responsible by regulators, not the vendor. Second, remember that HIPAA is about your organization's operational *processes*, not any specific software or hardware. Unless you're hiring a consultant specifically for that purpose, asking an equipment vendor to document that process for you makes about as much sense as asking your local car dealer to pass a driving test for you. Maybe you get a salesman who takes you up on it just to close the sale, but that doesn't really make it appropriate or legal (and it won't make you a safe driver).

So what needs to be documented? Each of the items within the four main categories of the security rule: Administrative, Physical, and Technical Safeguards, plus Organizational Requirements. Since these are lengthy sections, I'm going to summarize and highlight specific parts from each that are likely to come into play with VoIP systems. You'll want to consult the Security Rule for specific details if you believe a listed standard will apply to the VoIP system.

Administrative Safeguards with VoIP Applicability

- Documented security management process to prevent, detect, contain, and correct security violations. Required elements: risk analysis, risk management, sanction policy, and logging/activity review.
- Authorization policies and procedures must be established to grant access to PHI only to those who require it. Addressable elements: Authorization and/or supervision, workforce clearance procedure, termination procedure.

- Security awareness and training program. Addressable elements: security reminders, malicious software protection, log-in monitoring, password management.
- Security incident procedures. Required elements: response and reporting.
- Contingency plan. Required elements: data backup plan, disaster recovery plan, emergency mode operation plan. Addressable elements: testing and revision procedures, applications and data criticality analysis.

Physical Safeguards with VoIP Applicability

- Physical access controls implementation. Addressable elements: contingency operations, facility security plan, physical access control and validation procedures, maintenance records.
- Device and media controls. Required elements: disposal, media reuse. Addressable elements: accountability, data backup and storage.

Technical Safeguards with VoIP Applicability

- Access control. Required elements: unique user identification, emergency access procedure. Addressable elements: automatic logoff, encryption and decryption.
- Audit controls (record of activity within systems containing PHI).
- Integrity. Addressable element: authentication mechanism (for PHI).
- Authentication (individual and entity seeking access to PHI).
- Transmission security. Addressable elements: integrity controls, encryption.

Organizational Requirements

These will generally not have any VoIP applicability except in the unusual case where there is a business relationship established with a service provider with access to recorded information containing PHI.

Other Considerations

Don't assume that because VoIP runs over IP it is considered to be transmission via electronic media by HIPAA. Within HHS General Administrative Requirements there is an official definition stating that:

> Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission

In general this excludes VoIP from HIPAA so long as the transmission is not recorded. Recording is the critical distinction. Within that same section HHS notes:

> Health information means any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

From this, we see that a *recorded* VoIP call or voicemail clearly will fall within the scope of the HIPAA Privacy and Security Rules even though a nonrecorded call would not.

What a HIPAA Consultant Will Tell You

My experience with HIPAA consultants is that few of them have thought much about what happens when you record a VoIP conversation and what documentation is required for the system overall when you do. Nearly all

agree that VoIP by itself does not create any HIPAA requirements. The question is how much documentation is required for voicemail and other call recording technologies.

Given the flexibility that the Security Rule allows, my suggestion is to document just that part of the system involved in recording, but even with that limited scope there will be plenty to document. If the VoIP system includes or interfaces with an Interactive Voice Response (IVR) system, that may need to be documented as well if it can be used as a gateway to PHI contained on a database system behind it.

Tools & Traps…

Core HIPAA-Compliance Issues for IP Communications Systems

Although HIPAA regulations only briefly touch on voice communication systems at all, several general principles still apply. First, the use of VoIP by itself does not create any electronic records unless some related system is recording a session containing Protected Health Information (PHI). In that case, the system doing the recording will fall under HIPAA requirements. This means that voice messaging and call recording equipment may require fully documented HIPAA-compliant operational processes. Second, if a VoIP-related system (such as a VoiceXML server) is a gatekeeper to databases or other record-keeping systems that contain PHI, then HIPAA also will apply. Another example of this is an IVR system that front-ends patient records or billing systems.

HIPAA Compliance and Enforcement

The Department of Health and Human Services (HHS) delegated compliance and enforcement of the HIPAA Privacy Rule to the Office for Civil Rights (OCR) along with authority for allowing exceptions where certain state laws may conflict with HIPAA. The Centers for Medicare and Medicaid services (CMS) received delegated responsibility from HHS for enforcing the security rule, transactions, and code set standards (and identifiers standards

when those are published). Through its Office of HIPAA Standards (OHS), CMS will enforce these rules and continue to enforce the insurance portability requirements under Title I of HIPAA.

No Certification

No official certification process exists for covered entities under HIPAA, although HHS did receive authority to perform compliance reviews as part of the Act. Products are not certified as part of HIPAA (although it's not uncommon to see them promoted as if they were). Regardless, documentation as specified in the Security Rule and Privacy Rule must exist and might be reviewed by a business partner, for example, as part of a due-diligence process. Other than that, the only time you would have to produce it is if you are investigated by HHS or OCR in response to a complaint or as part of a compliance review.

Enforcement Process and Penalties

In general, OCR acts on Privacy Rule violations in response to complaints that are registered with it. OCR requires written notification but does accept e-mail at OCRComplaint@hhs.gov (see "How to File a Health Information Privacy Complaint" at www.hhs.gov/ocr/privacyhowtofile.htm for more details). CMS has stated that the enforcement process for its portion of HIPAA will be primarily complaint-driven, although their primary strategy is to achieve "voluntary compliance through technical assistance." Penalties would be imposed as a last resort. When a complaint is received (typically through their Web site at www.cms.hhs.gov/Enforcement or via mail), CMS first allows the provider the opportunity to demonstrate compliance (or submit a plan for corrective action). Only if the provider fails to respond would penalties be considered.

The Administrative Simplification Compliance Act (ASCA) permits the Secretary of HHS to exclude noncompliant covered entities from the Medicare program. In addition, the original HIPAA legislation permits civil monetary penalties of not more than $100 for each violation, with a cap of $25,000 per calendar year. In addition, criminal penalties can be imposed for certain wrongful disclosures up to a $250,000 fine and 10 years imprisonment for willful conduct.

CALEA: Communications Assistance for Law Enforcement Act

The Communications Assistance for Law Enforcement Act first arrived from the U.S. Congress in 1994 with a simple goal: improving wiretapping effectiveness for law-enforcement in an increasingly digital PSTN. Advances in telecommunications made prior wiretapping methods less effective and CALEA was intended to force all carriers and carrier-grade equipment vendors to provide consistent and accessible electronic monitoring capabilities. For private equipment, including PBX and similar business-class voice equipment, CALEA doesn't apply except when that equipment was deemed a "substantial replacement" for the public telephone service.

Between 1994 and 2004, CALEA eventually progressed to a rough set of technically feasible standards backed by FCC regulations (and deep involvement by the Federal Bureau of Investigation (FBI) and Department of Justice (DOJ), though packet communications was still a CALEA minefield. These VoIP and broadband issues came to a head in August 2004 when the FCC issued a Notice of Proposed Rulemaking and Declaratory Ruling (NPRM) for public comment, stirring up anew the privacy and civil-liberties debate (see the sidebar, "CALEA and the Xbox?"). Lost to many observers was the fact the new NPRM might now be broad enough to force enterprises, universities, and other previously excluded organizations that deploy VoIP to become subject to the revised regulations. Although several requests for clarification on that topic still are pending at the FCC, it's clear these rules could substantially affect the design and deployment of enterprise VoIP.

If you're a carrier (of Voice, VoIP, or even just broadband IP), CALEA regulation is already a certainty (although in the case of broadband, there is a lot of work remaining even to agree on the technical standards, and the FBI has yet to specify capacity requirements as required by the Act). And in spite of the fact that in November 1994, the FCC had ruled that VoIP was a "data service" for other regulatory purposes, the FCC and DOJ agreed that data services were still within the scope of CALEA. Although predictable, this nevertheless came as a shock to many carriers who had in recent years become comfortable with the FCC hands-off approach to data networks and VoIP despite pressure from the FBI and Department of Justice (DOJ).

Notes from the Underground…

CALEA and the Xbox?

With the latest CALEA guidance for broadband, it's applicability to VoIP and data networks that has become a new privacy battleground. Groups Like the Electronic Frontier Foundation have been heavily involved in the debate, and from their perspective, the consequences of the revised CALEA rules could have long-ranging—and possibly dire—consequences:

"If the FBI gets its way, the NPRM's tentative regulations will only be the tip of the iceberg. Soon, software companies, under threat of an expansive definition of CALEA's requirements, will face economic incentives to create email and IM programs that are surveillance-ready. Many computer game consoles that people can use to play over the Internet, such as the Xbox, allow gamers to chat with each other while they play. If any communication program running on the Internet has to be CALEA-compliant before being bought and sold, what would stop law enforcement from pushing for a tappable Xbox?"

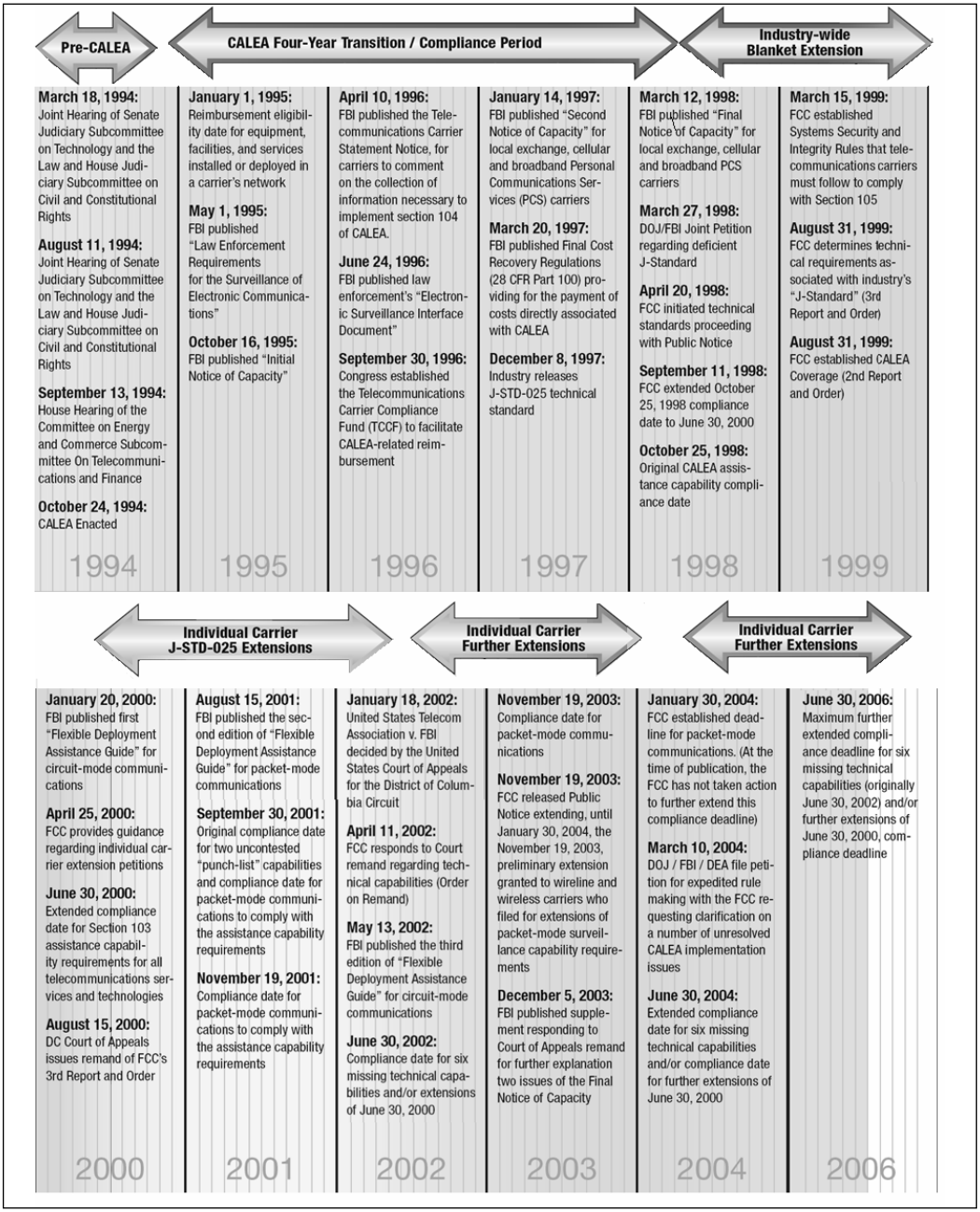
Although it remains to be seen just how far the FCC and DOJ take enforcement of CALEA, it seems unlikely that serious enforcement will happen outside of the carrier space (with the possible exception of organizations like universities that provide phone service over a large campus).

Figure A.1 shows a timeline for the development of the CALEA.

Since the publication of this guide, the following developments have taken place:

- September 23, 2004: FCC rules that all "push-to-talk" services are subject to CALEA
- September 23, 2005: FCC responds to DOJ / FBI / DEA petition and issues Notice of Proposed Rulemaking (NPRM) that will require broadband and VoIP providers to comply with CALEA; compliance deadline will be 18 months after final order.

Figure A.1 CALEA Timeline*



* Published in the Communications Assistance for Law Enforcement Act (CALEA) Flexible Deployment Assistance Guide, Fourth Edition

CALEA Regulatory Basics

Several critical documents are required reading for those wanting to understand the intent of the original Act, and subsequent VoIP policy from the FCC, FBI, DOJ, and other agencies, particularly in the context of VoIP and its place in the latest CALEA rules. Here's the short list; we'll cover each of these in more detail later in the section:

- The 1994 Act itself as passed by Congress (see www.askcalea.net/calea.html for a full copy) broadened wiretap applicability to new telecommunications technologies and added a new requirement to gather "call-identifying information" as part of a legal communications intercept.
- J-STD-025, "Lawfully Authorized Electronic Surveillance" published by the Telecommunications Industry Association (TIA) as a result of work started in 1995 to address CALEA; known initially as TIA/EIA SP 3580. J-STD-025 was first published by TIA in December, 1997. (The current version required for FCC compliance is J-STD-025-A, published by the TIA in December, 2000—available for purchase at www.tiaonline.org/standards/catalog/ for nonmembers.)
- FCC "CALEA Third Report and Order,? August 31, 1999 (for a full copy, see www.fcc.gov/Bureaus/Engineering_Technology/Orders/1999/fcc99230.pdf or .txt), defined capability requirements in terms of J-STD-025 for wireline, cellular, and broadband PCS carriers, and specified that six of the nine additional capabilities in the FBI "CALEA punch list" for J-STD-025 would be required for CALEA compliance (subsequently incorporated into J-STD-025-A).
- DOJ, FBI and Drug Enforcement Agency (DEA), "Joint Petition for Expedited Rulemaking" (www.askcalea.net/docs/20040310.calea.jper.pdf) filed before the FCC March 10, 2004 requested clear rules for how CALEA will be implemented on a wide variety of services, including packet technologies generally and VoIP specifically. Although not itself a regulation, this document

serves as a roadmap for FCC rulemaking that will take place in 2006 and beyond, directly affecting VoIP service providers.

- FCC "First Report and Order and Further Notice of Proposed Rulemaking," FCC 05-153 (get a copy at www.askcalea.net/docs/20050923-fcc-05-153.pdf or at www.fcc.gov), September 23, 2005, issued in response to the March 2004 Joint Petition.

Direct from the Regulations

The basic technical requirements of the Act can be found in the first part of Section 103. In a nutshell, when a court order is present, the law enforcement requires access to all communications and their surrounding context without letting the target discover the "wiretap" (known in CALEA as a "lawful intercept"):

> **SEC. 103. ASSISTANCE CAPABILITY REQUIREMENTS.**
>
> (a) CAPABILITY REQUIREMENTS- Except as provided in subsections (b), (c), and (d) of this section and sections 108(a) and 109(b) and (d), a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—
>
> (1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to

> access call-identifying information that is reasonably available to the carrier—
>
> (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
>
> (B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);
>
> (3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and
>
> (4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects—
>
> (A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and
>
> (B) information regarding the government's interception of communications and access to call-identifying information.

Bottom line: CALEA even at this level not only requires the media itself for a VoIP call, but a good deal of signaling information as well (labeled "call-identifying information" in the Act). In addition, you must facilitate the process and provide appropriate equipment to enable the surveillance to

take place, although some cost recovery is permitted (this is an open issue, however, as you'll see in the 2004 Joint Petition). If you're a carrier (or substantial replacement for one) and fall under CALEA, every communications service that you provide to your customers must be capable of meeting these requirements.

NOTE

Although these terms are by no means unique to CALEA, it's useful to review the different types of legal interception available to Law Enforcement Agencies (LEAs) today:

1. Pen Register—what numbers were called by the target?
2. Trap and Trace—what numbers called the target?
3. Interception (Title III)—recorded conversation of the target (plus the other two items in this list). Most of the time, CALEA talks about this type of legal intercept.

The rest of the act lays out specific regulatory mandates and responsibilities, mainly targeted at the FCC. Sections 102, 104, 107, and 109 mandate that the FCC establish regulations for systems security and integrity, associated technical requirements, and determinations for specific equipment, facility, or services. An important compliance concept is also part of Section 107 and are known as "Safe harbor standards." Section 107(a)(2) of CALEA allows a carrier to be deemed in compliance with CALEA's capability requirements in Sections 103 and 106 if it complies with an appropriate publicly available technical standard. Also in Section 107 is a provision that allows a carrier to petition for an extension of the CALEA deadline when appropriate standards or technology isn't available. Here's the complete text of Sections 106 and 107:

SEC. 106. COOPERATION OF EQUIPMENT MANUFACTURERS AND PROVIDERS OF TELECOMMUNICATIONS SUPPORT SERVICES.

(a) CONSULTATION- A telecommunications carrier shall consult, as necessary, in a timely fashion with manufacturers of its telecommunications transmission and switching equipment and its providers of telecommunications support services for the purpose of ensuring that current and planned equipment, facilities, and services comply with the capability requirements of section 103 and the capacity requirements identified by the Attorney General under section 104.

(b) COOPERATION- Subject to sections 104(e), 108(a), and 109 (b) and (d), a manufacturer of telecommunications transmission or switching equipment and a provider of telecommunications support services shall, on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its equipment, facilities, or services such features or modifications as are necessary to permit such carriers to comply with the capability requirements of section 103 and the capacity requirements identified by the Attorney General under section 104.

SEC. 107. TECHNICAL REQUIREMENTS AND STANDARDS; EXTENSION OF COMPLIANCE DATE.

(a) SAFE HARBOR-

(1) CONSULTATION- To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 103, the Attorney General, in coordination with other Federal, State, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry, with representatives of users of telecommunications equipment, facilities, and services, and with State utility commissions.

(2) COMPLIANCE UNDER ACCEPTED STANDARDS- A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications

support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103.

(3) ABSENCE OF STANDARDS- The absence of technical requirements or standards for implementing the assistance capability requirements of section 103 shall not—

(A) preclude a telecommunications carrier, manufacturer, or telecommunications support services provider from deploying a technology or service; or
(B) relieve a carrier, manufacturer, or telecommunications support services provider of the obligations imposed by section 103 or 106, as applicable.

(b) COMMISSION AUTHORITY- If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that—

(1) meet the assistance capability requirements of section 103 by cost-effective methods;

(2) protect the privacy and security of communications not authorized to be intercepted;

(3) minimize the cost of such compliance on residential ratepayers;

(4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and

(5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period.

(c) EXTENSION OF COMPLIANCE DATE FOR EQUIPMENT, FACILITIES, AND SERVICES-

(1) PETITION- A telecommunications carrier proposing to install or deploy, or having installed or deployed, any equipment, facility, or service prior to the effective date of section 103 may petition the Commission for 1 or more extensions of the deadline for complying with the assistance capability requirements under section 103.

(2) GROUNDS FOR EXTENSION- The Commission may, after consultation with the Attorney General, grant an extension under this subsection, if the Commission determines that compliance with the assistance capability requirements under section 103 is not reasonably achievable through application of technology available within the compliance period.

(3) LENGTH OF EXTENSION- An extension under this subsection shall extend for no longer than the earlier of—

(A) the date determined by the Commission as necessary for the carrier to comply with the assistance capability requirements under section 103; or
(B) the date that is 2 years after the date on which the extension is granted.

(4) APPLICABILITY OF EXTENSION- An extension under this subsection shall apply to only that part of the carrier's business on which the new equipment, facility, or service is used.

These extensions, once routine, are now scrutinized much more closely by the FCC, FBI, and DOJ. Even for packet-based solutions like VoIP, the existence of adequate technical standards is forcing equipment manufacturers and carriers to show compliance with CALEA.

J-STD-025 and Other Technical Standards

Shortly after CALEA was enacted, work began in Subcommittee TR-45.2 of the Telecommunications Industry Association (TIA) to create an appropriate technical interface between Law Enforcement Agencies (LEAs) and carriers. Interim standard J-STD-025 was developed specifically to define services and features required by CALEA for "wireline, cellular, and broadband PCS carriers to support lawfully-authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information to a law enforcement agency."

NOTE

J-STD-025 and subsequent TIA technical standards referenced by FCC regulations—although available to the public—are not free. They can be purchased on the TIA Web site (see www.tiaonline.org/standards/CALEA_JEM for more information) or through the Alliance for Telecommunications Industry Solutions (ATIS—see www.atis.org/atis/docstore/ for more information). In general, most of the standards referenced in this section require membership or document fees to be paid in order to access the associated standard.

Originally published in December, 1997, J-STD-025, the standard was the subject of a March 27, 1998, Joint petition to the FCC from the DOJ and FBI, which argued that it was deficient in nine specific areas. This list commonly is referred to as the FBI "punch list" of additional capabilities, six of which were subsequently required by the FCC and incorporated into the revised J-STD-025-A specification, published by TR-45.2 in May, 2000.

Since that time, a number of standards have been developed by other industry groups and are recognized by the FBI and FCC as meeting the safe harbor provisions of CALEA. Many of these have been coordinated with ongoing TIA TR45 LAES work on J-STD-025. Among these standards are:

- TIA TR45 LAES J-STD-025B for CDMA2000 packet data intercepts
- T1P1 T1.724 for GPRS packet data intercepts

- T1S1 T1.678 for VoIP and other wire-line data intercepts
- PKT-SP-ESP-I03-40113 for PacketCable data intercepts
- AMTA Electronic Surveillance for ESMR Dispatch Version 1.0 for ESMR Push-To-Talk intercepts
- American Association of Paging Carriers (AAPC) Paging Technical Committee (PTC) CALEA Suite of Standards, Version 1.3 for Traditional Paging, Advanced Messaging, and Ancillary Services (see www.pagingcarriers.org/ptc.asp for this freely available standard)

FCC CALEA Third Report and Order (August 1999)

By 1999, the FCC was ready to require all carriers to implement the capabilities of the TIA J-standard and six FBI punch list capabilities by June 30, 2002. Packet-mode communications capability (including VoIP) was to be implemented by September 30, 2002 (though in practice CALEA extensions for packet continued routinely until late 2005). In addition, the FCC reached important conclusions regarding location information (not directly specified by the Act itself) and packet-mode communications capabilities. The FCC press release states:

> **Actions Regarding the Interim Standard (J-STD-025)**
>
> The FCC concluded the following regarding the location information and packet-mode communications capabilities of the interim standard:
>
> **Location information:** The FCC required that location information be provided to law enforcement agencies (LEAs) under CALEA's assistance capability requirements for "call-identifying information," provided that a LEA has a court order or legal authorization beyond a pen register or trap and trace authorization. The FCC found that location information identifies the "origin" or "destination" of a communication and thus is covered by CALEA. The FCC, however, did not mandate that carriers be able to provide LEAs with the precise physical location of a caller. Rather, it permitted LEAs

with the proper legal authorization to receive from wireline, cellular, and broadband PCS carriers only the location of a cell site at the beginning and termination of a mobile call.

Packet-mode communications: The FCC required that carriers provide LEAs access to packet-mode communications by September 30, 2001. However, the Commission acknowledged that significant privacy issues had been raised with regard to the J-STD-025 treatment of packet-mode communications. Under the J-STD-025, law enforcement could be provided with access to both call identifying information and call content, even where it may be authorized only to receive call identifying information. Accordingly, the FCC invited TIA to study CALEA solutions for packet-mode technology and report to the FCC by September 30, 2000 on steps that can be taken, including particular amendments to the interim standard, that will better address privacy concerns.

Actions Regarding the Capabilities Requested by DoJ/FBI

Of the nine items in the DoJ/FBI punch list, the following capabilities were required by the FCC:

Content of subject-initiated conference calls— A LEA will be able to access the content of conference calls initiated by the subject under surveillance (including the call content of parties on hold), pursuant to a court order or other legal authorization beyond a pen register order.

Party hold, join, drop on conference calls— Messages will be sent to a LEA that identify the active parties of a call. Specifically, on a conference call, these messages will indicate whether a party is on hold, has joined, or has been dropped from the conference call.

Subject-initiated dialing and signaling information— Access to dialing and signaling information available from the subject will inform a LEA of a subject's use of features

(e.g., call forwarding, call waiting, call hold, and three-way calling).

In-band and out-of-band signaling (notification message)— A message will be sent to a LEA whenever a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy, call waiting signal).

Timing information— Information will be sent to a LEA permitting it to correlate call-identifying information with the call content of a communications interception.

Dialed digit extraction—The originating carrier will provide to a LEA on the call data channel any digits dialed by the subject after connecting to another carrier's service., pursuant to a pen register authorization. The FCC found that some such digits fit within CALEA's definition of call-identifying information, and that they are generally reasonably available to carriers

In requiring the six punch list capabilities, the FCC noted that it determined that five of them constitute call-identifying information that is generally reasonably available to carriers and therefore is required under CALEA. The FCC found that although the cost to carriers of providing some of these five capabilities is significant, no automatic exemptions will be provided. Exclusions must be filed and approved on a case-by-case basis.

The following punch list items were not required by the FCC:

Surveillance status—Carriers would have been required to send a message to a LEA to verify that a wiretap had been established and was functioning correctly.

Continuity check tone (C-tone)— Electronic signal would have alerted a LEA if the facility used for delivery of call content interception failed or lost continuity.

> **Feature status**— A LEA would have been notified when, for the facilities under surveillance, specific subscription-based calling services were added or deleted.

The FCC found that these three capabilities, although potentially useful to LEAs, were not required by the plain language of CALEA. However, carriers are free to provide these capabilities if they wish to do so.

DOJ-FBI-DEA Joint Petition for Expedited Rulemaking (March 2004)

Given CALEA's stated purpose, namely to "preserve law enforcement's ability to conduct lawful electronic surveillance despite changing telecommunications technologies," the DOJ, FBI, and DEA felt that key aspects of the law and its original intent were not being addressed by the FCC, carriers, and equipment manufacturers. The petition states:

> CALEA applies to all telecommunications carriers, and its application is technology neutral. Despite a clear statutory mandate, full CALEA implementation has not been achieved. Although the Commission has taken steps to implement CALEA, there remain several outstanding issues that are in need of immediate resolution.
>
> To resolve the outstanding issues, law enforcement asks the Commission to:
>
> (1) formally identify the types of services and entities that are subject to CALEA;
> (2) formally identify the services that are considered "packet-mode services";
> (3) initially issue a Declaratory Ruling or other formal Commission statement, and ultimately adopt final rules, finding that broadband access services and broadband telephony services are subject to CALEA;
> (4) reaffirm, consistent with the Commission's finding in the CALEA Second Report and Order, that push-to-talk "dispatch" service is subject to CALEA;
> (5) adopt rules that provide for the easy and rapid identifica-

> tion of future CALEA-covered services and entities;
> (6) establish benchmarks and deadlines for CALEA packet-mode compliance;
> (7) adopt rules that provide for the establishment of benchmarks and deadlines for CALEA compliance with future CALEA-covered technologies;
> (8) outline the criteria for extensions of any benchmarks and deadlines for compliance with future CALEA-covered technologies established by the Commission;
> (9) establish rules to permit it to request information regarding CALEA compliance generally;
> (10) establish procedures for enforcement action against entities that do not comply with their CALEA obligations;
> (11) confirm that carriers bear sole financial responsibility for CALEA implementation costs for post-January 1, 1995 communications equipment, facilities and services;
> (12) permit carriers to recover their CALEA implementation costs from their customers; and
> (13) clarify the cost methodology and financial responsibility associated with intercept provisioning.

In general, existing FCC rules are incomplete, inconsistent, or otherwise inadequate in these areas and you should expect to see new or clarified regulations from the FCC over the next few years that address the DOJ/FBI/DEA concerns. Many of these will directly impact VoIP systems design and operational practices within carriers.

FCC First Report and Order and Further Notice of Proposed Rulemaking, (September, 2005)

In response to the DOJ-FBI-DEA Joint Petition, the FCC ruled that CALEA does apply to providers of certain broadband and interconnected VoIP services. From the FCC press release:

> The Commission found that these services can essentially replace conventional telecommunications services currently subject to wiretap rules, including circuit-switched voice service and dial-up Internet access. As replacements, the new services are covered by the Communications Assistance for

Law Enforcement Act, or CALEA, which requires the Commission to preserve the ability of law enforcement agencies to conduct court-ordered wiretaps in the face of technological change.

The Order is limited to facilities-based broadband Internet access service providers and VoIP providers that offer services permitting users to receive calls from, and place calls to, the public switched telephone network. These VoIP providers are called interconnected VoIP providers.

The Commission found that the definition of "telecommunications carrier" in CALEA is broader than the definition of that term in the Communications Act and can encompass providers of services that are not classified as telecommunications services under the Communications Act. CALEA contains a provision that authorizes the Commission to deem an entity a telecommunications carrier if the Commission "finds that such service is a replacement for a substantial portion of the local telephone exchange."

Because broadband Internet and interconnected VoIP providers need a reasonable amount of time to come into compliance with all relevant CALEA requirements, the Commission established a deadline of 18 months from the effective date of this Order, by which time newly covered entities and providers of newly covered services must be in full compliance. The Commission also adopted a Further Notice of Proposed Rulemaking that will seek more information about whether certain classes or categories of facilities-based broadband Internet access providers – notably small and rural providers and providers of broadband networks for educational and research institutions – should be exempt from CALEA.

The Commission's action is the first critical step to apply CALEA obligations to new technologies and services that are increasingly used as a substitute for conventional services. The Order strikes an appropriate balance between fostering

> competitive broadband and advanced services deployment and technological innovation on one hand, and meeting the needs of the law enforcement community on the other.

The potential impact of this ruling is huge and will reverberate within the VoIP and broadband communities over the next few years. What is perhaps most surprising is the determination that broadband data services will need to support a lawful intercept function. Lawsuits have already been filed (partly over the unfunded mandate the FCC created for higher education: an estimated $7 billion in CALEA implementation costs are expected for colleges and universities alone, according to EDUCAUSE). Much of the story has yet to be written but the impact of this round of FCC rulemaking on the VoIP community will be hard to overstate. How this will affect Skype and other consumer services in the long run remains to be seen, but in the meantime this FNPR has served as a shot across the bow of the VoIP industry.

Telecommunications Carrier Systems Security and Integrity Plan

The FCC mandates that carriers file this plan as part of their CALEA compliance. From the FCC CALEA page:

> CALEA also requires telecommunications carriers to file with the Commission information regarding the policies and procedures used for employee supervision and control, and to maintain secure and accurate records of each communications interception or access to call-identifying information. In particular, all carriers that must comply with CALEA's capacity and capability requirements must also comply with 47 C.F.R. §§64.2100 - 64.2106 of the Commission's rules (available at www.access.gpo.gov/nara/cfr/waisidx_03/47cfr64_03.html) by filing with the Commission a Telecommunications Carrier Systems Security and Integrity Plan. Resellers of local exchange services, both facilities-based and switchless, must also comply with these rules by filing a Systems Security and Integrity Plan.

What a CALEA Consultant Will Tell You

First and foremost, it's very important to know for sure if your organization is required to comply with CALEA. At this point, the FCC has issued extensive guidance but it still does not cover all cases. A CALEA expert can help guide you through existing precedent and determine which—if any—of the services offered by your organization must be compliant with CALEA. From there, identifying any safe harbor standards accepted by the FCC and FBI is the next step. If you can implement one or more safe harbor standards, then do it and consider yourself lucky.

If you can't, you'll need some help determining which section to file under (107 or 109) so that the FCC can grant you a little breathing room while you figure out what your long-term solution will be (presumably with the help of your VoIP system vendor(s). Unfortunately, today's VoIP systems are a little behind the curve on implementing CALEA standards, and if your software or hardware providers don't already have a plan to address CALEA, you may want to consider alternatives since the FCC has signaled that it will no longer routinely grant deferrals and other exceptions when adequate technical solutions exist and are available to the market.

Tools & Traps…

Core CALEA-Compliance Issues for IP Communications Systems

Unlike regulations like HIPAA, GLBA, or SOX, within CALEA there is more focus on equipment capabilities and standards as part of CALEA compliance. Know which standard to apply (start with J-STD-025B or T1.678 for VoIP). Retrofitting a compliant solution over a noncompliant system can be difficult and expensive for VoIP, so if you are required to comply with CALEA, make sure that your equipment (or software) supplier evaluation / procurement process adequately screens for CALEA support, and be sure to stay on top of FCC filings (and the latest FCC orders, since VoIP rules under CALEA are still being worked out). Consider filing a comment with the FCC if you're reading this early enough in the rulemaking process.

CALEA Compliance and Enforcement

In general, the FCC (with input from the DOJ and FBI) is responsible for compliance (although there are minor aspects of CALEA that the DOJ can enforce directly).

Certification

Individual LEAs can be CALEA-certified, but in general that term isn't applied to equipment or carriers. Equipment sold to carriers can (and should) be CALEA Section 106-compliant in the sense that if it meets a standard accepted by the FCC (and/or FBI in some cases where a technical standard hasn't been adopted by the FCC regulations directly). Use of CALEA-compliant equipment by a carrier will bring Section 107 Safe Harbor provisions into play to deem that service to be CALEA-compliant. In general, however, it is a carrier and associated service that can be certified as compliant, by meeting Section 103 requirements directly with the agreement of the FBI (these have been phased out as technical standards now fill the gap that once required this FBI consent).

Enforcement Process and Penalties

The FCC requires appropriate CALEA filings by each carrier and can impose fines when those filings are missing, incomplete, or otherwise not in line with CALEA regulations. At this point, there have been no major fines but the threat of fines has kept most carriers on top of all required filings. With the inclusion of VoIP it will be interesting to see if the FCC takes a "get tough" stance on CALEA enforcement once the current set of VoIP and packet-related CALEA lawsuits has been resolved.

Elliott Eichen at Verizon suggests a "Four-Step Process" to describe the regulatory experience surrounding CALEA (and E911) compliance; it rings particularly true for me:

1. Denial: "Not us!"
2. Depression: "We can't do it technically."
3. Anger: "This is going to cost a fortune!"

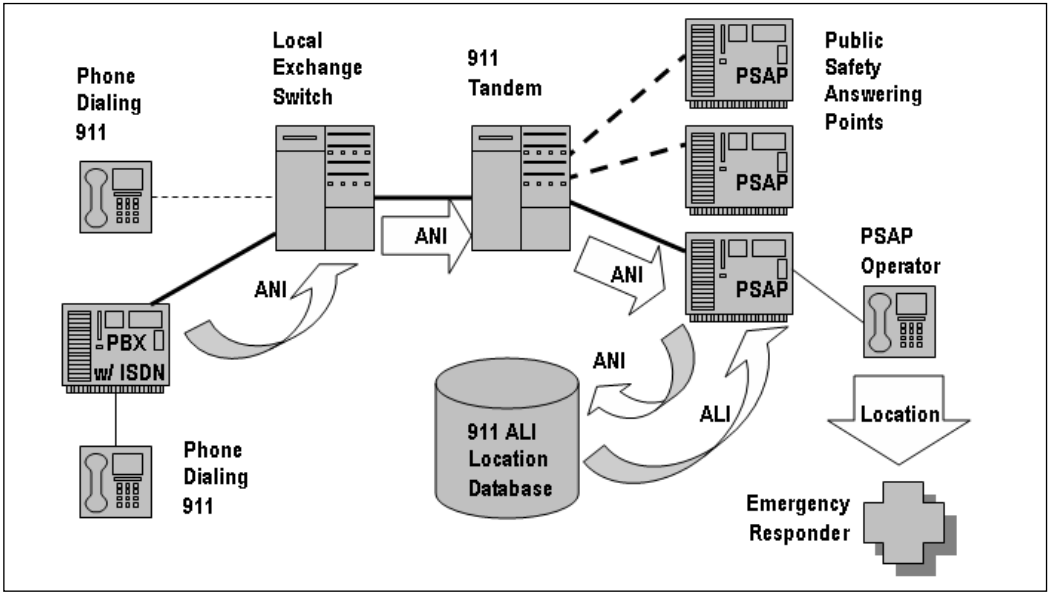
4. Acceptance: "CALEA and E911 are not going away; let's make it work."

E911: Enhanced 911 and Related Regulations

Within the United States and Canada, 911 is the official national emergency number; calls to 911 are directed to the most appropriate Public Safety Answering Point (PSAP) dispatcher for local emergency medical, fire, and law enforcement agencies via specialized infrastructure. Enhanced 911 (E911) systems automatically show the PSAP a calling number telephone number and location for wireline phones using the Automatic Location Identifier (ALI) database (maintained specifically for PSAP use, it translates a phone number from Automatic Number Identification (ANI) to a physical location). In 1996 the FCC established the wireless E911 program; which, when fully implemented, will provide a PSAP with a precise location for wireless 911 calls. Figure A.2 is an example of an enhanced 911 system. In this example, the ALI Location Database translates an ANI identifier into a physical location that can be used for emergency dispatch.

Given all the progress around E911 it may come as a surprise to you that 911 failures due to incomplete VoIP E911 design have led to several high-profile, preventable deaths (accompanied by lawsuits and demand for increased regulation). In fact, the rise of VoIP carriers that are interconnected with the PSTN has been accompanied by two massive breakdowns in E911 capability that eventually forced an urgent VoIP E911 order from the FCC in June, 2005. The first involves VoIP carriers not having adequate interconnection arrangements to pass E911 calls. But the second is the more interesting problem. What happens when you can register a VoIP phone over an IP network from any physical location in the world (so long as it can be connected to the Internet)?

Figure A.2 An Enhanced 911 System



E911 Regulatory Basics

There are several dimensions to E911, the most important being the distinction between wireline and wireless regulations. But in this section we will focus exclusively on the FCC VoIP E911 rulings in 2005 that have added an important new dimension to FCC rules for E911.

Direct from the Regulations

On June 3, 2005 the FCC released the *VoIP 911 Order* requiring interconnected VoIP providers to provide their new and existing subscribers with 911 service no later than November 28, 2005. The FCC accompanying press release gives an excellent summary of the resulting regulations:

> Specifically, as a condition of providing interconnected VoIP service, each interconnected VoIP provider must, in addition to satisfying the subscriber notification, acknowledgment, and labeling requirements set forth in section 9.5(e) of the Commission's rules.

- Transmit all 911 calls to the public safety answering point (PSAP), designated statewide default answering point, or appropriate local emergency authority that serves the caller's "Registered Location." Such transmissions must include the caller's Automatic Numbering Information (ANI) [ANI is a system that identifies the billing account for a call and, for 911 systems, identifies the calling party and may be used as a call back number] and Registered Location to the extent that the PSAP, designated statewide default answering point, or appropriate local emergency authority is capable of receiving and processing such information;

- Route all 911 calls through the use of ANI and, if necessary, pseudo-ANI [Pseudo-ANI is "a number, consisting of the same number of digits as ANI, that is not a North American Numbering Plan telephone directory number and may be used in place of an ANI to convey special meaning. The special meaning assigned to the pseudo-ANI is determined by agreements, as necessary, between the system originating the call, intermediate systems handling and routing the call, and the destination system], via the Wireline E911 Network, [a "dedicated wireline network that: (1) is interconnected with but largely separate from the public switched telephone network; (2) includes a selective router; and (3) is utilized to route emergency calls and related information to PSAPs, designated statewide default answering points, appropriate local emergency authorities or other emergency answering points."] and make a caller's Registered Location available to the appropriate PSAP, designated statewide default answering point or appropriate local emergency authority from or through the appropriate Automatic Location Identification (ALI) database;

- Obtain from each of its existing and new customers, prior to the initiation of service, a Registered Location; and

- Provide all of their end users one or more methods of

manner. At least one method must allow end users to use only the same equipment (such as the Internet telephone) that they use to access their interconnected VoIP service.

Compliance Letters

Additionally, given the vital public safety interests at stake, the VoIP 911 Order requires each interconnected VoIP provider to file with the Commission a Compliance Letter on or before November 28, 2005 detailing its compliance with the above 911 requirements. To ensure that interconnected VoIP providers have satisfied the requirements set forth above, we require interconnected VoIP providers to include the following information in their Compliance Letters:

- 911 Solution: This description should include a quantification, on a percentage basis, of the number of subscribers to whom the provider is able to provide 911 service in compliance with the rules established in the VoIP 911 Order. Further, the detailed description of the technical solution should include the following components:

1. 911 Routing Information/Connectivity to Wireline E911 Network: A detailed statement as to whether the provider is transmitting, as specified in Paragraph 42 of the VoIP 911 Order, "all 911 calls to the appropriate PSAP, designated statewide default answering point, or appropriate local emergency authority utilizing the Selective Router, the trunk line(s) between the Selective Router and the PSAP, and such other elements of the Wireline E911 Network as are necessary in those areas where Selective Routers are utilized." If the provider is not transmitting all 911 calls to the correct answering point in areas where Selective Routers are utilized, this statement should include a detailed explanation why not. In addition, the provider should quantify the number of Selective Routers to which it has interconnected, directly or indirectly, as of November 28, 2005.

2. Transmission of ANI and Registered Location Information: A detailed statement as to whether the provider is transmitting via the Wireline E911 Network the 911 caller's ANI and Registered Location to all answering points that are capable of receiving and processing this information. This information should include: (i) a quantification, on a percentage basis, of how many answering points within the provider's service area are capable of receiving and processing ANI and Registered Location information that the provider transmits; (ii) a quantification of the number of subscribers, on a percentage basis, whose ANI and Registered Location are being transmitted to answering points that are capable of receiving and processing this information; and (iii) if the provider is not transmitting the 911 caller's ANI and Registered Location to all answering points that are capable of receiving and processing this information, a detailed explanation why not.

3. 911 Coverage: To the extent a provider has not achieved full 911 compliance with the requirements of the VoIP 911 Order in all areas of the country by November 28, 2005, the provider should: 1) describe in detail, either in narrative form or by map, the areas of the country, on a MSA basis, where it is in full compliance and those in which it is not; and 2) describe in detail its plans for coming into full compliance with the requirements of the order, including its anticipated timeframe for such compliance.

- Obtaining Initial Registered Location Information: A detailed description of all actions the provider has taken to obtain each existing subscriber's current Registered Location and each new subscriber's initial Registered Location. This information should include, but is not limited to, relevant dates and methods of contact with subscribers and a quantification, on a percentage basis, of the number of subscribers from whom the provider has obtained the Registered Location.

- Obtaining Updated Registered Location Information: A detailed description of the method(s) the provider has offered its subscribers to update their Registered Locations. This information should include a statement as to whether the provider is offering its subscribers at least one option for updating their Registered Location that permits them to use the same equipment that they use to access their interconnected VoIP service.

- Technical Solution for Nomadic Subscribers: A detailed description of any technical solutions the provider is implementing or has implemented to ensure that subscribers have access to 911 service whenever they use their service nomadically.

The Bureau notes that in an October 7, 2005 letter submitted in WC Docket Nos. 04-36 and 05-196, AT&T outlined an innovative compliance plan that it is implementing to address the Commission's 911 provisioning requirements that take effect on November 28, 2005. In letters filed on October 21, 2005 in these dockets, MCI and Verizon each outlined similar compliance plans. Each of these plans includes an automatic detection mechanism that enables the provider to identify when a customer may have moved his or her interconnected VoIP service to a new location and ensure that the customer continues to receive 911 service even when using the interconnected VoIP service nomadically. These plans also include a commitment to not accept new interconnected VoIP customers in areas where the provider cannot provide 911 service and to adopt a "grandfather" process for existing customers for whom the provider has not yet implemented either full 911 service or the automatic detection capability.

The Bureau applauds the steps undertaken by AT&T, MCI and Verizon and strongly encourages other providers to adopt similar measures. The Bureau will carefully review a provider's implementation of steps such as these in deciding whether and how to take enforcement action. Providers should include in their November 28, 2005, Compliance Letters a

mented such measures. To the extent that providers have not implemented these or similar measures, they should describe what measures they have implemented in order to comply with the requirements of the VoIP 911 Order.

Although we do not require providers that have not achieved full 911 compliance by November 28, 2005, to discontinue the provision of interconnected VoIP service to any existing customers, we do expect that such providers will discontinue marketing VoIP service, and accepting new customers for their service, in all areas where they are not transmitting 911 calls to the appropriate PSAP in full compliance with the Commission's rules.

What an E911 Consultant Will Tell You

This is a very active and emerging space, particularly around VoIP E911, but the National Emergency Number Association (NENA) has some excellent recommendations in this area. They have published a 9-1-1 System Reference Guide (go to www.nena.org for more information) that is "a single-source reference for PSAP and Selective Router administrative data"—invaluable information for a VoIP carrier that needs to comply with the new FCC order. Also underway is a NG E9-1-1 Program, a public-private partnership to improve the nation's 9-1-1 system and provide necessary VoIP and PSAP standards to make deployable VoIP E911 more achievable.

Tools & Traps…

Core E911-Compliance Issues for IP Communications Systems

As with CALEA, there is a bit more focus on equipment capabilities and standards as part of compliance. However, retrofitting a compliant solution over a noncompliant system isn't necessarily difficult and expensive if it's well planned. Regardless, E911 should be a critical part of your vendor-facing solution evaluation / procurement process.

For enterprise VoIP systems, the critical considerations involve local regulations that require accurate information for ALI tables. Many enterprise system vendors have location databases, capabilities for end-user location self-reporting, and partnerships with third-party solutions for maintaining location information even when IP phones are moved.

E911 Compliance and Enforcement

The FCC and the National Association of Regulatory Utility Commissioners (NARUC) formed the Joint Federal/State VoIP Enhanced 911 Enforcement Task Force to facilitate compliance with FCC VoIP 911 rules as well as any necessary enforcement. The Task Force is made up of FCC staff and representatives from various State PUCs, and operates in conjunction with NENA, the Association of Public Safety Communications Officials, and various state and local emergency authorities. The Task Force's mission is to "develop educational materials to ensure that consumers understand their rights and the requirements of the FCC's VoIP 911 Order; develop appropriate compliance and enforcement strategies; compile data; and share best practices."

Self-Certification

At this point, the FCC process requires a self-certification by each VoIP carrier that must be filed with the FCC. As standards emerge, some form of product certification for VoIP E911 may eventually take place.

Enforcement Process and Penalties

Despite the number of extensions granted by the FCC in 2005, a number of fines and other penalties have been levied recently against noncompliant VoIP carriers. State and local agencies also are involved in enforcement and follow their own enforcement regimes.

EU and EU Member Sates' eCommunications Regulations

In April 2002, a European Union (EU) regulatory framework for electronic communications was adopted and went into effect in July 2003. In its intro-

duction to the framework, the EU Information Society Directorate-General explains:

> The convergence of the telecommunications, media and information technology sectors demands a single regulatory framework that covers all transmission networks and services. The EU regulatory framework addresses all communications infrastructure in a coherent way, but does not cover the content of services delivered over and through those networks and services. There are five different directives: the Framework Directive6 (2002/21/EC) and four specific directives, being the Authorisation Directive7 (2002/20/EC), the Access Directive8 (2002/19/EC), the Universal Service Directive9 (2002/22/EC) and the Privacy Directive10 (2002/58/EC). In addition, the Competition Directive (2002/77/EC) applies.
>
> The objectives set out in the EU regulatory framework are:
>
> –To promote competition by fostering innovation, liberalising markets and simplifying market entry;
>
> –To promote the single European market and;
>
> –To promote the interest of citizens.
>
> All Member States are required to implement the EU framework in their national law. The framework lays down the role of Member States and national regulatory authorities, the rights and obligations for market players, and the rights of users of electronic communications networks and services. In addition, Member States may take measures justified on the grounds of public health and public security as set out in the EC Treaty, for example by imposing requirements for legal interception or critical infrastructure protection, and such measures are not covered by the EU regulatory framework.

What many non-EU readers may not realize is the degree to which EU regulations (particularly privacy regulations) will force specific policy and practice outside of the EU. Its effects (particularly with respect to VoIP) will be briefly discussed in this final section. At the present, the EU IS Directorate-General is soliciting public comment on VoIP policy for input into a future regulatory regime for VoIP.

EU Regulatory Basics

Seven active EU Communications Directives with potential VoIP Implications that your organization may need to consider are listed here. Note that each of these directives is required to be expressed within the law for each EU nation, which may have additional regulatory measures of their own. In some cases (such as with the German Data Privacy Law) national laws are considerably more restrictive than the overall EU directive. Here is the list:

- **Directive 97/66/EC** Processing of personal data and protection of privacy (up to October 30, 2003)
- **Directive 2002/58/EC** Privacy and electronic communications (from October 31, 2003 onward)
- **Directive 2002/19/EC** Access and interconnection
- **Directive 2002/20/EC** Authorization of electronic communications networks and services (i.e., allocation of radio frequencies)
- **Directive 2002/21/EC** Common regulatory framework
- **Directive 2002/22/EC** Universal service and users' rights relating to electronic communications networks and services
- **Directive 2002/77/EC** On competition in the markets for electronic communications services

Although VoIP is directly or indirectly addressed in each of these, this section will focus on the only VoIP security concern addressed in the EU electronic communications regulations, namely the privacy and electronic communications directive.

Direct from the Regulations

Central to understanding EU privacy laws are the broad definitions used for personal data and its processing. We will focus on Directive 2002/58/EC since it establishes the minimum go-forward privacy framework for EU member states going forward with respect to electronic communications services. Note that despite specific references to ISDN and mobile networks in this directive, subsequent guidance from the EU IS Directorate-General has indicated that VoIP services will be expected to comply with this directive as well. Here is the relevant text within the directive:

> **Article 3 - Services concerned**
>
> 1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.
>
> 2. Articles 8 (www.bild.net/dataprEU1.htm#HD_NM_8), 9 (www.bild.net/dataprEU1.htm#HD_NM_9) and 10 (www.bild.net/dataprEU1.htm#HD_NM_10) shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.
>
> 3. Cases where it would be technically impossible or require a disproportionate investment to fulfill the requirements of Articles 8 (www.bild.net/dataprEU1.htm#HD_NM_8), 9 (www.bild.net/dataprEU1.htm#HD_NM_9) and 10 (www.bild.net/dataprEU1.htm#HD_NM_10) shall be notified to the Commission by the Member States.
>
> **Article 4 - Security**

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

Article 5 - Confidentiality of the communications

Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized.

Article 8 - Presentation and restriction of calling and connected line identification

1. Where presentation of calling-line identification is offered, the calling user must have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling-line identification is offered, the called subscriber must have the possibility via a simple means, free of charge for reasonable use of this function, to prevent the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the called subscriber must have the possibility via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9 - Exceptions

Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification:

(a) on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls; in this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organizations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10 - Automatic call forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

Article 11 - Directories of subscribers

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this is applicable linguistically.

2. Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of this right.

3. Member States may limit the application of this Article to subscribers who are natural persons.

Article 12 - Unsolicited calls

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing, by means other than those referred to in paragraph 1, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, the choice between these options to be determined by national legislation.

3. Member States may limit the application of paragraphs 1 and 2 to subscribers who are natural persons.

What an EU Data Privacy Consultant Will Tell You

In addition to the EU eCommunications framework, you may need to worry about data contained in corporate directories. Any collection, use, disclosure, or other processing about an individual that resides within the EU requires careful handling that goes far beyond that prescribed by the privacy provisions contained in U.S. law for GLBA or HIPAA with their associated regulations. This can create legal issues within the EU regardless of whether the individuals are employees, consumers, suppliers, or other legal entities. Cross-border data transfer restrictions may prohibit the transfer of such data to a jurisdiction without an equivalent data protection regime. For export to the United States, the FTC provides a Safe Harbor program that can meet this test, but there are significant tradeoffs to taking this route so you should consult with an EU data privacy expert before committing to this route. In many respects, addressing EU data privacy rules is more art than science.

Tools & Traps…

Core EU-Compliance Issues for IP Communications Systems

EU member countries do have important differences in data privacy rules, so be sure to consult appropriate experts for the countries in which you operate. Rules for VoIP as an eCommunication service may vary somewhat from the data-centric rules used for data applications. Unless your organization is a vendor or carrier, most other EU compliance issues will be addressed by purchasing equipment and services approved for sale within the EU.

EU Compliance and Enforcement

Within the EU and member states, compliance and enforcement happens at several levels. Some member states, such as Germany, have enforcement of privacy and electronic communication laws at a more local level as well as on a national basis. Decisions at the national level can be appealed at the EU level, and critical precedents are often set at this level.

No Certification

In general, the EU and member countries do not have certification processes for the privacy and eCommunications regulation.

Enforcement Process and Penalties

Data privacy fines can be stiff within the EU and its member states, though they do vary considerably by jurisdiction.

Summary

Unfortunately, the trend is clearly heading toward *more* regulation, not less. By the time you read this, another VoIP-affecting regulation will have been enacted in some part of the world. In the United States, regulations like California's SB 1386 (which forces security breach notifications or end-to-end encryption of Social Security and credit card numbers and could impact you if you operate a VoIP call center) are being considered at the U.S. federal level and by other countries around the world.

Solutions Fast Track

SOX: Sarbanes-Oxley Act

- ☑ Focus on any internal financial controls that may exist within your VoIP system.
- ☑ Consider applicability of cross-IT security standards to your VoIP system.

GLBA: Gramm-Leach-Bliley Act

- ☑ Make sure that your VoIP system is included in risk management processes for GLBA compliance plans.
- ☑ Consider FDIC VoIP recommendations when evaluating GLBA compliance.
- ☑ Document VoIP system compliance as you would any other part of the data infrastructure.

HIPAA: Health Insurance Portability and Accountability Act

- ☑ Pay special attention to VoIP components or adjuncts that record calls or conversations.

- ☑ Don't forget Interactive Voice Response (IVR) systems when evaluating HIPAA impact to VoIP systems.
- ☑ Ensure you have complete documentation per HIPAA requirements.

CALEA: Communications Assistance for Law Enforcement Act

- ☑ Don't assume you're not considered a carrier (or substantial replacement) for CALEA purposes—if you provide communication services to the public in any form the new rules may apply to you too.
- ☑ Find an appropriate technical standard and drive your software or equipment vendor toward compliance.
- ☑ Be sure to file all necessary paperwork with the FCC.

E911: Enhanced 911 and Related Regulations

- ☑ Be sure to investigate and comply with local regulations that mandate ALI support, even if you're not a carrier.
- ☑ If you are a VoIP carrier, you must provide E911 services or risk substantial penalties or fines.

EU and EU Member States' eCommunications Regulations

- ☑ Remember that VoIP services are treated equally with other communications services in the eCommunications regulatory framework.
- ☑ Pay close heed to data privacy regulations and any export of private data.
- ☑ Remember to investigate privacy and other regulatory policies at the national level as well.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Where can I go for more information about SOX compliance and SOX-related resources?

A: The Sarbanes-Oxley Compliance Journal has a good summary of their articles at at www.s-ox.com/resources/.
The Securities and Exchange Commision has a SOX page at www.sec.gov/spotlight/sarbanes-oxley.htm.
The Public Company Accounting Oversight Board operates www.pcaobus.org with audit-related information.

Q: How do information security frameworks like ISO 17799, COSO, and CoBIT relate to SOX?

A: The Cyber Security Industy Alliance has published an excellent report on this topic, "IT Security and Sarbanes-Oxley Compliance: Conference Summary of Findings and Conclusions," which can be found online at www.csialliance.org/resources/pdfs/CSIA_PostSox_Summit_Report.pdf.

Q: Where can I go to learn more details about HIPAA?

A: The HHS/OCR Web site is excellent. Go to www.hhs.gov/ocr/hipaa/. Another excellent site with a large FAQ is the CMS site at http://cms.hhs.gov/HIPAAGenInfo/ (click on the "Questions" link on the top menu bar to get there).

Q: Where can I go to learn more details about CALEA?

A: 1. The FBI CALEA Implementation Unit runs a very well designed, comprehensive Web site—www.AskCALEA.com—aimed at telecommunications carriers and law enforcement personnel.
2. The FCC also runs an equally comprehensive CALEA site focusing on

FCC regulations at www.fcc.gov/calea/ (and within the IATD sub-site at www.fcc.gov/wcb/iatd/calea.html—note that while they look similar, there are differences between the two).
3. TIA standards and related CALEA information can be found at www.tiaonline.org/standards/CALEA_JEM.
4. For a privacy-advocate's point of view, try the Electronic Frontier Foundation's CALEA pages at www.eff.org/Privacy/Surveillance/CALEA/ or the Electronic Privacy Information Center (EPIC) at www.epic.org/privacy/wiretap/.

Q: If my organization successfully files a Section 109 (or 107) petition with the FCC to avoid implementing CALEA requirements within our current VoIP systems, will that make us exempt from CALEA?

A: The FCC has stated that "a carrier's obligation to comply with all CALEA requirements is only deferred by FCC grant of a section 109 (or section 107) petition. No qualifying carrier is exempt from CALEA." Any change in equipment or services could require full CALEA compliance in the future.

Q: What does CALEA require from the carrier if encryption is used?

A: If a carrier possesses the keying material, it must decrypt the communications when a lawful interception order is presented, but if the encryption is not provided by the carrier then it has no responsibility for decryption of the target communications.

Q: Where can I find more help on E911 and VoIP?

A: Start with www.fcc.gov/911/ for the basics. The National Emergency Number Association (NENA) is involved with E911 and VoIP at several levels, including the creation of advanced standards for PSAP and VoIP—see www.nena.org for details. Other helpful information about VoIP and E911 can be found at www.voip911.gov.

Q: Where can I go for more details about EU and EU member countries' electronic communications and data privacy regulations?

A: A good place to start is http://europa.eu.int/information_society/policy.

Index

Numbers

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z