IBM Smart Business
Unified Communications
and IP Telephony

Learn how to deploy IP Telephony by example with practical scenarios

Increase productivity with centralized collaboration

Unleash the power of Unified Communications

Hernando Bedoya
Laurent Itin
Fabrizio Picca
Chris Snowdon

ibm.com/redbooks
Note: Before using this information and the product it supports, read the information in “Notices” on page vii.
## Contents

Notices ................................................................. vii
Trademarks ............................................................. viii

Preface ................................................................. ix
The team that wrote this paper ........................................... ix
Become a published author .............................................. x
Comments welcome ..................................................... xi

Chapter 1. Overview of IBM Smart Business and IBM Smart Cube .... 1
  1.1 IBM Smart Business .................................................. 2
  1.1.1 IBM Smart Market ................................................ 3
  1.1.2 IBM Smart Cube .................................................. 3
  1.1.3 IBM Smart Desk .................................................. 4
  1.1.4 IBM Smart Support ............................................... 5
  1.2 Services provided by IBM Smart Cube .......................... 6
  1.2.1 E-mail and calendars ............................................ 7
  1.2.2 E-Mail and calendars via Web Access ......................... 8
  1.2.3 Instant messaging ............................................... 8
  1.2.4 Office Productivity Applications ............................ 9
  1.2.5 Backup and recovery .......................................... 9
  1.2.6 Print server .................................................... 10
  1.2.7 File Server ...................................................... 10
  1.2.8 User management .............................................. 11
  1.2.9 Smart Business home page ................................. 11
  1.2.10 Private intranet .............................................. 12
  1.2.11 Public Internet website ..................................... 12
  1.3 Summary .................................................................. 12

Chapter 2. Overview of Voice over IP Technology in IBM Smart Business .... 13
  2.1 Telephony overview .................................................. 14
    2.1.1 Plain old telephone service (POTS) ....................... 14
    2.1.2 Integrated Services Digital Network (ISDN) .......... 14
    2.1.3 Private branch exchange (PBX) ........................... 14
    2.1.4 The dial plan ................................................. 14
  2.2 Voice over IP overview ............................................ 16
    2.2.1 Advantages of using VoIP ................................ 16
    2.2.2 Session Initiation Protocol (SIP) and Real-Time Transport Protocol (RTP) .... 17
  2.3 VoIP in IBM Smart Business ..................................... 20
    2.3.1 Digium Asterisk for Smart Cube ....................... 20
    2.3.2 Nortel SCS 2.0 ............................................. 20
  2.4 Summary .................................................................. 20

Chapter 3. Network considerations ........................................ 21
  3.1 Network analysis .................................................... 22
    3.1.1 Network topology ............................................ 22
    3.1.2 Public and private access .................................. 26
    3.1.3 Security issues ............................................... 27
  3.2 Network Infrastructure consideration .......................... 30
    3.2.1 Hardware and cabling ..................................... 31
<table>
<thead>
<tr>
<th>Chapter 6. Deploy and configure IBM Smart Business and Nortel SCS 2.0 on IBM i</th>
<th>121</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Overview of IBM Smart Business on IBM i</td>
<td>122</td>
</tr>
<tr>
<td>6.2 Pre-installation tasks</td>
<td>123</td>
</tr>
<tr>
<td>6.2.1 Network preparation</td>
<td>123</td>
</tr>
<tr>
<td>6.2.2 Connect the power system to your network</td>
<td>124</td>
</tr>
<tr>
<td>6.2.3 Preparing the administration PC</td>
<td>125</td>
</tr>
<tr>
<td>6.2.4 Install IBM i Access for Windows and configure operations console</td>
<td>125</td>
</tr>
<tr>
<td>6.3 Setting up the IBM Smart Business environment on IBM i</td>
<td>126</td>
</tr>
<tr>
<td>6.4 The Smart Business Administration Panel</td>
<td>132</td>
</tr>
<tr>
<td>6.5 Basic SCS 2.0 configuration</td>
<td>133</td>
</tr>
<tr>
<td>6.5.1 Nortel SCS 2.0 EULA</td>
<td>134</td>
</tr>
<tr>
<td>6.5.2 Licensing the SCS 2.0 system</td>
<td>135</td>
</tr>
<tr>
<td>6.5.3 Dial plans and call routing</td>
<td>136</td>
</tr>
<tr>
<td>6.5.4 User groups</td>
<td>138</td>
</tr>
<tr>
<td>6.5.5 Provisioning users</td>
<td>139</td>
</tr>
<tr>
<td>6.5.6 Adding phones</td>
<td>141</td>
</tr>
<tr>
<td>6.6 Advanced SCS 2.0 configuration</td>
<td>143</td>
</tr>
<tr>
<td>6.6.1 AutoAttendant</td>
<td>144</td>
</tr>
<tr>
<td>6.6.2 Hunt groups</td>
<td>146</td>
</tr>
</tbody>
</table>
Chapter 7. Differences between x86 and IBM i for VoIP

7.1 Telephony offered ........................................ 159
7.2 System architecture ........................................ 160
  7.2.1 x86 .................................................. 160
  7.2.2 IBM i .................................................. 160

Chapter 8. Configuring and deploying Voice over IP (VoIP) hardware for x86

8.1 Attaching handsets (SIP phones) .................................. 162
8.2 Attaching analog phones using FXS gateways ......................... 164
8.3 Attaching FXO gateway devices ................................... 167
8.4 Working with telephones and adapters that are not IBM verified ........ 168

Chapter 9. Unified communications configuration

9.1 Unified communications overview ................................ 170
9.2 Overview of interaction between IBM Smart Business Phone and Sametime voice ........ 170
9.3 Configuring the IBM Smart Business Phone and Sametime voice on x86 ............ 171
   9.3.1 Requirements ......................................... 171
   9.3.2 Installation and configuration ................................ 172
9.4 Using the IBM Smart Business Phone and Sametime voice ................. 175
   9.4.1 Place a call ............................................ 175
   9.4.2 Call transfer .......................................... 175
   9.4.3 Click-to-call ........................................... 177
   9.4.4 Receive a call: Basic configuration ......................... 180
   9.4.5 Conference up to five participants ........................ 180
   9.4.6 Record a call ........................................... 183
   9.4.7 Advanced usage of the IBM Lotus Sametime voice functionality ........... 183
9.5 Configuring the IBM Smart Business Phone on IBM I .................... 187
   9.5.1 Requirements ......................................... 188
   9.5.2 Installation and configuration of the IBM Smart Business Phone ............ 188
9.6 Using the IBM Smart Business Phone with IBM i ....................... 192
   9.6.1 Place a call ............................................ 193
   9.6.2 Receive a call .......................................... 193
   9.6.3 Conference up to five participants ........................ 194
   9.6.4 Record a call ........................................... 194

Chapter 10. Troubleshooting VoIP configuration

10.1 IBM Smart Cube troubleshooting (x86) ................................ 196
   10.1.1 My power light is not on ................................ 196
   10.1.2 The amber system-error light is on ....................... 196
   10.1.3 I do not have my IBM Smart Desk V1.1.0 CD ............. 196
   10.1.4 I need help configuring a new printer ................... 196
   10.1.5 I need help recovering my system ....................... 197
   10.1.6 I need help accessing the Linux command line ........... 198
   10.1.7 I need help accessing Linux files ....................... 198
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.8</td>
<td>I must rediscover my IBM Smart Cube</td>
</tr>
<tr>
<td>10.2</td>
<td>IBM Smart Cube troubleshooting (IBM i)</td>
</tr>
<tr>
<td>10.2.1</td>
<td>I do not have my IBM Smart Desk V1.1.0 CD.</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Operations Console does not find my system.</td>
</tr>
<tr>
<td>10.2.3</td>
<td>The IBM Smart Business Setup Wizard did not find my IBM Smart Cube</td>
</tr>
<tr>
<td>10.2.4</td>
<td>The IBM i Access for Windows DVD was not included in my order</td>
</tr>
<tr>
<td>10.2.5</td>
<td>Manage your IBM Smart Cube profiles.</td>
</tr>
<tr>
<td>10.2.6</td>
<td>Find the serial number of my IBM Smart Cube</td>
</tr>
<tr>
<td>10.2.7</td>
<td>Verify that your network is set up properly</td>
</tr>
<tr>
<td>10.2.8</td>
<td>Rediscover my network.</td>
</tr>
<tr>
<td>10.2.9</td>
<td>Run a CL command from IBM i Access for Windows</td>
</tr>
<tr>
<td>10.3</td>
<td>IP telephone call troubleshooting</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Poor quality calls.</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Dropped/unsuccesful calls</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Configuration issue with IBM Smart Business Phone for IBM i.</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Setting up IBM i for Nortel SCS 2.0</td>
</tr>
<tr>
<td>Creating the Ethernet line description on IBM i</td>
<td>208</td>
</tr>
<tr>
<td>Enabling datagram forwarding</td>
<td>210</td>
</tr>
<tr>
<td>Implementing proxy ARP on IBM i</td>
<td>210</td>
</tr>
<tr>
<td>Creating a System Service Tools (SST) profile for Console Access</td>
<td>214</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Installing Nortel SCS 2.0</td>
</tr>
<tr>
<td>Connecting a virtual console</td>
<td>218</td>
</tr>
<tr>
<td>Activating the SCS 2.0 LPAR</td>
<td>219</td>
</tr>
<tr>
<td>Reconfiguring and restarting the SCS 2.0 LPAR</td>
<td>221</td>
</tr>
<tr>
<td>Initial configuration of Nortel SCS 2.0</td>
<td>222</td>
</tr>
</tbody>
</table>

**Related publications**

- IBM Redbooks publication | 229
- Online resources | 229
- How to get IBM Redbooks publications | 229
- Help from IBM | 229
This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (© or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

| AS/400® | Lotus® | Sametime® |
| DB2® | Notes® | Symphony™ |
| Domino® | Passport Advantage® | System i® |
| i5/OS® | POWER® | Tivoli® |
| IBM® | Redbooks® | |
| Lotus Notes® | Redbooks (logo) © | |

The following terms are trademarks of other companies:

Adobe, and Portable Document Format (PDF) are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

SUSE, the Novell logo, and the N logo are registered trademarks of Novell, Inc. in the United States and other countries.

eXchange, Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows Vista, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.
Preface

Small and medium-sized businesses deserve more from IT—more choice, less complexity, better integration, and comprehensive support. IBM® saw an opportunity to rewrite the rules of IT for these businesses by partnering with world-class solution providers and open source developers and by bringing together its best technologies to create IBM Smart Business. The premise of IBM Smart Business is to make IT invisible so that business owners can concentrate on growth and serving their customers. Solutions that can increase operational efficiency, improve customer satisfaction, reduce working capital and many other business issues from leaders in the field such as Infor, Cincom, Kronos, Digium, Nortel, and others are listed on IBM Smart Market. With this approach, IBM has made IT effortless and made core business applications available where they were either too complex or costly for many companies in the past. One of the solutions where this radically simple approach pays big dividends is in the area of Unified Communications. With IBM Smart Business, you get a complete solution up and running quickly and if there is ever a problem, IBM will take care of it. Now you can enjoy the benefits of Unified Communications (improved productivity, higher customer satisfaction, and improved collaboration with suppliers) without the hassle of getting it all to work or the worry of where to turn if you need help. IBM makes Unified Communications smart for your business.

In this IBM Redbooks® publication we provide a complete overview the IBM Smart Business solution, from a description of the services to an installation guide, and a step-by-step scenario that describes how to configure, deploy, and manage the Voice over IP (VoIP) element of the IBM Smart Cube.

The team that wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Rochester Center.

Hernando Bedoya is an IT Specialist at the IBM ITSO in Rochester, Minnesota. He writes extensively and teaches IBM classes worldwide in all areas of DB2® for i5/OS®. Before joining the ITSO more than seven years ago, he worked for IBM Colombia as an IBM AS/400® IT Specialist doing presales support for the Andean countries. He has 24 years of experience in the computing field and has taught database classes in Colombian universities. He holds a master’s degree in Computer Science from EAFIT, Colombia. His areas of expertise are database technology, application development, and high availability.

Laurent Itin joined IBM in 2003 as an IT Specialist. Laurent started in the Remote Access Technology area before he began with voice over IP IBM internal implementation projects. In 2006, Laurent lead a 2-year VoIP Softphone deployment project in IBM Europe. His current focus is on Collaboration and Communication technologies, leading the Lotus® Notes® 8 client and Lotus Symphony™ deployment project in IBM Europe. Laurent graduated from a Swiss Information Technology vocational school.
**Fabrizio Picca** is a Unified Collaboration and Communications Solutions Designer for IBM Global Technology Service Italy. His main focus is integration issues of different communication platforms (Messaging, IP Telephony, videoconferencing) for large vendors such as Lotus, Microsoft®, Cisco, Radvision, and Polycom. Before joining IBM he mainly worked as developer on different languages/platforms. He holds a degree in Computer Science (focused on Digital Communication) from Università degli Studi di Milano, Italy.

**Chris Snowdon** is a Systems Engineer at Typex, an IBM Premier Business Partner based in Newcastle, England. Typex hold further partnerships with 3Com and Nortel for Unified Communications and Collaboration on IBM i and with IBM Lotus and is a founding member of TeamUC, a worldwide alliance of IBM UC Business Partners (more details at [http://www.teamuc.org](http://www.teamuc.org)). Chris is a 3Com-certified VCX on System i® Expert with a strong background in networking and IP Telephony on both POWER® and x86 platforms. He holds an honors degree in Network Computing from the University of Sunderland in England. Chris can be reached at info@typex.com.

Thanks to the following people for their contributions to this project:

Jim Cook  
Thomas Gray  
James Hansen  
Joanna Pohl-Miszczyk  
International Technical Support Organization, Rochester Center

Belinda C. Herrison  
John D. Gresset  
Daniel Vega  
Daniel J. Strauss  
Mike D. Gordon  
Charlie Quigg  
Belinda C. Herrison  
Fant Steele  
Keith D. Cramer  
Katherine K. Richardson  
George Weaver  
IBM Rochester

---

**Become a published author**

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.
Find out more about the residency program, browse the residency index, and apply online at:
ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks in one of the following ways:

- Use the online Contact us review Redbooks form found at:
  ibm.com/redbooks

- Send your comments in an e-mail to:
  redbooks@us.ibm.com

- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400
Overview of IBM Smart Business and IBM Smart Cube

The first part of this chapter provides a general overview of what IBM Smart Business is and what its components are. We cover the following topics:

- “IBM Smart Business” on page 2
- “IBM Smart Market” on page 3
- “IBM Smart Cube” on page 3
- “IBM Smart Desk” on page 4
- “IBM Smart Support” on page 5

The second part of this chapter focuses on one main component of the IBM Smart Business, IBM Smart Cube. The applications and services delivered with the IBM Smart Cube are described in the following sections:

- “E-mail and calendars” on page 7 and “E-Mail and calendars via Web Access” on page 8
- “Instant messaging” on page 8
- “Office Productivity Applications” on page 9
- “Backup and recovery” on page 9
- “Print server” on page 10 and “File Server” on page 10
- “User management” on page 11
- “Smart Business home page” on page 11
- “Private intranet” on page 12 and “Public Internet website” on page 12
1.1 IBM Smart Business

IBM Smart Business is an IBM initiative in concert with independent application software vendors/providers across the world that aims to radically simplify the way small and medium-sized businesses buy, manage, and build upon their IT solutions. IBM Smart Business delivers an integrated business solution (hardware, software, business applications) that is pre-integrated and easy to install, run, and maintain. Additionally, IBM Smart Business provides a services platform where clients can manage and grow their IT.

Figure 1-1 provides an overview of the four components of the IBM Smart Business. They are explained in more detailed in the following sections.
1.1.1 IBM Smart Market

Before IBM Smart Market (Figure 1-2), businesses looked for new technology online by using Web search engines like Google, or they heard about new solutions by word-of-mouth or print advertising. Now businesses have access to a Web-based community and solutions marketplace, providing a single source where customers can:

- Connect with independent software vendors (ISVs), partners, and each other.
- Browse IBM and ISV applications.
- View and learn from user ratings.
- Receive business and technical advice.

More information about the IBM Smart Market is available on:
http://www.ibm.com/smartmarket

1.1.2 IBM Smart Cube

Before IBM Smart Cube, businesses had to wade through stacks of CDs, manuals, patches, wires, and cords in order to set up and install new technology. A typical system for a small or medium-sized business could require as many as 17 manuals with 1,600 pages of text to load all programs onto a single system.
Now with IBM Smart Cube, businesses have a complete application platform with all server hardware and software needed, with a minimum of manuals required. In a few easy steps, businesses can be up and running with a complete IT solution to run their business, including the operating system, integrated middleware, and back-office functionality including e-mail, calendaring, and backup and recovery, combined with the business application that they acquired, all with integrated fix and security management as well as integrated problem determination and reporting.

Services provided by the IBM Smart Cube are described in more detail in 1.2, “Services provided by IBM Smart Cube” on page 6.

There are several different options available for the server platform. In general, which server platform is chosen depends on the needs of the applications chosen by the customer. Today, server platform options include x86 tower or POWER, as shown on Figure 1-3. More server platform options will be added over time as they are needed.

<table>
<thead>
<tr>
<th>IBM Smart Business Software: Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>x86</strong></td>
</tr>
<tr>
<td>- SUSE Linux Enterprise</td>
</tr>
<tr>
<td>Server 10 SP2</td>
</tr>
<tr>
<td><strong>POWER</strong></td>
</tr>
<tr>
<td>- IBM i operating system</td>
</tr>
<tr>
<td>Version 6 Release 1</td>
</tr>
</tbody>
</table>

*Figure 1-3  IBM Smart Cube operating systems: SUSE® Linux® running on x86 and IBM i on POWER

### 1.1.3 IBM Smart Desk

Before IBM Smart Desk, managing and maintaining IT for a business was complex, expensive, and time intensive. To safeguard a company’s critical business data from online threats such as hacking and viruses, and the liabilities of loss of sensitive data, manual updates to security patches and backup and recovery were required. As a business grew, adding technology assets and capabilities for new employees meant creating new e-mail accounts and configuring printers and phones.

Now businesses can outsource the management of their IT to a trusted vendor: IBM. Solutions are always connected for autonomic management, updates, and new application deployment through an easy-to-use dashboard. Businesses can set up their system to allow updates to occur automatically or on demand through subscription-based services. With as little as a few easy clicks, employees can have access to messaging services like e-mail and instant messaging, printers, Telephony services (to be purchased and installed separately), and the key applications that they need to complete their job on a daily basis.
The IBM Smart Desk is spread into two parts dependent on the users’ access rights, the administrator view and the user view. End users are required to install the IBM Smart Business Quick Start application in order to get started using the IBM Smart Business environment. By doing so four applications are made available, as shown in the user view in Figure 1-4. Users are able to access the users’ directory, change their passwords, add printers, and access the software catalogue to install additional products.

![Figure 1-4 IBM Smart Desk overview: Administrator and end user view](image)

Administrators are required to install the so-called IBM Smart Desk software package, which, in addition to the linked applications shown in Figure 1-4 under the Administrator view, installs three more applications:

- **Setup Wizard:** Initiates the first setup of a new IBM Smart Cube
- **Application Installer:** Installs new applications acquired though the IBM Smart Marked
- **Network Wizard:** Updates an existing IBM Smart Cube network configuration

All of these applications are accessible through `Start → Programs → IBM Smart Desk`.

### 1.1.4 IBM Smart Support

IBM Smart Business offers a single point of contact (SPOC) for solution-level support, allowing you to stay focused on managing the business rather than managing your equipment. The end-to-end support experience allows the customer to have fast, easy service through IBM Smart Desktop and online assistance. Support for all applications, including those from non-IBM vendors, are part of the complete business solutions on IBM Smart Market. Online communities allow customers to read blogs, ask questions in forums, and contribute to wikis, in addition to accessing knowledge bases maintained by IBM. IBM Global Technology Services, IBM Global Finance, and other third-party service partners are available to promote and ensure comprehensive business value, help reduce costs and
technical complexity, increase productivity, and provide support—all with a single click of the IBM Smart Market Web portal. See Figure 1-5.

1.2 Services provided by IBM Smart Cube

This section provides an overview of the many applications and services that are installed on IBM Smart Cube during the initial setup.
1.2.1 E-mail and calendars

IBM Lotus Domino® provides the product information management applications (PIM). This includes mail, the calendar, a to do list, contacts, and others (Figure 1-6). Domino ISV applications will be deployed on the same Domino server that is running the PIM applications. The IBM Smart Business Lotus client applications include Lotus Notes and Domino Web Access. These are used by end users to access the Domino server. The IBM Smart Business client applications help your organization access information more easily, work more productively, and collaborate more effectively. Domino Admin is also included for administration of the Domino server. Domino Designer is not included but can be purchased as an upgrade option.

Figure 1-6   Lotus Notes 8 calendar and mail

More information about Lotus Notes 8 is available at:
1.2.2 E-Mail and calendars via Web Access

Domino Web Access (DWA) is the flexible, high-function Web-browser-based client option that provides security-rich messaging and collaboration capabilities online and offline. The HTTP server for the primary Domino server uses a redirector database that only allows an end user to enter his name and password on the browser, and then redirector looks up the user's mail file and gives him access to his mail. See Figure 1-7.

![Lotus Domino Web Access: Login and redirect, in box in browser window](image)

Figure 1-7 Lotus Domino Web Access: Login and redirect, in box in browser window

1.2.3 Instant messaging

The IBM Lotus Sametime® server, which provides the instant messaging capabilities, features multi-way chat, time stamps, spell check, chat history, and emoticons (Figure 1-8). Sametime Connect is the client application that is used to access the Sametime server. Included with Sametime Connect is an Integrated IP Telephony soft phone for integrated IP Telephony with Sametime.

Refer to Chapter 9, “Unified communications configuration” on page 169, to set up and configure Sametime to work with a VoIP telephony environment.

![Lotus Sametime multi-way chat and announcement](image)

Figure 1-8 Lotus Sametime multi-way chat and announcement
1.2.4 Office Productivity Applications

IBM Lotus Symphony is a richly featured set of productivity tools that are intuitive and easy to use. There are three applications that comprise Lotus Symphony:

- Lotus Symphony Documents
- Lotus Symphony Spreadsheets
- Lotus Symphony Presentations

Using IBM Lotus Symphony Documents, Presentations, and Spreadsheets (Figure 1-9) allows you to create, view, edit, and export files in a variety of formats, including those of existing Microsoft Office documents. You can also export Symphony content as Adobe® PDF documents.

Lotus Notes users can use the integrated version of Lotus Symphony, which is built into the Lotus Notes 8 client user interface.

![IBM Lotus Symphony Documents, IBM Lotus Symphony Presentations, IBM Lotus Symphony Spreadsheets](image)

Figure 1-9  Lotus Symphony Documents, Presentations, and Spreadsheets

More information about IBM Lotus Symphony is available at:

http://symphony.lotus.com

1.2.5 Backup and recovery

The backup and restore function is designed to provide a seamless solution for backup and recovery of files, databases, as well as the entire system if the need arises. By design, the backup and recovery process works out of the box with default settings for daily backups of the entire system. Tivoli® Data Protection is implemented to support the ability to back up Domino data while Domino is active. Each system is shipped with a backup of the initial system configuration.

The backup process implements an incremental backup scheme. In this scheme a full system backup is performed for each media set and subsequent backups on the media set only contain files that have been changed or added since the previous backup. This allows for restores to be performed against any backup date and time by applying the full backup and then any subsequent checkpoint backups up to the date/time selected for the restore.

**Note:** The backup process does not allow for the exclusion of any data from the backup, and all IBM Lotus Domino files are backed up.

**Note:** The IBM i on Power solution would need to use either Backup and Recovery Media Services (BRMS) or the normal IBM i save/restore capabilities.
1.2.6 Print server

Printing and print serving are vital parts of the overall IBM Smart Business solution. All applications that reside on an IBM Smart Cube can use network-attached and USB-attached printers. In addition, workstations that are connected to IBM Smart Cubes can also use these network-attached and physically attached printers.

The default IBM Smart Cube setup configures the system as a print server. IBM Smart Business supports both direct-attached printers (via USB connection) and network-attached printers. Printers attached to the USB port on the IBM Smart Cube, as well as printers attached to the same LAN segment as the IBM Smart Cube, may be automatically detected and configured while printers on a different LAN segment from the IBM Smart Cube must be configured manually. Go to the IBM Smart Business software knowledge base and search for the article "Will my printer work with IBM Smart Business" to determine whether your printer will work.

The Administrator panel provides basic administration tasks such as:

- The ability to view what is being printed
- Putting a printer's queue on hold
- Deleting print jobs
- Holding individual print jobs
- Deleting printer definitions

A more advanced printer configuration, such as changing the paper size or duplex action of a printer and configuration of printers on different LAN segments, is performed through the Common UNIX® Print System (CUPS).

Windows® drivers for the IBM Smart Business supported printers are made available to client workstations through the IBM Smart Business printer setup utility, which is part of the IBM Smart Business Quick Start application. Once a client has successfully mapped an IBM Smart Business printer it can print to that printer in the same way that the client would print to a locally attached printer.

Note: There is no direct print support on the IBM i Power solution. The IBM i print scheme is available to these customers.

1.2.7 File Server

The file server is configured on IBM Smart Business during the initial system setup. The firewall ports are configured to enable access to the file server by internal users and it is started automatically when the IBM Smart Cube starts.

The IBM Smart Cube provides a pre-configured file sharing environment. When the IBM Smart Business administrator adds a person to the IBM Smart Business directory, a private and public shared directory are created for each user. All users can save and access files in the public directories.

Administrators can create more shared directories and modify the default configuration of the file server using the Suse Linux administrator tool Yast or editing the Samba configuration file for the file and print server, located at /etc/samba/smb.conf.
In order to ease access to the preconfigured shares users are recommended to install the IBM Smart Business Drive Mapper from the IBM Smart Business Users Programs Catalog. The IBM Smart Business Users Programs Catalog can be accessed by opening the IBM Smart Business Launch shortcut on the computer's desktop and clicking User Programs Catalog (Figure 1-10).

![IBM Smart Business User Programs Catalog](image)

**Figure 1-10** IBM Smart Business User Programs Catalog

### 1.2.8 User management

In order to be able to use all the services provided by the IBM Smart Cube a user must be created. In 4.3, “User management” on page 52, we provides step-by-step instructions for creating a new user on the IBM Smart Cube and assigning available services.

### 1.2.9 Smart Business home page

The Smart Business home page is installed by default when you first set up your system. It runs on the private intranet website and can be accessed at http://your-system/. The home page is a wiki, which is a special type of website that can easily be customized for your business. Everyone in your company can read the wiki and use the links. Only the administrator can edit, delete, and modify this site to personalize it for your company. This site is based on technology from DokuWiki, which is a standards-compliant, easy-to-use wiki, mainly aimed at creating documentation of any kind. It is targeted at developer teams, workgroups, and small companies. It has a simple but powerful syntax, which makes sure that the datafiles remain readable outside the wiki and eases the creation of structured texts. All data is stored in plain text files. No database is required.
The links on the wiki can easily be updated online by any administrator of the IBM Smart Cube. Log in and enter your user ID and password, then click the **Customize this page** button, as shown on Figure 1-11, to modify the wiki. You can also change the administrative settings by clicking the **Admin** button on the lower right of the page.

![DokuWiki on the IBM Smart Cube](image)

**Figure 1-11  DokuWiki on the IBM Smart Cube**

### 1.2.10 Private intranet

During the initial setup of the IBM Smart Cube, a Web server is installed for your company's intranet site. During the install and configuration process, a home page is created that can be edited by the administrator.


### 1.2.11 Public Internet website

The IBM Smart Cube can also host an external facing website. Detailed step-by-step instructions are described in 4.5, “Public Internet website” on page 66.

### 1.3 Summary

In this chapter we provided you with a general overview of the IBM Smart Business and its four major components, which are:

- IBM Smart Market
- IBM Smart Cube
- IBM Smart Desk
- IBM Smart Support

Then we though all the services that are available to you on the IBM Smart Cube after the initial install.
Overview of Voice over IP Technology in IBM Smart Business

In this chapter we provide a brief introduction to telephony technologies and concepts, as well as an overview of the Voice over IP (VoIP) technology in IBM Smart Business. This chapter is not intended to give detailed technical explanations.

In this chapter we discuss:

- “Telephony overview” on page 14
  - “Plain old telephone service (POTS)” on page 14
  - “Integrated Services Digital Network (ISDN)” on page 14
  - “Private branch exchange (PBX)” on page 14
  - “The dial plan” on page 14
- “Voice over IP overview” on page 16
  - “Advantages of using VoIP” on page 16
  - “Session Initiation Protocol (SIP) and Real-Time Transport Protocol (RTP)” on page 17
- “VoIP in IBM Smart Business” on page 20
  - “Digium Asterisk for Smart Cube” on page 20
  - “Nortel SCS 2.0” on page 20
2.1 Telephony overview

In addition to new technologies, many Voice over IP systems utilize long-established telephony standards to communicate with external parties, so here we provide a brief overview of some key terms and technologies associated with telephony as a whole.

2.1.1 Plain old telephone service (POTS)

This is the regular analog telephone network that is used to make traditional voice telephone calls. Typically, a socket on the wall to which you would attach an analog device, such as a telephone or fax machine, represents one telephone line from the telephone company (telco).

2.1.2 Integrated Services Digital Network (ISDN)

This is a digital communication network and is used for more than just telephony. As the name suggests, integrated services means that this network can provide voice, data, video, and fax services simultaneously across the same lines. One wall socket can accommodate many lines and is a more suitable technology for when many lines are required, as it saves having an excessive number of wall sockets.

There are two main types of ISDN. The first is basic rate interface (BRI). This provides two 64 kbps bearer (B) channels, which carry data and one 16 kbps delta (D) channel, which is used for signalling. One ISDN BRI line can accommodate two concurrent telephone calls. ISDN BRI is also known as ISDN2.

The other ISDN service is primary rate interface (PRI) and offers far greater capacity than BRI. In North America, ISDN PRI is also known as T1, which provides 23 B channels, giving a total bandwidth of 1544 kbps. Elsewhere (especially Europe) ISDN PRI is known as E1, which has a higher capacity than T1 with 30 B channels giving 2048 kbps total bandwidth. E1 is also known as ISDN30. There is a higher cost involved in having PRI lines, which is why many telcos offer reduced capacity PRI packages, often starting from eight channels.

The public switched telephone network (PSTN) provides both analog and digital services.

2.1.3 Private branch exchange (PBX)

A PBX is a private, internal telephone system common in businesses that connect to the PSTN via connections to either POTS or ISDN lines known as trunks. They can be fully customized and are managed internally and are entirely separate from the PSTN. Enterprise VoIP systems are based on the same idea, and hence are referred to as IP-PBXs. The IBM Smart Business environment provides IP-PBX functionality. There are several IP-PBX options available depending on the platform on which IBM Smart Business is running.

2.1.4 The dial plan

One of the main elements of a telephony system (IP or traditional) is the dial plan. The dial plan is a kind of reference that must be checked in order to route than phone call properly. The dial plan manages both incoming and outgoing phone calls. We split the dial plan into the inbound dial plan and the outbound dial plan. The former tells the PBX how to route an incoming call and how to treat it. The later one manages outgoing calls.
The incoming dial plan is the list of the extensions plus some rules to route incoming calls properly. We discuss later how Asterisk PBX and Nortel Software Communication System (SCS) 2.0 deal with incoming calls. The outbound dial plan is slightly more difficult, so here we provide an overview of its functioning. In Figure 2-1 you can see what happens when someone wants to place a call. The first step is to check whether the number dialed corresponds with an emergency call (that is, 911 for the United States or 118 in Italy). If so, the call will be directly placed.

Note: Access to emergency numbers is mandatory and regulated by country laws. A user must be able to dial an emergency number without any modifications, prefixes, or particular procedures.

Once verified that we are not in an emergency, the second step is to check whether the number dialed is internal (that is, the user wants to dial another user’s extension). In order to have this done the number processing unit inside the PBX must match the receiver ID of the call upon a table that contains patterns. These patterns are a standard defined in IETF-RFC 2705. For a complete reference refer to the following website and search for RFC 2705:

http://www.ietf.org

In the case of an internal call, the pattern matched will be something like xxxx, where x stands for a digit. For an example of an outbound dial plan see Table 2-1.

Table 2-1  An example of an outbound dial plan

<table>
<thead>
<tr>
<th>Call type</th>
<th>Matching pattern</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency number</td>
<td>nnn</td>
<td>911 (exact match)</td>
</tr>
<tr>
<td>Internal extension</td>
<td>xxxx</td>
<td>1001</td>
</tr>
<tr>
<td>External local</td>
<td>9xxxxxxx</td>
<td>95554301 (9 for external line)</td>
</tr>
<tr>
<td>External long distance</td>
<td>91xxxxxxx</td>
<td>91555554301</td>
</tr>
<tr>
<td>External international</td>
<td>9011xxxxxxx</td>
<td>901139055555555 (Italy)</td>
</tr>
</tbody>
</table>
For external calls everything is now straightforward. Take the number, match the correct pattern, and then route the call. As seen in Figure 2-1 on page 15, you can see that there is another step before having the call routed to the receiver. You may want some users not to be allowed to place external calls. In order to do this, once established, check the call type and whether the caller is allowed to place the call. During the extension setup process you probably have been asked about giving the extension access to external calls. Somewhere, depending on PBX implementation, all this information is stored and used to determine extension capabilities. We discuss later how the dial plan is implemented in the IBM Smart Business platform.

2.2 Voice over IP overview

Voice over Internet Protocol is a technology that allows telephone communications over IP networks such as local area networks (LANs), wide area networks (WANs), and the Internet. Other names for VoIP include IP Telephony (IPT), Network Telephony, and Internet Telephony. The concept of sending voice over an IP network is similar to sending any other type of information, such as an e-mail. The voice is converted into data packets, which are sent across the connection and reassembled in the correct order on the receiving end. This is very time sensitive and requires a solid network to function correctly. This is discussed in more detail in Chapter 3, “Network considerations” on page 21.

2.2.1 Advantages of using VoIP

VoIP system design and implementation can vary greatly, from simple conversations between two computers across the Internet using special VoIP software (Figure 2-2), to complex multi-site implementations with sites in several different countries, utilizing a wide range of SIP-based hardware including physical phones with phone calls going over both network connections and regular telephone lines. SIP is an open standard signalling protocol used for setting up and tearing down (starting and ending) communication sessions over SIP-enabled IP-PBXs.

Considerable cost savings can be had from deploying a VoIP system. Larger installations for multi-national companies can make calls between offices in different countries entirely free of charge. Due to the open nature of SIP, a great deal of interoperability exists between different vendors of IP PBXs and associated hardware. This means that you are not locked to a specific vendor for the life of your system and are free to use a great deal of SIP-based hardware with your IP-PBX. This provides far more flexibility than closed-system, proprietary PBXs.
Figure 2-3 gives an example of how a company with several offices may deploy VoIP. They can utilize a WAN connection to make free calls between sites, while still having the use of the PSTN to make calls to other companies. Company B in the diagram does not have to be an IP-PBX. If company B did have a compatible IP-PBX, calls could also be made between them for free with some additional equipment and configuration. This is known as SIP trunking and is discussed in greater detail in Chapter 3, “Network considerations” on page 21.

![Diagram of PSTN and WAN calling](image)

Despite the growth of VoIP, the traditional telephone network still plays a vital role in modern day communication. It is common for smaller companies to have their VoIP system running on their LAN, which connects to the PSTN via a special kind of device called a gateway. The type of gateway depends on how the company connects to the PSTN. Connecting VoIP systems to the PSTN is discussed in Chapter 8, “Configuring and deploying Voice over IP (VoIP) hardware for x86” on page 161.

A VoIP system is definitively more flexible than an old PBX system. That is why a lot of companies are adopting this kind of system.

The last advantage that we want to mention is related to total Cost of Ownership (TCO). Maintenance and upgrading of PBX systems is usually expensive and, on very old systems, impossible. If you are planning an upgrade of your old PBX, VoIP is definitively an interesting option.

### 2.2.2 Session Initiation Protocol (SIP) and Real-Time Transport Protocol (RTP)

SIP is an open standard signalling protocol used for setting up and tearing down (starting and ending) communication sessions over SIP-enabled IP-PBXs. Two examples of such sessions are a voice call and a videoconferencing session. As SIP’s focus is call setup and signalling,
the actual communication stream once the session has been created is done over RTP. Figure 2-4 illustrates this process.

Phone A wants to call phone B. At this point, phone A sends a SIP INVITE to the IP-PBX. The IP-PBX keeps record of where a phone is registered (in a LAN, this would simply be by IP address) and forwards the invite from phone A to phone B. The invite includes information about what kind of session is to be established, such as voice or video. This is called Session Description Protocol (SDP). When phone A and phone B acknowledge this request, RTP is then used to handle the transmission and the IP-PBX is no longer required for the transmission. When the call ends and either party hangs up, a SIP BYE is sent via the IP-PBX and the call is terminated.

![Figure 2-4  SIP call setup and RTP transmission on an IP-PBX](image)

**Conference calls**
The process is slightly different if we want three or more participants to join the call. This is the case of a conference call. In a conference call there is always a host or conferencing bridge that is a special PBX extension. All the participants have to dial this number (that will be an extension for internal users and a normal telephone number for external users) in order to join the conference call. Typically, each user is asked to dial a conference code by an Interactive Voice Response (IVR) system in order to join the right call if more than one is ongoing. In a conference call there is usually a moderator (a special user able to kick participants off the call, mute microphones, and so on). Inside an IP PBX (such as Asterisk) the conference call extension is managed by a media server (usually embedded into IP PBX box) that is in charge of taking all the audio streams from each participant, mixing them together, and resending them back. In this way each participant can hear the voice of the others.
From a signalling point of view (Figure 2-5) this is similar to a normal phone call. Each phone exchanges SIP messages with the IP PBX that hosts the conference. There are two exceptions. If one of the users joins the conference from PSTN, the signalling is translated from POTS to SIP by the Telephony Gateway. Another exception is an external user using an IP phone registered on an external IP PBX. This call can be routed through the Internet via a technique called *SIP trunking*, which we discuss in Chapter 3, “Network considerations” on page 21.

As shown in Figure 2-5, you can also have different phones connected from different locations and from different networks. The RTP streams (marked in red in Figure 2-5) in this case are directed from each phone to the host IP PBX. In the case of a participant coming from the PSTN network, the RTP stream will be translated by the telephony gateway in a *plain-old* telephony stream.

**SIP as integration strategy**

SIP protocol is used not only for phone calls. As a signalling protocol it can be used to initiate any kind of real-time interaction sessions. You may think of SIP as a thread able to couple together different SIP-compliant systems. For instance, SIP can be used to link together Lotus Sametime and videoconferencing systems, create portal applications, and so on.

The idea is simple: SIP does not transport any kind of data (that is, during a phone call SIP packets are not carrying voice since RTP is in charge of doing this), it just initiates a sessions (that is, makes a system aware that another system wants to interact). It is up to you to think possible applications of this.
2.3  VoIP in IBM Smart Business

Thinking of communication systems as separate from the rest of the other business applications is an old concept. Unified Communications and Collaboration services opens a new world for business communications by linking together personal productivity tools (such as word processors, spreadsheets, and so on), new communication tools (instant messaging, blogging, wikis), and traditional communication systems like telephony or videoconferencing. IBM Smart Business has been designed with Unified Communications as one of the core services made available by the platform. That is why IBM Smart Business can be extended in order to become a fully featured IP PBX. We discuss Unified Communications features of IBM Smart Business in Chapter 9, “Unified communications configuration” on page 169.

IBM Smart Business does not have a native IP PBX system. The modular architecture of the Cube allows you to choose between different IP PBX vendors directly from the IBM Smart Marketplace.

At the time of writing there are two IP PBXs available for IBM Smart Business:

- Digium Asterisk
- Nortel SCS 2.0

2.3.1  Digium Asterisk for Smart Cube

Asterisk is a widely used open source IP PBX. It offers the main features of a normal PBX and is compliant with the VoIP standard SIP. At the time of writing, Asterisk is available for the x86 version of the IBM Smart Cube. For more details on Asterisk deployment see Chapter 5, “Deploying and configuring Asterisk for Smart Cube deployment (x86)” on page 71.

2.3.2  Nortel SCS 2.0

SCS 2.0 is the new IP PBX targeted for SMB companies. It is compliant with the SIP standard and is widely diffused as a reliable telephone system for IBM System i. At the time of writing, Nortel SCS 2.0 is available for the System i version of IBM Smart Business. You can find details about SCS 2.0 deployment in Chapter 6, “Deploy and configure IBM Smart Business and Nortel SCS 2.0 on IBM i” on page 121.

2.4  Summary

In this chapter we discussed telephony and the new frontier of telephony, Voice over IP. In particular, we covered concepts of public telephone networks like POTS and ISDN along with some concepts of telephone systems like PBX and dial plans. In the second section we provided a brief overview of Voice over IP technology along with the principal protocols that it relies on, SIP and RTP. You will find the concepts learned in this chapter discussed further later in this publication.
Network considerations

This chapter discusses elements of networking issues that should be considered while setting up the IBM Smart Business environment. We do not provide an exhaustive network guide, but just what you need to know about networking and VoIP.

In this chapter we discuss network analysis, network infrastructure issues, and some issues about PSTN network access.

In this chapter we discuss:

- “Network analysis” on page 22
  - “Network topology” on page 22
  - “Public and private access” on page 26
  - “Security issues” on page 27
- “Network Infrastructure consideration” on page 30
  - “Hardware and cabling” on page 31
  - “Networking best practices” on page 32
- “Telephony considerations” on page 33
  - “PSTN access” on page 33
  - “Quality of service (QoS)” on page 35
  - “SIP trunking” on page 37
3.1 Network analysis

While setting up the IBM Smart Cube, networking is one of the most important things to consider in order to provide a fully functional environment. A bad network setup directly affects services offered by the platform and the overall user experience. For these reasons and others, having the correct knowledge of your network is not a secondary issue.

Let us start by looking at a general network schema that will probably fit every small business environment (Figure 3-1).

![Network Diagram](image)

*Figure 3-1  A schema of a typical network environment*

3.1.1 Network topology

Deploying the IBM Smart Cube could be as easy as just plugging it into power and a network port, but if you are setting up an entire environment you may have to think at your network and where to place each component. This is what network topology is all about.
Keeping in mind Figure 3-1 on page 22, in the following section we go through each of the elements shown.

**Office router**
A router is a network device that interconnects different networks. It usually has at least two ports—one attached to the local network and the other one attached to another network (that is, the Internet). The port eventually attached to Internet (possibly through an Internet service provider equipment) is often called the wide area network (WAN) port.

**Multiport Ethernet Switch**
A switch is a *dumb* device that interconnects different devices (such as PCs, network printers, and so on) inside the *same* network. This device is optional in the case that the office router has an embedded multiport switch.

**Telephony gateway**
A telephony gateway can be seen in different ways. It can be a gateway to access the Public Switched Telephone Network (PSTN) or it can be used to connect analog phones (the phones that you have at home, for instance). We discuss more details later in this chapter.

**Printers**
There are two kinds of printers shown in the diagram. USB printers are directly attached to IBM Smart Cube and are then shared through operating system native printer sharing facilities. There can be also printers provided with a network interface card (so-called network printers) that are not attached directly to the IBM Smart Cube but are located in the premises attached to the network. In both cases each user must *map* them in order to use them. A printer mapping facility is provided with IBM Smart Business software.

**Phones and fax machines**
The IBM Smart Business platform supports three kinds of phones:

- Analog phones
- Desktop IP phones
- Softphones
**Analog phones**

These are the most widely used phones. You can find them at home, they are inexpensive, and you can buy them in an electronic equipment store (Figure 3-2 on the left). In order to use analog phones inside the IBM Smart Business environment you must plug them to a telephony gateway.

![Analog phone and desktop IP phone](image)

*Figure 3-2  An analog phone (left) and a desktop IP phone (right)*

**Desktop IP phones**

These phones are functionally equivalent to analog phones, but instead of being attached to the phone wall plug they are part of the network. You can plug them directly into your data network (that is, with a normal Ethernet cable) and they transmit packets as every device that is network-attached does. See Figure 3-2.

**Softphones**

While analog phones and desktop IP phones are physical devices, softphones are computer programs that run on PCs and offer the same features as desktop IP phones.
Smart Business provides the IBM Smart Business Phone that comes embedded in a Sametime client and allows users to place phone calls directly from a PC (Figure 3-3).

Fax machines
Fax machines from a network point of view are similar to analog phones. Since they are attached to a telephone network in order to work they should be attached to a telephony gateway.

Going back to Figure 3-1 on page 22, we can refer to our network as a star topology, with our router and switch in the center of it.
3.1.2 Public and private access

When talking about public and private access we are thinking of whether a user is allowed to access our services based upon his location. To clarify this, look at Figure 3-4.

Suppose that we have two users, A and B, who are trying to reach our services from different locations. User A is not an employee of your company and he has an Internet connection of some kind. User B, a company employee, is sitting at his desk working on his workstation. Both of the users are connected to a network. User A is connected to the wide area network (WAN). A typical example of a WAN network is the Internet. User B is connected to the local office network or local area network (LAN). Another very common name to identify a LAN is intranet (as opposed to Internet). The two networks can be separated, or, as in our case, they can have a junction point. Recalling what we said about our office router in “Office router” on page 23, we can say that this will be the junction point between the two networks.

So far, it seems that user A and user B can access every service available on our network. That is what we do not want. The idea is to offer different services to users like user A (external users) and users like user B (internal users). We refer to services available only to internal users as private or internal services and services available to others (that is, everyone) as public services. That given, we say that a user has public access if he can use only public services and private access if he can access private services.
In Table 3-1 we list the most common services and the kind of access to which they mostly refer.

**Table 3-1  Examples of typical network services and their accessibility**

<table>
<thead>
<tr>
<th>Service</th>
<th>Public access</th>
<th>Private access</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>File sharing</td>
<td></td>
<td>X</td>
<td>File sharing is mainly an internal service. It can also be used to share files with external customers.</td>
</tr>
<tr>
<td>Printing</td>
<td></td>
<td>X</td>
<td>We want to give access to our printers only to our internal users.</td>
</tr>
<tr>
<td>Company website</td>
<td>X</td>
<td>X</td>
<td>The website should be accessed by both external and internal users.</td>
</tr>
<tr>
<td>Company internal website</td>
<td></td>
<td>X</td>
<td>Private access. On our internal website we want to public information (that is, company results, marketing briefings, and so on) available only to our employees.</td>
</tr>
<tr>
<td>Mail service</td>
<td>X</td>
<td>X</td>
<td>Sending mail should be a service available only for our employees, while receiving e-mails is a public service.</td>
</tr>
<tr>
<td>Telephony services</td>
<td>X</td>
<td>X</td>
<td>Incoming calls should be allowed (public access), while placing calls should be limited to employees (internal access).</td>
</tr>
<tr>
<td>Backup services</td>
<td></td>
<td>X</td>
<td>We provide a backup service only for our internal systems.</td>
</tr>
<tr>
<td>Collaboration services</td>
<td></td>
<td>X</td>
<td>We want to make collaboration easy not only between our employees but also with our customers.</td>
</tr>
</tbody>
</table>

If we now go back to Figure 3-4 on page 26, beside the office router we see our IBM Smart Cube. The IBM Smart Cube provides all the services available both to external and internal users and that is why it has been put in the middle of the two networks. It must be reached from both kind of users. In order to do this the IBM Smart Cube has two network cards. One should be plugged to the LAN network and the other one to the WAN. We discuss this further later.

### 3.1.3 Security issues

A discussion of security is not just about hackers and viruses, even if these two issues are definitely important. When we discuss security we think about technologies and techniques that protect both our systems and our internal and external users from accidents and attacks—from the attack of an hacker to the loss of data due to hardware failure.
Figure 3-5 summarizes the security issues. In the following sections we describe each of these elements.

![Security Issues Diagram]

**Access control**

We mentioned public and private access in 3.1.2, “Public and private access” on page 26. Access control is necessary to give our users the correct kind of access. In order to put access control in place we must consider two elements:

- Network security
- Authentication

Consider again Figure 3-4 on page 26. Let us extend that schema by adding important elements such as a firewalls and a user directory.

**Network security**

We need something to prevent user A (the external user) from having access to private services. We can do this mainly in two ways. First of all, we can decide which services should be accessed from outside (Internet) and which should have only private access. Without getting too detailed, let us say that each service corresponds to a port.

In order to use a service, a user should have access to a port on the remote host (that is, the IBM Smart Cube). So when we are speaking of giving access services we are thinking about opening doors to our users. The device that works as doorkeeper is called a firewall. A firewall is based on rules stating wether a user (also called a host) is allowed to access a port. A firewall has rules such as x can access port y (where x is a host identified by an IP address or an entire network if we want to prevent access from the Internet, for instance). This is a very simple explanation of how a firewall works. The important thing here is that in order to offer services in the correct way to the correct users, the firewall must be configured accordingly.
In the case of the IBM Smart Business Platform we have at least two firewalls: one in front of IBM Smart Cube (embedded in the Cube) and the other one in front of the office router (eventually embedded), as shown in Figure 3-6.

**Authentication**

The other way to allow a user to access a particular service is by authentication. In this way we are controlling each user. The idea is very simple. Each time that a user wants to access a service the authentication system asks him his credentials (that is, user name and password) and verifies that they match upon a kind of table, then from the same table checks whether the user has access to the service that he is requesting. Based on the results, the user is granted or denied access.

We will call the table mentioned before *user directory*, or simply *directory*. A directory is made up of two main elements:

- The list of the users with their passwords and details (that is, phone number, e-mail address, and so on)
- The *access control list* (ACL)

The list of users is used to match the user name and password upon authentication. The ACL is used to determine whether a user has access to a particular service. An ACL is made up of *policies* that sounds like *x has access to service y*, where *x* can be a user or a group of users (that is, employees).

The IBM Smart Business platform provides an embedded user directory.

**Data security**

Data is everything for your business. You deal with data every day, and you can understand how important data security is. There are at least two issues about data security that you should know:

- Backup strategy
- System availability

**Backup**

Backup is the essence of data security. IT guys used to say that if data is not backed up it simply does not exist. It is fundamental to keep copies of your data on a weekly basis or, even better, on daily basis. But is just not all about backing up: You must verify that the copies that
you made are fully functional. So, remember on regular basis to access the data that you backed up to see whether everything is OK.

An IBM Smart Business environment offers you a backup service based on scheduled backup sessions on a removable hard drive so that you can store it in a safe place (preferably far from where systems are located). Later we discuss issues related to backup that (for instance, service availability during backup sessions).

**Availability**

There is not a proper, certified solution to have high availability (HA) of an IBM Smart Business platform since it is targeted to small offices. Having two Smart Cubes and keeping them synchronized and in hot standby is not provided natively. Our suggestion is to rely on the backups for Cube and consider an external box with a PBX installed in order to provide HA just for telephony services. We discuss this later.

**User security**

Up to now we have only discussed security related to our systems and services. We also want users to be safe, so in this section we discuss what you need to know about user security.

**Privacy**

Privacy is one of the most important things to consider when dealing with everyday work activities. Privacy is regulated by the law, so you must take care of it. When we talk about privacy, we mean keeping information from being accessed by an unauthorized person. If the external users are kept away and only have access to public areas, internal users are still able to access information that they may are not be supposed to. Privacy affects all users, not just external ones. In order to maintain privacy it is mandatory to define policies that control access to information. We already talked about policies in “Authentication” on page 29.

**Internal user security**

It is very important that details about your employees be kept in a safe place and be accessible only to designated users (for instance, the human resources department). Another important thing to consider is forcing internal users to store every kind of data relevant to the business in the shared storage facility provided by IBM Smart Business Platform. Only in this way will it be possible to preserve data (with backups, for instance) and keep it safe from external attacks (such as a mobile worker's mobile computer being stolen).

**External user security**

We also want users who externally access our services (that is, our public website) to be safe. It is important also to consider measures to make this possible. Using certificates over secured connections (https) will grant our external users safe access to our services and also privacy (an encrypted channel is very difficult to intercept).

### 3.2 Network Infrastructure consideration

While designing a network that must carry not only data but voice, too, it is very important to consider some principles and standards that will allow you to achieve the best results. In this section you will find what we think you need to know while designing a network.
3.2.1 Hardware and cabling

Designing a data-only network is easier than considering a data and voice network. From an infrastructure point of view you should consider some basic elements. You cannot deploy a voice-compliant network relying on an old cabling infrastructure (or, at least, do not expect optimal results). We recommend using at least Category 5 (CAT 5) cables, which offer good performances at an affordable price (Figure 3-7).

![A CAT 5 cable](image)

**Figure 3-7  A CAT 5 cable**

CAT 5 cables come in two types:

- Shielded
- Unshielded

The CAT 5 unshielded (or CAT5 UTP, Unshielded Twisted Pair) are the cheaper and most common cables that you can find. CAT5 Shielded (CAT5 STP) are more expensive, but provide some protection against electromagnetic interferences. Consider using this kind of cable if you know that your building is near an large source of electromagnetic radiation (RADARs, for instance).

Keep compliant to Ethernet standards, which you can easily find them on the Web, so there is no need to mention them here.

In 3.1.1, “Network topology” on page 22, we mentioned two kinds of network devices:

- Multiport Ethernet Switches
- Office routers

Pay attention while choosing these devices. Regarding routers, plan to buy a router supporting quality of service (QoS), virtual local area networks (VLANs), and possibly with an embedded firewall. In our laboratory we used a CISCO 870 Router that provides full support of what we discussed earlier (Figure 3-8 on page 32).

**IEEE 802.3af Power Over Ethernet (PoE)**

A lot of network devices, such as wireless access points or IP desktop phones, must be powered. Since it is not always possible to have a spare plug everywhere in the office, and in order to limit power cables all around, we must find an alternative way to power up network devices. An answer to this problem comes from PoE. PoE provides power to network devices through Ethernet cables. In order for this to work you should have both PoE-compliant...
switches and phones. In this way the multiport Ethernet, PoE-compliant switch becomes a power source for each PoE device in the network.

PoE is well defined in the IEEE 802.3af standard. For more information about this standard do an Internet search for IEEE 802.3af.

IEEE 802.3af is not the only standard for PoE. Cisco has a proprietary implementation of it, but this does not affect PoE devices.

### 3.2.2 Networking best practices

There are some best practices that can help you while designing a voice-compliant network. In many cases, following the tips provided in this section will greatly assist you.

**Dynamic Host Configuration Protocol (DHCP) issues**

DHCP is a very common technique used to propagate network settings without any manual intervention. As a network device is set up it is provided with the correct network configuration parameters. For this to happen you must have a DHCP server properly configured. A router, such the Cisco one mentioned earlier, has an embedded DHCP server. A good idea is to have dynamic configurations for phones and workstations and a fixed configuration for servers and network equipment.

A DHCP server can transmit typical IP configurations (IP address, DNS servers) to the hosts, but can be also be used to transmit extra information. DHCP has some options given, and each option can carry extra information. When working with VoIP, option 184 provides extra information, such as alternative Private Branch Exchange (PBX) address for failover.

**Using Differentiated Services Code Point (DSCP) for QoS**

DSCP is a widely used QoS packet-labeling technique. It works by adding an additional value to each packet, which represents the QoS level of the packet. In order for this to work each router and switch in the network should understand (or trust) this marking protocol. If the DSCP value of a packet on its way to the receiver is not recognized, it will be treated as a normal packet, and may be slowed down or dropped.
Ban unauthorized Peer to Peer (P2P) communications
P2P applications like eMule are very popular and widely used. Since these applications use a lot of bandwidth you should block them in order to preserve your network from congestions. A good practice is to properly configure firewalls in order to block the protocols that these applications are using and set up policies to prevent users even from installing them into their workstations. Applications like Skype, for instance, represent a potential risk for our network and should not be installed on user workstations either.

3.3 Telephony considerations

In Chapter 2, “Overview of Voice over IP Technology in IBM Smart Business” on page 13, we briefly introduced IP Telephony. In this section we discuss considerations for interconnecting our telephone system to public telephone networks.

When a user wants to place a phone call he probably does not care whether his call will be routed through the Internet. But while designing our network is very important to understand how calls are routed and through which network. See Figure 3-9 to understand how calls are routed. There are two possibilities:

► Routing a call through the PSTN network (the old way)
► Routing our call through the Internet using SIP trunking

Figure 3-9  IBM Smart Business telephony interconnection with public networks

3.3.1 PSTN access

In order to receive calls from public telephone network we need a Telephony Gateway.
A Telephony Gateway is a device that translates signals coming from PSTN in packets sent through our network. We expect to find at least two ports on it:

- One to connect the PSTN line
- The other one to connect to our network (Figure 3-10)

![Figure 3-10  A Telephony Gateway](image)

The port on which we connect the PSTN line is called the Foreign eXchange™ Office (FXO) port. An FXO port receives an analog line from the network.

Telephony Gateways are often provided also with a Foreign eXchange Subscriber (FXS) port that gives the line to devices (such as analog phones).

In our laboratory environment we use a Linksys SPA3102 Voice Gateway, which has both FXO and FXS ports, along with an Ethernet Port.

An FXO port is not the only way to connect to a PSTN network. You may have an Integrated Services Digital Network (ISDN) digital subscription. In this case you need a different Telephony Gateway equipped with a different port called E1 or T1 (E1 is used mainly in Europe and Australia, T1 for the U.S., Canada, and Japan) for both the Primary or the Basic Rate Interface (PRI and BRI are two kinds of ISDNs—one for big companies, the second one for small and home offices).

Table 3-2 summarizes which gateway you need depending on PSTN access.

<table>
<thead>
<tr>
<th>Type of PSTN access</th>
<th>Telephony gateway required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog</td>
<td>With FXO port</td>
</tr>
<tr>
<td>Digital (ISDN) Europe, Australia</td>
<td>With E1 port</td>
</tr>
<tr>
<td>Digital (ISDN) U.S., Canada, Japan</td>
<td>With T1 port</td>
</tr>
</tbody>
</table>

Digium/Asterisk supports access via a modem card that can be installed directly in the IBM Smart Business Cube. They support both digital (E1/T1) and analog cards.
This is a link to the Digium-supported analog cards:
http://store.digium.com/products.php?category_id=1

This is a link to the Digium-supported digital cards:

3.3.2 Quality of service (QoS)

Another important consideration about network infrastructure is a very important concept: Quality of Service.

When designing a network in order to provide support also to voice services, keep in mind how important network performance is. A under-scaled network can lead to bad voice communication.

When you are sending data on a network you probably know that everything is split into packets and each packet is sent over the wire. The receiver will take care of reassembling all the packets and obtain the original data. This process takes time and relies strongly on the network. Since our network has limited transmit capacity we can easily imagine that if everyone is sending data in the network congestions are likely. And if you send a packet to the Internet everything becomes even more and more difficult.

Congestions, along with poor network quality (you should consider not only your network, but also old or slow networks that your packets may traverse) is something that you must deal with. This problem is even more important when you think about transmitting voice over your network or over the Internet. If an asynchronous communication (e-mail, for instance) is not very affected by network slowdowns (maybe your e-mail will take a little longer to reach the receiver), when thinking of synchronous communication (that is, a phone call) everything is different. Try to imagine what can happen if, during a phone call, the network slows and your packets are not sent with the correct timing. The communication will be heavily affected: You will start hearing interruptions and delays, and the overall quality of the communication will be so poor that you cannot even understand what the other person is trying to say. That is why there are some concepts that you must be familiar with, which we grouped in Table 3-3.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Definition</th>
<th>Effect on the communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay</td>
<td>When a packet due to network problems slows and takes a long time to reach the destination.</td>
<td>Voice services are heavily affected. Quality decreases, and there are delays in the communication.</td>
</tr>
<tr>
<td>Jitter</td>
<td>Packets arrive in the wrong order, maybe due to different delays during transmission. Delays due to packet reassembling.</td>
<td>Voice garbled, bad experience perceived by the user.</td>
</tr>
<tr>
<td>Packet loss</td>
<td>When network nodes (such as routers) are very busy, it happens that some packets cannot be handled and are, in the end, dropped.</td>
<td>Words are chunked, interruptions in the stream.</td>
</tr>
<tr>
<td>Transmission errors</td>
<td>Packets can be corrupted, becoming unusable at the receiver side.</td>
<td>Delays in voice, bad quality.</td>
</tr>
</tbody>
</table>
QoS is all about these issues. Imagine a highway with different lanes and different speeds for each lane. Each lane represents a level of service and each lane is reserved for only that service. QoS is exactly this: A way to reserve resources through networks in order to avoid delays, jittering, and other issues that can lower the quality of the communication.

There are different ways to implement QoS that we do not go into detail about now since it is a complex topic. We just want to give you just the big picture here.

Let us start by splitting the argument in two: QoS inside our network and outside it. Inside our network things should be simpler since we have direct control of the infrastructure. The idea is very simple. We must mark (or label) each packet that we are transmitting in order to have it recognized and given the correct priority on its way to the receiver. We can assign a number to each level of priority, and let us say that we have eight levels of QoS starting from 0 (low priority) to 7 (highest priority).

Imagine our user who is placing a phone call with his IP desktop phone and sending an e-mail with his workstation. From what we said up to this point, packets for voice communication are more critical than those related to e-mails. So we are marking packets coming out of the phone with a certain QoS level (assume 5, low latency and jittering) and packets exiting from the workstation for our user's e-mail with a lower level (assume 2, standard quality). The packets now have been labeled differently. As long as our packets flow through the cable nothing significant is happening. The crucial point is on network nodes such as switches and routers. When our packets reach a router they will be treated differently accordingly to their QoS level. So our QoS 5 packet (phone call related) will have priority over our QoS 2 (e-mail). In this way our phone call is secured from delaying and jittering.

The last element that we should consider is how to label packets. We go through this later on, introducing Virtual LANs (VLANs).

As we said before, the packet flow inside our network is just one element, and we have full control of it. Since our packets are likely to go through the Internet, too, we also must reconsider QoS in this case. It is not our business managing packets on the Internet: Our Internet service provider (ISP) will take care of our packets, and so it is at the ISP side that we should focus.

ISPs offer different kinds of WAN connections with different kinds of QoS. Having high levels of quality costs more. Prices and services may vary between ISPs, and we cannot mention each one here. AT&T, for instance, offers CoS1 (Class of Service 1, a very high performance WAN connection) over Multiprotocol Packet Switching (MPLS) technology. MPLS is the best choice if you want QoS over WAN.

In order to have QoS in your network, you should verify that your network equipment (routers and switches) are QoS compliant.

**VLAN tagging**

A good method to label our packets is using VLAN. A VLAN is a virtual network, where devices are grouped not physically (for instance, through a multiport Ethernet switch), but logically. This means that we can have devices belonging to the same VLAN even if they are not attached to the same switch.

VLAN are useful for a lot of reasons. In our case, we use different VLANs for different QoS levels. Keeping in mind the highway example, that is exactly what we are doing. A lane on the highway corresponds to a VLAN. Then it is just a matter of assigning the correct QoS level to the correct VLAN and connect devices to the VLAN accordingly so we have VLANs for IP phones, VLANs for workstations, and so on. VLANs are configured on routers and switches. Their implementation may vary from vendor to vendor.
3.3.3 SIP trunking

Another way to route calls outside our network is using the Internet. We already mentioned SIP and how SIP works in Chapter 2, “Overview of Voice over IP Technology in IBM Smart Business” on page 13. Using SIP we can route our calls through the Internet, and, in many cases, this is the correct choice in order to cut telephone expenses.

With SIP trunking we substantially replace our Telephony Gateway with a direct connection with our service provider though the Internet. Roughly speaking, we put in place a kind of channel (or SIP trunk) between our IP PBX and our service provider SIP proxy and we send through this channel SIP packets. At the provider’s side our packets will be delivered to another subscriber (if using SIP) or through the provider’s PSTN access (Figure 3-11).

Since there are different service providers (that offer service at different costs) we can also think to route our calls on a least cost principle. Depending on the call nature (for instance, international or local) we can decide to route our calls to a provider or to another.
We said that SIP trunking has direct impact on telephone expenses. When we place a phone call the carrier makes us pay a *toll* based upon the destination location. Internet costs are mainly fixed (flat rates are widely used). The idea is to keep our phone call on the Internet as long as we can. In this way the carrier will make us pay just the “last mile” of the call (what it takes to reach the destination). This principle is called *toll bypass*. See Figure 3-12.

![Figure 3-12  Toll bypass](image)

Let us make an example to clarify toll bypass. Imagine a company with its headquarters (HQ) in the U.S. and a branch office in Brazil. Assume that we have a SIP trunk active between the two sites. Now suppose that an HQ employee wants to contact a Brazilian customer. There are two routes available for our call. The first one is a traditional international call between our HQ and a subscriber in Brazil (very expensive). Using SIP trunking instead, our call will be routed though the Internet until it reach our branch office in Brazil (less expensive, Internet connection has fixed costs), and then it exits our branch office telephony gateway to reach our Brazilian customers. The bottom line is that we paid our carrier just the price of a local Brazilian call.

SIP trunking offers a very flexible way to route our calls through the Internet. A good understanding of this concept can lead to cost savings.

We explain how to route calls when we will introduce the dial plan.

### 3.4 Summary

In this chapter we introduced networking concepts that you should know while preparing your network for the IBM Smart Business deployment. We analyzed network topology, discussed network issues, and provided some best practices in order to optimize performances of your network. In particular, we saw how network performances can directly affect the quality of our services (and for telephony this is even more important). Having a good understanding of networking principles will help you get the best from your network.
Then we went through telephony concepts that you should know when deploying a VoIP telephone system. We mentioned access to a PSTN network in order to place calls, and how SIP technology can help us reduce telephone expenses through smart call routing.

What is written here is not intended as an exhaustive networking guide. Consider this chapter as a starting point to understand the complexity of networking and telephony. On the Internet you will find plenty of further information about each concept that we mentioned here.
Getting started

In this chapter we discuss both required and recommended steps to take before and during the setup of your Smart Business environment. We discuss the following topics:

- “Pre-setup networking considerations” on page 42
- “Initial setup of the IBM Smart Cube” on page 42 with “The Smart Business Setup Wizard” on page 43
4.1 Pre-setup networking considerations

Keeping in mind what we said in Chapter 3, “Network considerations” on page 21, here we provide you with advice about network configuration parameters.

During the installation process, the system tries to auto-determine the best network parameters for the Smart Cube according to your network. However, the following information should be available:

- **Internal IP address**: This is the address at which internal users have to point in order to use internal services. The IBM Smart Desktop configures a host name that is easier for users to remember than the plain IP address.
- **Subnet mask**: This should be set as 255.255.255.0 in the most common cases.
- **Gateway address**: The IP address of your office router.
- **DNS server (internal)**: This is an optional parameter. You can leave it blank if you do not know the address.
- **Domain name (internal)**: Pick the domain name that you prefer.
- **SMTP relay server**: You must ask your Internet service provider (ISP) how to get this address. This is very important in order to send e-mails on the Internet.
- **Public IP address**: In order to provide public services (website, SIP trunking, and so on) a public IP address should be available. You must ask your ISP how to get one.
- **Public host name**: This is not asked during the setup process, but if you want your customers to reach your website (www.mybusiness.com) or to send you e-mails (info@mybusiness.com) you must register one of these names. Refer to your ISP to get one.
- **Public DNS**: Ask your ISP for this parameter.

If you are creating your network from scratch, refer to Chapter 3, “Network considerations” on page 21, for useful considerations for these parameters.

4.2 Initial setup of the IBM Smart Cube

Now that the environment has been prepared correctly, the IBM Smart Business platform can be installed. Insert the disk labelled *IBM Smart Desk*. If the software does not launch automatically, navigate to your DVD drive and launch setup.exe.

**Note**: An active Internet connection to the IBM i machine is required to be able to authenticate with IBM Smart Market.
The Smart Business Setup Wizard
To setup the IBM Smart Cube:

1. Launch the setup wizard from Start → Programs → IBM Smart Desk → Setup Wizard. On the welcome page, carefully read the requirements before continuing with the installation. A window like the one shown in Figure 4-1 appears.

![Figure 4-1 Installation of IBM Smart Desk](image1)

2. Click the Next button and the license agreement page appears, as shown in Figure 4-2.

![Figure 4-2 License Agreement window](image2)
3. Select the **I accept the terms of the License Agreement** option and click the **Next** button and a summary window appears, as shown in Figure 4-3.

![Figure 4-3  Summary window of the installation](image)

4. Click the **Install** button and a Installation progress window appears, as shown in Figure 4-4.

![Figure 4-4  Installation progress window](image)
Once the installation has been successfully completed a window like the one shown in Figure 4-5 appears.

![Install Complete window](image1)

**Figure 4-5** Install Complete window

5. Click the **Done** button and then the wizard appears, as shown in Figure 4-6.

![The IBM Smart Business Welcome window](image2)

**Figure 4-6** The IBM Smart Business Welcome window
6. When you have the information listed, click **Next**. Help is available on each page, as seen in Figure 4-6 on page 45.

7. Enter your IBM Smart Market user ID and password and click **Next**.

8. Select your system descriptive name from the drop-down menu and click **Next**.

9. Click **Rediscover Systems** to scan your local subnet for the newly added Smart Cube.

**Note:** The discovery only works when the cube is in the network segment as the administration PC. If the discovery is not successful, enter the host name or IP address of the Smart Cube in the box.

The IBM Smart Cube needs an active Internet connection to be able to authenticate with IBM Smart Market.

10. When your Smart Cube has been discovered, click **Next**.

11. Read and accept the license agreement and click **Next**.

12. The following pages are where the networking information is set up. Review the diagram and then click **Next**.
13. The Host name, Domain name, Private IP address, and Subnet mask fields should be pre-populated based on the IP address configured on IBM i. Verify this information and click **Next**. See Figure 4-8.

![Figure 4-8 Configuring host name and IP address](image)

14. If you are planning on running public services such as a website, select **Yes** on the following page and enter the networking information and click **Next**. Otherwise, select **No** and click **Next**.

**Note:** You must make configuration changes on your firewall and register DNS information with your provider in order to access public services externally on the Smart Cube. If you are not sure about public services, this can be configured at a later date via the Smart Business Web interface.

Typically, the private IP address on the Linux solution will be a DHCP address. Users must change this to a static IP address. On IBM i it is usually a static IP address and does not need to be changed.
**Note:** If public services are being configured, it is important to select the line descriptor for your external interface and *not* the line descriptor used for virtual Ethernet. The line description shown in Figure 4-9 is only for the IBM i solution.

![Figure 4-9 Configuring external services using external line descriptor](image)

15. Enter the default gateway and DNS server details and click **Next**. This step may take a few moments to complete.
16. Configure the administrator account and click **Next** (Figure 4-10). Click **Next** again on the ADMINSYS information page.

![Figure 4-10: Entering the administrator credentials](image)

17. Fill in your contact information and click **Next**.
18. Specify your organization name and click **Next**.
19. Click **Next** on the notification of Web server creation page. This will be the same IP address that you configure for your Smart Cube.
20. If your ISP provides an outgoing mail (SMTP) server or SMTP relay, select **Yes** then click **Next** and fill out the required details (Figure 4-11). Otherwise, select **No**, then click **Next**.

*Figure 4-11  Optional SMTP configuration*
Finally, you are presented with a summary page (Figure 4-12). If you configured external services, you will see this here also.

Figure 4-12   Summary of IBM Smart Cube Setup

21. Carefully check the details provided. If everything is correct, click Finish. Otherwise, go back and rectify any errors.
22. The Smart Cube will then be set up based on the details entered. This process takes about 30 minutes, as seen in Figure 4-13.

![Image of Smart Cube setup progress](image.png)

*Figure 4-13  Smart Cube setup progress*

### 4.3 User management

In order to have a user using all the services provided by the IBM Smart Cube a user must be created. This section provides a step-by-step introduction to creating a new user on the IBM Smart Cube and assigning available services.
Prior to starting the user setup we would like to provide you with an overview of the applications that are impacted when changing the password of an ID. The left side of Figure 4-14 shows the applications impacted when an administrator changes its password. On the right side of Figure 4-14 you can see the applications impacted when a user changes its password.

**Important:** The initial password assigned by the administrator to the IBM Smart Business person will be also the Lotus Notes ID file password. When users change the IBM Smart Business password, the Lotus Notes ID password is not synchronized. That applies to administrator and user IDs.

![IBM Smart Cube: ID management](image-url)
The following steps must be executed by the administrator of the IBM Smart Cube:

1. Double-click the **IBM Smart Business Launch** icon on the desktop (Figure 4-15). The window shown in the top left corner of Figure 4-16 opens.

![IBM Smart Business Launch icon](image)

2. Launch the Administrator panel and then log in using your administrator login identification (ID) and password, as indicated on Figure 4-16.

3. After the login you are lead to the administrator home page of the IBM Smart Cube. The administrator home page is shown in Figure 4-16. Click **Go to the Administrator Panel** to continue.

![Administrator Log in page](image)

![Administrator home page](image)
4. The Administrator Panel page (Figure 4-17) is the overview page for all the services managed by the IBM Smart Cube.

5. Click the **People** link to enter the people administration section.

6. The People administration page (Figure 4-18) is where the creation of a new user ID starts. Click **Add a person** to get started.

7. Follow the instructions on the page to create new users.
8. Define the user’s first, middle, and last name. Ensure that the names are spelled correctly, as their could be problems with changing the name later on. No duplicate names are possible.

Note: Fields indicated with a red asterisk (*) are mandatory fields and therefore require information.

9. A user ID is automatically suggested based on the user’s name. However, the user ID can be defined manually.

Note: When an user ID is created a username.id file and a username.password file are created in the system. If an administrator logs in to the IBM Smart Business cube as root she can look at the original ID file password.
10. In case a user with administrator access should be created, select Yes (Figure 4-21).

![Figure 4-21 Administrator authority](image)

Figure 4-21 Administrator authority

11. This is not a mandatory field and can also be changed later on. The phone number entered in this field is not related to any telephone solutions that can be installed on the IBM Smart Cube. We recommend that you enter a phone number that would also be used on a business card. See Figure 4-22.

![Figure 4-22 Work phone number](image)

Figure 4-22 Work phone number

12. Select the applications that should be made available to the user once the ID is active. The list displayed depends on which applications have been deployed by using the setup wizard or the application installer.
Note: The *IP telephone system* is not delivered as a standard service with the IBM Smart Cube. It must be purchased via the IBM Smart Market and installed via the application installer.

By checking the IP telephone system users will be assigned a telephone extension, as shown in Figure 4-23, which is used to receive and place calls from the IBM Smart Business Phone, which is integrated in Sametime 8.0.1. In case the IP telephone system is not checked, the extension can be created and assigned to the user later on.

The following figures include the IP telephone system in order to match with the other chapters in this publication.

13. We recommend using the suggested e-mail in order to have the user use the IBM Smart Cube E-Mail system. More details can be found by selecting the Help link in the top right corner of the page.

The e-mail prompt (Figure 4-24) is only shown if the administrator chooses to deploy Lotus Domino e-mail by selecting the check box shown in Figure 4-23.

14. Our general recommendation is to use the extension that is suggested by the system.
Each extension that is created can be set up with its own voice mail. Assign a numeric password and ensure that you keep note of it, as the password cannot be looked up. Each voice mail can also automatically be mailed to the end user. This option can also be changed later on.

If you intend to allow users to place external calls, the Place external calls option should be checked (Figure 4-25). This option can also be modified at a later stage, as described at the end of this chapter.

– For a general overview of the public telephony system refer to Chapter 3, “Network considerations” on page 21.

– To configure a connection to the public telephony system refer to Chapter 8, “Configuring and deploying Voice over IP (VoIP) hardware for x86” on page 161.

Note: We strongly recommend planning the extensions from the beginning in order to have a consistent distribution of the extensions.

Note that the passcode can be changed in edit extension.
15. The Optional Information panel (Figure 4-26) is to enter optional user information. This information can also be added later on if required.
16. The Summary page (Figure 4-27) is the final page before the user ID gets created. Carefully review and print user information if required.

17. When the panel shown in Figure 4-28 is displayed, the user ID for the selected services was created successfully. Click either **Yes** to create another user or **No** to exit to the People Administration page.
18. Use the People administration page (Figure 4-29) to make modifications to existing users by selecting a user. Refer to Chapter 5, "Deploying and configuring Asterisk for Smart Cube deployment (x86)" on page 71, to create and assign an IP softphone extension to an existing user.

Figure 4-29 People administration page

4.4 Customizing a private intranet

In this section we explain how to customize a private intranet website. Your administrator can customize your site by following these steps:

1. Read the following website for information about customizing the site:

   http://www.dokuwiki.org/manual

2. To customize the site, log into your internal website with your administrator ID and password.

3. Customize the page for your business:
   a. Click Customize on this page to edit the page.
   b. Click Admin to change the administrative settings.

4. Distribute the internal website to interested people.

**Note:** This configuration should be done by a Linux administrator or someone with good working knowledge of Linux.

Before files can be placed in the internal Web directory, appropriate user and group permissions must be set. It is not good practice to change the default settings for the root user, as this is pre-set with security in mind. Therefore, we strongly recommend modifying an existing user or creating a new user with appropriate permissions to put files in the htdocsInt directory.
Note: We do not recommend editing user profiles of factory default users such as admins.

Creating a user requires a remote desktop session to the SUSE Linux operating system on the IBM Smart Cube. (Advanced users may also wish to use an secure shell (ssh) client, but root access via ssh is disabled by default.) To do this go to the IBM Smart Business Administrator panel and scroll down to Services. Select More Services and click OK when the pop-up box appears. A new tab or window appears in your browser. When presented with the login page, log in as root.

The following instructions are equally valid for creating any type of user. Permissions and required groups will vary, however. The focus here is to create a user with enough permission to modify Web pages on the Smart Cube.

1. From the SUSE desktop, select Computer → Control Center → User Management. See Figure 4-30.

2. To create a new user click Add at the bottom of the User and Group Administration page.

3. Under the User Data tab, enter a suitable name, user name, and password. For security reasons, the password should be a mixture of lowercase letters, uppercase letters, and numbers, and not based on a dictionary word.

4. Open the Details tab. If the user is only being created to edit files in the htdocs/int folder, only the www box must be checked under Groups. As good security practice, users should have the minimum permissions required to perform a task. This is especially important in larger organizations with many users, or if you are using an external contractor for management of your website and they have remote access to your system.

5. Set the default group to www.
Other values can be left as their defaults. See Figure 4-31.

6. Click **Accept**.

![User and Group Administration page](image)

**Figure 4-31  Setting new user group access**

The User and Group Administration page will be shown again, where the new user can be seen.

7. Click **Finish** to commit the changes.

The first step is now complete. However, before files can be added, the permissions of the htdocsInt directory must be modified because the default permissions in SLES do not allow members of the www group to write to this directory.

1. From the SLES desktop, double-click **Gnome Terminal** (if this is not visible, you can open a terminal by selecting **Computer** → **More Applications** → **System** → **Gnome Terminal**).

2. Change to the htdocsInt parent directory by issuing the command:
   
   `cd /usr/local/Zend/apache2`
3. Enter the command `ls -l` and look for the line ending with htdocsInt, as shown in Example 4-3 on page 69.

**Example 4-1  Output of ls -l before permissions are changed**

```
xe8000:/usr/local/Zend/apache2 # ls -l
total 92
<output omitted>
drwxr-xr-x  2 wwwrun www  4096 Nov 10 17:12 htdocsInt
<output omitted>
```

4. At the command prompt, enter `chmod 775 htdocsInt` to modify the permission of the directory to allow members of the www group to write.

5. Run the `ls -l` command again. You will notice that the permissions have changed, as seen in Example 4-4 on page 69.

**Example 4-2  After changing the permissions of htdocsInt**

```
xe8000:/usr/local/Zend/apache2 # ls -l
total 92
<output omitted>
drwxr-xr-x  2 wwwrun www  4096 Nov 10 17:12 htdocsInt
<output omitted>
```

To explain what is being done here, see Example 4-1. `drwxrwxr-x` represents four separate elements:

- `d` indicates that it is a directory.
- The first three letters (`rwx` in this case) indicate that the *owner* of the directory (wwrun) has permission to read, write, and execute.
- The second three letters (`rwx` in this case) indicate that members of the *group* (www) can also read, write, and execute.
- The final three letters (`r-x` in this case) indicate the *general public* permission, which in this scenario allows read and execute.

**Note:** Certain permissions apply to certain scenarios. For example, in this case the permissions are being set for a public-facing Web directory. Specified users who are part of the www group may write to the directory, which is necessary to place files onto the site. For all users in your company to view the site, they need to be able to not only read files in htdocsInt, but also to execute them, because scripts such as php are considered executable, and without execute permission they will not load. Public permission to write to the directory is disabled.

Now that the correct permissions have been set, authorized users can write to the directory. There is a default `index.php` file in the directory that redirects the user to the wiki. It is wise to rename this file before copying new files, rather than having it overwritten. The recommended method to transfer files to the above-mentioned folder is using a Secure File Transfer Protocol (SFTP) program. Regular FTP will not work by default. You can easily move and rename files, add folders, and so on, via an SFTP client.

Files can now be placed into the htdocsInt directory and can be viewed by using the internal IP address or host name configured during the initial setup of the cube. The Cube supports PHP.
4.5 Public Internet website

The IBM Smart Cube can also host an external facing website. In this section we discuss the steps required to configure a public Internet website. In order to make an existing website available files must be copied to the `/usr/local/Zend/apache2/htdocsExt` directory on the IBM Smart Cube. You also must configure your corporate firewall to allow communication from the Internet to the external interface of the Smart Cube. If the public network interface was not enabled and you have no intention of hosting a public site on your Smart Cube, this process can be skipped.

**Note:** This configuration should be done by a Linux administrator or someone with good working knowledge of Linux.

Before files can be placed in the public Web directory, appropriate user and group permissions must be set. It is not good practice to change the default settings for the root user, as this is pre-set with security in mind. Therefore, we strongly recommend modifying an existing user or creating a new user with appropriate permissions to put files into the `htdocsExt` directory.

**Note:** We do not recommend editing user profiles of factory-default users such as `adminsys`.

Creating a user requires a remote desktop session to the SUSE Linux operating system on the IBM Smart Cube. (Advanced users may also wish to use an secure shell (ssh) client, but root access via ssh is disabled by default.) To do this go to the IBM Smart Business Administrator panel and scroll down to Services. Select More Services and click OK when the pop-up box appears. A new tab or window appears in your browser. When presented with the login page, log in as root.
The following instructions are equally valid for creating any type of user. Permissions and required groups vary, however. The focus here is to create a user with enough permission to modify Web pages on the Smart Cube.

1. From the SUSE desktop, select **Computer → Control Center → User Management**. See Figure 4-32.

![Figure 4-32 Accessing the Control Center in SUSE Linux Enterprise Server (SLES)](image)

2. To create a new user click **Add** at the bottom of the User and Group Administration page.

3. Under the User Data tab, enter a suitable name, user name, and password. For security reasons, the password should be mixture of lowercase letters, uppercase letters, and numbers and not based on a dictionary word.

4. Open the **Details** tab. If the user is only being created to edit files in the `htdocsExt` folder, only the www box must be checked under Groups. As good security practice, users should have the minimum permissions required to perform a task. This is especially important in larger organizations with many users or if you are using an external contractor for management of your website and he has remote access to your system.

5. Set the default group to www.
Other values can be left as their defaults. See Figure 4-33.

6. Click **Accept**.

![Image of User and Group Administration page](image)

**Figure 4-33  Setting new user group access**

The User and Group Administration page will be shown again, where the new user can be seen.

7. Click **Finish** to commit the changes.

The first step is now complete. However, before files can be added, the permissions of the htdocsExt directory must be modified because the default permissions in SLES do not allow members of the www group to write to this directory.

1. From the SLES desktop, double-click **Gnome Terminal**. (If this is not visible, you can open a terminal by selecting **Computer** → **More Applications** → **System** → **Gnome Terminal**.)

2. Change to the htdocsExt parent directory by issuing the command `cd /usr/local/Zend/apache2`. 

```bash
cd /usr/local/Zend/apache2
```
3. Enter the command `ls -l` and look for the line ending with `htdocsExt`, as shown in Example 4-3.

**Example 4-3**  Output of `ls -l` before permissions are changed

```bash
xe8000:/usr/local/Zend/apache2 # ls -l
total 92
<output omitted>
drwxr-xr-x 2 wwwrun www 4096 Nov 10 17:12 htdocsExt
<output omitted>
```

4. At the command prompt, enter `chmod 775 htdocsExt` to modify the permission of the directory to allow members of the www group to write.

5. Run the `ls -l` command again. You will notice that the permissions have changed, as seen in Example 4-4.

**Example 4-4**  After changing the permissions of `htdocsExt`

```bash
xe8000:/usr/local/Zend/apache2 # ls -l
total 92
<output omitted>
drwxrwxr-x 2 wwwrun www 4096 Nov 10 17:12 htdocsExt
<output omitted>
```

To explain what is being done here, see Example 4-3. `drwxrwxr-w` represents four separate elements:

- `d` indicates that it is a directory.
- The first three letters (rwx in this case) indicate that the owner of the directory (wwwrun) has permission to read, write, and execute.
- The second three letters (rwx in this case) indicate that members of the group (www) can also read, write, and execute.
- The final three letters (r-w in this case) indicate the general public permission, which in this scenario allows read and execute.

**Note:** Certain permissions apply to certain scenarios. For example, in this case the permissions are being set for a public-facing Web directory. Specified users who are part of the www group may write to the directory, which is necessary to place files onto the site. For the general public to view the site, they must be able not only to read files in `htdocsExt`, but also to execute them, because scripts such as php are considered executable, and without execute permission they will not load. Public permission to write to the directory is disabled.

Now that the correct permissions have been set, authorized users can write to the directory. The recommended method to transfer files to the above-mentioned folder is using a Secure File Transfer Protocol (SFTP) program. Regular FTP will not work by default.

Files can now be placed into the `htdocsExt` directory and can be viewed by using the external IP address (if specified) configured during the initial setup of the cube. The Cube supports PHP. You can easily move and rename files, add folders, and so on, via an SFTP client.
Deploying and configuring Asterisk for Smart Cube deployment (x86)

In this chapter we work on the installation and configuration of Asterisk in the IBM Smart Business. We go through the installation process, the initial configuration, and the advanced feature. At the end of the chapter you will have a fully functional VoIP system.

In this chapter we discuss:

- Installing Asterisk
- Configuring the basic features
  - Configuring extensions
  - Configuring incoming calls behavior
  - Phones and adapters
  - Gateways
- Advanced configuration
  - Ring groups
  - Call routing
  - Class of service
  - Find me/follow me
  - Call parking
  - Blacklisting
  - Advanced interactive voice response (IVR)
- SIP trunking
5.1 Application installer walkthrough

In this section we provide you with a walkthrough for installing and uninstalling Asterisk.

5.1.1 Installing Asterisk

The installation process of asterisk is very simple:

1. Once you got the Asterisk module from the IBM Smart Marketplace, from the workstation on which you installed the IBM Smart Desk software go to the Application Installer (Figure 5-1) and log on as bbpadmin or adminsyst.

   **Note:** Packages downloaded from the IBM Smart Marketplace are temporarily kept in the `/usr/local/ibm/bbp/applications` directory for x86 Smart Cube and in `/qibm/userdata/ibmb/import/applications` for i5. Making a backup copy before installing the modules is a manual operation. Keep in mind that the zip files downloaded will be removed after installation. Do not place any files in these system directories manually, since they are managed automatically by the system itself.

![Figure 5-1 The application installer](image)
2. The Application Installer window opens. Click **Next** on the first screen. You will arrive at the step to verify your applications. You will notice that Asterisk is available and ready to be installed (Figure 5-2).

![IBM Smart Business application installer](image)

**Figure 5-2**  IBM Smart Business application installer
3. Check the Asterisk box and click **Next**. The licensing information (Figure 5-3) appears. Accept it and click **Next**.

![Figure 5-3  Licensing information of Asterisk](image)

4. The next step is very important. You will be prompted to enter the Asterisk administration password. Remember to write it down and store it in a safe place.

   **Note:** The password specified here is related to the astadmin user, the default Asterisk Administrator. These credentials will be used later while using the Asterisk GUI.

![Figure 5-4  Asterisk administrator password form](image)
5. Once given the password click **Next**. The next screen is also very important. You will be asked to specify which networks you want available for Asterisk. Recalling what we said about internal and external services in Chapter 3, “Network considerations” on page 21, consider which is the best choice here. If you want your IP PBX to connect to other IP PBXs (for instance, via SIP trunking, as we discuss later in this chapter), select the option **Private and public**. Otherwise, select just **Private only** for private access.

![Figure 5-5 Giving private, public, or private and public access to Asterisk](image-url)
Once you click **Next** a small recap panel appears (Figure 5-6).

6. The recap panel provide you with information about the network ports used by Asterisk. Print it if needed through the **Print** button on the bottom left corner. Click **Finish** and the installation process begins (Figure 5-7).
The Installation process takes about four minutes to complete. Once finished, a box like one shown in Figure 5-8 appears.

Figure 5-8  Installation process completed

7. The installation process of Asterisk has now been successfully completed. By clicking Yes on the pop-up that appears after clicking Close on the installation process panel, you will be redirected to IBM Smart Business Administrator Panel. Once logged in, you will find a new section called Asterisk. From the IBM Smart Business Administrator Panel click Asterisk (Figure 5-9). Click the Asterisk link to start configuring your IP PBX.

Figure 5-9  IBM Smart Business Administrator Panel
8. You will be redirected to the Asterisk Administrator Panel (Figure 5-10). This is where all Asterisk settings should be configured. There are two other ways to access the Asterisk core:

– The Asterisk Configuration GUI
– Via the command line

We will see Asterisk Configuration GUI later on. The Asterisk command line is not discussed in detail in this book.

![Asterisk Administrator Panel](image)

Figure 5-10 The Asterisk Administrator Panel

From the Asterisk Administrator Panel you have access to the main administration features of the IP PBX system:

– Stop Asterisk/Restart Asterisk: If for any reason you must stop or restart the IP-PBX service do so by selecting either Stop or Restart.
– Investigate User-Reported Problem: This self-help service is provided for every service installed on the IBM Smart Cube.
– Problem Notification settings: This service is provided for every service installed on the IBM Smart Cube. It allows you to define if and to whom an e-mail notification should be sent in case of a IP-PBX-related problem.
– Incoming Call Settings: Here you specify how to manage incoming calls. We will see the details later on.
– IP Telephone System Extensions: Here you can configure extensions, one of the main configuration panels.
– Phones and Adapters: This panel allows you to configure voice over IP (VoIP) hardware (such as phones and adapters for analog phones eventually attached to the network).
– Gateways: From here you can configure gateways to the public telephone network.
– Change IP Telephone System password: Here you can change the password for the astadmin user on the IP PBX.
– Uninstall Asterisk: This allows you to remove Asterisk IP PBX from the Smart Cube (discussed in 5.1.2, “Uninstalling Asterisk” on page 79).
– Advanced Asterisk Administration: This bring you to the Asterisk GUI. We will see something later on.
– View readme file: Versioning and license information.

5.1.2 Uninstalling Asterisk

Uninstalling Asterisk from the Smart Cube is very easy:

1. Go to IBM Smart Business Administrator Panel → Asterisk → Uninstall Asterisk.
2. You will be asked to confirm what you are about to do (Figure 5-11). Click Yes.

![Figure 5-11 Uninstalling Asterisk](image)

**Note:** When you uninstall Asterisk all the configuration files contained in /etc/asterisk will be lost. It is a good practice to back up the entire directory before uninstalling the system. In case of a new installation you will not start from scratch again.
3. The removal process begins. The first step takes a while to complete. During the removal process you will see a waiting message, as in Figure 5-12. During this step the Asterisk process is stopped and the first removal steps committed. Eventually, active phone calls are dropped.

![Figure 5-12 Removal in process](image-url)

4. Once the first step ends, you will be prompted to perform two further steps (Figure 5-13). Make sure to follow the correct order. The first step is to perform the Additional Asterisk uninstall instructions. Clicking the link on the uninstall panel opens a pop-up page saying to perform the Linux command `/usr/sbin/astuninstall.sh`. To do that, continue on to the next step.

![Figure 5-13 Additional Asterisk uninstall instructions](image-url)
5. Without closing the Asterisk Administration panel (click the right tab on the top), go to IBM Smart Business Administrator Panel → IBM Smart Cube → Open IBM Smart Business remote administration. Click OK on the confirmation pop-up and the Remote Administration Panel appears. On the logon screen log in as root. You will enter the Remote Administration Console (Figure 5-14). Double-click the Gnome Terminal icon and the system console will appear.

6. Issue the commands shown in Example 5-1. Execute each command by pressing Enter on the keyboard.

   **Example 5-1 Performing Asterisk uninstall commands from Remote Administration Console terminal**
   
   1. `cd /usr/sbin`
   2. `./astuninstall.sh`

   After a while the console outputs the lines shown in Example 5-2.

   **Example 5-2 Console output**

   Stopping asterisk
   Unable to connect to remote asterisk (does /var/run/asterisk/asterisk.doneexist?)
   warning: /etc/asterisk/manager.conf saved as /etc/asterisk/manager.conf.rpmsave
   ERROR: Removing 'zaptel': Resource temporarily unavailable

7. Close the console by clicking Disconnect on the upper panel. For the last step, go back to IBM Smart Business Administrator Panel → Asterisk → Finish Uninstalling Asterisk.
8. A confirmation pop-up appears. Click **Close** and the final step will be committed. You will be redirected to IBM Smart Business Administrator Panel, and you will notice that the Asterisk entry on the menu no longer appears. This means that Asterisk has been completely removed from your Smart Cube.

### 5.2 Initial configuration

From now on each step should be performed through the Asterisk Administration Panel.

#### 5.2.1 Telephony considerations

In this section we describe some considerations regarding user extensions.

**User extensions (x86)**

When a user is created on the Smart Cube and enabled for VoIP, this implies use of the IBM Smart Business Phone. If you wish for the user to have a desktop phone also, then they must have a separate extension configured.

In order to keep examples clear, extensions have been provisioned as follows:

- Softphones in the 1000 range
- Desktop Phones in the 2000 range

For clarity, there is minimal difference between the two, for example, see Table 5-1.

#### Table 5-1  Extensions

<table>
<thead>
<tr>
<th>User</th>
<th>Softphone extension</th>
<th>Hardphone extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabrizio Picca</td>
<td>1001</td>
<td>2001</td>
</tr>
<tr>
<td>Laurent Itin</td>
<td>1002</td>
<td>2002</td>
</tr>
<tr>
<td>Chris Snowdon</td>
<td>1003</td>
<td>2003</td>
</tr>
</tbody>
</table>

For ease of administration, we recommend devising a similar structure that will allow users to easily differentiate softphone and desktop phone extensions.

#### 5.2.2 Allocating extensions

Adding extensions to Asterisk is a very straightforward process. There are three main moments in which you might add an extension to the PBX system:

1. When you are adding a new user to the IBM Smart Business platform.
2. When you want to provide an existing user with a desktop phone (IP or FXS-attached).
3. When you want to add a new softphone to the system.

Even if all of these events will come up in a new extension, the process to create these extensions is different. We mentioned this in case 1 in Chapter 1, “Overview of IBM Smart Business and IBM Smart Cube” on page 1, while dealing with the user creation process. We discuss case 2 in Chapter 8, “Configuring and deploying Voice over IP (VoIP) hardware for x86” on page 161, because it is part of the hardphone setup. Here we discuss case 3.

We discussed what a softphone is in Chapter 3, “Network considerations” on page 21. A softphone works as a normal phone but is actually a program running on a user’s workstation.
Every phone in the system (hard and soft) needs an extension in order to be reached. You will see that while configuring a new extension you will be asked for a user that should be linked with that extension. A user in Asterisk is something apart from the extension. A user can have multiple extensions assigned (that is, a user can have a softphone and a desktop phone). Inside IBM Smart Business platform users are specified inside Smart Cube’s directory and then linked to an Asterisk extension.

What we are doing here is creating a new softphone extension, linking it to a user (already present), and adding extra information (for instance, voice mail).

To start adding click **IP telephone system extensions** (Figure 5-15) from the Asterisk Administration Panel.
Once the IP Telephone System Extensions panel appears, you will be able to see all the existing extensions (both softphone and desktop phone related) with some other useful information (Figure 5-16).

![IP Telephone System Extensions panel](image)

Looking at the Extension column, you will notice that some numbers start with an asterisk (*). This notation denotes them as primary extensions (as written in the small caption under the panel title). We explain what a primary extension is meant for later, when we go through dial plan basics.
To add a new extension, on the IP Telephone System Extensions panel click **Actions → Add Extension** (Figure 5-17). Once you do this the extension configuration panel shows up and you will be asked for some parameters, of which you should be aware.

![Figure 5-17 Adding a new extension](image)

First of all you will be asked for the extension number (Figure 5-18 on page 86). You have two choices:

- Let the system determine the next free available extension.
- Specify a number.

If you chose the second option you should have in mind which extensions are already taken. Pay attention when you choose extension numbers. We go through numbering and the related best practices later in the book.

After specifying an extension number you will be asked whether that extension is primary. Again, it depends on your dial plan.

The next step is to assign the extension to a particular user *already present* in the system. You must specify it along with the related caller ID that you want to be shown on receiver's phone when this user is placing a call (for instance, you may assign two extensions to the same user but have different caller IDs showing up when the user is calling). Then you will be asked for an additional (and optional) description for the extension that you are about to add. Even if this is an optional step, we recommend that you write proper descriptions that will be very helpful in the future (that is, in the case you have 200 users with different extensions associated and you want to modify a particular extension).

In the Account Settings section you will be asked to enter a password for the extension. This information should be given to the user to whom the extension is associated. When the user configures his IBM Smart Business Phone (or any other SIP-compliant phone) he will be asked for this account settings. IBM Smart Business Phone installer can retrieve your
extension and the related password specifying your IBM Smart Business username and password.

The last information requested from you involves voicemail. Here you can decide whether to assign this extension a voicemail box. If you check the box here, you will be asked to specify a passcode (a secret numeric code) that must be given to the user who this extension belongs to in order to give him access to the voicemail. You can also specify an e-mail address where all the voice messages should be sent (you can put an internal mail address or an external one).

The last thing to do is to decide whether our user will be able to dial external numbers. We discuss later how external calls work. Here you just must decide whether our user is allowed to make them, regardless of the external call type (international, local, and so on).

![IP Telephone System Extensions](image)

*Figure 5-18  Configuring a new extension through the Add Extension panel*

Once you do this, click OK on the panel and you will be redirected to the IP Telephone System Extensions panel. Now you should see the newly created extension in the table shown.
5.2.3 Allocating conference call extensions

A conference call extension is a special extension that allows users to participate in a conference call. We explained what a conference call is in Chapter 2, “Overview of Voice over IP Technology in IBM Smart Business” on page 13.

The Asterisk system provides a conference bridge facility. In a typical conference call there are two kinds of users:

- **Moderator**: This is the chairman of the conference call. He opens the conference, closes the conference, and can also control the participants, allowing them to talk or muting their microphones remotely. To identify yourself as a moderator typically you must enter a moderator passcode as you dial the conference extension number.

- **Participant**: This is a normal user with no rights over other participants' phones. He can be optionally asked for a meeting passcode to access private conference calls.

![Figure 5-19 Adding a conference extension](image)
To add a conference call extension you must go to the IP Telephone System Extensions panel (IBM Smart Business Administrator → Asterisk → IP Telephone System Extensions) and click Actions → Add Conference Extension. The conference extension configuration panel opens (Figure 5-20). In this panel you can configure up your conference extension.

![IP Telephone System Extensions](image)

**Figure 5-20  Conference call configuration panel**

The first thing that you are asked is to provide an extension number or let the system choose the next available. The best thing to do is to set the number accordingly to the dial plan.

Once you have set the extension number you must assign it to a user. Different users may have different conference call extensions if you would like. Once decided, remember to write a good description (that is, sales department conference extension).

The passcodes section is very important and you should write down what you are typing here. As we mentioned earlier, there are two passcodes that should be given. One is the moderator passcode and the other one is the participant passcode. Once you have entered the codes click **OK** and the conference extension will be properly configured.

### 5.2.4 Configuring incoming call behavior

The first thing that you expect form your IP PBX system is receiving calls. Asterisk can be configured in different ways to do that. It is up to you to decide which way is the best fit for you. Following what we said in Chapter 2, “Overview of Voice over IP Technology in IBM Smart Business” on page 13, about dial plans, this is actually the **inbound dial plan** of an Asterisk system. We shows advanced configurations of the inbound dial plan in 5.3, “Advanced Asterisk configuration” on page 92.
In order to configure how incoming calls should be handled go to Asterisk Administrator panel → Incoming call settings. The Incoming Call Settings panel appears (Figure 5-21).

![Incoming Call Settings Panel](image)

**Figure 5-21  Incoming Call Settings panel**

You have two available choices:

- The first one is to have an IVR to answer the call and ask the caller what she wants to do, providing her with a menu accessible with DTMF tones.
- The other choice available is to route the call to a particular extension (such as the operator).

**Interactive voice response (IVR) System**

Select this choice to have incoming calls answered by an IVR system. The default IVR will let callers be routed to the extension that they specify when prompted. Select an extension to use for the telephone operator. When callers choose to be routed to an operator, the selected extension rings.

You can record a custom welcome message that plays before the automated response. To record your message, use the extension and passcode provided in the information message on the Incoming call settings panel, as shown on Figure 5-21.

In the case shown in Figure 5-21, an incoming call would be sent to the IVR and forwarded to extension 2001 if the caller chooses the option to call an operator.

You can customize the IVR to have advanced features like sub-menus, interaction with other systems, and so on. We discuss advanced IVR later in this chapter.
**Route to the following extensions**

If this option is selected, when a call comes in, all extensions on the Selected extensions list ring until one answers the call. In the case shown in Figure 5-22, extensions 2001 and 2002 would ring.

![Incoming Call Settings](image)

*Figure 5-22  Specifying where to route incoming calls*

Select one or more extensions from the available extensions, then click **Add**. To select multiple extensions, hold down the Ctrl key while selecting the extensions.

To remove extensions from the list, select the extensions, then click **Remove**. To select multiple extensions, hold down the Ctrl key while selecting the extensions.

**5.2.5 Configuring phones and adapters**

To configure phones and adapters for analog phones, go to **Asterisk Administrator Panel → Phones and Adapters**.
Figure 5-23 shows details about each phone and adapter (device) in your network. From this panel, you can change the settings for existing devices, set up new devices, and remove device settings. The devices listed have already been configured or are waiting to be configured.

Refer to Chapter 8, “Configuring and deploying Voice over IP (VoIP) hardware for x86” on page 161, for detailed instructions for configuring a handset.

5.2.6 Gateways

You need gateways to be configured in order to access the public telephone network, as mentioned in Chapter 3, “Network considerations” on page 21.

You can access the Gateways configuration page by selecting Asterisk Administrator Panel → Gateways. The Gateways panel appears (Figure 5-24).

For more details on how to configure a gateway refer to Chapter 8, “Configuring and deploying Voice over IP (VoIP) hardware for x86” on page 161.
5.2.7 Change IP telephone system password

This password is associated with the ID required to log in using the Advanced Asterisk Administration. Changing it is straightforward. Go to Asterisk Administrator Panel → Change IP Telephone system password and fill the form (Figure 5-25).

Note: All passwords must follow these rules:
- Passwords must contain a minimum of eight characters.
- Passwords can contain a maximum of 63 characters. Password can contain a maximum of 40 characters if the user ID is admins or root.
- Passwords must contain only alphanumeric characters.
- Passwords must not contain four or more consecutive characters from the user ID.
- Passwords must begin and end with an alphabetic character.
- Passwords must contain at least one digit.

![Change IP telephone system Password](Figure 5-25)

5.2.8 Setting up the default dial plan

As we mentioned in Chapter 2, “Overview of Voice over IP Technology in IBM Smart Business” on page 13, while introducing the dial plan, the last step is permitting the users to place external calls if allowed. This is done by configuring the default dial plan in Asterisk. The configuration of the default dial plan is as easy as doing nothing. The Asterisk default dial plan allows users provided with an extension enabled for external calls to dial 9 and then the receiver number. You can modify the default behavior by adding rules for the calls to be placed. We discuss the advanced dial plan in 5.3.2, “Call routing” on page 94.

5.3 Advanced Asterisk configuration

In this section we discuss advanced configuration of Asterisk. To access the Asterisk graphical user interface (GUI) go to IBM Smart Business Administrator Panel → Asterisk → Advanced Asterisk Administration. Unless otherwise specified, all instructions below are to be performed from the Asterisk GUI.
5.3.1 Ring groups

Ring groups allow a group of phones, or devices, to ring simultaneously or in sequence (ring order). This provides the opportunity for multiple people to answer a call (ring all) or one person can answer a call from any phone. Select the **Ring Groups** tab to configure this feature.

The Asterisk GUI does not come with a default ring group. In order to create a new ring group, click **New Ring Group**, as shown in Figure 5-26.

![Figure 5-26 New ring group](image)

**Note:** You will not be able to define a ring group without any user extensions defined in the IBM Smart Business Administrator Panel. See 5.2.2, “Allocating extensions” on page 82, to do this. You will need to add at least one ring group member in order to define a ring group.

Once you click **New RingGroup** a window appears, as shown in Figure 5-27.

![Figure 5-27 New ring group definition](image)

Use the following procedure to create a ring group:
1. Define the name of the group. The name can be any mnemonic, such as sales or technical support.

2. Specify an extension to associate with the ring group. This is the extension that can be dialed to ring all members of the group simultaneously or in order of listing.

3. Choose the members of the ring group from the Available Users list. Click a user extension or trunk, and then click the arrow that is pointed at the Ring Group Members list to transfer. Select a user extension or trunk in the Ring Group Members list, and then click the arrow that is pointing toward available users to transfer the selected item back to the list. Click the double arrow symbol to transfer all group members back to the Available Users list.

4. Choose a ring group strategy from the Strategy drop-down list. You can choose either Ring All Simultaneously, which will ring all phones in the defined group simultaneously, or Ring in Order, which will ring phones in sequence determined by the order of the users or trunks in the group.

5. Specify the number of seconds that each phone (or all phones) should ring before ringing the next phone in order.

6. Lastly, determine which action you want the system to take if no one answers the call. You can direct the call to another user extension, the voicemail of a user, an IVR menu, the operator, and so on.

7. Click the Save button.

When you are returned to the Ring Group summary page, you will see the newly created group. Ensure that you click Activate Changes to enable the group.

5.3.2 Call routing

With call routing we mean how the calls should be handled by the PBX. Actually, everything relies on the dial plan as we saw in Chapter 2, “Overview of Voice over IP Technology in IBM Smart Business” on page 13. We mentioned the default dial plan in 5.2.8, “Setting up the default dial plan” on page 92.
Outbound calling rules

An outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks (for example, local 7-digit dials through an analog line, but long-distance 10-digit dials through a low-cost SIP trunk). You can set a failover trunk to use when the primary trunk fails. The outgoing calling rules give you the ability to use basic pattern matching to differentiate outbound calls and route them accordingly. The Outgoing Calling Rules tab displays every rule name established, the pattern that the rule will match against, the trunk used to complete the call, and the failover trunk to be used, as shown in Figure 5-29.

Note: Outbound calling rules manages only individual outgoing call rules. See the Dial Plans section to associate multiple outgoing calling rules to be used for user outbound dialing.

<table>
<thead>
<tr>
<th>Calling Rule</th>
<th>Pattern</th>
<th>Trunk</th>
<th>Failover Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Longdistance</td>
<td>_91XXXXXXXXX!</td>
<td>Span 1</td>
<td>Bandwidth.com (Sp)</td>
</tr>
<tr>
<td>IAXTEL</td>
<td>_51700XXXXXXX!</td>
<td>Span 1</td>
<td>Bandwidth.com (Sp)</td>
</tr>
<tr>
<td>Local</td>
<td>_000000000!</td>
<td>Span 1</td>
<td>Bandwidth.com (Sp)</td>
</tr>
<tr>
<td>Local</td>
<td>_32365XXXXXXX!</td>
<td>Span 1</td>
<td>Bandwidth.com (Sp)</td>
</tr>
<tr>
<td>International</td>
<td>_9011XXXXXXX!</td>
<td>Span 1</td>
<td>Bandwidth.com (Sp)</td>
</tr>
<tr>
<td>911</td>
<td>_911!</td>
<td>Span 1</td>
<td>Bandwidth.com (Sp)</td>
</tr>
<tr>
<td>Digium</td>
<td>6xxx</td>
<td>Viveli</td>
<td>Span 1</td>
</tr>
</tbody>
</table>

You may restore the default calling rules at any time by clicking Restore Default Calling Rules.

Note that any other custom calling rules will not be edited or deleted.
Click **Add a Calling Rule** to define a new calling rule. The window shown in Figure 5-30 will be displayed.

![New Calling Rule Window](image)

**Figure 5-30  New Outgoing Calling Rule definition**

A calling rule comprises the following items:

- **Calling Rule Name**: Choose a name that describes the type of rule that you are creating, for example, local or long distance.

- **Pattern**: The Pattern field gives you the ability to use basic pattern matching to differentiate calls and route them accordingly. All patterns begin with an underscore (_). For instance, if a number begins with 9256 and is followed by seven or more digits, that would define a call within the state of Alabama. The pattern for this calling rule would be specified as _9256NXXXXXX. If a call began with 9, followed by seven digits, it would be a local call that probably does not require a long-distance charge. The pattern for this calling rule would be specified as _9NXXXXXX. Instead of adding a rule for every extension or phone number that you call, specify the pattern in this rule similar to the examples. The letters shown in the example patterns are special characters, which are described below:

- **X**: Any digit from 0–9.
- **Z**: Any digit from 1–9.
- **N**: Any digit from 2–9.
- **[12345-9]**: Any digit within the brackets, in this instance 1, 2, 3, 4, 5, 6, 7, 8, 9.
- **.**: The period is the wildcard that will match anything remaining (for example, the pattern _9011 matches anything starting with 9011).
- **!**: The exclamation point is a wildcard that causes the matching process to complete as soon as it can determine that no other matches are possible.
5.3.3 Dial plans

A dial plan is a collection of outgoing calling rules and local contexts. A dial plan can also be known as a class of service. Dial Plans are assigned to user extensions to specify the dialing permissions associated with that extension. For example, you might have one dial plan for local calling that only permits extensions associated with that dial plan to dial local numbers via the local outgoing calling rule. Another extension may be permitted to dial long-distance numbers, and would need to have a corresponding Dial Plan that includes both the local and longdistance outgoing calling rules.

On the Dial Plans page click the New DialPlan button, as shown in Figure 5-31.

<table>
<thead>
<tr>
<th>DialClass</th>
<th>Options</th>
<th>Calling Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Default: Longdistance, Local, International, 911, default, parkcalls, conferences, ringgroups, voicemail, queues, voicemail/grouops, directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Longdistance, Local, International, 911, default, conferences, ringgroups, voicemail, queues, voicemail/grouops, directory</td>
</tr>
</tbody>
</table>

Figure 5-31  Dial Plans page
A window appears like the one shown in Figure 5-32.

You can then add calling rules for that dial plan definition by specifying the following options:

- **Dial Plan Name**: Choose a name that describes this collection of dial plans (for example, DialPlan1).
- **Include Outgoing Calling Rules**: Specify the outgoing call rules associated with this dial plan.
- **Include Local Contexts**: Specify the local contexts (conferences, voicemenu, queues, and so on) associated with this dial plan.

Once you have completed the dial plan definition, click **Save** to accept the dial plan or **Cancel** to abandon your changes. Click **Apply Changes** in the upper right corner of the page to make your changes immediately available. Click **Edit** next to a dial plan in the list to edit a previously defined plan, or **Delete** to delete a dial plan.

### Assigning dial plans to users

The dial plan should be bound to the extensions that you want to be part of it. The IBM Smart Business Administration Panel does not provide this feature. By default each extension created is part of the default dial plan. The only way to change the dial plan of an extension is via the Asterisk GUI.

To assign an extension:

1. On the Users tab, click **Edit** next to the user that you want to edit.
2. Change the **DialPlan** drop-down list to match the desired dial plan (Figure 5-33).
3. Click the **Update** button to save the user and close the edit page.

If you would like to modify multiple users’ dial plans at one time:

1. Select all the users to be edited by checking the check box next to each user’s name.
2. Click **Modify Selected Users** and a box displays with the options available to edit the users.
3. Select the check box next to **DialPlan** (Figure 5-34).
4. Select the desired dial plan in the DialPlan drop-down list.
5. Click the **Update** button.

![Figure 5-34   DialPlan option for multiple users](image)

Once completed, click the **Apply Changes** button in the top right corner of the page to immediately activate the changes.

### Configuring an inbound dial plan

In the previous section, we saw how Asterisk can be configured in order to route calls properly. In this section, we show how to configure Asterisk to manage incoming calls.

Incoming calling rules give you the ability to use basic pattern matching to route incoming calls based on time intervals for each analog or VoIP trunk with which you receive inbound calls. Select the **Incoming Calling Rules** tab to access the Incoming Calling Rules page, as shown in Figure 5-35.

![Figure 5-35   Incoming Calling Rules page](image)
The main page displays the incoming calling rules created for each trunk, as shown in Figure 5-36.

![New Incoming Rule](image)

Figure 5-36 New Incoming Calling Rule definition

Click **New Incoming Rule** to create a new incoming calling rule. The new incoming rule form will be displayed. In order to create a new incoming call rule, you must define the following options:

- **Trunk**: Select the trunk that the incoming rule should apply to from the drop-down list. The trunk can be either an analog or VoIP trunk.
- **Time Interval**: Select the time interval from the list available in the drop-down list. You may have created time intervals for business hours, weekend hours, holiday time, and so on. You can also select **None** if you want to bypass any time intervals or patterns.
- **Pattern**: This field gives you the ability to use basic pattern matching to differentiate inbound calls and route them accordingly. All patterns begin with an underscore (_). If you have a VoIP or T1/E1/BRI trunk connected to your system, it is likely that you have purchased a group of Direct Inward Dial (DID) numbers from your telephone provider. Many providers will send the DID to you as 4 or 10 digits in length on an inbound call (for example, a DID for 256-428-6000 may be sent as 6000 or 2564286000). You will need to confirm the DID length with your provider. If someone external to your phone system calls 256-428-6000, the phone system will need to know how to route the call based on the DID that it receives. For instance, if the provider of your VoIP or T1/E1/BRI trunk sends 6000 as the DID when someone calls 256-428-6000, you will need to specify the pattern as _6000 to route accordingly. If you have purchased a range of DIDs from 6000 to 6999, and want all of them to route to the same destination, you may save time specifying routes by entering the pattern as _6XXX. Instead of adding a rule for every phone number that routes to your phone system, you may use the special characters in the following list to construct a pattern that matches a group of numbers:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>Any digit from 0–9.</td>
</tr>
<tr>
<td>Z</td>
<td>Any digit from 1–9.</td>
</tr>
<tr>
<td>N</td>
<td>Any digit from 2–9.</td>
</tr>
<tr>
<td>[12345-9]</td>
<td>Any digit within the brackets. In this instance, 1, 2, 3, 4, 5, 6, 7, 8, 9.</td>
</tr>
<tr>
<td>.</td>
<td>The period is the wildcard that will match anything remaining. For example, _9011 will match anything starting with 9011.</td>
</tr>
<tr>
<td>!</td>
<td>The exclamation point is a wildcard that causes the matching process to complete as soon as it can determine that no other matches are possible.</td>
</tr>
</tbody>
</table>

Note that if you have selected an analog trunk, this field will be grayed and populate with an s. This is not a pattern, but an indication that an analog call should proceed to the destination.
Destination: Select the destination for the incoming call. You can choose to send the call to either an interactive voice menu, specific extension, voicemail box, ring group, and so on. The rules that you must create are dependent on your needs. If you are configuring your system for a business, for example, you will probably want to set up rules for business hours, off hours, weekend hours, and so on. In any case, you should also create a calling rule that utilizes the time interval and uses a catch all pattern to route any calls that do not fit the other rules that you have created. This ensures that you do not miss any calls.

Once you have completed the definition of each incoming calling rule, click **Update**. Click **Apply Changes** in the upper right corner of the page to make your changes immediately available. Each rule that you create will be listed on the Incoming Calling Rules page, organized by trunk. From the main page, you can either edit or delete the rule.

**Class of Service**
This section is directly tied to dial plans and calling rules. The documentation is already here to cover this.

**Find me/follow me**
This feature is available in Asterisk, but unsupported by the GUI. This feature is being added to the GUI, and may be available in a future release.

**Tie line**
This is not currently supported with the included GUI.

**Call park**
Call parking is an Asterisk feature that allows a user to place a call on hold so that it can be taken off hold from another extension. The Call Parking tab gives you the ability to define the call parking options that will enable use of this feature (Figure 5-37).

![Call parking page](image)

The following options must be configured to enable call parking:

- **Extension to Dial to Park a Call**: Specify the extension to call when transferring a call to hold in the **parking lot**.
- **What Extensions to Park Calls On**: The Extension range specified here will be the parking lot designations for the calls that you place on hold. Dialing one of these extensions will retrieve the call on hold.
- **Number of Seconds a Call Can be Parked**: The number of seconds that a call can be placed on hold in the parking lot. After the time has elapsed the call will ring the originating extension.
Usage
You can park a call using either an analog or VoIP phone. To use an analog phone, press the flash button, or quickly depress the hook switch, wait for a dial tone, and then dial the extension (700 is default). With a VoIP phone, initiate the transfer, dial the call parking extension (for example, 700), and then complete the transfer (such as by pressing send). The method using a VoIP phone will vary depending on the phone.

At this point, the parking number for the caller will be announced. The number that it prompts you with is a number from the extension range specified. This is the number that can be entered to retrieve the call. To retrieve the call, pick up a phone and dial the parking number that was previously announced. The amount of time that the call remains parked is determined by the number of seconds specified. If the call is not retrieved in this time, the call will be redirected to the user that originally parked the call.

Note that you must use the attended transfer function in order to properly park a call. Using a blind transfer function does not provide the parking number to the person parking the call. This makes recovery of the call difficult, except for the fall through time-out.

Black lists
Black lists are not configurable in the GUI, as the CLI and file editor are unsupported features.

IVR/AutoAttendant
A valuable feature of Asterisk is the ability to create an interactive voice response, also known as voice menus. Voice menus are designed to allow for more efficient call routing. The menus provide a caller with specific instructions, receive responses from the caller, and process those responses into an action. See Figure 5-38.

![Figure 5-38 Voice Menus page](image-url)
Voice menus are constructed depending on your needs. Just like your business, you must create the solution best suited for your customers. To better understand the creation and operation of these menus, we examine the sample Welcome voice menu, as shown in Figure 5-39. In order to follow along, select the Voice Menus tab on the left menu, then click Create New Voice Menu.

![Figure 5-39 Sample welcome voice menu](image)

The options for this sample menu are displayed similar to Figure 5-39. The following steps make up this sample:

- Answer the call (answer step).
- Pause dialplan execution for ‘1’ seconds (wait step).
- Play ‘thank-you-for-calling’ & Listen for KeyPress events (background step).
- Play ‘if-u-know-ext-dial’ & Listen for KeyPress events (background step).
- Play ‘otherwise’ & Listen for KeyPress events (background step).
- Play ‘to-reach-operator’ & Listen for KeyPress events (background step).
- Play ‘pls-hold-while-try’ & Listen for KeyPress events (background step).
- Wait ‘6’ sec for the user to enter an extension (WaitExten step).

In this example, when a caller dials your company number ending in 7000, the call is answered. Then after a pause of one second, the caller is greeted in the following manner: “Thank you for calling. If you know your party’s extension, please dial it now. Otherwise, to reach an operator, please dial 0.” If the caller tries an extension, the menu responds with “Please wait while I try that extension.” If the caller takes no action within six seconds, the call is disconnected.

Each action is a step chosen from the list of available menu options. The available menu options are:

- **Answer**: This step answers the incoming call.
- **Authenticate**: This step is used to restrict access to one or more areas of your phone system. This is useful when one wants to require users to enter a PIN code in order to proceed to a particular part of the current menu, to a different menu, or to ring an extension.
- **Background**: This step is used to play an audio file in the background while waiting for the caller to enter an extension or number. Playback is terminated once the user begins to enter an extension. In order to scroll through a list of prerecorded sound files to play, click and hold in the field next to the background choice. "Play ‘otherwise’ & Listen for KeyPress" is an example of using the background option.
Busy Tone: This step should be selected if you want to play a busy signal to the caller. You would play the busy tone to the caller if, for instance, the call were over.

Congestion: This step is similar to the busy tone step. The congestion step should be selected if you want to play a congestion signal to the caller. You would play the congestion signal to the caller if, for instance, you want to indicate that the line is not available.

Digit Timeout: This step is used to set the maximum amount of time in seconds allowed between key presses. If a full extension is not entered in the specified time, the entry will be considered invalid. A field for entering the number of seconds before timeout appears next to the option.

DISA: (Direct Inward System Access) This step allows callers from outside the system to get access to an internal dial tone and place calls from within your internal system. You may specify a numeric passcode in the DISA Password field that will be required in order to get access to an internal dial tone. In addition, you must specify the dial plan that DISA should access for determining the available calling routes. If the passcode entered is correct, the caller is given an internal dial tone on which a call may be placed.

Response Timeout: This step is used to set the maximum amount of time in seconds that the phone system will wait for the caller to enter a response before executing the option selected for the t KeyPress Event, or terminating the call if the t KeyPress Event is not enabled. This step could be put at the end of a series of menu choices.

Playback: This step is similar to the background step because it will play a sound file that you select. However, this option does not allow interruption from a KeyPress event, and will move on to the next step in your list only after the sound file has finished playing.

Set Music on Hold Class: Set the group of music on hold files to be associated with this voice menu.

Wait: This step pauses the execution of steps in the voice menu list for the number of seconds that you specify. A caller will not be able to enter an extension during that time.

WaitExten: This step is similar to the wait step because it will pause the execution of steps in the voice menu list for the number of seconds that you specify. However, this option will allow a caller to enter an extension during that time and skip the remainder of the wait period.

Goto Destination: This step can be used to route a caller to a different destination on the phone system (for example, interactive voice menu, specific extension, voicemail box, ring group, and so on).

Set Language: This step gives you the ability to set the language for voice prompts in your voice menu. This is especially useful if you want to begin with the default language, and then give the option of setting a different language for the rest of the menu. For example, voice prompts will begin in English, but if a user is given a choice and presses 2 for Spanish, all further voice menu prompts will be in Spanish (provided that soundpack is installed).

Goto Directory: This step sends a caller to the system phone directory. This gives the user the chance to select a user name from the directory if the extension is unknown to the caller.

Hangup: This step terminates the call.
Creating a Voice Menu

Use the following procedure as a guide to create a voice menu:

1. On the Voice Menus page, click **Create New Voice Menu** to create a new voice menu.
2. Specify a name and an extension. The extension will be the direct dial to the voice menu.
3. Specify the steps of your voice menu using the sample Welcome menu and step descriptions as guides.
4. Select the **Dial Other Extensions** check box if you want to give a user the ability to break out of the menu selections and dial an extension within your system.
   
   Caution: The Dial Other Extensions option is important. This option allows an inbound caller to break out of the listed KeyPress Events and dial another extension. A malicious person may be able to hack through your Asterisk implementation to find an outside dial tone and use it for fraud. Any extensions that are known to the public should be completely handled by the KeyPress Events. Callers should not be allowed to dial other extensions. Sticking to this policy protects your Asterisk system from being compromised.
5. Specify the KeyPress Event actions for digits 0–9 as well as *, #, t, and i. The options available for a KeyPress Event are:
   - None: The associated key is not enabled.
   - Voice Menu: Pressing a key with this option sends the caller to a specified voice menu.
   - User Extension: Pressing a key with this option sends the caller to a specified extension.
   - Queue: Pressing a key with this option sends the caller to the specified queue.
   - Operator: This option sends the caller to the designated operator.
   - Hangup: Pressing a key with this option terminates the call.
   - Congestion: Pressing a key with this option plays a busy signal.
   
   Note that both the t key and i key should be used for specific actions. The action associated with the t key should be the desired action if a user response has timed-out. The action associated with the i key should be the desired action if a user makes an invalid entry.
6. Once you have constructed your voice menu, click **Save**. You can then click **Apply Changes** to add the voice menu to your current configuration.

Recording a voice menu

In the event that one wants to record custom menu prompts for Asterisk that can be used in a voice menu, the Voice Menu Prompts tab may be used.

![Custom Voice Menu Prompts page](image-url)
A list of previously recorded prompts is displayed on the Custom Voice Menu Prompts page. Here, the user may modify several options:

- **Record Again**: Clicking this button allows the user to make another attempt at recording and replacing an existing custom sound file.
- **Play**: Clicking this button brings up a dialog entry box to allow the input of an extension that Asterisk will dial and play the prompt.
- **Delete**: Clicking this button deletes the selected prompt.

![Record a new Voice Menu prompt dialog](image)

**Figure 5-41  Record Custom Voice Menu prompt dialog**

Click **Record a new Voice Menu prompt** to record a custom voice menu prompt. The following options will be available:

- **File Name**: This text entry box specifies the save name of the file that is to be recorded.
- **Extension Used for Recording**: This drop-down box allows the user to choose which extension Asterisk will dial to wait for the user to speak the prompt.
- **Record**: Clicking this button causes Asterisk to launch the call that will record a file.

Once your recording of a custom voice menu prompt is finished, it will be listed on the Custom Voice Menu Prompts page. You will be able to play back the prompt, re-record the prompt, or delete the prompt. The prompts that you record cannot be included when creating voice menus.

### 5.3.4 Configuring and deploying SIP trunking

In Chapter 3, “Network considerations” on page 21, we provided an explanation of what a SIP trunk is and what it is meant for. Now we explain how to implement a SIP trunk using the advanced Asterisk administration.
A SIP trunk is a channel (the trunk) between two IP PBXs used to exchange SIP signals (Figure 5-44 on page 106). This channel can be used, for instance, to place calls via the network (or the internet).

1. Set up the trunk between the two PBXs. You can do this from Asterisk GUI service providers.

2. Select the **VoIP Trunks** tab to add a SIP trunk. The Manage SIP & IAX Trunks page will be displayed (Figure 5-42).

3. Click **New SIP/IAX Trunk** to add a new VoIP trunk.

4. Fill in the initial SIP/IAX trunk definition with the following information (Figure 5-43):
   - **Type**: Select the SIP protocol.
   - **Provider Name**: Enter a unique name to help you identify this trunk for use in calling rules, and so on.
   - **Hostname**: The host name or IP address assigned to the VoIP provider or server.
   - **Username**: Specify the user name associated with this trunk.
   - **Password**: Specify the password associated with this trunk.

5. Click **Add** once you have completed your definition or **Cancel** to discard your changes.

6. Once you have added a VoIP trunk it will appear in the SIP/IAX trunks list. There are Edit and Delete buttons associated with each VoIP trunk listing.
7. Click **Edit** to further refine your trunk definition. The following options will be available (Figure 5-44):

- **Provider Name**: Enter a unique name to help you identify this trunk for use in calling rules, and so on.
- **Hostname**: The host name or IP address assigned to the VoIP provider or server.
- **Username**: Specify the user name associated with this trunk.
- **Password**: Specify the password associated with this trunk.
- **Codecs**: Codecs provide the ability for your voice to be converted into a digital signal and transmitted across the Internet. The quality of your call can be affected by the choice that you make. The codecs available to you depend on what is supported by the service provider that you choose. You can select the order in which the codecs are used. The codecs available are ulaw, alaw, GSM, ILBC, SPEEX, G.726, ADPCM, LPC10, and G.729.
- **Caller ID**: This is the number that the trunk will try to use when making outbound calls. For some providers, it is not possible to set the caller ID with this option. Thus, this option may be ignored. When making outbound calls, the following rules are used to determine which caller ID is used, if they exist:
  - The first caller ID used is the global CID defined in the Options tab.
  - The caller ID set in the VoIP Trunks configuration, if defined, takes precedence over the global CID.
  - The caller ID set for the user making the call as defined under the Users tab on the User Extensions page takes precedence over the global CID set in VoIP trunks.

8. Click **Add** when you have completed your changes or **Cancel** to discard your changes.

**Emergency calls**

Asterisk may be used to implement, supplement, or replace telephone systems and telecommunications services. In some cases, certain government regulations about their implementation or use may apply and compliance with such emergency call regulations is your sole responsibility. Users of Asterisk may attempt to place emergency calls, and your system or application must be properly configured. Asterisk and associated networks and systems must be implemented and configured such that emergency calls are properly
handled, and that any system or application based on the products complies with all applicable laws and regulations.

Once done with the form, click **Save** and you will see our new provider listed on the Service Providers Panel.

The SIP trunk is now configured let us see how to use it.

### 5.3.5 Telephony hardware configuration

You must configure your telephony hardware according to the needs of your system as part of your initial configuration. The Configure Hardware page gives you the ability to configure your analog and digital telephony ports, as well as your tone region, operation mode, message waiting indicator mode (MWI), and other items. The number of ports available for configuration depends on the number and types of telephony boards installed in your Asterisk system. Click the **Configure Hardware** tab to configure your hardware interfaces, as shown in Figure 5-45.

![Configure hardware](image-url)

**Figure 5-45 Configure hardware**

**Note:** The Configure Hardware tab only allows configuration of hardware that is physically present in the system. If no Digium telephony hardware is installed in your Asterisk system, the Configure Hardware tab will not be present. Additionally, within the Configure Hardware tab, only sections applying to installed hardware will be available.

#### Analog hardware configuration

The Analog Hardware section lists the FXS and FXO ports available on the analog cards installed in your system.

#### FXO and FXS ports

FXS and FXO ports provide the ability to receive and send calls through the traditional telephone network, or plain old telephone system (POTS). FXS modules provide both dial tone and ringing voltage to an analog phone. FXO modules accept dial tone and provide an
an interface to the traditional phone lines. You plug a telephone line into an FXO port and an analog telephone into an FXS port.

**Signaling preference**
You can specify the signaling type for your FXS and FXO ports. You have two choices:
- Kewl start
- Loop start

The loop start method uses a short circuit to request a dial tone. All North American home phone lines use loop start signaling. Kewl start is very similar to loop start, but is better able to detect disconnects. Select either Kewl start or loop start for each FXS and FXO module. Kewl start is the default and is preferred for analog circuits in Asterisk.

**Note:** Ground start signaling is not supported.

**Tone regions**
You also must select a tone region, which defines the set of tones (dial tones, ringing tone, busy tone, and so on) used in your region. Select your country, or the nearest neighboring country, from the tone region drop-down list. The default setting is North America (United States/Canada).

**Advanced analog options**
There are also some advanced settings, which are applied to your analog hardware. Specify them as needed, or accept the default values:
- Opermode: Setting operation mode, or Opermode, sets the on hook speed, ringer impedance, ringer threshold, current limiting, tip/ring voltage adjustment, minimum operational loop current, and AC impedance selection as predefined for each country's analog line characteristics. Select the country in which your Asterisk system is operating.
- A-law Override: Set the audio compression scheme. The setting that you choose is dependent on the country of operation. U-law is used in the United States and Canada. A-law is used in most other countries.
- FXS Honor Mode: This setting lets you choose whether you apply the opermode setting to your FXO modules only, or to both FXS and FXO modules.
- Boostringer: Set the voltage used for ringing an analog phone. Normal will set ring voltage to a normal level, and peak will set the voltage to 89V.
- Fast Ringer: The fast ringer tone can be set to normal or to a 25Hz tone.
- Lowpower: The low power setting can be set to normal or to a fast ringer peak of 50v.
- Ring Detect: Users who are experiencing trouble detecting a caller ID from analog service providers or whose lines exhibit a polarity reversal before the caller ID is transmitted from the provider should select full wave. Otherwise, choose standard.
- MWI Mode: This option allows the user to specify the type of message waiting indicator detection to be done on trunk (FXO) interfaces. The options are:
  - None, which performs no detection
  - FSK, which performs frequency shift key detection
  - NEON, which performs Neon MWI detection

The default value is none. Once you have made the required configuration changes to your hardware, click **Save Changes**.
Digital hardware

Digital telephony interfaces allow your Asterisk system to connect to advance digital telephone circuits such as T1s, E1s, and basic rate ISDN. A detailed explanation of digital telephony is outside the scope of this manual. However, it should be noted that generally digital telephone circuits provide more advanced features, better call quality, and are more standardized than analog interfaces.

Primary rate ISDN (PRI) hardware

The digital hardware section lists each T1, E1, or J1 card that is currently part of your system. The following information is listed for each card:

- **Span**: The span column shows the type of digital card.
- **Alarms**: The alarm column lists active alarms, if present, that indicate the card performance.
- **Framing/Coding**: This column lists the type of framing (bandwidth division into channels) and coding (method of signal encoding).
- **Channels Used/Total**: This column lists the number of channels used by the card, and the number of channels available on the card. In the example below, only 1 of 24 channels is used.
- **Signalling**: The signalling column lists the type of signalling that the T1, E1, or J1 card is using.
- **LoadZone**: This drop-down list lets you specify the set of tones that should be used with your digital card.
- **Edit**: The edit button listed for each card gives you the ability to edit several options associated with each card’s performance. Click the **Edit** button and a dialog for the card selected will be displayed, similar to the one shown in Figure 5-46.

![Edit digital card](image-url)
The Edit Card dialog gives you the ability to edit the following options:

- **Framing/Coding**: Select the type of frame format/encoding that you would like to use. The two options available are:
  - ESF/B8ZS: Extended Super Frame framing and Bipolar with 8 Zeros Substitution encoding. This is the newer and generally preferred framing and coding to use.
  - D4/AMI: D4 framing and Alternate Mark Inversion. This is an older methodology and should be used if your T1 service provider does not support ESF/B8ZS.

- **Signaling**: The signaling options available are:
  - PRI: CPE
  - PRI: NET
  - FXOKS - FXO Kewl Start
  - FXOLS - FXO Loop Start

- **Switch Type**: The switch type options available are:
  - National ISDN 2 (This is the default switch type.)
  - Nortel DMS 100
  - AT&T 4ESS
  - Lucent 5ESS
  - Euro ISDN
  - Old National ISDN 1
  - Q.SIG

- **Sync/Clock Source**: The following sync/clock source options are available:
  - Master 0: Provide timing to the remote device.
  - Slave 1: Take timing from the remote device.

- **Line Build Out**: The following line build-out options are available:
  - -22.5dB (CSU): This setting allows you to reduce transmit gain on the ISDN circuit. You might need to do this if connected directly to a device that expects a very weak T1 signal.
  - -15dB (CSU).
  - -7.5dB (CSU).
  - 0dB (CSU)/0-133 feet (DSX1): Generally, you will be connecting equipment directly together. In that case, this is the setting that should be used.
  - 133-266 feet (DSX1): Signal is amplified to allow a cable run length of up to 266 feet.
  - 266-399 (DSX1): Allows a run length of up to 399 feet (122 meters).
  - 399-533 (DSX1): Allows a run length of up to 533 feet (162 meters).
  - 533-655 (DSX1): Allows a run length of up to 655 feet (200 meters).

- **Channels**: This option lets you specify the number of channels that you must use. Click **Update** on the Card Edit Dialog when you have completed your choice of card options.
Basic Rate ISDN (BRI) hardware
The mISDN Config page is used to configure a Basic Rate Interface (BRI) ISDN card, such as Digium's B410P, as well as to define and configure ISDN service providers that the card will utilize. Click the mISDN Config tab to access the page, as shown in Figure 5-47.

![Figure 5-47  mISDN configuration page](image)

There are two sections within the mISDN configuration page:

- The BRI card section
- The service provider section

BRI cards
The BRI card section lists the cards currently installed in your system as well as the number of ports associated with each card. A table lists each port for the cards installed. You can set the mode for each port as well as the timing. The ISDN mode options available are:

- TE Mode: Terminal equipment (TE) mode sets the port to act as an ISDN endpoint connected to an ISDN device (in most cases, a phone). If the port is set to PTP, only one device can be connected. More than one device can be connected to the ISDN port if PTMP is chosen. There are four options available for TE mode:
  - PTP: Point-to-point mode. One device will handle all calls.
  - PTMP: Point-to-multi-point allows the connection of multiple devices to a single port.
  - PTP (CAPI): PTP mode using the CAPI driver.
  - PTMP (CAPI): PTMP mode using the CAPI driver.
- NT Mode: Network terminator (NT) mode should be used when a port is acting as an ISDN originator, or telephone switch. The port set to NT mode will act as the synchronization/timing master, and all devices connected to it will act as slaves.
  - PTP: Point-to-point mode. One device will handle all calls.
  - PTMP: Point-to-multi-point allows the connection of multiple devices to a single port.
Timing
Timing is set at the same time that TE or NT mode is set. Timing can be set to either Master Clock, which delivers the timing for other devices, or None, which indicates that timing will be received from the master. If your port is set to NT mode it should act as the timing master. If your port is set to TE mode, it should be set to receive timing synchronization (none).

Configure trunks
Once you have configured any telephony hardware that might be present in your Asterisk system, you are ready to set up your trunks. Trunks are outbound lines used to make calls. Trunks can be analog (FXO), digital (BRI or PRI), or VoIP. Click Trunks from the main menu to access the trunk configuration page, as shown in Figure 5-48.

Figure 5-48 Configure trunks main page

Trunk definitions are used in calling rules, dial plans, and call routing. You can use a mixture of the different types of trunks available. For example, you may want to configure your system to route local calls through an analog or digital trunk while long distance (or international) calls are routed through a VoIP trunk.
Analog trunks

Select the Analog Trunks tab to access the Manage Analog Trunks page. Here you can create an analog trunk definition for each analog port installed in your Asterisk system. Click New Analog Trunk to open the New Analog Trunk definition page, as shown in Figure 5-49.

![New Analog Trunk](image)

Figure 5-49  New Analog Trunk

Analog trunks operate very differently from locale to locale and in some cases from service provider to service provider. Therefore, a great number of settings may be required to allow advanced call features, such as Message Waiting Indication and Caller Identification, to work in your area. Use the following field definitions as a guide in creating your new analog trunk definition:

- **Channels**: Select one or more analog channels (ports) to be associated with this trunk.
- **Trunk Name**: Specify a unique name to help you identify this trunk when it is referred to in other menus such as calling rules.
- **Busy Detection**: This setting is used to detect far end hangup or for detecting busy signals. Select Yes to enable this feature.
- **Busy Count**: If busy detection is enabled it is also possible to specify how many busy tones to wait for before hanging up. The default is 4, but better results may be achieved by setting this option to 6 or 8. The higher the number, the longer it will take to hang up a channel. A higher number also lowers the possibility of false detections.
- **Busy Pattern**: If busy detection is enabled, it is also possible to specify the cadence of your busy signal. In many countries the correct setting is 500 milliseconds on followed by 500 milliseconds off. Without busy pattern specified, Asterisk will accept any regular sound/silence pattern that repeats multiple times as a busy signal. If you specify busy pattern, then Asterisk will check the length of the sound (tone) and silence, which will further reduce the chance of a false positive.
- **Ring Timeout**: Trunk (FXO) devices must have a timeout to determine if there was a hangup before the line was answered. This value can be configured to shorten how long it takes before Asterisk considers a non-ringing line to have hung up.
Answer on Polarity Switch: If this option is enabled the reception of a polarity reversal will mark when an outgoing call is answered by the remote party.

Hangup on Polarity Switch: In some countries, a polarity reversal is used to signal the disconnect (or hang up) on a phone line. If the Hangup on Polarity Switch option is enabled, the call will be considered hung up on a polarity reversal.

Call Progress: On trunk interfaces it can be useful to follow the progress of a call through ringing, busy, and answering. If turned on, call progress attempts to determine answer, busy, and ringing on phone lines. This feature is highly experimental and can easily detect false answers and hang-ups. This may cause a hang up during the middle of a call. Few zones are supported, but can be selected with the progress zone option.

Progress Zone: This option defines the call progress zone for the trunk interfaces.

Use CallerID: If this option is enabled caller ID detection is also enabled.

Caller ID Start: This option allows one to define the start of a caller ID signal. Select Ring from the drop-down list to start caller ID when a ring is received, or Polarity to start caller ID when a polarity reversal is detected.

Caller ID: This option allows the lines to report the caller ID string as received from your telephone service provider or as a fixed value by using the advanced option.

Pulse Dial: If this option is enabled, pulse dialing, instead of DTMF, will be used.

CID Signalling: This option defines the type of caller ID signalling to use:
- bell: Bell202, as used in the United States
- v23: Used in the UK
- v23_jp: Used in Japan
- dtmf: Used in Denmark, Sweden, and Holland

Mailbox: This setting allows any message waiting indicator received across the associated trunk to be forwarded to a local user, such as a SIP phone.

Flash Timing: Flash timing defines the duration, in milliseconds, that Asterisk will use if it is sending a flash signal to another system.

Receive Flash Timing: Receive flash timing defines the duration, in milliseconds, that Asterisk requires in order to consider a flash operation that it receives to be valid.

Once you have completed the analog trunk definition click Add, then click Apply Changes.

Digital trunks
Digital trunks are somewhat more standardized and therefore require the configuration of fewer detailed settings.
Primary Rate ISDN (PRI) trunks
PRI trunk configuration is entirely driven by settings applied in the Configure Hardware page. There are no higher level options to be set from this screen. You may use the Digital Trunks screen to determine what names have been automatically assigned to the channel groups that you defined in the Configure Hardware page, as shown in Figure 5-50. You will refer to the channel groups by those names when defining calling rules, a later step in configuring your Asterisk system.

Figure 5-50 Digital trunk configuration

Basic Rate ISDN (BRI) trunks
Settings for BRI trunks are configured under the mISDN Config tab in the second section, which is labeled mISDN Service Providers. The mISDN Service Providers section is used to define a provider and the port used by the provider. To create a provider definition click Add. A Service Provider dialog will be displayed. There are two fields that comprise a service provider definition:

- TrunkName: The name of the service provider associated with one or more ports.
- Ports: Specify the ports that should be associated with the trunk. Each port number is comma separated.

VoIP trunks
VoIP trunks do not rely on any underlying telephony-specific hardware. They simply operate using the network interface of your Asterisk system. It is often for this reason that VoIP trunks are the first type of trunk that customers wish to configure on an Asterisk system. To make this configuration even easier, we have included several VoIP Service providers for which VoIP trunks can be configured virtually automatically. These connections are configured in the Service Providers section.

Pre-configured service providers
You must configure a VoIP service provider in order to connect to the Public Switched Telephone Network (PSTN) via a VoIP connection. Access to the PSTN gives you the ability
to place calls to telephone numbers no matter how they connect to the PSTN (VoIP or standard analog system). Click the Service Providers tab to add a VoIP (SIP or IAX) service provider, as shown in Figure 5-51.

![Add New Service Provider](image)

**Figure 5-51  Add New Service Provider**

The list of VoIP service providers and corresponding configuration information is pulled dynamically from a secure Digium Web service. If you are already a VoIP provider customer, select the provider from the list, click Add, and input your user name and password. Once you have added a service provider it will appear in the Service Providers list. There are Edit and Delete buttons associated with each service provider listing. Click Edit to further refine your service provider definition. A detailed definition will be displayed.

The Edit Service Provider page gives you the ability to change your caller ID, as well as select a range of codecs, as shown in Figure 5-52:

- **Username/Password:** You must provide your logon credentials in order to update your service provider information.
- **Caller ID:** The caller ID sent to the PSTN will be set to the value specified in this field.
- **Codecs:** Codecs provide the ability for your voice to be converted to a digital signal and transmitted across an IP network. The quality of your call can be affected by the choice that you make. The codecs available to you depend on what is supported by the service provider that you choose. You can select the order in which the codecs are used. The codecs commonly available are u-law, a-law, GSM, G.726, and G.722. Click Update when you have completed your changes or Cancel to discard your changes.

![Edit Service Provider - Bandwidth.com (Sip)](image)

**Figure 5-52  Edit VoIP service provider**
Custom VoIP trunks

If you do not have a subscription to one of the VoIP providers listed above, or you have a special VoIP setup, you can add a custom VoIP trunk. Click the VoIP Trunks tab to add a VoIP (SIP or IAX) service provider. The Create New SIP/IAX Trunk page will be displayed. Fill in the initial SIP/IAX trunk definition with the following information:

- **Type:** Select either the SIP or IAX protocol:
  - SIP: Identifies that the trunk sends and receives calls using the VoIP protocol SIP
  - IAX: Identifies that the trunk sends and receives calls using the VoIP protocol IAX

- **Provider Name:** Enter a unique name to help you identify this trunk for use in calling rules, and so on.

- **Hostname:** The hostname or IP address assigned to the VoIP provider or server.

- **Username/Password:** You must provide your logon credentials to the VoIP trunk server.

Click **Add** once you have completed your definition or **Cancel** to discard your changes.

Once you have added a VoIP trunk it will appear in the SIP/IAX trunks list. There are Edit and Delete buttons associated with each VoIP trunk listing. Click **Edit** to further refine your trunk definition. The following options will be available:

- **Provider Name:** Enter a unique name to help you identify this trunk for use in calling rules, and so on.

- **Hostname:** The hostname or IP address assigned to the VoIP provider or server.

- **Username/Password:** You must provide your logon credentials to update your service provider information.

- **Codecs:** Codecs provide the ability for your voice to be converted to a digital signal and transmitted across the Internet. The quality of your call can be affected by the choice that you make. The codecs available to you depend on what is supported by the service provider that you choose. You can select the order in which the codecs are used. The codecs commonly available are u-law, a-law, GSM, G.726, and G.722.

- **Caller ID:** This is the number that the trunk will try to use when making outbound calls. For some providers it is not possible to set the caller ID with this option. Thus, this option may be ignored. When making outbound calls the following rules are used to determine which caller ID is used, if they exist:
  - The first caller ID used is the global CID defined on the Options tab.
  - The caller ID set in the VoIP Trunks configuration, if defined, takes precedence over the global CID.
  - The caller ID set for the user making the call as defined on the Users page will take precedence over the global CID and the CID set in VoIP trunks.

### 5.4 Summary

In this chapter we described the deployment of an Asterisk IP PBX on the IBM Smart Business Platform. We provided you with an installation process walkthrough to help you in every phase of the process. We also provided some information about the removal process of Asterisk. These are straightforward operations, but you must pay attention in order to do everything the best way.

Next we discussed the configuration process. You learned how to configure extensions, phones, adapters, and gateways. These first steps have been made mainly from the IBM
Smart Business Administrator Panel. After setting up the basics, you also learned how to configure basic incoming call behaviors and you had a brief introduction to dial plans.

Next we discussed advanced features and how to configure them using the provided Asterisk GUI, writing configuration files, and even using the Asterisk CLI. Inbound and outbound dial plans were covered in detail.

Finally, we discussed SIP trunking. This is one of the features that makes a IP PBX a very flexible telephony solution.

We did not cover everything about Asterisk here, but provided the information that you need to understand how an IP PBX works.

For more information about Asterisk refer to the Asterisk website at:

http://www.asterisk.org
Deploy and configure IBM Smart Business and Nortel SCS 2.0 on IBM i

In this chapter we discuss deployment of IBM Smart Business Platform on IBM i with the Nortel SCS 2.0 Telephony Solution. This chapter includes the following topics:

- “Overview of IBM Smart Business on IBM i” on page 122
- “Pre-installation tasks” on page 123
- “Setting up the IBM Smart Business environment on IBM i” on page 126
- “The Smart Business Administration Panel” on page 132
- “Basic SCS 2.0 configuration” on page 133
- “Advanced SCS 2.0 configuration” on page 143
- “Backing up and restoring SCS 2.0 data” on page 154
- “Uninstalling the Nortel SCS 2.0 Smart Business Connector” on page 156
6.1 Overview of IBM Smart Business on IBM i

An IBM Smart Cube Power System with Nortel SCS 2.0 IP Telephony Solution includes an IBM i (previously i5/OS) operating system environment with the Nortel SCS 2.0 server hosted on a Linux Logical Partition (LPAR) within IBM i using virtual network and hard disk resources. The IBM Smart Cube services are installed on the i operating system. This includes IBM Smart Business Software Pack, IBM applications (Lotus Notes and Domino, Sametime, and so on), and additional independent software vendor (ISV) applications.

An SCS 2.0 Connector application is added to the Smart Cube services to allow the SCS 2.0 server environment to be integrated into the IBM Smart Business environment and to be accessible via the Smart Business Administration Panel. The Connector relays IBM Smart Business control commands such as start, stop, restart, and monitor status to the SCS 2.0 server running in the SCS LPAR. The existing SCS 2.0 browser-based configuration GUI can be launched from the Smart Business Administrator Panel. Finally, IBM Smart Business provides a mechanism for retrieving system information for problem reporting (archived in a zip file). The SCS 2.0 logs and configuration files are made available to the IBM Smart Business system via an NFS (IBM i File System) link to the SCS-LPAR disk. This is illustrated in Figure 6-1.

An IBM Smart Business Power System ordered with SCS 2.0 is preloaded with all the necessary components to install and run SCS 2.0, including end user clients and optional device firmware. No additional CDs or software downloads are required.

Also, Lotus Notes and Domino, Sametime, and Web services come with one-click installers, which are deployed on the Smart Cube using the Smart Business Application Integrator, and then deployed to users via the Smart Business wiki.

---

**Figure 6-1** The IBM Smart Business and Nortel SCS 500 Power System environment
6.2 Pre-installation tasks

Before IBM Smart Business and Nortel SCS 2.0 can be deployed, several steps must be completed, which include initial server setup and network considerations.

6.2.1 Network preparation

Before adding the IBM Smart Cube to your network, some considerations must be made:

- Network IP address and subnet range:
  - Subset IP address range to allocate to the SCS LPAR virtual LAN
  - Eight-address subnet is recommended, which has a subnet mask of 255.255.255.248.
  - Four-address subnet with a subnet mask of 255.255.255.252 is the minimum requirement.
  This is covered in more detail in "Implementing proxy ARP on IBM i" on page 210.

- IP address to be assigned to the Smart Cube physical connection on the local area network.
  If Public services are to be deployed (for example, a company website), a public IP address will be required along with the necessary firewall configuration.

- The default gateway IP address is required.

- The DNS server IP addresses are required.

- Select (reserve) one of the addresses from the virtual LAN IP address range that will be used for the SCS 2.0 server. Use this address to configure the site’s DNS with a fully qualified domain name (FQDN) for the SCS 2.0 server. Both the SCS 2.0 server IP address and FQDN will be required when the SCS 2.0 server initializes (for example, nortelscs.rchland.ibm.com, not nortelscs).

**Note:** The IP address assigned to the SCS 2.0 Server cannot be changed once the SCS 2.0 server initializes.

For clarification, take the following example:

- Smart Cube Physical IP address (IBM i): 9.5.92.12
- Smart Cube Virtual IP address (IBM i): 9.5.92.25
- Nortel SCS Virtual IP address (SCS LPAR): 9.5.92.26

Only the host name/IP address of the physical connection will be used on a day-to-day basis. Everything else is accessed via the Smart Business Administrator Panel.

If you are unsure as to how to acquire network information, click Start → Run and enter cmd into the box. At the command prompt, type ipconfig /all. The output will be similar to Example 6-1.

**Example 6-1 Example output of ipconfig /all command**

C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

  Host Name . . . . . . . . . . . . . . : PKCTT69L
  Primary Dns Suffix . . . . . . . . . . : 
  Node Type . . . . . . . . . . . . . . : Hybrid
IP Routing Enabled. ...............: No
WINS Proxy Enabled. ...............: No
DNS Suffix Search List. ............: rchland.ibm.com IBM.COM

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix .: rchland.ibm.com
Description . . . . . . . . . . . : Intel(R) PRO/1000 MT

Physical Address. . . . . . . . . . .: 00-0D-60-49-3A-DE
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 192.168.1.99
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 192.168.1.1

Note: The above is sample workstation output, not all of this is required for the Smart Cube configuration. The Smart Cube will require a unique IP address within the same network subnet. For example, 192.168.1.100.

► DHCP Server Option 66:
- Option 66 allows attached Nortel phones to discover the SCS 2.0 and download files containing relevant information about the SCS 2.0 IP-PBX automatically. Option 66 is configured with the IP address of the SCS 2.0 from which devices can receive configuration files.
- Configuration of this feature varies, depending on your DHCP server. Consult the documentation of your DHCP server for information about configuring options.
- Other SIP phones support other options such as 120 and 184. Consult the documentation of your particular handset for DHCP configuration requirements.

6.2.2 Connect the power system to your network

To do this:
1. Ensure that you have at least one Ethernet cable. You will need two if you will set up a private and a public network. If you want to deploy public services, such as a website, you need both a public and a private network.
2. Go to the following website to get a planning checklist for your server. The planning checklist provides you with the planning tasks that you must perform:
3. Locate the kitting report (inventory list) for your server. Verify that you received all of the parts that you ordered. Your order information should be located in the ship group next to your system box. You can also obtain order information from your marketing representative or IBM Business Partner.
6.2.3 Preparing the administration PC

The administration PC acts as the system console for the IBM Smart Cube. You will use the console to accept license agreements, perform basic networking configuration, and set up a connection to IBM service and support. The requirements for this task are:

- The administration PC must be running Microsoft Windows XP Professional, Windows Vista® Business, or Windows Vista Ultimate operating system.
- The workstation must be located within the same network segment as your Smart Cube. Two devices are on the same LAN segment if configured on the same physical network without a router between them, as in Figure 6-2.
  - Ensure that your administration PC and Smart Cube are connected to the same router, network switch, or hub.
  - Ensure that there is not a router between your administration PC and Smart Cube.
  - If your network is not configured correctly or if you cannot determine whether your administration PC and Smart Cube are on the same LAN segment, contact your network administrator or service provider.

If you are running a software firewall on your workstation, accept all warnings or turn it off for the duration of the installation. For more information consult the documentation for your firewall.

6.2.4 Install IBM i Access for Windows and configure operations console

You need the operations console component of IBM i Access for Windows installed on the PC that you will use to perform the initial setup of your IBM Smart Cube. If IBM i Access for Windows is not installed on your administration PC, install it from the DVD included with your
order. When installing, select the **Full** installation option. Your PC will be rebooted during the installation process. For more information see System i Access for Windows: Installation and setup in the IBM Systems Information Center:

http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp

Once IBM i Access for Windows has been installed, the following steps must be performed in order to establish a console session to the machine:

1. Ensure that the PC is connected to the same subnetwork as the Smart Cube.
2. Ensure that the Smart Cube and the administration PC are turned on.
3. Wait until the Smart Cube starts and establishes communication with the network. This could take a few minutes.
4. Open the operations console on the administration PC by clicking **Start** → **Programs** → **IBM System i Access for Windows** → **Operations Console**. Your Smart Cube will appear under the Connection column on the IBM i Operations Console page.
5. Right-click the name of your IBM i in the Connection column and click **Connect**. This could take a few minutes.
6. If this is the first time that you are connecting to the system with the administration PC you will be prompted for a user ID and password. Enter the user ID QSECOFR and password QSECOFR. User IDs and passwords are case sensitive. After you enter the user ID and password, the console will still display a status of **Disconnected**.
7. A Remote Control Panel is displayed. This virtual panel matches the physical panel on the front of your IBM i. You can either close this window or move it out of the way.
8. The sign-on page displays. Sign on using the details entered in step 6.
9. You will be prompted to change the QSECOFR password.
10. A 5250 session is started.

**Note:** Record the ID and password that you create and store them in a secure location.

11. The Work with Software Agreements page displays. Review and accept all license agreements for all products shown. There may be more than one page of license agreements. Use F8 to page down and verify that all licenses are reviewed and accepted. Use F15 (Shift + F3) to accept all license agreements for a given product at one time. After you accept all the license agreements, the Command Entry page displays. This page can be used to do later tasks, such as network configuration.

**Note:** For detailed instructions on setting up IBM i for Nortel SCS 2.0 refer to Appendix A, “Setting up IBM i for Nortel SCS 2.0” on page 207.

For detailed instructions on Installing Nortel SCS 2.0 refer to Appendix B, “Installing Nortel SCS 2.0” on page 217.

### 6.3 Setting up the IBM Smart Business environment on IBM i

Now that the environment has been prepared correctly, the IBM Smart Business platform can be installed. Insert the disk labelled IBM Smart Desk. If the software does not launch automatically, navigate to your DVD drive and launch **setup.exe**.
The Smart Business Setup Wizard
Launch the setup wizard from Start → Programs → IBM Smart Desk → Setup Wizard. Refer to 4.2, “Initial setup of the IBM Smart Cube” on page 42, for specific tasks.

1. When the Setup Wizard has finished, you will be prompted to set up applications now. Select Yes. The Smart Business Application Installer will launch to allow you to deploy software to the IBM Smart Cube to be made available to users. This included Nortel SCS 2.0.

   **Note:** The Application Installer can be run later if required. The Installer is launched via Start → Programs → IBM Smart Desk → Application Installer.

2. On the Welcome page, read the information and click Next. See Figure 6-3.

   **Note:** The following windows vary, depending on the applications selected. The applications available for deployment also vary, depending on what has been purchased from the IBM Smart Market. Future software purchased from the IBM Smart Market will be deployed using the Application Installer.

![Figure 6-3 Welcome page of the Smart Business Application Installer](image-url)
3. The list of applications is displayed. Select the desired applications and click **Next**. In this example, all applications are to be installed (Figure 6-4):

- Lotus Notes and Domino provides mail and calendar functionality.
- Lotus Sametime provides instant messaging functionality.
- Web page serving provides public Web services.
- Nortel SCS 2.0 installs the Smart Business Connector for SCS 2.0.

![Figure 6-4  Selecting the applications to install on your Smart Business environment](image)
4. Select the Lotus Notes and Domino components to be deployed and click **Next**. See Figure 6-5.

![Selecting Lotus Notes and Domino components](image)

**Figure 6-5  Selecting Lotus Notes and Domino components**

5. On the next page, enter your e-mail domain (for example, ibm.com) and click **Next**.

   **Note:** The e-mail domain is the second half of an e-mail address. In the address jsmith@example.com, example.com is the domain.

6. Depending on the network interface settings defined in the setup wizard (private and public) and internal policy, select the option for access to Notes and Domino. If it is for internal use only, it is likely to be **private only**. Click **Next** when a selection is made.

7. For Sametime, select private only, public only, or both, as in the previous step. If it is for internal use only, it is likely to be private only. The option to view TCP/IP port details is provided here. When a selection is made, click **Next**.

   **Note:** Ports will be required for firewall configuration.
Sample port output is given in Figure 6-6.

![Figure 6-6 TCP/IP ports](image)

8. Select the access for any Web pages to be hosted (private, public, or both). As with the previous step, detailed port information can be optionally viewed. When a selection has been made, click Next.
9. At this point, the remaining details for the SCS 2.0 are entered. Enter the SCS 2.0 server fully qualified domain name (FQDN) and the root password set during the initialization of the SCS 2.0 server (Figure 6-7). The SCS 2.0 server host name must be a valid network name and be configured in the network's DNS with the IP address of the SCS 2.0 server on the LPAR. When you have entered the information, click Next.

![Figure 6-7  Nortel SCS 2.0 parameters](image)

10. Accept the end user license agreement (EULA) and click Next to continue the installation. This EULA is for the SCS Smart Business connector component only. An EULA will also be presented on first use of the SCS 2.0 administration tool.

11. Select the access for the SCS 2.0 system. It is most likely to be private only. Click Next.

12. This completes the procedure. Review the information on the Summary page. Click Finish to confirm and configure the services. Otherwise, go back and rectify any errors.
The selected applications will be installed and will be available through the IBM Smart Business Administration Panel. It will take around 20 minutes for this step to complete. A progress indicator will be displayed, as seen in Figure 6-8.

![IBM Smart Business Application Installer](image)

**Figure 6-8  Installation progress of selected applications**

Once the process is complete, you will be notified of successful installation.

**Note**: If information was input inaccurately for the SCS 2.0 component, you may see installation error 104: SCS Smart Business failed to connect to the SCS 2.0 Server. The possible causes are:

- SCS 2.0 server host name incorrect.
- SCS 2.0 Linux root password incorrect.
- SCS LPAR is not running (varied off).
- SCS LPAR virtual network not enabled (varied off) or incorrectly configured.
- SCS 2.0 server not installed.

### 6.4 The Smart Business Administration Panel

Access the Smart Business Administrator Panel using the following link (where `<smartcube>` is the host name of the Smart Cube LPAR):

```
```

**Note**: Firefox 3 users may receive a security warning. An exception should be added for the Smart Cube.

The Administrator Panel home page will indicate Additional steps to complete, which includes a step to View Read me for Nortel SCS 2.0. The readme file contains general information about Nortel SCS 2.0.
When you have finished reviewing the home page, click **Go to the Administrator Panel**. A sample is shown in Figure 6-9. The applications that were installed in 6.5, “Basic SCS 2.0 configuration” on page 133, should be shown.

**Note:** If public services have not been configured, then you may see **Partially Configured** against certain elements such as networking. Clicking the link will reveal that the public services are not configured.

![Figure 6-9 Part of The IBM Smart Business Administrator Panel](image)

The Smart Business Administrator Panel was introduced and discussed in Chapter 1, “Overview of IBM Smart Business and IBM Smart Cube” on page 1. The remainder of this chapter discusses the setup of Nortel SCS 2.0.

### 6.5 Basic SCS 2.0 configuration

Nortel SCS 2.0 is now ready for user provisioning and setup. In this section we discuss the basic setup of a new SCS 2.0 server.

**Note:** Some graphics in this section have been edited to remove some text for clearer presentation.

Select **Nortel SCS 2.0** from the Administrator Panel. The functions on the Nortel SCS 2.0 tab provide control over the SCS 2.0 Server as well as the ability to launch the SCS 2.0 configuration manager.
The steps to complete in this section are:
1. Accept the SCS 2.0 Server EULA.
2. Add optional files to the SCS 2.0 Server.
3. Provision users.
4. Deploy handsets.
5. Configure the SCS 2.0 VoIP services.

6.5.1 Nortel SCS 2.0 EULA

The steps are:
1. From Nortel SCS 2.0 select **SCS 2.0 Administration**.

   **Note:** Make sure that pop-ups are enabled for this website or allow pop-ups when prompted. Depending on the security settings for your browser, you may be required to accept the certificates presented at this time.

2. Since this is the first use, read and accept the license agreement to proceed to configure the system.
3. You will be prompted to change the Superadmin password. Change it.
4. After you have changed the password, log in. You will be presented with the SCS 2.0 home page, as seen in Figure 6-10.

![Figure 6-10 SCS 2.0 home page](image-url)
6.5.2 Licensing the SCS 2.0 system

Before any users can be added and any features configured, the necessary license must be obtained:

1. Log into SCS 2.0 Administration.
2. Select System → Licensing. You will notice that there are no licensed users on the system. See Figure 6-11.

![Figure 6-11 Retrieving the system ID](image)

A system ID is required to obtain a license for the correct number of users required on your system. This is a unique identifier for the machine and produces a unique license.

To obtain the system ID:

1. Click Retrieve System ID.
2. When prompted to save or open, select Save.
3. Save the file to a convenient location.
4. When you have your license file, select Browse.
5. Navigate to the location where it is stored and click Open.
6. Click Apply.
7. A License file applied successfully message is displayed and this is reflected in the licensing overview, as shown in Figure 6-12.

![Figure 6-12 Successful license application](image)
6.5.3 Dial plans and call routing

The dial plan is an essential component in a new IP telephony system. Number patterns are specified that are specific to your country. Rules are triggered by a number consisting of a PSTN prefix followed by, for example, a long distance prefix and a telephone number. It is necessary to configure elements such as emergency, internal, local, long distance, international, and toll/premium telephone number patterns. Elements in the dial plan, known as dial rules, have a gateway assigned to them. For single-site installations, typically this will be to your PSTN gateway. However, there is a great deal of flexibility offered by this feature, as you can also route calls via SIP trunks and remote office IP-PBXs should your organization span across several different geographical locations.

To access the dial plan go to **System → Dial Plans**. See Figure 6-13.

![Figure 6-13 The default dial plan on a new SCS 2.0 system](image)

On a new system, many of the elements will be disabled. It is necessary to either edit and enable these elements to suit your needs, or create new custom elements. It may be necessary to create a custom element to achieve certain goals.
For the purpose of our example, the default dial rules will be modified.

**Note:** Number patterns vary between countries, so this should be modified to suit your needs.

1. Click the rule that you wish to change.
2. Set it to **enabled**.
3. Give the rule a name and a meaningful description.
4. The elements of each rule are described on the Dial Rule page (Figure 6-14). These values should be modified to reflect local telephony standards.
   - **Permission**: Specifies the permission that callers need in order to be able to dial this number. When modifying default rules, these can be left at their default values.
   - **PSTN Prefix**: The number that users will dial to get an outside line (for example, 9)
   - **Long Distance Prefix**: The prefix, in this case, for long distance calls (for example, 1)
   - **Area Codes**: An optional parameter to specify to which area codes the rule will be applied. For general long distance dialling, this can be left blank.
   - **External Number Length**: The number of digits of the external number (for example, 10).

![Dial Rule](image)

*Figure 6-14  Provisioning an international dial*
5. After these values have been set, a gateway must be defined for the rule. Assign the gateway required, which is often the PSTN gateway.

**Note:** We assume that a gateway has been provisioned either using the device files included with Nortel SCS 2.0 or a manually configured device. Consult the gateway documentation for more information.

6. Under Gateways select **More Actions** and select the gateway to be used for this rule.

7. To finish, click **Apply** then **OK**.

This completes the international dial rule. This process should be repeated for all required rules, including emergency and mobile/cell dial patterns.

**Blacklisting**

The steps required to blacklist a specific number pattern are the same for as creating an allowed dial rule. However, when the rules have been defined they are set to disabled so that when the SCS 2.0 detects an unauthorized pattern, the call will be blocked. There is a restricted dial rule in SCS 2.0 by default, which can be modified if required.

### 6.5.4 User groups

We recommend creating user groups and assigning users to these groups for simplified control of the dialling permissions that specific users have (also known as class of service). SCS 2.0 has a great deal of flexibility for achieving this. For example:

- Company directors and executives have no call restrictions.
- Department managers may make emergency, local, national, mobile/cell, and international calls only.
- General users may make emergency, local, and national calls only.

**Note:** As codes for dialling numbers vary between countries, it may be necessary to modify the dial plan rules associated with calling permissions to ensure that the correct numbers for dialling external connections are known to SCS 2.0. We recommend ensuring that these dial rules, plus any other custom rules, are configured *before* creating user groups to save later changes. This is discussed in 6.5.3, “Dial plans and call routing” on page 136.

Creation of a user group is simple:

1. Go to **Users → User Groups → Add Group**.
2. Enter a suitable name and description, then click **Apply → OK**.
3. You will be taken back to the User Groups page. Click the new group.
4. Set the desired permissions for the group, as seen in Figure 6-15. The fields are self explanatory. However, there are two points to note:

- Attendant Directory: This lists a user in the AutoAttendant, which is discussed later.
- Superadmin Access: This gives users the highest level of access to the system. This box should not be ticked for non-admin users. It defaults to unchecked.

![Figure 6-15 Sample dialing permissions](image)

5. When you have finished assigning permissions to the group, click **OK**.

### 6.5.5 Provisioning users

By default, when a user is created he is automatically assigned the next available extension from the extension pool. The size of the pool varies based on the licensing on the SCS 2.0 Server. The default pool starts at extension 200. If you wish to modify this, select **Users → Extension Pool** and enter the desired range of extensions.

To begin adding users:

1. Select **Users → Users → Add User**.

   **Note:** Users can also be added via a spreadsheet import and from an LDAP directory. Consult *Configuring User Profiles* from the Task Based Guides for more information about these features.

2. The first available extension appears. Carefully read through the page to understand the requirements for each field. This is mostly self explanatory.
Note: If the user will be using a softphone or non-Nortel IP phones, then it may be necessary to use a simpler SIP password. If only a hardphone is to be used, which has been configured and deployed automatically, then there is no need to change the SIP password.

For initial user configuration, the options from the left hand menu are not required (Figure 6-16). However, these options can be summarized as follows:

- Identification: This is the initial page for creating users.
- Phones: If phones have already been detected by or added to the system (as discussed in the next section), this option can be used to assign a phone to the new user.
- Schedules: Allows creation of scheduled calling.
- Speed Dial: Adds speed dial for the user.
- Group Supervisor: The user becomes a supervisor for specified groups. Supervisors have read-only access to call statistics for users who are members of groups that they supervise.
- Personal AutoAttendant: Creates a personalized auto-attendant that callers will reach when they call the user's extension.
- Registrations: Shows both the IP-PBX and the telephone IP addresses to which the user is registered.
- Permissions: Dialling permissions, as discussed in the previous section.
- Caller ID: If left unchanged, the caller ID will be the user's extension (unless it is blocked on the gateway or ISDN line). An alternative ID can be set or it can be blocked altogether.

Figure 6-16  User settings

3. If the user is to be added to a previously created group or groups, enter the group name in the Groups field. SCS 2.0 will suggest group names based on the first characters entered.
Alternatively, if you want to set individual permissions for the user, do so from the permissions menu on the left-hand side.

### 6.5.6 Adding phones

On networks with DHCP option 66 enabled (in addition to others, depending on the phone) there is very little configuration to perform on the phones, as they detect configuration files automatically as the phones will receive the correct information about the location (IP address) of the SCS 2.0 server automatically.

SCS 2.0 has a device discovery tool that will find phones on the local subnet. Phones outside of the local subnet must be added manually.

**Note:** If DHCP is not in use and phones are not on the same subnet, phones will need to be configured and added manually. If DHCP is in use but with option 66 not configured, it is necessary to manually configure the phone to point to the SCS 2.0 server to download configuration files. Consult the SCS 2.0 Task Based Guides for instructions on configuring particular models. For non LG-Nortel LIP phones, refer to manufacturer documentation.

Phones are identified by serial number (which for the LG-Nortel LIP-68xx phones is the MAC address). Before deploying phones to users, we recommend making note of which phone is being allocated to a user.

Once the phones are identified by SCS 2.0, users can be assigned to handsets. In SCS 2.0, this is done by adding *lines*.

**Note:** If phones are already created, it is valid to assign a phone to a user during the user creation process by using the Phones option on the left menu on the user creation page.

To add lines:

1. Go to **Devices → Phones**.
2. Select the phone that you wish to configure for use (uniquely identified by MAC address).
3. From the menu on the left, select **Lines → Add Line**.
4. Enter the name or extension that you wish to provision, then click **Search**.
5. Select the check box of the correct extension from the results, then click **Select** (Figure 6-17).

![Software Communication System](image)

**Add Line**

1 user found.

Enter user ID, name, alias or description and press Search button. Leave empty and press Select for all.

<table>
<thead>
<tr>
<th>User ID</th>
<th>Last Name</th>
<th>First Name</th>
<th>Aliases</th>
</tr>
</thead>
<tbody>
<tr>
<td>203</td>
<td>Snowden</td>
<td>Chris</td>
<td></td>
</tr>
</tbody>
</table>

Select

6. Click **Apply → OK**. You will notice that the line now shows against the phone.
7. To complete the process, select the phone and click **Send Profile** (Figure 6-18).

8. The profile will be sent to the phone. It is necessary to restart the phone to apply the settings.

The phone is now ready for use.

### 6.6 Advanced SCS 2.0 configuration

**Note:** The user integration between the Smart Cube and SCS 2.0 on IBM i differs from the x86 solution. Users added in Smart Business *People* will not be automatically imported into SCS 2.0. SCS 2.0 supports LDAP integration. However, configuration such as this is not within the scope of this publication. Consult the SCS 2.0 Task Based Guides for more information about all aspects of SCS 2.0 configuration. The guides are included with your IBM Smart Cube as a software download. Refer to Chapter 9, “Unified communications configuration” on page 169, for instructions on downloading software from the Smart Cube.

In this section we present advanced features of the SCS 2.0 IP telephony solution. It is not feasible to cover all configuration possibilities, so the Task Based Guides should be consulted for further information.

Unless otherwise stated, all tasks discussed are performed from the advanced SCS 2.0 Administration interface, accessible via **Smart Business Administration Panel → Nortel SCS 2.0 → SCS 2.0 Administration**.
6.6.1 AutoAttendant

SCS 2.0 provides the ability to create a fully customized AutoAttendant, also known as a digital receptionist or an interactive voice response (IVR) system. The options for customizations are extensive and can be tailor-made to specific needs. Examples of destinations of options made by callers from the AutoAttendant are individual extensions, hunt groups, and voice mailboxes.

The default AutoAttendant dial plan is available once the system has been initially installed. The default attendant within this plan is called operator and is accessed by dialing 100. These default settings can be changed if required. To change these settings the AutoAttendant dial plan must be selected and edited. The actions performed by the attendant can be modified also.

Changing the default AutoAttendant dial rule

To access the dial rule for the default attendant:

1. Go to System → Dial Plans and ensure that AutoAttendant is enabled, as illustrated in Figure 6-19.

![Figure 6-19   Ensuring that the default AutoAttendant dial rule is activated](image-url)
2. Click the dial rule to make changes:
   - Extension: The internal extension of the attendant.
   - Attendant Aliases: Additional extensions for the same attendant.
   - Default Attendant: The default is operator. This can be changed later.
   - Working Time Attendant: This can be the daytime attendant. Requires separate configuration.
   - Holiday Attendant: Attendant for holiday periods. Requires separate configuration.

3. When you have finished making any required changes, click **Apply → OK**.

**Modifying and creating AutoAttendant prompts**

As mentioned, the default AutoAttendant is called *operator* and comes pre-configured with limited options. These options can be extended. Alternatively, a new attendant can be made from scratch if desired. For the purpose of this example, the operator attendant will be modified.

1. Go to **Features → Auto Attendants** (Figure 6-20).

   ![Figure 6-20 Main Auto Attendant panel](image)

   - Select the **Operator** attendant.
   - If you wish, change the name and add a description.
   - If required, custom voice files can be added to the attendant. These must be recorded in WAV format outside of SCS 2.0 and uploaded manually by clicking **Browse** next to Prompt, and then selecting your file (for example, “Welcome to Company ABC. For sales, press 1, for IT press 2, hold or press 0 to speak to an operator.”) The attendant would be configured based on these options.
5. Some default rules are already configured. To add a new rule, select it from the drop-down menu (Figure 6-21).

![Figure 6-21 Adding rules]

6. In this example we create an extra rule to transfer to extension. To do so, select it from the list and then assign an available key from the dialpad (0–9, *, and # are valid inputs) and then click Add.

7. The parameter prompt is used to specify the destination extension. For example, if you customize a voice prompt and wish option 1 to be used to call the sales department, the parameter could be a hunt group defined for sales or the extension of a sales person.

8. When you have finished customizing the attendant, click Apply → OK.

### 6.6.2 Hunt groups

A hunt group is a group of phones that are configured to behave in a certain way when a particular event occurs. A main example of this event would be that an external caller dials an extension that is bound to a hunt group. Hunt groups significantly reduce the chances of a call being missed because more than one person has the ability to pick up the call. IP (SIP) phones, analog phones (with correct FXS gateway configuration), and softphones can be used in hunt groups. To create a hunt group:

1. Log in to the SCS 2.0 console and go to Features → Hunt Groups → Add Hunt Group.
2. Enter a suitable name, extension, and description.
3. Click Add User.
4. To add specific users, enter their name, then click **Search**. Otherwise, search on the blank field to show all users. See Figure 6-22.

![Hunt Group](image1.png)

**Figure 6-22 Creating a hunt group**

5. Select the users that you wish to add to the group, then click **Select**.

6. Provision the call sequence for the hunt group:
   a. If you wish to change *initially call* (the first action taken when the hunt group is called), select the extension that you wish to move and then click **Move Up**.
   b. Set the expiration time of each extension.
   c. If you wish for the phones of the group to be rung in sequence, leave subsequent *sequence* values as **If no response** (Figure 6-23). If you wish them to call at the same time, change this to **At the same time**.

![Call Sequence](image2.png)

**Figure 6-23 Setting the call sequence**

7. Set voicemail and call forwarding if desired.

8. When you have finished, click **Apply**.
6.6.3 Incoming calls and DDI/DID

Rules are required for incoming calls as well as outgoing calls. If direct dial in (DDI), also known as direct inward dialling (DID), is to be used, this can be configured in SCS 2.0 also.

Take the example of directing the main office number to an AutoAttendant. Use of the default AutoAttendant extension (100) is assumed.

1. Ensure that the default AutoAttendant dial rule is enabled in System → Dial Plans.
2. Open System → Dial Plans → Add New Rule → Custom and provision the dial rule as shown in Figure 6-24.
3. Enable the rule and give it a meaningful name and description.
4. For prefix, enter the incoming telephone number (for example, 555-1234).
5. For resulting call enter 100 and append nothing.
6. Click Apply, then OK.

**Note:** Permissions and gateways are not required for this process.

![Figure 6-24 Provisioning an inbound call to the AutoAttendant](image)
The same principles can be applied for configuring other inbound rules.

6.6.4 Call park

Call parking is similar to holding a call, however, Parked calls are placed in a specific area within Nortel SCS 2.0 and do not tie up a line on a particular phone. An example of call park is if you receive a call that you would like to take in another room. You can dial a park feature, which places the caller into a specific range of numbers on your system. When parking the call, you will be notified of which park extension the call has been assigned to. When you hang up and move to the next room, you simply dial the park extension and the call will be retrieved.

Setting up the call park extension

To set up call parking:

1. Select Features → Call Park → Add Call Park Extension (Figure 6-25).

![Figure 6-25 Setting up call park](image)

2. Enable the park extension and give it a name.
3. Provision an extension for the call park number. This should be outside of the user extension range.
4. Enter a description.
5. Select the default sound file or upload your own. Callers will hear this while they are parked.

Note: Your service provider can determine what received digits are being presented from the public network. For example, they could be the received digits that are being used for DDI. For further details relating to the configuration of scenarios such as DDI numbering schemes, refer to the gateway manufacturer’s own documentation.
6. Configure optional parameters if required:
   - Enable Time Out: After a specified time period passes, the call will be transferred back to the user who parked the call. Click Show Advanced Settings to configure this.
   - Allow Multiple Calls: Allows multiple calls to be placed into the same park queue.
   - Allow Transfer: The parked caller can dial 0 at any time to transfer back to the person who parked the call.

![Software Communication System](image)

**Figure 6-26 Configuring the call park extension**

7. When you are finished, click **Apply → OK**.
Using the call park feature
If you wish to park a call, perform the following steps:

1. During an active call, press Transfer and enter the number of the call park extension (for example, 900), then press the Call button.
2. When you hear the hold music, hang up. The other caller is placed on hold in the park queue.
3. To retrieve the call from any handset active on the SCS 2.0, dial *4 followed by the park extension (for example, *4900). The remote caller is taken out of the park queue and the call is re-established.

Note: *4 is the default feature code for call park. You can verify or change this in System → General → Call Pickup.

6.6.5 SIP trunking
SIP Trunking was introduced in Chapter 3, “Network considerations” on page 21. As discussed, a major advantage of the SIP standard is interoperability between SIP-compliant IP-PBXs. SIP trunking is supported in Nortel SCS 2.0. In the lab environment, we connected the SCS 2.0 system to an Asterisk system on the same LAN.

Note: SIP has known issues with Network Address Translation (NAT) and may require extra hardware such as a STUN server to perform NAT traversal.

Figure 6-27  SIP trunking example

The requirements are to configure an appropriate dial plan for calling the remote system and creation of a SIP trunk gateway (to Asterisk):

2. Select the Enabled box for the rule.
3. Give a meaningful name and description.
4. For Dialled Number enter the extension plan of the remote IP-PBX. For example, extensions on the remote IP-PBX start with 1 and are 4 digits in total. The prefix would be specified as 1, followed by three numbers, as shown in Figure 6-28.

![Configuring dialed number](image)

**Figure 6-28** Configuring dialed number

5. Enter any required permissions. In the example, there were no specific permissions, as it was only for calling between local IP-PBXs. This would be configured, however, if you were going to place external calls via the remote IP-PBX and wanted to control what kind of calls could be made (for example, international).

6. For resulting call the Dial field is what users on the local IP-PBX will use to place calls to the remote IP-PBX. For example, if you wish to use 6 to dial the remote IP-PBX, users would dial 6-1xxx (where xxx is the remainder of the 4-digit extension starting with 1). Dial is 6 and append in this case is *entire dialed number*.

7. Specify the schedule for the plan. Often this will be set to **Always**.

8. This completes the dial rule, but a *gateway* is required to route the example calls with a 6 prefix to the remote IP-PBX. The gateway can be defined from the bottom of the Dial Rule page.

9. From the Dial Rule page, scroll down to Gateways.

10. From the More Actions menu select **SIP Trunk** (Figure 6-29).

![Adding a SIP trunk](image)

**Figure 6-29** Adding a SIP trunk
11. Configure the trunk as in the example in Figure 6-30:

- **Name**: A meaningful name for the SIP trunk.
- **Address**:
  - PSTN Gateway IP address or fully qualified host name
  - SIP Provider IP address or fully qualified host name (requires session border controller)
- **Description**: Enter a meaningful description for the connection.
- **Route**: In this case, the route is to a proxy (the Asterisk server) on the same LAN and is the same as the address. This could also be the next-hop address (for example, firewall or SBC).

![SIP trunk configuration example](image)

When you have entered the necessary information, click **Apply → OK**.

This completes the necessary configuration for the SIP trunk on Nortel SCS 2.0. The remote IP-PBX configuration may differ. The Asterisk SIP trunking configuration can be seen in Chapter 5, “Deploying and configuring Asterisk for Smart Cube deployment (x86)” on page 71.
6.7 Backing up and restoring SCS 2.0 data

SCS 2.0 comes with the facility to back up and restore data via its administration interface. We recommend backing up data following the initial configuration, and then at appropriate intervals.

6.7.1 Backing up SCS 2.0 configuration data and voicemail

To do this:
1. Go to System → Backup.
2. Select the data to be backed up. The default is configuration and voicemail.
3. Enter the number of backups to keep. The default is unlimited. We recommend that you change this to a number that suits specific requirements.
4. Optionally, enter an e-mail address to receive e-mail notifications.
5. If you wish to add a schedule, configure this.
6. Click Backup Now (Figure 6-31).

![Backup settings](image)

**Figure 6-31  Successful backup**

7. Download the files as prompted and store them in an appropriate location, preferably off-site.

This completes the SCS 2.0 backup process.

6.7.2 Restoring SCS 2.0 configuration data and voicemail

Go to System → Restore.
Chapter 6. Deploy and configure IBM Smart Business and Nortel SCS 2.0 on IBM i

155

**Restore from SCS 2.0 Server**

To do this:

1. The default source for backup is *backup folder*, which is stored on the SCS 2.0 hard drive. You do not need to know the file location.

2. Select the data that you wish to restore, be it configuration, voicemail, or both, and click **Restore**.

3. When prompted to confirm, select **Yes**.

**Note:** The backup names are made up of a time stamp in the format *YYYYMMDDHHMM* (for example, 200811281448 is 28th November, 2008, 2.48PM). Use this to identify the correct backup. The newest files are at the bottom.

**Restore from backup file**

To do this:

1. Go to **System → Restore → Backup File Upload**.

2. For both configuration and voicemail click **Browse** and select the files that were saved at the time of backup.

3. Click **Restore**.

**Note:** You will *not* be prompted to confirm restoration with this method.

The server will restart and the data will be restored. This takes up to 5 minutes. When the restoration is complete, the login page appears.
6.8 Uninstalling the Nortel SCS 2.0 Smart Business Connector

To uninstall the SCS 2.0 Smart Business components, first uninstall the Nortel SCS 2.0 application from the Smart Business Administrator Panel. Then manually complete the uninstall by executing the SCS-SmartBus uninstall script.

**Note:** Uninstalling the Nortel SCS 2.0 application from the Smart Business Administrator Panel does not uninstall the SCS 2.0 server. However, all Nortel links and application downloads will be removed from the Smart Business Administrator Panel.

Running the SCS-SmartBus uninstall script removes files added during the install from the Nortel directory. Additionally, client install packages from the end user catalog are removed, along with NFS mounts to log files, SCS 2.0 Connector application files, and the `/etc/scsbbp` code directory.

**Note:** Both the Administrator Panel uninstall and the SCS-Smartbus uninstall script must be completed in order to allow a reinstall of the SCS-SmartBus components at a later date.

To uninstall SCS-SmartBus:

1. Navigate to **Smart Business Administrator Panel ➔ Nortel SCS 2.0.**
2. Select **Uninstall SCS 2.0** and accept the resulting prompt (Figure 6-33). This removes the SCS 2.0 links to the Smart Business Application Integrator, but it does not remove the directories and files added during the install.

![Confirming uninstallation of SCS 2.0 from Smart Business](image)

Figure 6-33   Confirming uninstallation of SCS 2.0 from Smart Business

This completes the steps to remove the components from the Smart Business Administration Panel. Next, the SCS Smart Business uninstall script must be run:

1. Start a 5250 session to IBM i. Log in with a user ID with admin privileges (for example, adminsys).

2. Start a Q-shell session by executing the command:
   ```
   QSH
   ```

   **Note:** The Q-shell should be used by experienced IBM i systems administrators only.

3. Check the current working directory by issuing the command:
   ```
   pwd
   ```
The result should be something like in Example 6-2.

**Example 6-2  Showing the present working directory in the IBM i IFS**

```
$ > pwd
/  
$  
```

/ indicates that you are in the root directory of the IFS. If your result appears as /etc/scsbbp/ then it is necessary to change the directory. Change to the root directory by issuing the command:

cd /'

**Note:** The uninstallation script removes the scsbbp directory, so a number of error messages appear if you attempt to run the script when the present working directory is /etc/scsbbp/.

Execute the uninstallation script by entering:

```
/etc/scsbbp/scsi5_uninstall.sh
```

Refer to IBM technical documentation for instructions for manually re-adding this package to the list of applications available for installation.

The SCS 2.0 server installation image (ISO) (which was pre-loaded in the Nortel directory) remains on the Smart Cube hard drive. If reinstalling the SCS 2.0 server, the SCS LPAR can be reconfigured to boot from the virtual optical driver (which is mapped to the ISO image), which reinstalls and initializes the SCS 2.0 server.

### 6.9 Summary

In this chapter the entire installation process of the Nortel SCS 2.0 IP Telephony system was discussed and illustrated. System preparation, installation, setup, and user-provisioning were all highlighted.
Differences between x86 and IBM i for VoIP

This chapter discusses the key differences between the x86 and the IBM i platforms for Voice over IP (VoIP) on IBM Smart Business.
7.1 Telephony offered

At the time of writing, the telephony package available on the x86 Smart Cube is Asterisk from Digium, while the IBM i solution is Nortel SCS 2.0. These are available from Smart Market.

IBM Smart Business for IBM i can also be ordered with Nortel pre-packaged, leaving minimal setup for customers and systems integrators.

7.2 System architecture

In this section we compare the different system architectures with the IP Telephony offered.

7.2.1 x86

The x86 solution is an appliance for running ISV applications. The operating system (SUSE Linux Enterprise Edition) and middleware are provided by IBM. The x86 Smart Cube is a black box solution. It only runs applications from the Smart Market. Also included is Samba, a file and print server for Linux.

Resources such as random access memory (RAM) and network adapters are all physical and owned by the single Linux operating system.

7.2.2 IBM i

The IBM i Solution is offered in two flavors:

- A prepackaged solution can be purchased, which is a new POWER system with pre-installed applications including Nortel SCS 2.0 if selected. Much of the setup is configured before shipping, but some specific configuration including network details must be performed after the Smart Cube is installed.

- The second option is to integrate Smart Business into an existing IBM i V6R1 environment. This requires far more setup than the pre-packaged solution, including creation of logical partitions (LPARs) and virtual resources for applications running on the LPAR (that is, Nortel SCS 2.0).

<table>
<thead>
<tr>
<th>Feature</th>
<th>x86</th>
<th>IBM i</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preloaded telephony – Nortel SCS</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td>Telephony offered in Smart Market – Nortel SCS</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td>Telephony offered in Smart Market - Asterisk</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td>Single partition/VM</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td>Dedicated partition/VM for IPBX server</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td>Softphone downloadable from Software Catalog</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

Figure 7-1  VoIP feature overview of IBM Smart Business on x86 and IBM i.
Chapter 8. Configuring and deploying Voice over IP (VoIP) hardware for x86

In this chapter we help you to plan and prepare for implementing a VoIP solution on the IBM Smart Business Platform. This chapter includes the following topics:

- “Attaching handsets (SIP phones)” on page 162
- “Attaching analog phones using FXS gateways” on page 164
- “Attaching FXO gateway devices” on page 167
- “Working with telephones and adapters that are not IBM verified” on page 168
8.1 Attaching handsets (SIP phones)

IBM Smart Business Platform supports a wide range of Session Initiation Protocol (SIP) compliant devices and has the ability to automatically discover devices attached to your network. Perform the following steps after you have attached handsets to your network:

1. Open the Asterisk panel found under Your Applications on the IBM Smart Business Administrator Panel (accessed via IBM Smart Cube Home and clicking the Go to the Administrator Panel button).

2. Within the Asterisk control panel, select Phones and Adapters from the menu on the left.

   **Note:** When deploying handsets to users, you must keep track of the MAC addresses of the devices in order to ensure that the correct users are assigned to the correct handsets.

The system then automatically runs a discovery and shows you what is currently connected. The time taken for this discovery to complete depends on the number of devices attached. On completion of the discovery, you will see the page shown in Figure 8-1.

![Figure 8-1 Results of the device discovery](image)

To configure a device:

1. Select the check box in the Select column corresponding to your device.

2. Open the Actions menu and select Change Settings.
3. In the Extension box, configure the details for the new phone, assigning an extension and user. In the Options box, provision voicemail if applicable. We recommend that you enable **Send voicemail to email address** if voicemail is in use, particularly for users who have both soft and hard phones. If this phone is to make external calls, ensure that the **Place external calls** box is selected. This process is highlighted in Figure 8-2.

*Figure 8-2  Adding a new SIP handset*
4. When you have entered all the details, click **Configure**. You will be taken back to the Phones and Adapters panel, where Unknown will be displayed in Status column while configuration is sent to the phone. After a few minutes, the phone will reboot and then become available for use. The list must be refreshed from the Actions menu before Active will be shown as the status, as shown in Figure 8-3.

![Phones and Adapters](image)

**Figure 8-3** A newly configured handset

This process should be repeated for all of the hardphones attached to your Smart Cube.

**Note:** If status is shown as Configuration Mismatch, this means that the phone configuration does not match the server configuration. To resolve this, remove the configuration and then perform the setup process again. If the status remains as is or changes to Unknown after a period of time, this means that the phone is configured but is currently not detected. Ensure that it is properly connected and powered on.

### 8.2 Attaching analog phones using FXS gateways

Analog devices can be integrated into your IBM Smart Business environment with the use of a Foreign Exchange Station (FXS) gateway. The process of adding an FXS gateway to the system is very similar to adding a phone.

**Note:** Not all FXS gateways are verified for use with the Smart Cube's automatic discovery and configuration utilities. Refer to 8.4, “Working with telephones and adapters that are not IBM verified” on page 168.

To set up your FXS gateway:

1. Attach your FXS gateway to your network infrastructure and power it on. Allow a few minutes for the device to boot.
2. Open up **IBM Smart Business Administrator Panel** → **Asterisk** → **Phones and Adapters**.
The discovery process runs and the results are displayed (Figure ).

![Phones and Adapters](image)

**Figure 8-4  Results of device discovery following FXS gateway connection**

**Note:** Each port on your FXS gateway is shown as a separate device and must be configured independently. A 4-port gateway was used in this example.

3. As with setting up an IP phone, select the check box of the FXS port that you wish to configure, then select **Actions → Change Settings**.
Figure 8-5 shows the setup page for the analog phone.

![Phones and Adapters](image)

Figure 8-5  Setting up an analog phone

4. When you have entered all the details, click **Configure** to apply the settings to the FXS port. You will be taken back to the Phones and Adapters page, where the status Unknown will be displayed while the device is configured. After a few minutes, the port will become available for use. The list must be refreshed from the Actions menu before the status will show as Active.

**Note:** If after configuration the status is Configuration Mismatch, this means that the device configuration does not match the server configuration. To resolve this, remove the configuration from the device and then perform the setup process again. If the status remains as or changes to Unknown after a period of time, this means that the device is configured but is currently not detected. Ensure that it is properly connected to the network and powered on.
8.3 Attaching FXO gateway devices

A Foreign Exchange Office (FXO) gateway allows your system to connect to the Public Switched Telephone Network (PSTN) via regular analog (plain old telephone service (POTS)) lines, allowing you to make external calls. The process of adding an FXO gateway to the system is simple, but some specific configuration will depend on the model that you are using. Refer to the manufacturer’s manual for any advanced configuration.

1. Attach your FXO gateway to your network infrastructure and power it on. Allow a few minutes for the device to boot.
2. Open up IBM Smart Business Administrator Panel → Asterisk → Gateways.

As in previous steps, a discovery will be performed and verified devices will be shown in the results, as seen in Figure 8-6.

3. To configure the FXO gateway, select the check box and then click Actions → Change Gateway Settings. As you can see from the configuration page, minimal configuration is required for supported gateways. If you wish to do an advanced configuration, use the link shown next to IP Address (Figure 8-7). Otherwise, give the device a description and then click Configure.
You will be taken back to the Gateways page, where the status Unknown will be displayed while the device is configured. After a few minutes, the device becomes available for use. The status shows as Active following a refresh of the page, as seen in Figure 8-8.

![Gateways](image)

**Figure 8-8  Successful FXO gateway configuration**

## 8.4 Working with telephones and adapters that are not IBM verified

When configuring a telephone or adapter that is not IBM-verified, you must assign an existing extension to it and then use the manufacturer's configuration page to set it up. To determine whether a device is IBM-verified, refer to:

https://clientcare.custhelp.com/cgi-bin/clientcare.cfg/php/enduser/acct_login.php

Select **Answers** from the options at the top and search for supported VoIP handsets. You must register if you have not done so previously. The verified device list in the knowledgebase means that the device can be found and configured by the Smart Cube. It does not mean that the device is verified to work on the PBX that you are running. Devices that are not verified do not appear in discovery results for either phones and adapters or gateways and cannot be automatically configured.

To set up such a device on your system:

1. Create an extension and assign it to a user.
2. Refer to the instructions from the device's manufacturer to configure the device. You will specify the server IP address, the extension (use this as the account number), and the account password that you specified when you created the extension.
Unified communications configuration

This chapter starts with a general overview of unified communications in Chapter 9, “Unified communications configuration” on page 169.

The remaining sections of this chapter discuss x86 and IBM i specific instructions for setting up and using the IBM Smart Business Phone.

For IBM Smart Business Phone for x86 we discuss:

- “Overview of interaction between IBM Smart Business Phone and Sametime voice” on page 170
- “Configuring the IBM Smart Business Phone and Sametime voice on x86” on page 171
- “Using the IBM Smart Business Phone and Sametime voice” on page 175

For IBM Smart Business Phone for IBM i we discuss:

- “Configuring the IBM Smart Business Phone on IBM i” on page 187
- “Using the IBM Smart Business Phone with IBM i” on page 192
9.1 Unified communications overview

Unified communications (UC) is the term used to simplify and integrate all forms of communications. It is typically a software program and infrastructure improvement. In general, it allows an individual to send or receive a message on one medium and received on another. For example, one can receive a voicemail message and then read it in her e-mail inbox using a unified communications program.

The communications leveraged by this term can include phone, e-mail, chat, voice mail, and fax. The typical software program unifies these communication mediums so that any activity or message can be easily transferred to another. A successful implementation can automate and unify all forms of human and device communications into a common user experience. Gains in efficiency can result through an optimization of business processes and enhancing human communications, reducing latency, managing flows, and eliminating device and media dependencies.

9.2 Overview of interaction between IBM Smart Business Phone and Sametime voice

This section introduces the upcoming sections and provides a common understanding of the interaction between the IBM Smart Business Phone and Sametime voice.

On the left in Figure 9-1 you can see a IBM Lotus Sametime client, which is made of different components. A default component of the Sametime client is the Sametime voice part. Other components would be instant messaging, chat history, and more.

The IBM Smart Business Phone is an independent application that is installed separately and is incorporated into Sametime. It is a so-called plug-in to the Sametime client. Once installed it appears as an additional application in the Sametime client and can be used to place calls. We discuss this in more detail in 9.4.1, “Place a call” on page 175, including step-by-step instructions.
The Sametime voice part of the Sametime client is used to offer the click-to-call functionality. Click-to-call is an easy way to start a voice conversation by just clicking a user’s name in the Sametime contact list instead of dialing a number. Click-to-call is explained in more detail in 9.4.3, “Click-to-call” on page 177.

However, it is important to understand that even if the IBM Smart Business Phone is part of the Sametime Client there is no direct interaction between Sametime voice and the IBM Smart Business Phone. This is highlighted by the red arrow in Figure 9-1 on page 170. When a click-to-call request is placed it is sent to the Sametime server, including all the information to establish the call. The TCSPI integration allows the Sametime server to communicate with the IP-PBX and the other way around. The TCSPI is a set of Java™ classes that enable telephony service providers to integrate audio conference call technology into IBM real-time collaboration server offerings.

9.3 Configuring the IBM Smart Business Phone and Sametime voice on x86

This chapter provides step-by-step instructions on how to configure the IBM Smart Business Phone and the Sametime voice part in order to have them work together. There are a couple requirements that must be met prior to configuring a IBM Smart Business Phone on a user’s computer.

9.3.1 Requirements

The requirements are:

- IP-PBX is installed on the IBM Smart Cube.
  Refer to Chapter 5, “Deploying and configuring Asterisk for Smart Cube deployment (x86)” on page 71, for guidance on how to install the IP-PBX.
- A user ID that is assigned a IP phone system extension.
  - Refer to Chapter 2, “Overview of Voice over IP Technology in IBM Smart Business” on page 13, to create a new user.
  - Refer to Chapter 5, “Deploying and configuring Asterisk for Smart Cube deployment (x86)” on page 71, to assign an extension to an existing user.
- Install the Lotus Sametime 8 client (explained in the following pages).
- Install the IBM Smart Business Phone on top of Lotus Sametime 8 (explained in the following pages).

Sametime instant messaging is a core component of IBM Smart Business. In order to take advantage of the VoIP and Sametime integration you must first configure the Sametime component on the IBM Smart Cube. To do this you must run the Smart Business Application installer and select to install the Sametime component.

Note that it is possible to download the Sametime client for use with the IBM Smart Business Softphone without using the Sametime server function.
9.3.2 Installation and configuration

The following steps explain how to install and configure the IBM Smart Business Phone and Sametime voice.

1. Open the IBM Smart Business Launch from your desktop, execute **User Programs Catalog** (Figure 9-2), and log in using the user ID.

![Figure 9-2 IBM Smart Business Launch: User Programs Catalog](image)

2. Download and install the Lotus Sametime 8 Entry Multi Language Installer. Once completed, download and install the IBM Smart Business Phone Installer.

   **Note:** Ensure that you select the **Install and Configure** option during the installation of the IBM Smart Business Phone.

   Your are prompted to enter a user ID and password in order to retrieve the associated extension. Use the IBM Smart Business user ID.

![Figure 9-3 Users Programs Catalog](image)

3. Start IBM Lotus Sametime from the icon on your desktop called Lotus Sametime Connect. Use your IBM Smart Business ID to log in to Sametime.
4. Once Sametime has started up it appears as shown on Figure 9-4 on the left. To see the IBM Smart Business Phone, select the **Restore** button, which is highlighted by the red arrow in Figure 9-4.

At the bottom of the IBM Smart Business Phone you see **Ready** followed by our extension. In the case in Figure 9-4 it appears to be **Ready 1002**. This means that the IBM Smart Business Phone is connected to the IP-PBX.

**Note:** You are not required to log into Sametime to use the softphone. You do need to log into Sametime if you want to use click-to-call on your Sametime contacts.

---

**Figure 9-4**  IBM Lotus Sametime including IBM Smart Business Phone
5. The IBM Smart Business Phone is now configured successfully and will allow you to place calls to other devices that are already configured. However, in order to also enable the telephony capabilities in Sametime that allow click-to-call, a little more configuration is required.

**Note:** What is click-to-call? Basically, it is a instant messaging (IM) related function that a lot of common IM solutions support. Instead of dialing a number to initiate a call you simply click a user’s name in Sametime and choose **Call**. Sametime then starts the call for you.

a. Go to **File → Preferences → Telephony, Audio and Video → Preferred Numbers**.

b. Click the **Add New Number** button.

c. Enter your extension shown as ready at the bottom of the IBM Smart Business Phone (Figure 9-4 on page 173).

d. Select **Apply** so save all the settings and close the window.

![Preferred Numbers](image)

*Figure 9-5  IBM Lotus Sametime: Preferences*

The IBM Smart Business Phone and the click-to-call capabilities in Sametime are now configured and ready to place/receive calls.
9.4 Using the IBM Smart Business Phone and Sametime voice

This section assumes that all the steps described earlier in this chapter were completed successfully and that IBM Lotus Sametime is running and connected to the server.

9.4.1 Place a call

The IBM Smart Business Phone offers five independent phone lines. The following steps explain how to place a call on line 1.

As shown in the left of Figure 9-6, you have either the possibility to Input phone number here or to dial a number by using the keypad. In either case click the Call button to initiate the call.

Once the Call button is clicked the calling status to extension 2001 appears, as shown in Figure 9-6 in the middle panel. Click the Cancel button if you would like to end the call while it is ringing.

The image on the very right in Figure 9-6 displays the status once the call is established. Press the End Call button to end the call.

In case you would like to place a second call, select Line 2 and repeat the steps mentioned earlier. The call on line 1 remains paused, which allows you to switch between line 1 and line 2.

![Figure 9-6 IBM Smart Business Phone: Place a call](image)

9.4.2 Call transfer

The IBM Smart Business Phone allows you to transfer an existing call to another extension. In order to transfer a call we assume that you to already have an existing call established, as described in 9.4.1, “Place a call” on page 175.
On the call window of the IBM Smart Phone select the Transfer to → Other option (Figure 9-7).

Another window called Transfer to opens asking you for the number to forward to. Enter the extension and click OK. You are informed that the call was transferred successfully. At the same time your IBM Smart Business Phone disconnects and the extension that you forwarded the call to starts ringing.

Figure 9-7 IBM Smart Business Phone: Call transfer
Let us look at Figure 9-8 to understand how the call transfer works based on the above example:

1. A call from the IBM Smart Business Phone extension 1002, in that case a desktop phone with extension 2001, is established.
2. The transfer from extension 1002 to 1001 is initiated.
3. The call between extension 1002 and 2001 is ended. At this point the IBM Smart Business Phone with extension 1002 is no longer part of the call.
4. Extension 1001 rings and the call is established.

![Diagram of call transfer](image)

**Figure 9-8** Transfer an existing call to another extension

### 9.4.3 Click-to-call

The embedded call functionality in IBM Lotus Sametime allows you to simply initiate a call out of Sametime instead of entering a number to dial. Ensure that you have completed all the steps described in 9.2, “Overview of interaction between IBM Smart Business Phone and Sametime voice” on page 170, in order to ensure that the click-to-call function works properly.

**Note:** The caller and the called person must be online in Sametime. Otherwise, the call cannot be placed or received.

There are two ways to start a click-to-call conversation starting from the main Sametime window.
Option one
The first option is to:
1. Select a person's name from the buddy list in Sametime.
2. Click the telephone icon, as shown in Figure 9-9.

Option two
The second option is to:
1. Right-click a person's name in your buddy list in Sametime.
2. Select Call, as indicated in Figure 9-10.

3. As soon as you initiate a call using click-to-call the IP-PBX sets up a call between you and the called person. For that reason you receive the pop-up message shown in Figure 9-11 to answer to decline the call.
4. Once the call from the IP-PBX is answered you will see yourself listed as connected in the call window (Figure 9-12). The same happens when the called party answers.

Figure 9-12 IBM Lotus Sametime: Click-to-call - Call window

Figure 9-13 explains how the click-to-call conversation is initiated.

1. Initiate the call in Sametime using click-to-call and clicking a user's name. The call is sent to the Sametime server, which tells the IP-PBX to take the next action.

2. The IP-PBX first calls the user who initiated the call, which is extension 1002.

3. Once this user accepted the call, the IP-PBX initiates the second call to the called person Fabrizio with extension 1003.

4. Once the two called parties accepted the call invitation the call is established.

Figure 9-13 Click-to-call using IBM Lotus Sametime
9.4.4 Receive a call: Basic configuration

When receiving a call the incoming call message (shown on the left in Figure 9-14) appears. That is the number defined in 9.2, “Overview of interaction between IBM Smart Business Phone and Sametime voice” on page 170, which is the number of the IBM Smart Business Phone.

Once the call is accepted the second incoming call window pops up to answer the call from the IP-PBX, as shown on the right in Figure 9-14.

![IBM Smart Business Phone: Incoming call](image)

9.4.5 Conference up to five participants

There are two ways to create a conference call using the IBM Smart Business Phone:

- Dial the numbers.
- Use click-to-call.
Option one
Set up a call as described in 9.4.1, “Place a call” on page 175, as shown on Figure 9-15:

1. Click the Line 2 tab at the bottom of the IBM Smart Business Phone and establish a second call.
2. Select the Start Conference button.
3. Select the lines that you want to conference together and click OK. The conference between the two lines and yourself is now established.
4. Either click the End Conference button to end the entire conference or click End Call to remain connected with extension 2001, as in case of the example in Figure 9-15.

![IBM Smart Business Phone: Conference](image)

Figure 9-15 IBM Smart Business Phone: Conference
Option two
Set up a call as described in 9.4.3, “Click-to-call” on page 177, as shown on Figure 9-16:

1. Select Invite Others in the top left corner of the call window.
2. Start typing the name of the person who you like to add the existing call.
3. Click the person’s name to add it to the Invite to Call window.
4. Click the Send button to call the appropriate user.

The last image shows that the person added the existing call.

Figure 9-16   IBM Smart Business Phone: Click-to-call conference
9.4.6 Record a call

By default, any recorded information is saved in the folder `C:\Documents and Settings\Administrator`. This setting can be changed under **File → Preferences → IBM Smart Business Phone → Application**. Then modify the record call location path as desired.

To record a call:
1. Place a call.
2. Once the call is set up, press the **Start Recording** button, as shown in Figure 9-17.
3. In order to stop recording click the Stop Recording icon again.

![IBM Smart Business Phone: Recording a call](image)

9.4.7 Advanced usage of the IBM Lotus Sametime voice functionality

Advanced configuration in IBM Louts Sametime allows you to personalize the way that you receive and place calls. The following is an example of using several phones in a office environment.

**Important:** Consider that the following explanations only apply to calls placed via click-to-call in IBM Lotus Sametime.

Any calls placed directly from the IBM Smart Business Phone are not impacted by the settings described in this advanced usage part of this chapter.

1. If you worked through the instructions given in 9.3, “Configuring the IBM Smart Business Phone and Sametime voice on x86” on page 171, you have already configured one preferred number in Sametime. We now add additional numbers to work with later:
   a. In Sametime go to **File → Preferences → Telephony, Audio and Video → Preferred Numbers** and create at least one other preferred number.
As shown on Figure 9-18, we used:

- 1002 as the IBM Smart Business Phone extension
- 2002 as the Deskphone extension of the same user assigned to the extension 1002
- 2003 as an additional extension assigned to someone else

Select **Apply** after each number that was created to save the changes.

![Preferred Numbers](image)

*Figure 9-18  IBM Lotus Sametime: Preferences - Preferred numbers*
2. In the Sametime Preferences window select **Notifications**. Uncheck the telephony notification to display incoming invitations, as shown on Figure 9-19, then close the Preferences window. By changing this setting you will no longer be prompted with the message described in 9.4.4, “Receive a call: Basic configuration” on page 180.

The next step explains how you are still able to manage your calls and how they are sent automatically to another extension.

![Figure 9-19 IBM Lotus Sametime: Preferences - Notifications](image1)

3. Going back to the Sametime client you can see the created extensions when selecting the green telephone icon on top (Figure 9-20).

In the case in Figure 9-20, the IBM Smart Business Phone with extension 1002 is selected as the phone to ring on an incoming click-to-call.

![Figure 9-20 IBM Lotus Sametime: Select desired device](image2)
Looking at page capture on Figure 9-21, a desk phone with extension 2002 is selected as the device to ring when receiving or placing a click-to-call.

![Figure 9-21  IBM Lotus Sametime: Select desired device](image)

Now let us look more closely at what it means to have set the ring device to MyDeskphone to extension 2002.

Figure 9-22 depicts the behavior of placing a click-to-call call.

![Figure 9-22  Click-to-call using IBM Lotus Sametime: Send call to other ring device - Place call](image)
Figure 9-23 explains the behavior when receiving a click-to-call call.

1. The caller starts a click-to-call conversion, in this example to user Fabrizio. The call is sent to the Sametime server with the information to establish a call between MyDeskphone (extension 2002) and user Fabrizio (extension 1003). This information is forwarded to the IP-PBX.


3. When this call is answered, the IP-PBX initiates the call to extension 1003.

4. Once that call is answered, the call between user Fabrizio and MyDeskphone is established.

5. The caller (Fabrizio) starts a click-to-call conversion to Laurent (extension 1002). This request is sent to the Sametime server, which hands it over to the IP-PBX.

6. The IP-PBX initiates a call to the caller's extension 1003 (user Fabrizio).

7. Once the call is answered, the second call to extension 2003 (user Laurent who has defined his ring device to be MyDeskphone) is placed.

8. Once that call is answered, the call between user Fabrizio and user Laurent on MyDeskphone is established.

9.5 Configuring the IBM Smart Business Phone on IBM i

This section provides step-by-step instructions for configuring the IBM Smart Business Phone with an extension.
There are a couple of requirements that must be met prior to configuring an IBM Smart Business Phone on a user’s computer.

9.5.1 Requirements

The requirements are:

- IP-PBX installed on the IBM Smart Cube: Refer to Chapter 6, “Deploy and configure IBM Smart Business and Nortel SCS 2.0 on IBM i” on page 121, for guidance on how to install the IP-PBX.
- A user extension on the IP-PBX (Nortel): Refer to Chapter 6, “Deploy and configure IBM Smart Business and Nortel SCS 2.0 on IBM i” on page 121, to create a new user extension.
- Install Lotus Sametime 8 client (explained in the following pages).
- Install the IBM Smart Business Phone on top of Lotus Sametime 8 (explained in the following pages).

9.5.2 Installation and configuration of the IBM Smart Business Phone

To install and configure the IBM Smart Business Phone for IBM i:

1. Open the IBM Smart Business Launch from your desktop, execute User Programs Catalog, and log in using the user ID (Figure 9-24).

![Figure 9-24 IBM Smart Business Launch: User Programs Catalog](image)
2. Download and install the Lotus Sametime 8 Entry Multi Language Installer (Figure 9-25).

![Software Catalog](Image)

**Figure 9-25  Users Programs Catalog**

3. Download the IBM Smart Business Phone Installer and start the installation. On the second installation page it is very important to select **Install only**. See Figure 9-26.

![IBM Smart Business Phone Installer](Image)

**Figure 9-26  IBM Smart Business Phone: Installation for IBM i**

4. Start IBM Lotus Sametime from the Lotus Sametime Connect icon on your desktop. Use your IBM Smart Business ID to log in to Sametime.

   **Note:** You are not required to log into Sametime to use the softphone. You do need to log into Sametime if you want to use click-to-call on your Sametime contacts.
5. Once Sametime started it appears as shown in Figure 9-27. To see the IBM Smart Business Phone, select the **Restore** button, which is highlighted by the red arrow.

![Figure 9-27](image)

**Figure 9-27** IBM Lotus Sametime: IBM Smart Business Phone

6. In IBM Lotus Sametime go to **File → Preferences → IBM Smart Business Phone**.
Complete the display name, extension, password, and domain settings, which are highlighted in Figure 9-28, and click **Apply**.

![Figure 9-28 IBM Lotus Sametime: IBM Smart Business Phone preferences](image)

**Important:** The password used for the configuration is the SIP password. This password is generated randomly when an extension is created. As the password is not known, you must define a new SIP password in the Nortel administration.

Enter the fully qualified domain name of the IP-PBX partition of IBM i. Otherwise, the IBM Smart Business Phone might not be able to connect.

Refer to Chapter 6, “Deploy and configure IBM Smart Business and Nortel SCS 2.0 on IBM i” on page 121, to set a new SIP password in Nortel.
7. When you can see Ready followed by the extension on the left bottom of the IBM Smart Business Phone it is configured and ready to use. See Figure 9-29, which shows Ready 202.

![IBM Lotus Sametime: IBM Smart Business Phone](image)

Figure 9-29 IBM Lotus Sametime: IBM Smart Business Phone

Refer to Chapter 10, "Troubleshooting VoIP configuration" on page 195, in case of installation or configuration problems.

### 9.6 Using the IBM Smart Business Phone with IBM i

In this section we describe the IBM Smart Business Phone with the IBM i solution.
9.6.1 Place a call

The IBM Smart Business Phone offers five independent phone lines. The following steps explain how to place a call on line 1.

1. As shown on the left in Figure 9-30, you have the possibility to input phone number here or to dial a number using the keypad. In either case, click the **Call** button to initiate the call.

2. Once the Call button is clicked the calling status to extension 2001 is shown in Figure 9-6 on page 175 in the middle. Click the **Cancel** button if you would like to end the call while ringing.

3. The image on the very right in Figure 9-6 on page 175 displays the status once the call is established. Click the **End Call** button to end the call.

4. In case you want to place a second call, select **Line 2** and repeat the steps mentioned earlier. The call on line 1 remains paused, which allows you to switch between line 1 and line 2.

![Figure 9-30 IBM Smart Business Phone: Place a call](image)

9.6.2 Receive a call

Figure 9-31 shows an incoming call. Either answer to establish the call or decline to cancel the call. When declining, the caller is sent to the message center.

![Figure 9-31 IBM Smart Business Phone: Incoming call](image)
9.6.3 Conference up to five participants

Set up a call as described in 9.6.1, “Place a call” on page 193. As shown on Figure 9-32:

1. Switch to the Line 2 tab at the bottom of the IBM Smart Business Phone and establish a second call.
2. Select the Start Conference button.
3. Select the lines that you want to conference together and click OK. The conference between the two lines and yourself is now established.
4. Either click the End Conference button to end the entire conference or click End Call to remain connected with the extension 2001 in the case of Figure 9-32.

![Figure 9-32 IBM Smart Business Phone: Conference](image)

9.6.4 Record a call

Refer to 9.4.6, “Record a call” on page 183.
Chapter 10. Troubleshooting VoIP configuration

In this chapter we discuss troubleshooting methods for issues that may occur on your Voice over IP (VoIP) system.
10.1 IBM Smart Cube troubleshooting (x86)

In this section we discuss common problems that you may encounter when working with the IBM Smart Cube on the x86 solution.

10.1.1 My power light is not on

When this LED is lit, it indicates that the server is turned on. When this LED is off, it indicates that power is not present or that the power supply or the LED itself has failed. The LED will flash if the system is turned off and the power cord is still attached to the server. Note that if this LED is off, it does not mean that there is no electrical power in the server. The LED might be burned out. To remove all electrical power from the server, you must disconnect the power cords from the electrical outlets.

10.1.2 The amber system-error light is on

When this amber LED is lit, it indicates that a system error has occurred. A LED on the system board might also be lit to help isolate the error. For more information consult the Problem Determination and Service Guide on the documentation CD that came with your system.

10.1.3 I do not have my IBM Smart Desk V1.1.0 CD

You can order a copy of the IBM Smart Desk V1.1.0 CD from IBM Passport Advantage®. Note that IBM Passport Advantage requires an IBM ID.

10.1.4 I need help configuring a new printer

To set up a printer to use with your IBM Smart Cube:

1. Remove the printer from the packaging materials. Set up the printer according to the instructions provided by the printer manufacturer.
2. Attach the power cord to the printer and plug it into the wall socket.
3. Make sure that the Smart Cube is turned on.
4. Attach the printer to the Smart Cube or router.
   - For a direct-attached printer (the printer attaches directly to the Smart Cube), use a USB cable to attach the printer to the system.
   - For a LAN-attached printer (the printer attaches to a router or switch), use a LAN cable to attach the printer to the local (internal) router or switch.

   **Note:** The Smart Cube might not be able to detect the printer if the printer and the Smart Cube are separated by one or more network switches or routers.

5. Turn on the printer.
6. Check to see whether the printer has been configured on the server.
   a. Go to the IBM Smart Business Administrator Panel and click **Printers**.
   b. If the new printer is listed, it has been configured.
7. If the printer is not configured, follow the steps in the User-reported problems page:
   a. From the Printers page, click the **User-reported problems** task.
   b. Specify yourself as the user and printers as the problem area, then click **Next**. The system automatically runs some checks.
   c. If no problems are found, click **Additional server checklist** and follow the instructions.

8. After the printer is configured on the system, follow the appropriate procedure to install it on a user's workstations so she can print to it:
   - If the user has not installed IBM Smart Desk or Quick Start, the printer can be discovered and installed automatically. When Smart Desk or Quick Start is run, accept the option to run the printer setup utility.
   - If the user has already installed Smart Desk or Quick Start, the printer setup utility must be run manually:
     i. From the desktop, open the **IBM Smart Business Launch** folder.
     ii. Double-click **Printer Setup Utility**. This searches for new printers and installs them on the workstation.

### 10.1.5 I need help recovering my system

Follow the steps in this section if you need to recover your system to the initial factory state.
For the latest information refer to the online version of this task at:


If you want to use a backup or your system to restore it instead, follow the steps described below.

**Note:** This procedure removes all data on the system. Data that is currently on the system will not be accessible after this procedure is initiated.

1. Verify that you have all of the image recovery discs including the IBM Smart Business initial image recovery version for SUSE Linux Enterprise Server. All six of the discs are labeled “IBM Smart Business Software Pack, Recovery for SUSE Linux Enterprise Server n of 6.”

2. (Optional) Connect a monitor, keyboard, and mouse. This lets you watch the recovery process.

3. Turn on the system and immediately insert the IBM Smart Business Initial Image Recovery Version for SUSE Linux Enterprise Server disc into the system.

4. When the CD drawer opens, remove the current disc, insert “IBM Smart Business Software Pack, Recovery for SUSE Linux Enterprise Server 1 of 6” and close the drawer. The recovery continues after the disc is properly inserted. Each disc takes approximately 10–15 minutes to process. Important: The discs must be inserted in the correct order. If you insert the wrong disc or insert the disc incorrectly, the CD drawer opens shortly after you close it. This process continues until you correctly insert the appropriate disc.

5. When the CD drawer opens, remove the current disc, insert “IBM Smart Business Software Pack, Recovery for SUSE Linux Enterprise Server n of 6,” as appropriate, and close the drawer. The recovery continues after the disc is properly inserted. Each disc takes approximately 10–15 minutes to process.

6. Repeat step 5 until all supplied discs are processed. After removing the final disc, close the CD drawer.
7. If system recovery encounters an error, the CD drawer opens again after processing all the discs and the system beeps periodically. If there is a monitor connected, the recovery log is displayed. Retry the restore process before contacting support.

8. When the recovery completes successfully, the system turns off.

9. Turn on the system. Open the CD drawer immediately and verify that it is empty.

10. Register your IBM Smart Cube again so that you can configure it. Note that this will mark all applications as inactive and delete the serial number from the profile.
   a. Open a browser and go to the Blue Inventory website:
      \[http://www.ibm.com/smartmarket/support/help\]
   b. Log on by using your Web identity.
   c. Select your site ID, then select the profile name of the Smart Cube that you want to manage.
   d. Click \textbf{Reset Installation Status}, then click \textbf{OK} when asked to confirm.

11. Configure your system by following the instructions in the IBM Smart Business Start Here Poster. You can find it in the IBM Smart Market at:
    \[http://www.ibm.com/smartmarket/support/help/start\]

\textbf{10.1.6 I need help accessing the Linux command line}

Whenever possible you should complete tasks on your Smart Cube using the interfaces provided. However, occasionally you may be directed to access a Linux command line by support personnel.

If you must enter commands on the Linux system, follow these steps to access the Linux command line:

1. From the IBM Smart Business Administrator Panel, click \textbf{IBM Smart Cube}.
2. Click \textbf{Open IBM Smart Business Remote Administration}.
3. Log in with the root user ID and password. The remote desktop opens.
4. Click the \textbf{Gnome Terminal} shortcut. Run the command STRQSH. A window opens that lets you issue Linux CL commands.

\textbf{10.1.7 I need help accessing Linux files}

Whenever possible you should complete tasks on your Smart Cube using the interfaces provided. However, occasionally you may be directed to access Linux files by support personnel.

You must be logged in with the proper authority to work with files on the Linux system. For example, to access files in /root or /etc you must be logged in as root.

1. Follow the first three steps in the previous paragraph to access the remote desktop.
2. Click \textbf{Home Folder File Browser}. The file browser opens.
3. In the left-hand panel, expand folders to access their subfolders. Click folders to view their contents.
4. To open a file in order to view, copy, or edit it, double-click the file name in the right-hand panel. You can use the buttons on the tool bar on top of the window to copy, paste, save, and so on.
10.1.8 I must rediscover my IBM Smart Cube

If you cannot connect to your IBM Smart Cube and it has already been configured, you might need to run the Network wizard. This is an advanced task. For help running this wizard, refer to the IBM Smart Business Network Wizard Guide in IBM Smart Market.

You will typically run the network wizard in one of these situations:

- Your system came preconfigured and you have never been able to access it.
- Your system was moved to a new network and you can no longer access it.

**Note:** In order to run the network wizard, your workstation must be set up this way:

- It must be on the same private network (Ethernet port 1 or eth0) as the Smart Cube that you are trying to access.
- There should not be any routers or firewalls between the Smart Cube and your workstation.
- It must have IBM Smart Desk installed.

To start the Network wizard from a workstation running Windows XP, follow this path: **Start → All Programs → Smart Desk → IBM Smart Business Network Wizard.**

To start the Network wizard from a workstation running Windows Vista, follow this path: **Start → Programs → Smart Desk → IBM Smart Business Network Wizard.**

10.2 IBM Smart Cube troubleshooting (IBM i)

In this section we cover the most common problems when running the IBM Smart Cube on the IBM i solution.

10.2.1 I do not have my IBM Smart Desk V1.1.0 CD

You can order a copy the IBM Smart Desk V1.1.0 CD from IBM Passport Advantage. (IBM Passport Advantage requires an IBM ID.)

10.2.2 Operations Console does not find my system

If you open Operations Console and it does not find your system within a few minutes, it starts a configuration wizard. If this happens, cancel the wizard and close Operations Console, then try the following:

1. Wait 60 seconds, then open Operations Console again. Try this several times, if necessary.

2. If your system still is not detected, there might be a network problem.
   a. Look at the code displayed on the operation panel on the front of the system.
   b. If the code is not C900xxxx or 01, there is probably a network problem.
3. If there is a network problem, try these steps:
   a. Check your network connections. Ensure that all cables are connected to the correct ports and verify that both ends of each cable are secure.
   b. If that still does not solve the problem, IPL (reboot) the system to reset the console:
      i. Press and hold the power button until the panel counts down to zero.
      ii. Wait for the power light to start blinking.
      iii. Press the power button again to start the system.

10.2.3 The IBM Smart Business Setup Wizard did not find my IBM Smart Cube

If the Setup Wizard did not find your Smart Cube, change your private network line to use a static IP address by running the commands in Example 10-1 from an IBM i system console.

Example 10-1 Commands

<table>
<thead>
<tr>
<th>ENDTCPICF</th>
<th>INETNADDR(*IP4DHCP) LIND(ETHPRIVATE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMVTCPICF</td>
<td>INETNADDR(*IP4DHCP) LIND(ETHPRIVATE)</td>
</tr>
<tr>
<td>ADDTCPICF</td>
<td>INETNADDR('private-ip-address') LIND(ETHPRIVATE)</td>
</tr>
<tr>
<td>SUBNETMASK('255.255.255.0')</td>
<td></td>
</tr>
<tr>
<td>AUTOSTART(*YES) TEXT('My Primary Private Address')</td>
<td></td>
</tr>
<tr>
<td>STRTCPICF</td>
<td>INETNADDR('private-ip-address')</td>
</tr>
</tbody>
</table>

10.2.4 The IBM i Access for Windows DVD was not included in my order

If you must install IBM i Access for Windows and the DVD was not included in your order, do the following:
1. Go to the System i Access Ordering and Installing Languages Web page at:
   http://www.ibm.com/systems/i/software/access/windows/languages.html
2. Follow option 1 of the Instructions for Acquiring and Installing Language Versions.

10.2.5 Manage your IBM Smart Cube profiles

Before you begin the Setup Wizard or to install applications using the Application Installer, you must register your IBM Smart Cube at IBM Smart Market:
1. Click Customer support. The IBM Smart Market customer support and FAQs page appears.
2. Under I need help, click the with something I already purchased twistie to expand the section, and then click Manage my IBM Smart Cube profiles.
3. Enter your IBM ID when prompted.
4. Select the profile for the Smart Cube that you are trying to configure and replace the administrator's or the backup administrator's IBM ID with your IBM ID.

While still in Manage my IBM Smart Cube profiles, verify that your applications are associated with the appropriate profile. If not, move it to the proper Smart Cube.

What an IBM ID is and how it is used
An IBM ID and password are associated with each IBM Smart Cube in IBM Smart Market. The administrator who gave you access to your Smart Cube or the person or reseller who
Chapter 10. Troubleshooting VoIP configuration

10.2.6 Find the serial number of my IBM Smart Cube

Your system’s serial number is on the front of your Smart Cube, on the bottom right-hand corner.

10.2.7 Verify that your network is set up properly

Your network must be set up this way for your IBM Smart Cube to work properly:
1. Verify that your administrator PC is on the same subnet as the private IP network for the IBM i dedicated system or partition.
2. Verify that you can connect to the private and public networks and the administrator PC, as applicable:
   a. Open a CL command prompt and run CALL QCMD.
   b. Run PING 'IP address or host name', specifying the following addresses or host names, one at a time, as necessary:
      - Private IP address
      - Public IP address (if a public network has been set up)
      - The host name of the administrator PC
   c. Specify these IP addresses or host names, one at a time, as necessary. If you are testing by using the host name, you must select the protocol for host names.
   d. Verify that the administrator PC can connect to the IBM i system by host name:
      i. Click Start → Run. For Open specify cmd, then click OK.
      ii. At the command line, run the command ping host name, where host name is the host name of your IBM i system.
3. Verify that the administrator PC can connect to the external Internet.
4. Disable any existing IBM i LDAP or SMTP servers, and any *DEFAULT HTTP servers, by running the commands in Example 10-2.

Example 10-2 Commands

```plaintext
ENDTCPSVR SERVER(*DIRSRV)
CHGTCPsvr SVRSPCVAL(*DIRSRV) AUTOSTART(*NO)
ENDTCPSVR SERVER(*SMTP)
CHGTCPsvr SVRSPCVAL(*SMTP) AUTOSTART(*NO)
ENDTCPSVR SERVER(*HTTP) HTTPSVR(APACHEDFT)
CHGTCPsvr SVRSPCVAL(*HTTP) SVRNAME(APACHEDFT) AUTOSTART(*NO)
```

10.2.8 Rediscover my network

If you cannot connect to your IBM Smart Cube and it has already been configured, you might need to run the Network wizard. This is an advanced task. For help running this wizard, refer to the IBM Smart Business Network Wizard Guide in IBM Smart Market:

You will typically run the Network wizard in one of these situations:

- Your system came preconfigured and you have never been able to access it.
- Your system was moved to a new network and you can no longer access it.

In order to run the Network wizard, your workstation must be set up this way:

- It must be on the same private network (ETHPRIVATE) as the Smart Cube that you are trying to access.
- There should not be any routers or firewalls between the Smart Cube and your workstation.
- It must have IBM Smart Desk installed.

To start the Network wizard from a workstation running Windows XP, follow this path: Start → All Programs → Smart Desk → IBM Smart Business Network Wizard.

To start the Network wizard from a workstation running Windows Vista, follow this path: Start → Programs → Smart Desk → IBM Smart Business Network Wizard.

10.2.9 Run a CL command from IBM i Access for Windows

After you have set up your private network, you can run any control language (CL) command from IBM i Access for Windows:

1. Open Start → Programs → IBM i Access for Windows → Emulator and double-click Start or Configure Session.
2. If you already have a session configured, select an existing session and click Start.
3. If you do not have a session configured, create a new session:
   a. Click New Session and enter the following information:
      • System name: The name of the IBM i system to which you will connect.
      • Workstation ID: Specify a name for this workstation. If you leave it blank, the system assigns a name.
      • Type of emulation: Select Display and the size of window that you want.
   b. Click OK. A window opens to let you specify your IBM i signon information. Specify your information and click OK.
4. The emulation session starts, from which you can run CL commands.

Do not use End Connection *YES to log off your emulator session and disconnect from the system. Instead, select Communication → Disconnect from the emulation session window.

10.3 IP telephone call troubleshooting

Occasionally, users may experience issues with telephone calls. Reported problems could include poor quality, low volume, dropped calls, and being unable to make calls. There are several steps that can be taken to avoid and rectify these issues. Ensuring that a solid network is in place, as discussed in earlier chapters (particularly in Chapter 3, “Network considerations” on page 21), is critical to end user acceptance and perception of a new telephony system.
10.3.1 Poor quality calls

Poor quality calls are often related to a network issue. Potential network issues were discussed in Chapter 3, “Network considerations” on page 21. In the event of complaints of poor quality, several checks should be made:

- Check physical cabling to problem handsets.
- Use a network sniffing tool such as Wireshark to analyze network traffic.
- If poor quality calls are isolated to the WAN and do not include PSTN calls, check bandwidth utilization on the line and ensure that a robust QoS policy is in place.

**Note:** If utilizing a WAN/Internet connection for calls, the type of line required varies depending on anticipated call volume. If several concurrent calls, for example, are placed onto an ADSL line, then it should be expected that quality will be poor. For larger call volumes, a WAN technology such as MPLS or a leased line with proper QoS policy should be used.

- Ensure that switchports are running at least 100 MB/Full Duplex and that devices such as gateways match this speed.
- We strongly recommend VLAN use for larger deployments of 50 users or more. This was introduced in Chapter 3, “Network considerations” on page 21.

10.3.2 Dropped/unsucessful calls

Gateway and PBX configuration mismatches (such as codec configuration errors) may cause issues with dropped calls.

**Gateway logs**

Consult your PSTN gateway logs for clues as to the cause of a dropped or unsuccessful call. The International Telecommunication Union (ITU) Q.931 standard defines ISDN call control codes. To access advanced PSTN gateway configuration using IBM verified hardware:

1. Go to **IBM Smart Business Administrator Panel → Asterisk → Gateways**.
2. After the discovery has run, select the check box in the Select column of the gateway that you wish to view.
3. Click **Actions → Change Gateway Settings**.
4. Click the IP address listed next to IP address (Figure 10-1).

![Figure 10-1 Accessing the advanced interface of a PSTN gateway](image)

5. The exact process of viewing logs differs between hardware. consult the manual of the particular product in order to set up and view logging. Typically, the debug level should be set to maximum. Some hardware may only log to a syslog server. There are many free, open-source syslog servers that could be used. Kiwi is one such example. Figure 10-2 shows setting up logging on a Linksys FXO gateway.

![Figure 10-2 Setting up logging on a Linksys FXO gateway](image)

**Codecs**
Some gateways support multiple codecs simultaneously and this can sometimes cause issues. Common protocols used on SIP VoIP solutions include:

- G.711u (typically North America and Japan)
- G.711a (typically Europe and the rest of the world)
- G.729 (much higher compression than G.711, resulting in poorer quality)
As part of the troubleshooting process, forcing your PSTN gateway to use only one codec is worthwhile. Unless you are in an environment where many calls are made over a WAN with low capacity, using a G.711 protocol is more favorable than G.729 due to better quality.

The exact setup of codecs varies depending on hardware. Consult the documentation for your particular product to learn how to check the settings. As a best practice, you should reboot the gateway after the change and, when convenient, ensure a stable running configuration.

**Telephone lines**
As mentioned, telephone lines could also be the cause of your problem. The telco providing the service will be able to perform line tests and traces. Problems should be reported to the telco if they persist after other methods have been pursued. It is likely that they will be able to get more information than the gateway logs can provide, depending on the model of gateway in use.
10.3.3 Configuration issue with IBM Smart Business Phone for IBM i

The following error messages can occur (Figure 10-3):

- BBP22652: Unable to connect to the server.
  Check whether the Nortel service on the IBM Smart Cube is running properly.
- BBP22653: Extension you are trying to use is not valid.
  The domain entered in the IBM Smart Business Phone settings might not be fully qualified.
- BBP22654: The specified password is incorrect.
  Ensure that the password matches the extension entered in the settings.

![IBM Smart Business Phone: Errors](image-url)
Setting up IBM i for Nortel SCS 2.0

This appendix describes the steps required to set up an IBM i for Nortel SCS 2.0.
Creating the Ethernet line description on IBM i

The SCS 2.0 LPAR comes preconfigured with virtual SCSI, virtual serial, and virtual Ethernet adapters. However, an Ethernet line description must be created in IBM i. A review of the communication hardware resources helps to identify the resource for the line description. Perform the following steps:

1. From a 5250 emulation session, issue the following Work with Hardware Resources (WRKHDWRSC) CL command to review the communication resources:

   ```cl
   WRKHDWRSC *CMN
   ```

2. On the Work with Communication Resources display (Figure A-1), a list of the communication resources allocated to the IBM i partition is displayed. The virtual Ethernet adapter will be a CMNxx resource with a type of 268C.

3. To identify the specific resource, type option 7 (Display resource detail) and press Enter next to the resources that meet the preceding criteria.

```
<table>
<thead>
<tr>
<th>Opt</th>
<th>Resource</th>
<th>Type</th>
<th>Status</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>LIN14</td>
<td>2793</td>
<td>Operational</td>
<td>Comm Adapter</td>
</tr>
<tr>
<td>2</td>
<td>CMN23</td>
<td>2793</td>
<td>Operational</td>
<td>Comm Port</td>
</tr>
<tr>
<td>2</td>
<td>CMN24</td>
<td>2793</td>
<td>Operational</td>
<td>Comm Port</td>
</tr>
<tr>
<td>2</td>
<td>LIN01</td>
<td>2849</td>
<td>Operational</td>
<td>LAN Adapter</td>
</tr>
<tr>
<td>2</td>
<td>CMN01</td>
<td>2849</td>
<td>Operational</td>
<td>Ethernet Port</td>
</tr>
<tr>
<td>2</td>
<td>CMB03</td>
<td>268C</td>
<td>Operational</td>
<td>Combined function IOP</td>
</tr>
<tr>
<td>2</td>
<td>LIN02</td>
<td>6B03</td>
<td>Operational</td>
<td>Comm Adapter</td>
</tr>
<tr>
<td>2</td>
<td>CMN02</td>
<td>6B03</td>
<td>Operational</td>
<td>Comm Port</td>
</tr>
<tr>
<td>2</td>
<td>LIN03</td>
<td>6B03</td>
<td>Operational</td>
<td>Comm Adapter</td>
</tr>
<tr>
<td>2</td>
<td>CMN03</td>
<td>6B03</td>
<td>Operational</td>
<td>Comm Port</td>
</tr>
<tr>
<td>2</td>
<td>LIN04</td>
<td>268C</td>
<td>Operational</td>
<td>LAN Adapter</td>
</tr>
<tr>
<td>7</td>
<td>CMN36</td>
<td>268C</td>
<td>Operational</td>
<td>Ethernet Port</td>
</tr>
<tr>
<td>2</td>
<td>CMB02</td>
<td>2844</td>
<td>Operational</td>
<td>Combined function IOP</td>
</tr>
<tr>
<td>2</td>
<td>LIN15</td>
<td>2849</td>
<td>Operational</td>
<td>LAN Adapter</td>
</tr>
</tbody>
</table>
```

Figure A-1  Work with Communication Resources display
On the Display Resource Detail panel (Figure A-2), the details for the selected resource are shown. The Location field indicates the mapping of the i5/OS resource to the LPAR resource. In this example, V1 indicates the partition number (1) and C2 indicates the slot number (2) of the virtual Ethernet adapter.

4. After the resource has been identified, the Ethernet line description can be created. Enter the Create Line Description (Ethernet) CL command, CRTLINETH, and press F4 to prompt the command.

5. On the Create Line Desc (Ethernet) (CRTLINETH) display (Figure A-3), enter the following values:

- **Line description**: We recommend that the line description name reflects that this is a virtual Ethernet adapter as well as the virtual LAN number. As an example, for a virtual LAN adapter on virtual LAN 1, a name like VRTETH01 might be appropriate.
- **Resource name**: Enter the communication resource (CMNxx) identified as the resource that maps to the virtual Ethernet adapter.

Press Enter.
6. Additional fields are now displayed (Figure A-4). Enter the following values:
   - Line speed: The setting of the line speed is dependent on the line speed of the physical interface. The line speed should be set to match the line speed of any associated physical interface to avoid fragmentation of the network packets.
   - Duplex: This setting is typically set to *FULL.

Press Enter.

![Create Line Desc (Ethernet) (CRTLINETH) display: Additional fields]

7. Additional fields will be displayed. Press Enter again to complete the creation of the Ethernet line description.

8. After the Ethernet line description has been created, vary it on by issuing the following Vary Configuration (VRYCFG) CL command:

   ```
   VRYCFG CFGOBJ(VRTETH01) CFGTYPE(*LIN) STATUS(*ON)
   ```

Enabling datagram forwarding

For Proxy ARP, the TCP/IP attribute *datagram forwarding* must be enabled. Datagram forwarding allows network packets to be forwarded between network interfaces on the system. To ensure that datagram forwarding is enabled, issue the following Change TCP/IP Attributes (CHGTCPA) CL command:

```
CHGTCPA IPDTGFWD(*YES)
```

Implementing proxy ARP on IBM i

The physical Network Interface Connections (NICs) on the power system are owned by the IBM i operating system. The SCS 2.0 LPAR uses an internal Virtual LAN with an internal router and *Proxy ARP* service running in the IBM i LPAR to access the LAN. The bulk of the virtual LAN setup is completed during manufacturing when the SCS LPAR is created.
However, as IP address ranges are specific to your environment, some configuration must be performed after the power system is installed.

Proxy ARP is a method for forwarding traffic between virtual and external (or physical) Ethernet networks. It is a built-in function of TCP/IP and uses transparent subnetting to associate a logical partition’s virtual interface with an external interface. Essentially, IBM i becomes a router for a subnet of addresses that will be assigned to the virtual LAN.

Figure A-5 shows an example of Proxy ARP. A subnet is established that has a usable address range of 9.5.92.25 to 9.5.92.30. This range of addresses is assigned to the virtual LAN and is associated with an interface on the physical LAN (which will most likely be your private Smart Cube IP address) to act as the router for the subnet. The range of addresses for the subnet is determined by an address in the network along with the subnet mask.

There are a number of rules that the subnet must meet:

▲ The size of the subnet must be a power of 2.
▲ The first address of the subnet cannot be assigned to a partition. The first address is the network address. In this case, that address is 9.5.92.24.
▲ The last address of the subnet cannot be assigned to a partition. The last address is the broadcast address. In this case, that address is 9.5.92.31.
▲ The subnet must be contained wholly within the overall network to which the associated IBM i physical network is attached.

Note: We recommend a range of eight IP addresses for the Proxy ARP.
Highlights of the proxy ARP environment can be summarized as follows:

- Traffic intended for partitions on the virtual LAN is routed to the IBM i physical network interface.
- Traffic is then re-broadcast on the Virtual LAN via the IBM i connection on that LAN.
- The Linux operating system running in the SCS 2.0 telephony partition sees the network traffic just like in any other network structure.
- DNS entries point to the address on the virtual LAN.
- The virtual LAN address range must be a subset of the physical LAN addresses.

The following steps walk through the setup of the components in IBM i to support proxy ARP.

**Determining the range of addresses for proxy ARP**

As indicated earlier, Proxy ARP is the establishment of a range of addresses that will be associated with a single physical interface. An IP subnet calculator is a useful tool to help determine a range of addresses for the subnet. One free example is the IP subnet calculator that is available from Wild Packets, located at the following website:

http://www.wildpackets.com/products/free_utilities/ipsubnetcalc/overview

Using the example in Figure A-5 on page 211, an IP subnet calculator could be used to establish the range of addresses. In Figure A-6, an address was specified that should fall within the range of addresses for the subnet. Then the subnet mask was used to indicate the size of the subnet (for example, 255.255.255.248 indicates a subnet of eight addresses.) By using the values in Figure A-6, a subnet is defined with the following values:

- Network address = 9.5.92.24
- Range of usable addresses = 19.5.92.25–9.5.92.30
- Broadcast address = 9.5.92.31

![Figure A-6  IP Subnet Calculator](image-url)
Now that the subnet range has been defined, the next step is to create the TCP/IP interface for IBM i on the virtual LAN.

**Creating the TCP/IP interface for the Virtual LAN Adapter**

After the Ethernet line description has been created and the subnet defined, you are ready to define the TCP/IP interface for i5/OS on the virtual LAN. Perform the following steps.

**Note:** Typically, IBM i is assigned the first usable address in the subnet. This address will also be the default gateway of SCS 2.0.

1. From an IBM i command line, issue the following Add TCP/IP Interface (ADDTCPIFC) CL command to create the TCP/IP interface:

   ```
   ADDTCPIFC INTNETADR('9.5.92.25') LIND(VRTETH01) SUBNETMASK('255.255.255.248')
   LCLIFC('9.5.92.12')
   ```

   Where:
   - **INTNETADR** is the address of the IBM i interface on the virtual LAN.
   - **LIND** is the name of the Ethernet line description for the virtual LAN.
   - **SUBNETMASK** is the size of the subnet.
   - **LCLIFC** is the address of the physical network interface in i5/OS that will forward traffic to the virtual LAN.

   You can also prompt the ADDTCPIFC CL command by pressing F4 and completing the fields as shown in Figure A-7.

   ![Add TCP/IP Interface (ADDTCPIFC) display](image)

   **Figure A-7**  Add TCP/IP Interface (ADDTCPIFC) display
2. After the TCP/IP interface has been created, it can be varied on with the following Start TCP/IP Interface (STRTCP) CL command:

```
STRTCPIFC INTNETADR('9.5.92.25')
```

At this point, the IBM i setup to support Proxy ARP is complete.

Creating a System Service Tools (SST) profile for Console Access

In order to use the Guest Partitions Console (discussed later), an SST profile with appropriate privileges must be created. In order to do this, start a 5250 session and log in as QSECOFR.

1. From the command line, use command `strsst` and sign on as QSECOFR.
2. From the menu, select option 8 - Work with Service Tools User IDs and Devices.
3. Select option 1 - Service Tools User IDs.
4. To create a new profile, enter 1, then press Tab, and enter a suitable name for the profile.
5. Configure the profile as follows:
   a. Password: Password of your choice.
   
   **Note:** It is normal for the page to remain blank when entering a password.
   b. Set password to expire: No (option 2).
   c. Enter suitable description (optional but recommended).
   d. Leave Linked User Profile blank.
   e. Press Enter to create the new profile.
6. Take option 7 against the new profile from the Work with Service Tools User IDs menu to assign the required privileges in order to gain console access.
In addition to the default privileges granted, add System Partitions - Administration and Partition Remote Panel Key by using option 1 against these options and pressing Enter, as seen in Figure A-8.

<table>
<thead>
<tr>
<th>Option</th>
<th>Functions</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disk units - operations</td>
<td>Revoked</td>
</tr>
<tr>
<td>1</td>
<td>Disk units - administration</td>
<td>Revoked</td>
</tr>
<tr>
<td>1</td>
<td>Disk units - read only</td>
<td>Revoked</td>
</tr>
<tr>
<td></td>
<td>System partitions - operations</td>
<td>Revoked</td>
</tr>
<tr>
<td>2</td>
<td>System partitions - administration</td>
<td>Granted</td>
</tr>
<tr>
<td>2</td>
<td>Partition remote panel key</td>
<td>Granted</td>
</tr>
<tr>
<td></td>
<td>Operator panel functions</td>
<td>Revoked</td>
</tr>
<tr>
<td></td>
<td>Operating system initial program load(IPL)</td>
<td>Revoked</td>
</tr>
<tr>
<td></td>
<td>Install</td>
<td>Revoked</td>
</tr>
<tr>
<td></td>
<td>Performance data collector</td>
<td>Granted</td>
</tr>
<tr>
<td></td>
<td>Hardware service manager</td>
<td>Revoked</td>
</tr>
<tr>
<td></td>
<td>Display/Alter/Dump</td>
<td>Revoked</td>
</tr>
<tr>
<td></td>
<td>Main storage dump</td>
<td>Granted</td>
</tr>
</tbody>
</table>

Figure A-8  Assigning privileges to a new SST profile
Installing Nortel SCS 2.0

This appendix provides detailed instructions about how to install Nortel SCS 2.0.

Once the final configuration has been performed in IBM i, the Power System is ready for the Nortel SCS 2.0 installation. The Logical Partition (LPAR) with correct CPU, memory, and hard disk is created as part of the system manufacturing process and is preconfigured to launch the Nortel installation ISO from a preconfigured Virtual Optical Drive. No further CDs or DVDs are required.

The installation and initialization of the SCS 2.0 server requires the following steps:

1. Activate the SCS 2.0 LPAR.
2. Connect a virtual console to the SCS 2.0 LPAR to control the installation and initialization.
3. Install the SCS 2.0 server software.
4. Reconfigure the LPAR to boot from the hard drive and then manually restart it.
5. Configure and initialize the SCS 2.0 server.
Connecting a virtual console

The installation and initialization of the SCS 2.0 server is controlled from a virtual console that can be run from any PC connected to the same network as the IBM Smart Cube. The virtual console requires a Telnet session to the Power System on port 2301. The session is connected to the TCP interface that was defined in Appendix A, “Setting up IBM i for Nortel SCS 2.0” on page 207. We recommend using PuTTY, which is a free, open source Telnet/SSH client (for both commercial and personal use) and can be downloaded from:

http://www.chiark.greenend.org.uk/~sgtatham/putty/

**Note:** The following instructions may apply equally to other Telnet clients including via a Windows command prompt, but for the purpose of example, PuTTY is used.

To start the Telnet session:

1. Launch PuTTY and configure the session with the following parameters (Figure B-1):
   - Enter the host name or IP address of the Ethernet interface of your power system.
   - Connection Type: Telnet.
   - Port: 2301.
   
   We recommend that you enter a name for the session and click **Save → Open**.

![PuTTY Configuration](image)

*Figure B-1  Launching a PuTTY Telnet session to IBM i*
2. A connection to IBM i is established and a list of guest partitions is displayed, as shown in Figure B-2. Input the number of the Guest Partition Console for the Nortel SCS 2.0 partition, then press Enter. You will then be prompted to enter a valid service tools user ID and password. Connect with the SST profile created in step “Creating a System Service Tools (SST) profile for Console Access” on page 214.

**Note:** The QSECOFR profile cannot be used for this task.

Once the service tools user ID and password has been entered, Console Connected will be displayed at the bottom of the session window. However, the partition must be activated before the installation can proceed. This is covered in the next section.

### Activating the SCS 2.0 LPAR

Before the installation can continue, the LPAR requires activation via a 5250 terminal session to the Power System (also referred to as a *green screen* session). Switch back to the Operations Console connection created.

From your Windows PC desktop, launch a 5250 session to the IBM Smart Cube:

1. Select **Start** → **Programs** → **IBM System i Access for Windows** → **Emulator** → **Start or Configure a Session** → **New Session**.
2. Enter the IP address or host name of the Smart Cube in the System Name field.
3. Specify the workstation ID as QSECOFR and click **Open**.
4. Log on as QSECOFR.
5. Once logged in, the Nortel SCS 2.0 LPAR must be activated (varied on). To view the partition, issue the command `wrkcfgsts *nws`. The output will be similar to Figure B-3.

**Note:** Take note of the value listed under Description, as this will be needed later for other commands. In this case, the value is SCS, but this may vary.

6. Take option 1 to activate the partition. After a short time, the status changes to Active.

7. Switch back to the virtual console and press Enter. You will see the partition booting. The installation of the SCS 2.0 will begin automatically (Figure B-4).
8. At this point, no input is required while the SCS 2.0 base operating system software is installed. This process takes approximately 20 minutes to complete. When it has finished installing, the partition must be manually restarted and some configuration changes must be made.

**Note:** Do not accept the prompt to reboot automatically.

### Reconfiguring and restarting the SCS 2.0 LPAR

Once the SCS 2.0 server software is installed on the hard drive and before the first reboot, the SCS LPAR is reconfigured to boot from the hard drive.

The SCS LPAR is manually shut down, rather than letting the SCS 2.0 server reboot. The SCS LPAR is then reconfigured so that it will boot from the hard drive instead of the virtual optical drive. Once this has been done, then the SCS 2.0 server is restarted.

**Note:** This process is only performed once during a new installation and requires use of the description value noted from the earlier `wrkcfgsts *nws` command. The example below shows this value as SCS, but this may vary.

1. Shut down the SCS 2.0 LPAR by switching back to the 5250 session and issuing the command:
   ```
   VRYCFG   CFGOBJ(SCS)   CFGTYPE(*NWS)   STATUS(*OFF)
   ```

2. Use the following command to change the boot source of the SCS 2.0 LPAR from the virtual optical drive to the hard drive:
   ```
   CHGNWSD   NWSD(SCS)   IPLSRC(*NWSSTG)
   ```

3. Restart the SCS 2.0 LPAR by issuing the command:
   ```
   VRYCFG   CFGOBJ(SCS)   CFGTYPE(*NWS)   STATUS(*ON)
   ```

The Nortel SCS 2.0 IP Telephony solution can now be configured. Switch back to the console window. You should see operating system startup messages displayed in the virtual console window. 5250 access is no longer required.
Initial configuration of Nortel SCS 2.0

Now that the Virtual Console has been configured and the SCS 2.0 LPAR has been activated, the configuration of the SCS 2.0 IP Telephony Server can be started. The initialization collects the basic server configuration data such as selecting optional network services and setting the IP networking parameters. The initialization and data entry is controlled from the virtual console (PuTTY) session running on the admin PC. This is a straightforward process and should take around 15 minutes.

1. When the partition has finished booting, log in with the following credentials, as prompted in the virtual console (as seen in Figure B-5):
   - Username: root
   - Password: setup

2. The installer launches automatically. Select OK to the message on the first page to continue.

```
[ OK ]
Starting MySQL: [ OK ]
Starting sendmail: [ OK ]
Starting sm-client: [ OK ]
Starting console mouse services: [ OK ]
Starting cron.d: [ OK ]
Starting anacron: [ OK ]
Starting atd: [ OK ]
Starting yum-updatesd: [ OK ]
Starting HAL daemon: [ OK ]
Fedora Core release 6 (Zod)
Kernel 2.6.18-1.2795.fc6 on an i686

Welcome to your new VoIP system

---------------------------
First time login: user - root password - setup
sipx.example.com login:
```

Figure B-5  First boot of the SCS 2.0
3. Configure the high-availability system. In a single server scenario, high availability will not be configured. Select the No HA System option on this page (Figure B-6).

![Figure B-6  High availability](image)

4. Choose additional services. SCS 2.0 can provide DNS, NTP, and DHCP network infrastructure services (Figure B-7). Typically, these services will not be run from SCS 2.0, but this may vary depending on the specific network design.

![Figure B-7  SCS 2.0 DNS, NTP, and DHCP service enablement](image)
5. Enter the network settings (Figure B-8):
   - Fully qualified host name
   - IP address and subnet mask on the virtual LAN
   - Default gateway
   - DNS server (Nameserver) addresses

   The network information here will be based on what was calculated earlier.

![Figure B-8 Configuring IP information](image)

6. Administrator settings (Figure B-9): Enter the admin password for the SCS 2.0 server. This is used for command-line access and also access to the Web Interface. Enter an e-mail address for SCS 2.0 logs and status independent of the Smart Business Administrator Panel.

   **Note:** This changes the password for the root account.

![Figure B-9 Changing the admin password and setting up e-mail notifications](image)
7. Enter your time zone information (Figure B-10). Use the down arrow to page down.

```
Select your continent.
Pacific
Poland
Portugal
ROC
ROK
Singapore
Turkey

254

Collect Time Settings
```

*Figure B-10  Setting up the time zone*

8. Enter your SIP domain name (Figure B-11).

```
Your SIP Domain name is the name to the right of the '@' in your SIP addresses, like this:
sip:user@rochland.ibm.com

If just the domain name is used, add DNS SRV records.
SIP Domain Name: rochland.ibm.com

OK

Collect SIP Domain Name Settings
```

*Figure B-11  Adding your SIP domain*
9. Enter information about your company as prompted by the TLS/SSL Security Parameters page (Figure B-12). This is to generate the self-signed certificate for the SCS Server (Web access is HTTPS).

```
Organization Name: ITSO
```

```
Section Name: VoIP Services
```

```
Country Code: 01
```

```
State or Province: MN
```

```
Locality (city): Rochester
```

```
OK
```

```
35%
```

Collect Security Settings

```
```

Figure B-12 Collecting Company Information for TLS/SSL certificate generation

10. Finally, set the correct date and time using the arrow keys (Figure B-13).

```
Select the date and time: Hours are 00-23.
Use the up and down arrow keys to increment and decrement each field; tab between fields.
```

```
Date (year-month-day) 2008-11-14
Time (hour:minute) 13:46
```

```
OK
```

```
45%
```

Set system clock

```
```

Figure B-13 Setting the system clock
This completes the initial SCS 2.0 server setup procedure. A progress indicator will be displayed on the virtual console, notifying you of the setup progress. This final step takes a short amount of time to complete. When finished, you will see the output as shown in Figure B-14. At this point, reboot the SCS 2.0 and proceed to the configuration of the Smart Business Environment in “The Smart Business Setup Wizard” on page 127.

```
$ Setup Completed
All parameters have been configured. The configuration will take effect at the next reboot.
When the system comes up after the reboot, open http://nortelsos.rehland.ibm.com in your web browser to begin configuring your PBX.
Reboot [Exit to Prompt]
100%
Ready
```

Figure B-14  Installation complete
Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this IBM Redpaper publication.

IBM Redbooks publication

For information about ordering these publications, see “How to get IBM Redbooks publications” on page 229. Note that some of the documents referenced here may be available in softcopy only.

- *IBM System i IP Telephony Configuring the System i Infrastructure, SG24-7382*
- *IBM System i IP Telephony and Integrated Collaboration, SG24-7412*

Online resources

These websites are also relevant as further information sources:

- IBM Smart Business
  

- IBM Smart Business technical paper
  

How to get IBM Redbooks publications

You can search for, view, or download IBM Redbooks publications, IBM Redpapers publication, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this website:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services
Small and medium-sized businesses deserve more from IT—more choice, less complexity, better integration, and comprehensive support. IBM saw an opportunity to rewrite the rules of IT for these businesses by partnering with world-class solution providers and open source developers and by bringing together its best technologies to create IBM Smart Business. The premise of IBM Smart Business is to make IT invisible so that business owners can concentrate on growth and serving their customers. With this approach, IBM has made IT effortless and made core business applications available where they were either too complex or costly for many companies in the past. One of the solutions where this radically simple approach pays big dividends is in the area of unified communications. With IBM Smart Business, you get a complete solution up and running quickly, and if there is ever a problem, IBM stands behind the product. Now you can enjoy the benefits of unified communications (improved productivity, higher customer satisfaction, and improved collaboration with suppliers) without the hassle of getting it all to work or the worry of where to turn if you need help. IBM makes unified communications smart for your business.

In this IBM Redpapers publication we provide a complete overview the IBM Smart Business solution, from a description of the services to an installation guide, and a step-by-step scenario that describes how to configure, deploy, and manage the Voice over IP element of the IBM Smart Cube.