The Axxess® IP Devices Installation Manual is released by INTER-TEL, INC. as a guide for certified service personnel. It provides information necessary to properly install, program, operate, and maintain the system.

The contents of this manual may include technical or other inaccuracies. Inter-Tel reserves the right to make revisions or changes without prior notice. Some features or applications mentioned may require a future release and are not available in the initial release. Future product features and applications are subject to availability and cost. Some features or applications may require additional hardware and/or specific software. Software packages released after the publication of this guide will be documented in addenda to the manual or succeeding issues of the manual.

For additional information and/or technical assistance, certified technicians may contact:

Customer Support Department
INTER-TEL, INC.
7300 West Boston Street
Chandler, AZ 85226-3224
188-777-EASY(3279)

If you have any questions or comments regarding this manual or other technical documentation, contact
Inter-Tel’s Technical Publications Department at:
Tech_Pubs@inter-tel.com

NOTICE

Part of the software embedded in this product is eCos - Embedded Configurable Operating System, a trademark of Red Hat. Portions created by Red Hat are Copyright (C) 1998, 1999, 2000 Red Hat, Inc. (http://www.redhat.com/). All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY RED HAT AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

All products and services mentioned in this publication are the trademarks, service marks, registered marks, or registered service marks of their respective owners.
Inter-Tel®, Axxess®, Unified Communicator®, and CommSource® are registered trademarks of Inter-Tel, Incorporated.
Eclipse™ is a trademark of Inter-Tel, Incorporated.
Microsoft® Windows® and ActiveSync® are registered trademarks of Microsoft Corporation.
eCos™ is a trademark of Red Hat, Inc.
AudioCodes™ is a trademark of AudioCodes Ltd.
Intel® Pentium® are registered trademarks of Intel Corporation.
PowerSense™ is a trademark of Red Hawk/CDT, Inc.
WinZip® is a registered trademark of WinZip Computing, Inc.
SpectraLink® is a registered trademark of SpectraLink Corporation.
Cisco® is a registered trademark of Cisco Systems, Inc.
Broadcom® is a registered trademark of Broadcom Corporation.

© Inter-Tel, Inc. April 2006 printed in USA
# Table of Contents

<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2. Changes and New Features</td>
<td>3</td>
</tr>
<tr>
<td>3. “Endpoints” and “Phones”</td>
<td>4</td>
</tr>
<tr>
<td>4. Firmware</td>
<td>5</td>
</tr>
<tr>
<td>A. IPRC Firmware Compatibilities</td>
<td>5</td>
</tr>
<tr>
<td>B. Multi-Protocol Endpoint Firmware Compatibilities</td>
<td>5</td>
</tr>
<tr>
<td>5. IP Network Specifications</td>
<td>6</td>
</tr>
<tr>
<td>A. Performance</td>
<td>6</td>
</tr>
<tr>
<td>B. Bandwidth Utilization</td>
<td>8</td>
</tr>
<tr>
<td>C. Processing Latency</td>
<td>10</td>
</tr>
<tr>
<td>D. Subnet Settings</td>
<td>11</td>
</tr>
<tr>
<td>E. Operation Behind Firewalls or Proxies</td>
<td>13</td>
</tr>
<tr>
<td>F. Port Configuration</td>
<td>16</td>
</tr>
<tr>
<td>G. QoS Settings</td>
<td>20</td>
</tr>
<tr>
<td>H. Application Programming</td>
<td>20</td>
</tr>
<tr>
<td>6. Virtual Local Area Network (VLAN) Tagging Support</td>
<td>22</td>
</tr>
<tr>
<td>7. Quick Start Installation Outline</td>
<td>26</td>
</tr>
<tr>
<td>8. Installing the IPRC</td>
<td>27</td>
</tr>
<tr>
<td>9. System Database Programming</td>
<td>30</td>
</tr>
<tr>
<td>10. Installing the IP and Multi-Protocol Endpoints</td>
<td>32</td>
</tr>
<tr>
<td>A. Physical Interfaces</td>
<td>32</td>
</tr>
<tr>
<td>B. Installation</td>
<td>41</td>
</tr>
<tr>
<td>C. Power Supply Compatibilities</td>
<td>43</td>
</tr>
<tr>
<td>D. Wall Mounting</td>
<td>44</td>
</tr>
<tr>
<td>E. IP Endpoint Status Displays</td>
<td>49</td>
</tr>
<tr>
<td>F. Hardware Revision Identification</td>
<td>52</td>
</tr>
<tr>
<td>G. Inter-Tel Protocol (ITP) Mode vs. SIP Mode</td>
<td>53</td>
</tr>
<tr>
<td>11. Installing the IP SLA</td>
<td>56</td>
</tr>
<tr>
<td>12. Updating Firmware</td>
<td>58</td>
</tr>
<tr>
<td>A. Upload Utility Application</td>
<td>58</td>
</tr>
<tr>
<td>B. TFTP Download Application</td>
<td>63</td>
</tr>
<tr>
<td>C. TFTP Server</td>
<td>66</td>
</tr>
<tr>
<td>D. Automated Boot Code Update</td>
<td>72</td>
</tr>
<tr>
<td>E. Download Error Message Displays</td>
<td>73</td>
</tr>
<tr>
<td>13. Programming the IP Devices on a v1.5.x Firmware IPRC</td>
<td>80</td>
</tr>
<tr>
<td>A. Learn Mode</td>
<td>81</td>
</tr>
<tr>
<td>B. Self-Programming Mode</td>
<td>82</td>
</tr>
<tr>
<td>C. HTTP/Web Interface Method</td>
<td>84</td>
</tr>
</tbody>
</table>
## Table of Contents

**AXXESS® IP DEVICES MANUAL – Revised, April 2006**

<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>D. RS-232 Connection Method (IPRC Only)</td>
<td>130</td>
</tr>
<tr>
<td>E. Telnet Connection Method</td>
<td>131</td>
</tr>
<tr>
<td>F. RS-232/Telnet Card Programming Fields</td>
<td>133</td>
</tr>
<tr>
<td>G. RS-232/Telnet Device Programming Fields</td>
<td>135</td>
</tr>
<tr>
<td>H. RS-232/Telnet IP Devices Programming Fields</td>
<td>138</td>
</tr>
<tr>
<td>14. Programming the IP Devices on a v8.2.x Firmware IPRC</td>
<td>141</td>
</tr>
<tr>
<td>A. Self-Programming Mode (Models 8620/8622 and 8662 Only)</td>
<td>142</td>
</tr>
<tr>
<td>B. IP Phone Web Client</td>
<td>145</td>
</tr>
<tr>
<td>C. TFTP Configuration Files</td>
<td>158</td>
</tr>
<tr>
<td>D. Axxess Database Programming</td>
<td>167</td>
</tr>
<tr>
<td>E. Windows CE .NET Programming (Model 8690 Only)</td>
<td>168</td>
</tr>
<tr>
<td>15. IP Local Loop Support</td>
<td>175</td>
</tr>
<tr>
<td>A. System Database Programming</td>
<td>177</td>
</tr>
<tr>
<td>B. AudioCodes MP-100 MGCP Gateway</td>
<td>178</td>
</tr>
<tr>
<td>C. AudioCodes MP-104 MGCP Gateway</td>
<td>188</td>
</tr>
<tr>
<td>D. AudioCodes MP-104 SIP Gateway</td>
<td>189</td>
</tr>
<tr>
<td>16. IP Softphone</td>
<td>190</td>
</tr>
<tr>
<td>A. Axxess IP SoftPhone</td>
<td>190</td>
</tr>
<tr>
<td>B. Eclipse IP SoftPhone</td>
<td>191</td>
</tr>
<tr>
<td>C. Model 8602</td>
<td>192</td>
</tr>
<tr>
<td>17. Troubleshooting</td>
<td>193</td>
</tr>
<tr>
<td>A. Connection Issues</td>
<td>193</td>
</tr>
<tr>
<td>B. Audio Issues</td>
<td>195</td>
</tr>
<tr>
<td>C. Echo Issues</td>
<td>198</td>
</tr>
<tr>
<td>D. Multi-Protocol Endpoint-Related Issues</td>
<td>199</td>
</tr>
<tr>
<td>E. VLAN Tagging-Related Issues</td>
<td>205</td>
</tr>
<tr>
<td>F. IPRC Diagnostics</td>
<td>205</td>
</tr>
<tr>
<td>18. Part Numbers</td>
<td>206</td>
</tr>
<tr>
<td>19. FCC Information</td>
<td>208</td>
</tr>
<tr>
<td>20. Glossary</td>
<td>208</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1 Inter-Tel® supports various Internet Protocol (IP) endpoints. These endpoints provide the functionality that allows you to make phone calls through the IP network to an IP Resource Card (IPRC) on the Inter-Tel Axxess® system. The endpoints that support IP are as follows:

**NOTE:** For those individuals who are already familiar with the Issue 7 of the Axxess IP Devices Manual, Revised May 2005 (document part no. 835.2195-17), "change bars" like the one next to this paragraph have been placed in the margins to indicate any new or revised information since the last revision of the IP Devices Manual.

**Soft IP Endpoints**

- **Axxess IP SoftPhone:** Operates like an Inter-Tel Executive endpoint on a PC and terminates on an IPRC (firmware v8.0 and earlier) in the system cabinet (see page 190 for details).

- **Eclipse™ IP SoftPhone:** Operates like an Inter-Tel Professional endpoint on a PC and terminates on an IPRC (firmware v8.0 and earlier) in the system cabinet (see page 190 for details).

- **Model 8602:** Operates like a Model 8662 multi-protocol endpoint and supports Inter-Tel Protocol (ITP) mode on a PC. It requires software v9.1 or later and IPRC firmware v9.0.0 or later (see page 192 for details).

**Hard IP Endpoints**

- **Axxess IP PhonePlus:** Looks and operates like an Executive endpoint (see page 33 for details).

- **Eclipse IP PhonePlus:** Looks and operates like a Professional endpoint (see page 33 for details).

- **Model 8660:** Looks and operates like a Model 8560 endpoint (see page 35 for details).

- **IP Single-Line Adapter (IP SLA):** Looks and operates like a standard SLA (see page 56 for details).

- **Models 8664, 8665, and 8668:** Are wireless, handheld portable endpoints. These new endpoints operate like a Model 8660 endpoint and support Inter-Tel Protocol (IPT) mode. For details, refer to the NetLink SVP Server and Model 8664/8665 Installation Manual (part no. 935.4521).

**Hard Multi-Protocol Endpoints**

- **Models 8600, 8620/8622, and 8662:** Look and operate like Models 8500, 8520, and 8560 endpoints, respectively. The main difference in the operation is that these endpoints do not have red and green LEDs. These endpoints support Inter-Tel Protocol (ITP) or Session Initiation Protocol (SIP) mode. The available features vary depending on the mode the endpoint is in. (See page 36 for details.)

- **Model 8690:** Unlike traditional Inter-Tel endpoints that have buttons built into the plastics, the Model 8690 has a touch screen that displays feature, dialpad, and menu buttons. This endpoint also supports ITP or SIP mode (see page 39 for details).

**Soft SIP Endpoints**

- **Model 8601 SoftPhone for Pocket PC:** Is a software-based SIP softphone that runs on selected Pocket PC 2002 (or later) Personal Digital Assistant (PDA) platforms. For information about installation and programming, refer to the Model 8601 SoftPhone for Pocket PC Installation Manual (part no.835.2736).
NOTE: IP Devices firmware Version 1.3 or later does not support the IP Card (IPC), part number 550.2260. For details about the IPC, refer to the IPC Installation and Programming Manual (document part no. 835.2554).

1.2 Except for the features listed in the bullets below, hard IP endpoints and multi-protocol endpoints that are configured to use Inter-Tel Protocol (ITP) operate the same as traditional endpoints such as the Executive endpoint, which are installed directly on the telephone system. Hard multi-protocol endpoints that are configured to use SIP also operate similar to traditional endpoints except that they have a reduced feature set (see page 53). The following lists the features and applications that are not supported on hard IP and multi-protocol endpoints.

Hard IP and multi-protocol endpoints:
- cannot use a PC Data Port Module (PCDPM) or Modem Data Port Module (MDPM).
- do not support Desktop Open Architecture Interface (OAI) applications.
- do not have a secondary voice path and cannot support Off-Hook Voice Announce (OHVA).
- do not support Enhanced Speakerphone Mode (except the Models 8600, 8664, and 8665).
- that are in SIP mode do not support Attendant Console.

CAUTION

Important Note for Administrators for Emergency Calls: Unless programmed for emergency outgoing access using a local loop (see page 175), when an IP endpoint such as the Model 8602, dials the emergency number, this includes 911 (default for US systems), 999 (default for European systems), or the appropriate emergency dial sequence for the locality, from a remote location, the call will be placed from where the phone system is physically located. Since these emergency services use Caller ID (CLIP) to help location the caller, emergency service could be misdirected or delayed. Also, the emergency service contacted may be local to the phone system, but not to the IP device. All IP device users should be alerted to this situation and instructed to use a local telephone line for placing emergency calls. Also note that the IP device may not function in the event of a power or network failure at either the local site or the phone system location unless operational backup power provisions have been implemented by the installing company.

1.3 The IP device interface to telephone system is an Ethernet IEEE 802.3 100Mbps unshielded twisted pair (UTP) interface (RJ-45). The IPRC and hard IP and multi-protocol endpoints use flash memory and their software can be updated over the Local Area Network (LAN).
2. CHANGES AND NEW FEATURES

2.1 The major enhancements described below:

- **Network Address Translation (NAT) Traversal for IP Endpoints:** The Axxess system now supports traversing near-end NAT using statically assigned NAT addresses. This capability allows an Axxess system to be placed inside a NAT or firewall and still communicate with IP endpoints outside the NAT/firewall. With system v9.1 or later, you can program each IP endpoint to use either the Native address or the NAT address in Database Programming. In other words, the system could be programmed with corresponding IP addresses for communicating with each IP endpoint, whether the endpoint was located inside or outside the NAT/firewall. You can also program an IP endpoint to be moved inside or outside the firewall (NAT) automatically without programming intervention. This is called “Automatic NAT Detection.” For details about NAT traversal and Automatic NAT Detection, refer to the v9.1 Addendum to Issue 9.0 of the Inter-Tel Axxess Installation and Maintenance Manual (part no. 550.8029).

- **New Model 8668:** Is a wireless, handheld portable endpoint. This endpoint is the Industrial Enterprise version of the Model 8664 which provides increased damage resistance and a longer warranty. For details, refer to the NetLink SVP Server and Model 8664/8665 Installation Manual (part no. 935.4521).

- **New Model 8602:** Is a softphone application that enables Voice over IP (VoIP) telephone calls from laptops or desktop computers. The Model 8602 connects to the Inter-Tel® telephone system through an existing IP network. The Model 8602 operates like a Model 8662 endpoint and supports Inter-Tel Protocol (ITP) mode. (see page 192).

- **Updated Port Configuration:** The Port Configuration table has been updated in this release (page 16).

- **New Plastic Rivets:** As of May 2005, the 8600 series IP endpoints were changed to make the metal plate easier to remove from the baseplate for wall mounting or cable management. To compensate for the reduced force now required to remove the metal plate, two plastic rivets were added to secure the metal plate to the baseplate located on the bottom of each endpoint. If the metal plate is removed for cable management, Inter-Tel recommends the rivets be reinserted after the metal plate is reassembled onto the baseplate of the endpoint, to lock it into place (see page 41).

- This manual contains a new section called “Endpoints and Phones.” This section helps you to understand the usage of the terms “endpoint” and “phone” (see page 4).
3. “ENDPOINTS” AND “PHONES”

3.1 As digital, wireless, and computerized communication methods have evolved, the language of telecommunications has had to change to keep pace. Not long ago, voice and modem-encoded text were communicated from one telephone instrument to another across a global network of copper wire, optical fiber, microwave antennas, and satellites. More recently, however, the development of the Internet and of World Wide Web (www) sites have introduced a multimedia dimension to information and made it all more readily accessible through computer networking. As this evolution has occurred, new words and meanings have been introduced to describe the new methods and equipment used for communicating.

3.2 Telephone systems that once provided only audio phone service to consumers have become “communication platforms” that support many devices that people can use for personal and business communication. Phones now share communication space with personal digital assistants (PDA), with wireless phones capable of text messaging, taking photos, and recording video, with fax machines that transmit and receive messages across Internet Protocol (IP), and with “soft” phones that are displayed and used from computer screens.

Computer Science Roots

3.3 When referring to communication protocols in computer science, the term “endpoint” describes an entity on one end of a Transport Layer connection. The Transport Layer is the Transmission Control Protocol/Internet Protocol (TCP/IP) layer in the Open Systems Interconnect (OSI) network model. Utilizing the TCP/IP layer standard, Internet servers send and receive packets of data across the World Wide Web.

Usage in This Manual

3.4 This manual uses the term “endpoint” to describe the entire category of devices that the Inter-Tel 5000 family of products supports. In this context, digital and IP phones are endpoints, as are data modules, fax machines, computer telephony (CT) gateways, Single-Line Adapters (SLA), IP Single-Line Adapters (IP-SLA), and answering machines.

3.5 And, to promote clear communication and understanding, commonly accepted names of endpoints are used as appropriate. In particular, desktop IP endpoints are also referred to as IP phones. Digital endpoints are also referred to as digital phones. Wireless endpoints are also referred to as wireless phones. And, analog single line endpoints are also referred to as single line phones or single line sets.

**NOTE:** In the manual and in the Database Programming, a phone may also be called a “station” when reference to the phone and its environment are intended. Or, it may be called “device” in the most general sense.
4. FIRMWARE

A. IPRC FIRMWARE COMPATIBILITIES

4.1 There are several versions of IPRC and IP endpoint firmware available, depending on the application and devices to be used. Refer to the IPRC/IP and IP Endpoint Firmware Notice (document part no. 835.2720) and verify that the firmware installed is the correct version that matches your intended configuration. For information about updating the IPRC firmware, see page 58.

B. MULTI-PROTOCOL ENDPOINT FIRMWARE COMPATIBILITIES

4.2 The following matrix lists the compatibilities of the multi-protocol endpoint firmware.

Table 1: Multi-Protocol Endpoint Firmware Compatibility Matrix
✓=supported  ✗=not supported

<table>
<thead>
<tr>
<th>ENDPOINT (HARDWARE TYPE) / DESCRIPTION</th>
<th>FIRMWARE VERSION</th>
<th>1.01S</th>
<th>1.0.31/1.0.33</th>
<th>1.1.5</th>
<th>2.0.06 or LATER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model 8600 (8600) 8 MB RAM, 2 MB flash memory, original</td>
<td>1.01S</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model 8620 (8620) 8 MB RAM, 4 MB flash memory, original</td>
<td>1.0.31</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model 8622 (8622) 16 MB RAM, 4 MB flash memory, original</td>
<td>1.0.33</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model 8662 (8662) 8 MB RAM, 4 MB flash memory, original</td>
<td>1.0.35</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model 8662 (8662i) 16 MB RAM, 4 MB flash memory, enhanced, noise-reduced</td>
<td>1.0.31</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model 8622 (8622v2) 16 MB RAM, 4 MB flash memory, enhanced, redesigned</td>
<td>1.0.33</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Model 8662 (8662v2) 16 MB RAM, 4 MB flash memory, enhanced, redesigned</td>
<td>1.0.35</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

1 See page 52 for details about hardware types.
2 Cannot be downgraded to v1.0.33 or earlier. These endpoints do not function with earlier firmware versions.
3 Cannot be downgraded to v1.1.5 or earlier. These endpoints do not function with earlier firmware versions.
4 Available in a future release.
5. IP NETWORK SPECIFICATIONS

CAUTION

Inter-Tel strongly recommends using the IP devices on a managed private network. If using a private network, the following recommended guidelines are relatively easy to attain. However, if connected to the public Internet, IP devices will function, but the quality may suffer due to the dynamic bandwidth availability. The possible problems could be voice quality degradation, garbled speech, dropped calls, equipment resets, etc. Also, the VoIP suitability of any Internet connection can change at any time, with no advance notice. Inter-Tel cannot guarantee any voice quality when connected to the public Internet. Therefore, Inter-Tel is not responsible for network quality issues that are caused by using the public Internet.

5.1 Because the Inter-Tel IP devices use IP to connect to other IP devices, your data network must meet certain specifications to ensure a quality phone system network. This section describes these network requirements.

5.2 Inter-Tel recommends that you run the Network Qualifier (for at least 24 hours) to assess your network before purchasing or installing the hardware required to set up Voice Over IP. Network Qualifier currently supports up to eight simulated VoIP connections. While in the Network Qualifier, set the Audio Frames/IP Packet and Minimum Playback Buffer Time fields to the appropriate values (see page 10). If the assessment reveals that your network is operating outside the specifications listed below, contact your network administrator. The Network Qualifier application is available on the Inter-Tel Web site (www.inter-tel.com/software) and on the system software CD.

WARNING

Security is the responsibility of the customer’s network administrator. Inter-Tel is not responsible for network problems due to security violations involving the IP address of the Inter-Tel IP devices. This includes, but is not limited to, toll fraud and interrupted network service.

A. PERFORMANCE

5.3 The quality of the data network is one of the most important factors in achieving a high-quality IP telephony call. The variables involved include the speed and capacity of the network configuration, type of connection, routing scheme, and amount of traffic being passed through the network.

5.4 Inter-Tel recommends the following network performance characteristics for voice:

- **Packet Loss**: (The percentage of unusable packets.) No more than 5% random packet loss.
- **Successful Packet Rate**: (The opposite of packet loss rate.) 95% or more.
- **Latency**: (The time it takes for information to pass from one point to another.) Less than 120ms of one-way delay and less than 250ms of total end-to-end delay.

**NOTE**: End-to-end delay is the sum of the one-way network, buffering, and processing delays. For example, at default, the total buffer and processing delays of the IPRC is 130ms, leaving 120ms (250ms - 130ms) of allowable network delay.
• **Jitter**: (Changes in delay.) 40ms or less (indicated by the results from the Network Qualifier).

**NOTE**: If the Network Qualifier returns a value greater than 40ms for jitter, voice packets received over the network may be unusable. If this occurs, the unused packets contribute to (and increase) the packet loss.

• **Hops**: (The number of router points a data packet must pass through during transmission.) 15 or fewer to minimize the number of potential problem points.

• **Committed Information Rate (CIR) and Burst Rate (BR)**: 512 Kbps/each. (This means that 512 Kbps will always be available, and the link may burst up to 1024 Kbps for short periods if the bandwidth is available from the WAN provider.) There is usually no guarantee of BR availability.

**NOTE**: It is recommended that the voice traffic stays below the CIR value. When voice traffic exceeds the CIR value, packets may begin to queue within the Frame Relay network and become subject to delay. These packets and could eventually be tagged as Discard Eligible (DE). (Packets marked as DE could be discarded before reaching their destination.) The potential queuing delay and packet loss can adversely affect voice quality.

5.5 Inter-Tel also recommends the following PSTN performance characteristics:

• **Loop Current**: 18 to 20mA.

• **Line Voltage**: 42.5 to 56.5V.

• **Ring Voltage**: 55 to 130Vrms (Class A).

• **db Level**: Must pass at least +3dBm without distortion into a 600ohm load.

• All the above PSTM requirements are consistent with the EIA/TIA-464B specifications.

5.6 Whenever possible, Inter-Tel recommends using Ethernet switching mechanisms rather than Ethernet hubs. The switches offer more inherent Ethernet advantages over hub (shared) technology, such as segmentation, full-duplex operations, layer 2 prioritization, etc.

**NOTE**: Using background music and paging on a hard IP endpoint, such as the IP PhonePlus, consumes as much bandwidth as a telephone call to the device. If your site has limited bandwidth, ensure that the IP endpoint users do not enable background music and that they limit pages.

5.7 For any router that will have VoIP traffic passing through it, program the router to prioritize the packets sent by the IP devices. You can usually do this by programming the router to prioritize the packets sent by a specific IP address (i.e., the IP addresses of the IP devices), by prioritizing UDP packets (because all audio packets sent by the IP devices are UDP packets), or by prioritizing the UDP port numbers that the IP devices use. You can also use Quality of Service (QoS) features, like Type of Service (ToS) or Differentiated Services (Diffserv). Under Card Configuration - Audio and Call Control on the IPRC, enable **RTP IP Precedence** by checking the check box. After a reset of the IPRC, both the IPRC and its devices will set the ToS in the IP header for audio packets. In addition, program the external router to fragment large data packets into smaller packets. This reduces the possibility that voice packets will have to wait for a large data packet at the router.
B. BANDWIDTH UTILIZATION

5.8 The IPRC uses all of the channels as talk paths, and signaling is transmitted via the Ethernet interface along with the voice traffic.

5.9 To ensure enough bandwidth (i.e., the IP, Ethernet, and/or Frame Relay overhead) is available, use the formulas listed below to calculate the amount required to make calls from the IP devices to the IPRC. Although bandwidth varies depending upon call control messages, fax/tone detection, voice activity detection (VAD), and the RTP profile, these formulas provide a good estimate for planning the network.

NOTE: The amount of bandwidth utilized on any network segment (LAN, WAN) should never exceed 75% of the available bandwidth. There should always be a 25% margin factored in when planning a network capacity (voice, data, etc.).

5.10 The bandwidth is calculated based on the following programmable settings:
- **Vocoder (voice codec):** Determines the codec bandwidth and the frame size (audio sample size).
- **Audio Frames per IP Packet:** Determines the number of voice frames placed into each packet.
- **RTP Profile:** Determines the Real-time Transport Protocol (RTP) header size.

5.11 The specific variables in the formula are defined in the following table.

### Table 2: Variables

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTPHeadSize</td>
<td>4 for Inter-Tel RTP; 12 for Standard RTP</td>
</tr>
<tr>
<td>IP/UDPHeadSize</td>
<td>28 bytes</td>
</tr>
<tr>
<td>EthHeadSize</td>
<td>18 bytes</td>
</tr>
<tr>
<td>FrameHeadSize</td>
<td>6 bytes (worst case)</td>
</tr>
<tr>
<td>AudioFramesPerIPPacket</td>
<td>Number of voice frames used per packet</td>
</tr>
<tr>
<td>VoiceFrameSize</td>
<td>Size, in milliseconds, for one voice frame, which is dependent on the voice codec (vocoder)</td>
</tr>
<tr>
<td>CodeBW</td>
<td>Codec bandwidth (in kbps)</td>
</tr>
<tr>
<td>BurstData</td>
<td>Data bursts in the call control socket</td>
</tr>
<tr>
<td>NumOfCalls</td>
<td>Number of calls</td>
</tr>
</tbody>
</table>

5.12 The CodecBW and VoiceFrameSize values for each of the supported vocoders are listed in the following table.

<table>
<thead>
<tr>
<th>Voice Codec</th>
<th>Codec Bandwidth</th>
<th>Voice Frame Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.729</td>
<td>8 kbps</td>
<td>10 ms</td>
</tr>
<tr>
<td>G.711</td>
<td>64 kbps</td>
<td>10 ms</td>
</tr>
</tbody>
</table>

**Voice Over IP**

\[
\text{Bandwidth in each direction} = \left( \frac{(\text{EthHeadSize} + \text{IP/UDPHeadSize} + \text{RTPHeadSize}) \times 8 \text{ (bits/byte)}}{\text{AudioFramesPerIPPacket} \times \text{VoiceFrameSize} (10\text{ms for G.729})} + (\text{CodecBW} + \text{BurstData}) \right) \times \text{NumOfCalls}
\]
Voice Over IP Across Frame Relay

\[
\text{Bandwidth in each direction} = \left( \frac{\text{FrameHeadSize} + \text{IP/UDPHeadSize} + \text{RTPHeadSize} \times 8 \text{ (bits/byte)}}{\text{AudioFramesPerIPPacket} \times \text{VoiceFrameSize (10ms for G.729)}} + (\text{CodecBW} + \text{BurstData}) \right) \times \text{NumOfCalls}
\]

**5.13** For example, using the default settings (G.729, three audio frames per packet, and Inter-Tel RTP) and including Ethernet overhead, the bandwidth for 32 concurrent voice over IP calls would result in the following:

\[
\left( \frac{(18 + 28 + 4) \text{ bytes} \times 8 \text{ bits/byte}}{3 \times 10 \text{ ms}} + (8 \text{ kbps} + 10 \text{ kbps}) \right) \times 32 \text{ calls} = 1002.7 \text{ kbps}
\]

**NOTE:** This example assumes an average of one kbps per channel of burst data to accommodate the call control type setup messages.
C. PROCESSING LATENCY

5.14 The amount of latency introduced by a VoIP call depends on the specific vocoder being used. When calculating latency, you must consider one vocoder-specific variable and two programmable parameters, as described below.

- **Frame Size (FS):** Is a fixed number and is inherent to the specific vocoder being used. The following table distinguishes the Frame Size for each vocoder in milliseconds.

<table>
<thead>
<tr>
<th>VOCODER</th>
<th>FRAME SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.729</td>
<td>10 ms</td>
</tr>
<tr>
<td>G.711</td>
<td>10 ms</td>
</tr>
</tbody>
</table>

- **Audio Frames per IP Packet (AF):** Is a programmable parameter (Audio Frames Per IP Packet under Circuit Configuration - Audio Settings) for each circuit that indicates how many vocoder frames are packed into a single packet. For minimal latency (but more IP or Frame overhead), configure the system with one audio frame per IP packet. For lower overhead, use larger values for this field. By default, a value of three is used for the Audio Frames Per IP Packet field because it provides a good balance between low latency and low overhead. You can also configure this value in the Network Qualifier when performing network tests.

- **Minimum Playback Buffer Time (MPBT):** Defines the minimum time, in milliseconds, that packets wait in the receive buffer before the system plays the audio. The higher this number, the more latency in the signal; however, it is less likely that network problems like jitter will cause lost or late audio packets. The lower the minimum playback time, the less latency there is in the signal; however, there is a greater chance of jitter affecting the call. The default is 80 ms, and the range is 1 to 320 ms. You can also configure this value in the Network Qualifier when performing network tests.

5.15 The basic formula for calculating end-to-end latency is as follows:

\[
\text{Latency} = ([\text{AF} + 2] \times \text{FS}) + \text{MPBT} + \text{estimated one-way network delay}
\]

*Where the estimated one-way network delay is based on dividing the round-trip ping time by two.*

**NOTE:** The actual end-to-end latency on a live network may be higher due to normal fluctuation in network delay.

5.16 The following is an example of how the total end-to-end latency value is calculated. This example uses the default settings (G.729, three audio frames per IP packet, and 80 ms buffer time) and assumes a 20 ms one-way network delay.

\[
\text{Latency} = ([3 + 2] \times 10) + 80 + 20 = 150 \text{ ms}
\]
D. SUBNET SETTINGS

5.17 You can operate a hard IP endpoint on either the same or different subnets from the IP card.

NOTE: Although you can program the database of the IP device directly, it is highly recommended that you change the device-specific settings through the HTTP/Web (see page 84) or RS-232/Telnet Device Programming (see page 131) on the IP card only. Once the device connects to the IP card, the IP card will reprogram the device’s local database with the copy of the database that is currently stored on the IP card. Therefore, if you make changes to the database of the IP device directly, those changes will be overwritten once the device connects to the IP card. In addition, it is highly recommended that you allow the device to connect to the IP card over the same subnet before attempting an alternate subnet. This step allows the device to get the database from the IP card, it may also allow the IP card to determine the device’s Ethernet address using the Learn Mode feature of the IP card (see for more information on page 81).

Subnet 1 — Main Subnet with IP Card

5.18 Using static IP addresses on this subnet:

- If this is the initial installation of the device, set the circuit on the IP card to Learn Mode (see page 81 for procedures). Note that only one IP card should be in Learn Mode at a time. Otherwise, you have no control over the IP card to which the IP device will connect.

- If you desire, the IPRC can act as a BOOTP server for its 16 devices; program the static IP address into the BOOTP IP Address field for the particular circuit using the HTTP/Web or RS-232/Telnet Device Programming. If you want to use an existing BOOTP server on the LAN, program the static IP address with the Ethernet address of the particular circuit as shown in the card circuit status on the IP card, after the IP device has connected or attempted to connect.

5.19 Using DHCP on this subnet:

- If this is the initial installation of the device, set the circuit on the IP card to Learn Mode (see page 81 for procedures). Note that only one IP card should be Learn Mode at a time; otherwise, you have no control over the IP card to which the IP device will connect.

- Using the HTTP/Web or RS-232/Telnet Device Programming, make sure the BOOTP IP Address field is zero for the particular circuit.

Subnet 2 — Alternate Subnet without IP Card

5.20 You will almost always need to program the Default IP Card Address field for a particular circuit using the HTTP/Web or RS-232/Telnet Device Programming on the IP card. The IP devices try to find their IP card by using broadcast messages first. If the broadcast messages from the alternate subnet fail to reach the IP card at the main subnet, the IP devices try a direct connection to the IP address in the Default IP Card Address field in their local database. Make sure this field contains the IP address necessary to reach the IP card from the alternate subnet. Note that it may be a different IP address than that used on the main subnet, if there is a Network Address Translation (NAT) taking place.
5.21 **Using static IP addresses on the alternate subnet:** If you want to use an existing BOOTP server on the LAN, program the static IP address with the Ethernet address of the particular IP device. You can determine the Ethernet address of the IP device by viewing the card circuit status on the IP card, after the IP device has connected with the IP card (usually from the same subnet). The Ethernet address of the hard IP endpoint is shown on its display during power up. The other common option is to have the IP device use its default values for the IP address, subnet, and gateway/router. These three fields should be programmed for the circuit through the HTTP/Web or RS-232/Telnet Device Programming on the IP card. Once these fields are programmed, allow the device to connect to the IP card from the same subnet so that the device receives the correct values.

5.22 **Using DHCP on the alternate subnet:** No further configuration is necessary except the Default IP Card Address as previously mentioned.
E. OPERATION BEHIND FIREWALLS OR PROXIES

5.23 This section contains important information about a usage of firewalls or Network Address Translation (NAT) tables in an IP network environment. The following lists the considerations regarding firewalls and IPRCs:

- It is recommended that device IPRCs be placed in a DMZ (demilitarized zone) or in front of a firewall because of the different requirements for IPRC firmware versions.
- The IP devices using a v1.5.x firmware IPRC can be configured behind a firewall with the appropriate port access (see page 16). However, it is recommended to place it in a DMZ or in front of a firewall.
- The IP devices using a v8.2.x or later firmware IPRC (especially if using peer-to-peer audio) cannot be installed behind a firewall using either SIP or ITP mode. Though it maybe feasible to configure the additional ports for v8.1 in a firewall, Inter-Tel does not support this.
- All Networking IPRC versions must be installed in front of a firewall (in a DMZ) and cannot use a NAT table.
- Firewalls are recommended where technically feasible to prevent unauthorized access from areas such as the public Internet, wireless IP, or other media.

**NOTE:** The firewall devices vary in operation from one manufacture mainly the way they handle the ports both in and out of the network. This is one of the main reasons why the IPRC should be located in a DMZ or in front of a firewall.

5.24 One complication associated with using an alternate subnet is the presence of firewalls, proxies, routers, etc. at the main subnet and/or the alternate subnet.

**IPRCs and Firewalls**

5.25 The diagrams shown on the following page illustrate sample IPRC configurations with firewalls. Keep in mind the following considerations regarding firewalls and IPRCs for IP endpoints:

- When using v8.2.x or later firmware IPRCs, do not place the IPRC behind a firewall. Place the IPRC into a DMZ, as shown in Figure 1 below (indicated with blue line).

If the connection also needs to support internal endpoint users, you can still place the IPRC into a DMZ, but an internal IPRC is recommended for optimization (indicated with red line).

- If a DMZ is not available, then use a v1.5 firmware IPRC, as shown in Figure 2 below. In this configuration, you must use a PAL. See page 5 for the compatibilities of IPRC firmware and IP devices.

- As in previous releases, the networking IPRC does not support NAT/firewalls on either side of the network connection.

- Because the Axxess system supports multiple IPRCs, one option for supporting IP endpoints from the Internet is to add an IPRC and connect its Ethernet port outside the firewall (NAT) to a DMZ or the Internet itself. However, a “mobile” IP endpoint, such as the Model 8602 (sometimes inside and sometimes outside), may not work well with this topology.
FIGURE 1. Sample v8.2.x Firmware IPRC Configuration with Firewalls

FIGURE 2. Sample v1.5.x Firmware IPRC Configuration with Firewalls
Network Address Translation (NAT) Traversal for IP Endpoints

5.26 The Axxess system now supports traversing near-end NAT using statically assigned NAT addresses. This capability allows an Axxess system to be placed inside a NAT or firewall and still communicate with IP endpoints outside the NAT/firewall. With system v9.1 or later, you can program each IP endpoint to use either the Native address or the NAT address in Database Programming. In other words, the system could be programmed with corresponding IP addresses for communicating with each IP endpoint, whether the endpoint was located inside or outside the NAT/firewall. You can also program an IP endpoint to be moved inside or outside the firewall (NAT) automatically without programming intervention. This is called “Automatic NAT Detection.” For details about NAT traversal and Automatic NAT Detection, refer to the v9.1 Addendum to Issue 9.0 of the Inter-Tel Axxess Installation and Maintenance Manual (part no. 550.8029).
F. PORT CONFIGURATION

5.27 Inter-Tel uses the port assignments shown in Table 3 by default. Keep the following considerations in mind when opening ports:

- Many of these port associations are configurable through Database Programming.
- Installing Windows components on Inter-Tel products may open other ports that are not necessarily open.
- Installing non-tested and non-supported software on Inter-Tel products may open ports and cause security risk.
- Inter-Tel products can interface with third-party products that may use different port numbers.

Table 3. Port Assignments

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Port Name</th>
<th>Inter-Tel Products</th>
<th>Access To:</th>
</tr>
</thead>
</table>
| 4000 | TCP/UDP | General   | • Call Processing Server (CPS)  
• Between a CPS and Voice Processing Unit (VPU)  
• CT Gateway 1  
• Desktop SoftPhone  
• Attendant Console  
• Interactive Voice Response (IVR)  
• Unified Communicator (UC)  
• Enterprise Conferencing (EC)  
• Phone system communications to external products, DB Studio, System Open Architecture Interface (OAI), Diagnostics Monitor, Station message detail recording (SMDR), and Message Print  
• IP sockets (used instead of RS232 ports)  
• Nodes, CPS and CPC (Call Processing Card), or applications 2 | |
| 4444 | UDP     | General   | VPU                | AvdadMon 2 |
| 7777 | UDP     | General   | Unified Messaging (UM) on VPU | The UM clients 2 |
| 3986 | TCP     | General   | Call Center Suite (CCS) | CCS Server 2 |
| 3001 | UDP     | General   | Non ATM CPU (EAC CPU to CPS Server) | 512 CPS communications port between the CPS and EAC CPU |
| 4001 | UDP     | General   | ATM ELAN            | ATM ELAN; Port used by the ATM system for communicating between Redundant Servers. |
| 5060 | TCP/UDP | SIP       | SIP Server          | Communications between the SIP server and IPRC or SIP devices |
| 5566 | TCP     | General   | • IP devices  
• IPRC Networking  
• IP Card (IPC) | IP terminal TCP Call Control port 2 |
| 5070 | TCP     | General   | IP Networking       | TCP Call Control port 2 |
| 5567 | UDP     | General   | • IP devices  
• IP Resource Card (IPRC) Networking  
• IPC | IP terminal General Purpose port 2 |
| 5568 | UDP     | General   | • IPRC | Message server port for sending IP diagnostic information from Axxess or 2 |
## Table 3. Port Assignments (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Port Name</th>
<th>Inter-Tel Products</th>
<th>Access To:</th>
</tr>
</thead>
</table>
| 5004-5569 4 | UDP  | General | • IP devices  
• IPC  
• IPRC Networking | IP devices and IPRC Networking (IP Random Voice Ports) 2  
Axxess Audio Stream Receive port 2 |
| 5004 | UDP  | General | • IPRC  
• IPC  
• IP endpoints 3 | Operations, Administration, and Maintenance (OAM) Event Console 2  
Voice Traffic (VoIP) |
| 5445 | TCP  | General | Enterprise Messaging (EM) | Operations, Administration, and Maintenance (OAM) Event Console 2  
OAM console 2 |
| 5000-5018 2 | TCP  | General | EM | OAM console 2  |
| 5000-5018 | UDP  | General | Interprise 3200 | Call Control for VoIP traffic 2  
Voice Traffic (VoIP) |
| 1638 | UDP  | General | Interprise 3200 | Voice Traffic (VoIP) |
| 5004 4 | UDP  | RTP | • IPRC  
• IP endpoints  
Ports must be odd numbers | IP Voice 2  |
| 5005 4 | UDP  | RTPC | • IPRC  
• IP endpoints  
Port must be odd numbers | IP Voice 2  |
| 4567 | TCP  | General | UC | UC communications for Client connections  
Required when using SIP server with UC and Microsoft Passports |
| 1863 | TCP  | General | UC | UC communications for Client connections  
Required when using SIP server with UC and Microsoft Passports |
| 80 | TCP  | HTTP | • CPC  
• IPRC  
• IPC  
• System Manager  
• UC  
• EC  
• IP endpoints  
• Web Conference | Various features depending on the product.  
Access programming information 2  |
| 8080 | TCP  | HTTP | IP products and IP endpoints | Access programming information 2  |
| 2427 4 | UDP  | MGCP | MGCP Gateway | MGCP equipment  
Required for troubleshooting |
| 3389 | TCP  | Terminal Services | • UC  
• System Manager | Required for troubleshooting  
File downloads and file transfers, Board or Upload Utility  
Used for remote access to IP products (Inter-Tel 5000, EC) 2 |
| 21 | TCP  | FTP | • System Manager  
• Engineering FTP |  
Used for remote access to IP products (Inter-Tel 5000, EC) 2 |
| 22 | TCP  | SSH | Secure Socket |  
Used for remote access to IP products (Inter-Tel 5000, EC) 2 |
### Table 3. Port Assignments (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Port Name</th>
<th>Inter-Tel Products</th>
<th>Access To:</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>TCP</td>
<td>Telnet</td>
<td>• CPC</td>
<td>System programming and general information²</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IPRC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IPC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• System Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• UC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• EC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IP endpoints</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Web Conference</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>SMTP</td>
<td>• System Manager</td>
<td>Used for sending mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AVDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IVR</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• CCS</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>TCP/UDP</td>
<td>WINS</td>
<td>Most Inter-Tel products</td>
<td>Name resolution IP to Equipment Name</td>
</tr>
<tr>
<td>53</td>
<td>TCP/UDP</td>
<td>DNS</td>
<td>Most Inter-Tel products</td>
<td>Name resolution IP to Domain Name</td>
</tr>
<tr>
<td>67</td>
<td>UDP</td>
<td>DHCP</td>
<td>Most Inter-Tel products</td>
<td>Dynamic IP Allocation.</td>
</tr>
<tr>
<td>67</td>
<td>UDP</td>
<td>BootP</td>
<td>Inter-Tel products are not Bootp servers only clients except v1.X IPRC.</td>
<td>Dynamic Allocation using the BootP process</td>
</tr>
<tr>
<td>68</td>
<td>UDP</td>
<td>BootP</td>
<td>Inter-Tel IPRC and IP endpoints</td>
<td>Client side of boot P</td>
</tr>
<tr>
<td>69</td>
<td>TCP</td>
<td>TFTP</td>
<td>IP products and IP endpoints</td>
<td>Used for uploading software and firmware updates</td>
</tr>
<tr>
<td>110</td>
<td>TCP</td>
<td>Pop3</td>
<td>• Pop 3 Exchange feature for Voice Mail products</td>
<td>Voice Mail e-mail features and UM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Interactive Voice Response (IVR)</td>
<td></td>
</tr>
<tr>
<td>135</td>
<td>TCP</td>
<td>RPC</td>
<td>• Voice Mail systems using UM features</td>
<td>Exchange services for e-mail features and UM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Messaging Application Programming Interface (MAPI) and faxing</td>
<td></td>
</tr>
<tr>
<td>143</td>
<td>TCP</td>
<td>IMAP</td>
<td>• Voice Mail systems using UM features</td>
<td>Exchange services for e-mail features and UM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• MAPI and faxing</td>
<td></td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP</td>
<td>Network troubleshooting information for the CPS servers</td>
<td>Using Simple Network Management Protocol (SNMP) management software with the CPS servers</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>SNMP</td>
<td>Network troubleshooting information for the CPS servers</td>
<td>Using SNMP management software with the CPS servers</td>
</tr>
<tr>
<td>389</td>
<td>TCP/UDP</td>
<td>LAPD</td>
<td>• UC</td>
<td>Database information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IVR</td>
<td></td>
</tr>
</tbody>
</table>
### Port Assignments (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Port Name</th>
<th>Inter-Tel Products</th>
<th>Access To:</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>SSL Secure Web https</td>
<td>• System Manager&lt;br&gt;• Automatic Diagnostics Delivery (ADD) feature on&lt;br&gt;CPC and CPS&lt;br&gt;• EC</td>
<td>• System Manager&lt;br&gt;• File transfer for the ADD feature&lt;br&gt;• EC features</td>
</tr>
<tr>
<td>8886</td>
<td>TCP</td>
<td>SIP Server</td>
<td></td>
<td>SIP Server</td>
</tr>
<tr>
<td>3707</td>
<td>TCP</td>
<td>Secure Real-Time Connection</td>
<td>System Manager</td>
<td>SIP Server</td>
</tr>
<tr>
<td>1800-1801</td>
<td>TCP/UDP</td>
<td>General</td>
<td>IVR MVEngine Service ports</td>
<td>IP messaging ²</td>
</tr>
<tr>
<td>1900</td>
<td>TCP/UDP</td>
<td>SQL</td>
<td>IP Telephony; Requires additional software ²</td>
<td></td>
</tr>
<tr>
<td>1433-1434</td>
<td>TCP/UDP</td>
<td>SQL</td>
<td>IVR database ⁵</td>
<td>Structured Query Language (SQL) database</td>
</tr>
<tr>
<td>3307</td>
<td>TCP</td>
<td>SQL</td>
<td>IVR</td>
<td>SQL database</td>
</tr>
<tr>
<td>5555-5556</td>
<td>TCP</td>
<td>General</td>
<td>IVR</td>
<td>Point Server</td>
</tr>
<tr>
<td>5631</td>
<td>TCP</td>
<td>General</td>
<td>CPS Servers</td>
<td>pcAnywhere for remote access ²</td>
</tr>
<tr>
<td>5632</td>
<td>UDP</td>
<td>General</td>
<td>CPS Servers</td>
<td>pcAnywhere for remote access ²</td>
</tr>
<tr>
<td>Various Ports ⁶</td>
<td>TCP/UDP</td>
<td>General</td>
<td>Third-party or custom applications</td>
<td>Various features depending on the product</td>
</tr>
</tbody>
</table>

1. CT Gateway has two programmable ports - one for communicating to the nodes and one for communicating to the applications. Both of these ports are programmable and default to port 4000.
2. The listed port numbers for these applications are the default values and can be changed in system programming.
3. IP endpoints (Axxess/Eclipse IP PhonePlus and Model 8660) use port 5004 for audio. Newer IP endpoints (Model 86XX, excluding the Model 8660) use port 6004 for audio.
4. Inter-tel recommends that QoS be configured in the network devices using the port settings (see page 20 for details).
5. The IVR can use other types of database engines where other network ports can be used.
6. Third-party products that interfaced with Inter-Tel products may use other port numbers other than what is listed in this document.

### 5.28
The IP devices allow you to configure most of these ports, except the port numbers below 1024. Make sure that all of these port numbers are unique values. Also, make sure at least the TCP call control port, the UDP general-purpose port, the audio stream receive port, and the RTCP port can get from the alternate subnet through any firewalls or proxies to the IP card on the main subnet.

### 5.29
In addition, you must make sure that the UDP RTP send port and RTCP port for the particular circuit can get from the main subnet through any network device (router, firewall, or proxy) to the IP device on the alternate subnet. Most firewalls allow bi-directional communication to take place provided it is initiated behind the firewall. Therefore, only one port is needed in the second direction, because the IP device initiates most of the communication to the IP card.
G. QoS SETTINGS

5.30 Inter-Tel recommends that you program the QoS settings for some of the IP ports that are listed in the table on page 16 (see footnote 4). The QoS settings are implemented to the routers and network switches to maintain the quality of the IP voice and call control ports. QoS improves the voice quality and avoids the audio from being interrupted where the user does not hear all the words from the other party.

5.31 If the reported audio issue is related to one-way audio, this issue can be related to the ports being blocked by a firewall or router. If the IP devices are not working, however, it may not be the firewall or proxy settings that are preventing them from functioning. Refer to the IPRC and IP devices firmware compatibility matrix (see page 5) to make sure the firmware of the IPRCs and IP devices are compatible with each other.

H. APPLICATION PROGRAMMING

5.32 The following table shows the recommended applications that should be programmed on the network devices (routers, switches, firewalls, or proxies) if the firewall or proxy is on the IP card, IP device, or MGCP endpoint side. The port numbers that are used for each application are described in the table on the previous page.

Table 4: Application Programming

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>THE FIREWALL OR PROXY IS ON THE:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP CARD (v1.5.x only)</td>
</tr>
<tr>
<td>Telnet Server</td>
<td>✓</td>
</tr>
<tr>
<td>BOOTP Server</td>
<td>✓</td>
</tr>
<tr>
<td>BOOTP Client</td>
<td>✓</td>
</tr>
<tr>
<td>TFTP Server</td>
<td>✓</td>
</tr>
<tr>
<td>HTTP Server</td>
<td>✓</td>
</tr>
<tr>
<td>MGCP Server</td>
<td>✓</td>
</tr>
<tr>
<td>RTP</td>
<td>✓</td>
</tr>
<tr>
<td>RTCP</td>
<td>✓</td>
</tr>
<tr>
<td>Call Control</td>
<td>✓</td>
</tr>
<tr>
<td>General Purpose</td>
<td>✓</td>
</tr>
<tr>
<td>Axxess Private Networking</td>
<td></td>
</tr>
</tbody>
</table>

1. Required.
2. Required; otherwise, background music may not work.

5.33 Programming of the firewall or proxy varies from product to product and from vendor to vendor. Please refer to the specific instructions for your product. Usually, you need to program a port-to-port mapping to get the firewall or proxy to always listen on a particular port. For example, if you have a public IP address of 172.18.10.228, and a private IP address for the IP card of 192.168.200.201, you must program the firewall or proxy to map 172.18.10.228 port TCP 5566 to 192.168.200.201 port TCP 5566.

5.34 If you have more than one IP devices sharing a single IP address, the IP card should have a unique IP address. Likewise, if multiple IPRCs are sharing a single IP address, the connected IP devices should have unique IP addresses.
5.35 If you want more than one IP device sharing a single IP address, the devices \textbf{must} have unique RTP/RTCP ports. Program the RTP send ports on the IP card(s) for the particular circuits to be unique. Be sure to reset the device after programming. \textbf{Do not} simply cycle power, as the device will perform a minor reset and will not reconnect to receive the new database.

5.36 Products support Windows 98 Second Edition, Windows ME, Windows 2000 Professional Workstation Internet Connection Sharing (ICS) and the Sygate, Wingate, and Midpoint proxies. (Sygate has proven to be the easiest to use and configure.) Microsoft Proxy and Winproxy will not work satisfactorily with the Inter-Tel IP card and IP devices.
6. VIRTUAL LOCAL AREA NETWORK (VLAN) TAGGING SUPPORT

6.1 Version 8.1 or later Axxess system now supports the IEEE 802.1Q standard (VLAN) to improve voice quality and provide a higher level of security. A VLAN-enabled network Ethernet switch (or network switch) inserts tags with unique identifiers called VLAN IDs into Ethernet frames. This breaks large networks into smaller groups so broadcast and multicast traffic will not grab more bandwidth than necessary. This is called “VLAN tagging.” The multi-protocol endpoints and devices (such as PCs, gateways, etc.) are tagged and behave as if they are connected to the same wire, even though they may be physically located on different segments of a network. For example, VLAN tagging can place the devices that are connected to the network switch port in a certain VLAN group and place the endpoints in a different VLAN group, as shown in Figure 3 below. When the network switch receives a tagged frame (containing a VLAN ID), it forwards the frame based on the destination MAC address but only to ports with the matching VLAN ID. The supported endpoints are:

- Models 8600, 8620/8622, and 8662 with v1.1.5 or later firmware
- Model 8690 with v1.1.5 or later firmware, v1.101 or later User Interface, and v1.101 or later Operating System

**FIGURE 3.** Router Routing between VLANs
VLAN IDs

6.2 When the VLAN tagging feature is enabled, the internal phone Ethernet switch inserts explicit VLAN tags in the incoming and outgoing frames to the network switch. Each endpoint has the uplink, downlink, and phone ports. The frame is forwarded from the phone or downlink port to the uplink port. The numbers of the available ports are shown in the table below. Note that the Models 8600 and 8620/8622 do not have a downlink port. An example of a common VLAN configuration is shown on the following page.

<table>
<thead>
<tr>
<th>MODEL</th>
<th>UPLINK PORT (LAN/POWER)</th>
<th>DOWNLINK PORT (PC)</th>
<th>PHONE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>8600/8620/8622</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>8662</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8690</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

**FIGURE 4. A Common VLAN Configuration**

**NOTE:** The internal phone Ethernet switch and phone port are located inside the endpoint and cannot be seen from the outside.

6.3 Each port, except the uplink port, has an associated VLAN group. The VLAN group must be uniquely identified by a VLAN ID (number 1 through 4094). The VLAN IDs for multi-protocol endpoints are generally configured in the network switch by your network administrator.

**NOTE:** The VLAN configuration for the network switch varies depending on the switch being used. Inter-Tel provides recommended VLAN programming guidelines for various switches. This information can be found in the Tech Central Knowledge Base Center on the Inter-Tel edGe Web site at www.inter-tel.com/knowledgebasecenter.

**ALSO:** The Tech Central Knowledge Base Center provides a storage point for resolved issues and common questions involving Inter-Tel products. The Knowledge Base Center articles are constantly being added and updated. Also, Answer IDs are not exclusively assigned to one article. Because there are several databases, an Answer ID can be assigned to several articles; therefore, make sure you are in the Knowledge Base for which you want the appropriate information.
6.4 To use the VLAN Tagging feature, you must first obtain the VLAN ID information from your network administrator and program the IDs in the endpoints using one of the following methods:

- Self-programming mode — for Models 8620/8622 and 8662 only (see page 144)
- Web interface (see page 154)
- Configuration files via TFTP server (see page 161)

**NOTE:** Do not use the configuration file to program the VLAN IDs for the Model 8690. The configuration file update does not overwrite Windows CE’s configuration, therefore, the changes will not be applied to the 8690. To program the 8690, use the 8690 Client Application.

- 8690 Client Application — for the Model 8690 only (see page 174)

**NOTE:** The Model 8690 can be programmed with up to three different VLAN groups because it has three downlink ports. This does not apply to the Model 8662 endpoint because this endpoint has only one downlink port and each downlink port can only be programmed with one VLAN with a unique VLAN ID.

**ALSO:** The VLAN Tagging feature does not require any Axxess Call Processing and Database Programming changes.

6.5 When the network switch receives an untagged frame (that is, does not contain a VLAN ID) from a port, it forwards the frame to the appropriate port based on the destination Media Access Control (MAC) address. If it receives a tagged frame (that is, contains a VLAN ID), it still forwards the frame based on the destination MAC address but only to ports with the matching VLAN ID. By default, VLAN IDs for the phone and downlink ports are set to zero.

6.6 By programming the VLAN ID differently for the endpoints and downlink devices, the internal phone Ethernet switch implicitly places the endpoints and downlink devices in different VLAN groups. As a result, the broadcast frames from the downlink device will not be transferred to the port that is in a different VLAN group. This also applies to the network switch because the network switch assigns the frames in the VLAN group based on the VLAN tags, which contains the VLAN ID. The network switch is normally connected to the uplink port. In a common configuration, the phone port is programmed with a VLAN ID other than zero and the downlink port with zero as the VLAN ID.

6.7 On the other hand, the endpoint and the downlink devices can be in the same VLAN group but different from the network’s default VLAN that is programmed in the network switch. This is done by programming the same VLAN ID in the phone and downlink ports.
LAN QoS for VLAN Tagging

6.8 When the endpoint is connected to a network switch that supports 802.1Q, it is strongly recommended that you enable LAN QoS to prioritize the Ethernet frames from the endpoint. LAN QoS is a MAC-level QoS. It involves the entire LAN, not just the internal phone Ethernet switch. When enabled, the pre-defined priority levels of the frame (the Diffserv value of “46” and the 802.1P priority level of “5”) are added to the 802.1Q (VLAN) tag and transferred from switch to switch. It is disabled by default.

6.9 The LAN QoS can be enabled using one of the following methods (the LAN QoS setting will take effect immediately):

- Web interface (see page 154)
- Configuration files via TFTP server (see page 161)
- Axxess Database Programming — Because the 802.1P priority levels are determined by the Diffserv value, DB Programming can change the priority levels by changing the RTP TOS bits (set to 184) in DB Programming (under System\Devices and Feature Codes\IP Connections\<P6xxx>\Audio RTP Type of Service). However, DB Programming cannot enable or disable the LAN QoS feature.
7. QUICK START INSTALLATION OUTLINE

7.1 To install the IPRC and IP devices:

1. Install the IPRC in the equipment cabinet. (See page 27.)

2. Update firmware onto the IPRC. (See page 58.)

3. Program the IPRC and its ports in the database. (See page 30.)

4. Set up the IP addressing for the IPRC through the RS-232 port. Program the default IP address, default subnet mask, and default gateway address. (See page 130.)

**NOTE:** For information on network configurations, subnets, and firewalls, see page 175.

5. *With a v1.5.x firmware IPRC,* connect the IPRC to the LAN and program the IPRC and IP devices using a Web browser or Telnet interface. (See page 84 for Web instructions or page 131 for Telnet instructions.) The Web browser is the recommended method, as it is the easiest to use. You will need a PC on the same network as the IP card and it must have Internet Explorer or Netscape installed.

   - Place the devices in “Learn Mode.” (See page 81.) When an IP device powers up it will broadcast a request on the LAN asking for a connection. The IPRC will respond and send the information programmed for that device to the IP device.

   - You can program the IP device through the dialpad on your IP device. It is called “Self-Programming Mode.” This allows you to program a static IP address, default subnet mask, default gateway address, remote IPRC IP address, remote UDP port, hostname, and control (Bootstrap Protocol) and Dynamic Host Configuration Protocol (DHCP). See page 82 for more information.

**NOTE:** Although you can program the database of the IP device directly, it is highly recommended that you change the device-specific settings through the IPRC database only. Once the device connects to the IPRC, the IPRC will reprogram the device’s local database with the information that is currently stored on the IP card. Therefore, if you make changes to the database of the IP device directly, those changes will be overwritten once the device connects to the IP card.

*With a v8.2.x firmware IPRC,* connect the IPRC to the LAN and program the IPRC in the Axxess Database Programming. Program IP devices using one of the methods listed below. For details, see page 141.

   - Self-Programming Mode (Models 8620/8622 and 8662 Only)
   - IP Phone Web Client
   - TFTP Configuration Files
   - Axxess Database Programming for IP Endpoints that are in ITP mode
   - Setup Wizard (Model 8690 Only)

6. Update the firmware for the IP devices, if necessary. (See page 58.)

7. Install the IP device(s). (See pages 32 through 56.)

8. If you are installing an MGCP gateway (AudioCodes MP-100 or MP-104) for IP local loop, see page 175.
8. INSTALLING THE IPRC

NOTE: This section describes how to install a device IPRC (v1.5.x firmware). For 32-device IPRC (v8.2.x firmware) installation instructions, refer to the Addendum to the Axxess v8.0 Installation and Maintenance Manual. For networking IPRC installation instructions, refer to the latest version of the Axxess Installation and Maintenance Manual.

8.1 The device IPRC accepts connections from all previous versions of hard and soft IP endpoints. It also accepts a database upload that had been saved from a previous IP card. The extra fields that did not exist on the previous IP card, namely the second set of eight ports, will be defaulted. A database saved from an IPRC cannot be downloaded to a previous IP card.

8.2 Software on the IPRC does not accept a download containing the code meant for the IPCs. The IPRC will not erase the flash and attempt to program the flash with this erroneous code; instead, it will send back an error message over RS-232 and Trivial File Transfer Protocol (TFTP), if used.

NOTE: While flashing an IPRC, the Voice Processor may generate a communication error in its message log (e.g., 208 Alarm). In this case, the 208 alarm indicates that the Voice Processor cannot refresh lamps on extensions that are unavailable while the IPRC is being flashed. Although some lamp refreshes may be delayed until the next refresh cycle, this does not otherwise affect the operation of the Voice Processor.

8.3 The device IPRC is equipped with the following resources:

- **Light-Emitting Diode (LED) Indicators:** Each card has seven LEDs:
  - **Card On-Line:** Indicates that the card is online.
  - **Circuit Busy:** Indicates that at least one of the Voice over IP (Digital Signal Processor - DSP) channels is busy.
  - **Make-Busy Indicator:** Shows the current state of the Make-Busy switch. It simply remains lit while the button is pressed, but does not change the state of the ports on the card.
  - **Halted:** Indicates that the card is not functioning due to a hardware or software error.
  - **Full-Duplex Indicator:** Indicates that the network connection is running in full-duplex mode.
  - **Collision:** Indicates that the network connection has experienced a collision while in half-duplex mode.
  - **100Base-T Indicator:** Indicates that the network connection is operating at a speed of 100 Mbps (Megabits per second).

- **Make-Busy Switch:** Reserved for future use.

- **Two RS-232 Ports:** Allow you to program the card’s database, perform diagnostics on the card, or upload new firmware. (To upload firmware to an IPRC, see page 58.)

- **RJ-45 10/100Base-T LAN Connection Port:** Provides a connection to either a 10 Mbps 10Base-T LAN or a 100 Mbps 100Base-T LAN. This port includes the following LEDs:
  - **Link Status LED:** When the network connection is valid, the green LED on the left side of the port is lit.
— **Transmit LED**: When the card transmits data to the network connection, the green LED on the right side of the port is lit.

- **DSPs**: The IPRC includes up to eight DSPs to encode and decode data for transmission on IP networks. Each DSP provides up to two, 2-way audio connections.

**FIGURE 5.** *IP Resource Card (IPRC)*

**NOTE**: For purposes of detail, this drawing does not show the EMI shield attached to the front edge of the card.
Installing the IPRC

8.4 To install the IPRC:

1. Verify that all components on the cards are seated securely in their sockets and that no pins are bent. See page 28 for an illustration of the IPRC.

2. Insert the IPRC in its appropriate slot in the cabinet. (The slot must be programmed for a DKSC16.) The component sides of the card must face right.

   **NOTE:** The IPRC might halt (red Halt LED remains lit) on hot-card insertion. If so, wait about 4-5 seconds for the CPU card to bring the card out of the halted state, rather than attempt to reseat the IPRC.

3. Connect one end of the Ethernet cable to the RJ-45 connector labeled “LAN” on the IPRC. Connect the other end of the cable to the RJ-45 connector on the LAN or network hub.

   **NOTE:** Do not connect the IPRC to the LAN until the IPRC is programmed. Some hubs have a straight-through/crossover switch. The switch must be selected for straight-through operation.

4. Upload firmware to the IPRC using the Upload Utility (previously called the Board Utility) or the TFTP Download program. The IPRC firmware is not automatically updated by Call Processing. The Upload Utility supports an RS-232 method as well as a network connection for uploading the firmware onto the IPRC. See page 58 for more details.

5. Configure all IPRC settings using the Database Programming interface (see page 30). An IPRC includes Web-based and telnet configuration interfaces.

6. For hard IP endpoints installation see page 32, and for SIP endpoints installation see page 56.

   **NOTE:** The programming of individual ports remains the same: IP PhonePlus, Model 8660 endpoint, or IP softphone must be on a phone port, and the IP SLA must be on dual-SLA, even though only the first single line device is used.

Upgrading the PAL

8.5 You can upgrade an 8-port PAL with the 16-port PAL. To upgrade the PAL, order the 16-port station PAL (part no. 827.9450) and upgrade fee (part no. 828.1637).

**NOTE:** Axxess v8.2.x uses the software licenses instead of PALs to determine the card functionality. Refer to the *Addendum to the Axxess v8.0 Installation and Maintenance Manual* for details.
9. SYSTEM DATABASE PROGRAMMING

NOTE: This section describes how to program device IPRCs (v1.5.x firmware) on Axxess Database programming. For 32-device IPRC (v8.2.x firmware) programming instructions, refer to the Addendum to the Axxess v8.0 Installation and Maintenance Manual. For Networking IPRC programming instructions, refer to the latest version of the Axxess Installation and Maintenance Manual.

9.1 Make sure you are using Inter-Tel system version 3.0 or later. The slot in the cabinet that will be used by the IPRC must be programmed as a DKSC-16.

NOTE: The "Amps Required" field will show that the card requires the 0.64 amps needed by a DKSC-16. However, an IPRC only requires 0.34 amps.

9.2 Program the port as Keyset if an IP endpoint, such as the IP PhonePlus, IP softphone, will be connected. Program the port as Dual Single-Line for an IP SLA (even though the IP SLA supports only one single-line endpoint).

9.3 To program an Loop Start Adapter (LSA) for IP local loop, see page 177.

NOTE: When configuring a SIP endpoint via Database Programming, the endpoint station flag “Handsfree Mode on/off” must be set to “no” (under System\Devices and Feature Codes\stations\<extension>\Flags).

Programming an Emergency Extension for IP Devices

9.4 The following is the recommended programming for a system that has remote loop termination with the need for emergency access for the remote IP endpoints.

1. Create a Trunk Group that contains the LSAs programmed in the DKSC-16.

2. Program this Trunk Group as the Emergency Extension for the remote IP endpoints that will use the LSAs for local loop access.

3. When programming the Emergency Outgoing Access for the Trunk Group containing the LSAs, give the remote IP endpoints outgoing access, but remove all other stations and extension lists.

4. Program the Local Trunk Group as the Emergency Extension for local endpoints.

5. When programming the Emergency Outgoing Access for the Local Trunk Group, include all local endpoints, but not the remote IP endpoints.

6. Create a facility group that contains the Local Trunk Group first, followed by the Trunk Group for the IP endpoints.

7. Program this facility group in Route Group 1.

8. Program the Emergency Outgoing Access for all node trunk groups to include no devices. Each node should have local trunk termination because emergency outgoing access across nodes is not warranted.
NOTE: If an installation needs Emergency Outgoing Access across nodes, make sure the Local Trunk Group is the first member in the facility group. This allows cross-node emergency calls to use the Local Trunk Group first and not the Remote IP Trunk Group.

NOTICE

It shall be the responsibility of the entity or person(s) completing installation and maintenance of hardware or software described herein to research, comply with and be responsible for the specific governmental rules and regulations regarding Emergency Outgoing Access (911) of the geographic location in which such functions are performed.
10. INSTALLING THE IP AND MULTI-PROTOCOL ENDPOINTS

**CAUTION**

*Inter-Tel strongly recommends using the IP devices on a managed private network. If connected to the public Internet, IP devices will function, but the quality may suffer due to the dynamic bandwidth availability. The possible problems could be voice quality degradation, garbled speech, dropped calls, equipment resets, etc. Also, the VoIP suitability of any Internet connection can change at any time, with no advance notice. *Inter-Tel cannot guarantee any voice quality when connected to the public Internet. Therefore, Inter-Tel is not responsible for network quality issues that are caused by using the public Internet.* For recommended guidelines on IP network specifications, see page 6.*

10.1 The installation of an IP or SIP endpoint is very simple. The device is connected to a power source and to the network. There is no direct wiring from the IP card to the endpoint. The available IP/SIP endpoints are the Axxess/Eclipse2 IP PhonePlus with a 10Base-T LAN hub, the Model 8660 endpoint, and Model 8600 series multi-protocol endpoints.

**NOTICE**

The IP softphone requires v1.5.x firmware and does not support IPRCs that have v8.2.x firmware. Other IP endpoints, such as the Model 8660 Phone, however, require the new (or upgraded) 8.1 or later firmware IPRCs to support the new features. For these reasons, Inter-Tel recommends that you do not connect IP softphones and other IP endpoints to the same IPRC. If you do, you may lose feature or endpoint functionality. See page 5 for the complete IPRC firmware matrix.

A. PHYSICAL INTERFACES

10.2 The following pages describe information about available features on each IP endpoint with illustration of the physical interface.
Axxess IP PhonePlus

10.3 Axxess IP PhonePlus with 10Base-T hub supports 10Base-T LANs. See below for a diagram of the 10Base-T hub.

10.4 The Axxess IP PhonePlus includes the following features:

- **Speaker:** Used for ring, group listen, speakerphone, and page.
- **LCD:** Supports six lines of display with 16 characters per line.
- **Handsfree Microphone:** Is a built-in microphone.
- **LAN/POWER Jack:** Connects to an external power supply or a network hub/switch.
- **POWER Jack:** Connects to a 24VDC external power supply.

**NOTE:** Use only one power source to connect the power supply.

- **OUT TO PC Jack:** Connects to a PC.
- **LEDs:** There are two indications on each port:
  - **Link Status:** When the link is valid, the green LED on the left side of the port is lit. When there is receive or transmit activity on the link, the LED flashes.
  - **Collision:** When there are both receive and transmit activities on the link, the yellow LED on the right side of the port is lit.

10.5 For information about programming an Axxess IP PhonePlus, see page 80.
**Eclipse IP PhonePlus**

10.6  Eclipse IP PhonePlus with 10base-T hub supports 10Base-T LANs. See below for diagrams of the 10Base-T hub.

10.7  The Eclipse IP PhonePlus contains the following features:

- **Speaker**: Used for ring, group listen, page, and speakerphone features.
- **LCD**: Supports six lines of display with 16 characters per line.
- **Handsfree Microphone**: Is a built-in microphone.
- **Message Indicator**: Flashes when there is a voice mail or station message for the phone.
- **LAN/POWER Jack**: Connects to an external power supply or a network hub/switch.
- **Barrel Jack**: Connects to an external power supply.
- **Ports 1-3 (OUT TO PC Jack)**: Connects up to three other IP devices, such as PCs, notebooks, and printers.
- **LEDs**: There are two indications on each port.
  - **Link Status**: When the link is valid, the green LED on the left side of the port is lit. When there is receive or transmit activity on the link, the LED flashes.
  - **Collision**: When there are both receive and transmit activities on the link, the yellow LED on the right side of the port is lit.
- **Handset Jack**: Connects to a handset.
- **LCD Contrast Knob**: Adjusts contrast of the LCD display.

10.8  For information about programming an Eclipse IP PhonePlus, see page 80.
Model 8660

10.9 Model 8660 endpoint supports both 10Base-T and 100Base-TX interfaces, but not 100Base-T4 (using four pairs of wires). See below for diagrams of the endpoint.

10.10 The Model 8660 includes the following features:

- **Speaker**: Used for ring, group listen, page, and speakerphone features.
- **LCD**: Supports six lines of display with 16 characters per line.
- **Handsfree Microphone**: Is a built-in microphone.
- **Message Indicator**: Flashes when there is a voice mail or station message for the phone.
- **LAN/POWER Jack**: Connects to a network hub or a switch and gets power from pins 7 and 8.
- **POWER Jack**: Connects to a 24VDC external power supply.

**NOTE**: Use only one power source to connect the power supply.

- **PC 1-3 Ports**: Connect to PCs or any other 10/100 Ethernet devices. The speeds on single uplink and three downlink ports are independent from each other and auto-negotiable.
- **Handset Jack**: Connects to a handset.
- **Headset Jack**: Connects to a headset.
- **LEDs**: There are two indications on each port:
  - **Link Status**: When the link is valid, the green LED on the left side of the port is lit. When there is receive or transmit activity on the link, this LED flashes.
  - **10/100 Mbps**: When the link is connected at a speed of 100 Mbps, the green LED on the right side of the port is lit.

10.11 For information about programming a Model 8660, see page 80.
Models 8600, 8620/8622, and 8662

10.12 Models 8600, 8620/8622, and 8662 multi-protocol endpoints operate like Models 8500, 8520, and 8560 endpoints, respectively. These endpoints support ITP (an Inter-Tel protocol) or SIP mode using 100Base-TX interfaces. See below for diagrams of the endpoints. All endpoints are configured to use ITP by default. For details about ITP and SIP modes, see page 53.

Model 8600

Model 8620
The Model 8600 series endpoints include the following features:

- **Speaker**: Used for ring, group listen, page, and speakerphone features.
- **LCD**: (Models 8620/8622 and 8662 only) Supports two/six lines of display with 16 characters per line.
- **Message Indicator**: Flashes when there is a voice mail or station message for the endpoint.
- **Headset/Handset Jack**: Connects to a headset or handset.
- **Handsfree Microphone**: (Models 8620/8622 and 8662 only) Is a built-in microphone.
• **LAN/POWER Jack:** Connects to an external power supply or a network hub/switch.

• **PC Port:** (Models 8622 and 8662 only) Connects to a PC or any other 10/100 Ethernet device. The speeds on single uplink and downlink port are independent from each other and auto-negotiable.

• **LEDs:** There are two indications on each port:
  — **Link Status:** When the link is valid, the green LED on the left side of the port is lit. When there is receive or transmit activity on the link, this LED flashes.
  — **10/100 Mbps:** When the link is connected at a speed of 100 Mbps, the green LED on the right side of the port is lit.

• **DRAM:** Located inside the endpoints. Models 8600, 8620, and 8662 (part no. 550.8662) support 8 MB, and Models 8622 and 8662 (part no. 550.8662E) support 16 MB (only one slot is occupied).

**NOTE:** Although there are two DRAM slots, you cannot upgrade the memory by adding an extra memory stick. Currently, the second slot is not used.

10.14 For information about programming Model 8600 series endpoints, see page 141.
10.15 The Model 8690 multi-protocol endpoint has a touch screen that displays feature, dial-pad, and menu buttons. It supports ITP or SIP mode using 100Base-TX interfaces. The Model 8690 endpoint is configured to use ITP by default. For details about ITP and SIP modes, see page 53.

10.16 The Model 8690 includes the following features:

- **Speakers**: Used for ring, group listen, page, and speakerphone features — supports mono for IP endpoint and stereo for Windows CE playback.
- **LCD**: Supports active matrix color LCD.
- **Message Indicator**: Flashes when there is a voice mail or station message for the endpoint.
- **LAN/POWER Jack**: Connects to an external power supply or a network hub/switch.
- **PC Ports 1-3**: Connect to PCs or any other 10/100 Ethernet devices. The speeds on the single uplink and three downlink ports are independent from each other and auto-negotiable.
- **Handsfree Microphone**: Supports high fidelity.
- **Headset/Handset Jack**: Connects to a headset or handset.
- **SPKR Jack**: Connects to a speaker — supports mono for IP endpoint and stereo for Windows CE playback.
- **MIC Jack**: Connects to a microphone (3.5 mm connector).
- **Reset Button**: Resets the endpoint (press and release the Reset button quickly).

**NOTE**: If you press and hold the Reset button until the four LEDs on the front of the endpoint (Message Lamp) start blinking, the system defaults the endpoint configuration (such as the configuration TFTP URL).

- **CF (Compact Flash) Port**: Connects to a compact flash memory card that can be used for copying music, pictures, etc. to the Model 8690. It also can be used as additional memory.
• **PCMCIA (Personal Computer Memory Card International Association) Port:**
  Connects to a memory card if additional memory is needed.

• **USB (Universal Serial Bus) HOST Port:**
  Connects to a standard USB keyboard, mouse, etc.

  **NOTE:** For details about how to connect a keyboard and/or mouse, refer to the *Model 8690 User Guide*.

• **USB CLIENT Port:**
  Connects to a host computer that runs Microsoft ActiveSync®.

• **LEDs:**
  There are two indications on each port:
  — **Link Status:** When the link is valid, the green LED on the left side of the port is lit. When there is receive or transmit activity on the link, this LED flashes.
  — **10/100 Mbps:** When the link is connected at a speed of 100 Mbps, the green LED on the right side of the port is lit.

• **DRAM:**
  Located inside the endpoint. Supports 128 MB (only one slot is occupied).

  **NOTE:** Although there are two DRAM slots, you cannot upgrade the memory by adding an extra memory stick. Currently, the second slot is not used.

10.17 For information about how to program a Model 8690, see page 141.

10.18 To use the Model 8690, you must first install the 8690 client application. See page 168 for details.
B. INSTALLATION

10.19 Install the endpoints as follows.

**NOTE**: For IP SLA installation instructions, see page 56.

1. Ensure that the IPRC is connected to the LAN and the On-Line LED is lit.

   **NOTE**: Some hub or switch ports have a straight-through/crossover switch. The switch must be selected for straight-through operation.

2. Attach the coiled handset cord to the handset and to the handset jack on the reverse of the endpoint. Place the handset on hook. If wall mounting the endpoint, refer to the instructions on page 44.

   **NOTE**: If you are installing an Axxess/Eclipse IP PhonePlus with a 10Base-T LAN hub, skip to step 4.

3. Remove the metal plate from the base of the endpoint as follows:
   a Remove the two plastic rivets to unlock it from the base.
   b Slide the cover off.
   The two plastic rivets are not included on endpoints built prior to May 2005.

4. Connect one end of the Ethernet cable to a PC port on the back of the endpoint. Connect the other end of the cable to the PC.

   **NOTE**: For Model 8660, use unbooted Ethernet cables. The Model 8660 does not support booted cables because the plastic "protective" ends on booted Ethernet cables get in the way when routing the cable away from the endpoint.

   **WARNING**

   Do not connect the PC ports to each other or to a hub. Doing so may cause adverse network conditions. Also, Inter-Tel does not recommend connecting additional hard IP endpoints to the PC ports. Due to the QoS (Quality of Service) present on these hard IP endpoints, the IP endpoints located behind an IP endpoint will have a lower priority when sending data upstream to the network. Under heavy network conditions, voice quality may be reduced.
5. Connect the power supply, using one of the following methods. Depending on the IP devices to be used, there are several power supplies available. Refer to page 43 for the matrix that lists the compatibilities of power supplies.

- **US/UK/Universal Power Supply using a LAN Jack:** Using the CAT5 cable, connect the LAN/POWER jack on the baseplate to the KS/SLA jack on the 24VDC adapter. Then using another cable, connect the LAN jack on the 24VDC adapter to the LAN. Connect the 24VDC adapter to a 110V wall socket.

  Inter-Tel currently offers the following power supply kits.

<table>
<thead>
<tr>
<th>PART NUMBER</th>
<th>CONTAINS:</th>
</tr>
</thead>
</table>
| 828.1642    | - US power supply (P/N 806.1113)  
              | - Network cable (P/N 813.1790)    |
| 828.1660    | - Universal power supply (P/N 806.1119)*  
              | - Network cable (P/N 813.1790)    |

* Requires a standard IEC (International Electrical Cord) power connector.

- **Universal Power Supply using a Barrel Jack:** Using the CAT5 cable, connect the LAN/POWER jack on the baseplate directly into the network. Do not connect this cable to the PC 1, PC 2, or PC 3 jack. Connect the adapter to an AC voltage power source and connect the barrel plug on the power adapter to the barrel jack on the baseplate (if available). The center of the barrel jack is positive. The minimum power requirements for the IP device is 24VDC at 500mA (using a Universal power supply) and 24VDC at 400mA (using a customer-provided power supply).

- **Power over Ethernet (PoE) hub (LAN Jack):** The Red Hawk PowerSense™ modular in-line PoE hubs (for multi-port) are available through the Inter-Tel CommSource® division. The power hub provides power to IP devices without the use of an external power supply for each device. Using the CAT5 cable, connect the LAN/POWER (RJ-45) jack on the IP device directly into the POWER/DATA (RJ-45) jack on the PoE connector. For details, see the Red Hawk PowerSense Power over Ethernet Installation Manual.

---

**NOTICE**

To reduce the effects of AC voltage surges and spikes that may cause damage to the electronic components, a surge/spike protector with the following specifications is recommended:

- Clamp voltage transients at 300VAC within 5 nanoseconds when exposed to waveforms as described in the ANSI/IEEE Standard C62.41-1980 (IEEE 587).
- RFI/EMI noise reduction by at least 20dB at frequencies between 5kHz and 30MHz.

Inter-Tel’s CommSource division sells a surge/spike protector (part number 900.0500) that has all of these specifications.

---

**CAUTION**

Only use a single, appropriate power adapter with the IP device. Do not connect a US power supply and a Universal power supply to the same IP device. Also, when using the Universal Power Supply with a barrel connector, no devices (e.g., hubs) should be inserted between the KS/SLA jack on the adapter and the LAN jack on the IP endpoint because power is supplied through the cable.
6. To hide the cables, route the Ethernet and power supply cables in the baseplate, in a way where you can replace the metal plate.

7. Re-attach the metal plate to the base.

8. Insert the two plastic rivets, if applicable, through the metal plate and press them firmly into the holes to lock the metal plate to the base.

9. While the endpoint is connecting to the IPRC, the display shows information about its connection state, including its Ethernet address, IP address, subnet mask, gateway address, and the address of the IP card to which it is connecting. The display then shows the station identification (port number, extension number, and assigned username) for several seconds. Then, the LCD changes to the appropriate display, depending on its current status. (See the chart on page 49 for an explanation of status displays.)

**NOTE:** If the endpoint appears to be stuck in "Waiting For Download" mode, try to ping its IP address. If you cannot ping the device, assign a valid BOOTP IP address from a BOOTP server (usually your IP card*) to the device's Ethernet address. Also, change the default IP address, subnet mask, and default gateway so that the device receives a better default when it reconnects to the IPRC after the download. When waiting for a download, the IP device will attempt BOOTP, even if BOOTP is disabled in IPRC programming. Cycle the power on the IP device and then download the software.

*The IPRC v8.2.x firmware does not provide a BOOTP server and requires a static IP address or the use of either a third-party BOOTP sever or a DHCP server for IP address assignment.

### C. POWER SUPPLY COMPATIBILITIES

**10.20** Refer to the *IP Device Power Supply Compatibility Matrix* (document part no. 835.2688) for the matrix of available power supplies.
D. WALL MOUNTING

**Axxess IP PhonePlus**

**10.21 To wall mount the Axxess IP PhonePlus:**

1. Remove the endpoint baseplate from the top half of the back of the endpoint.

2. Carefully unplug the ribbon cable.

3. On the back of the endpoint, use a pair of cutting pliers to remove the plastic knockout covering the lower connector on the endpoint control board.

**NOTE:** Be careful not to let the plastic knockout fall inside the endpoint. If this occurs, do not remove the plastic knockout.

4. Plug the free end of the ribbon cable into the connector on the endpoint control board (where the plastic knockout was previously removed).

**NOTE:** Use a pencil (eraser end) or other suitable rod-like instrument to press each end of the cable into the connector. Apply pressure until the connector clicks securely into place, one end at a time.

5. Rotate the baseplate 180° and attach it to the bottom half of the back of the endpoint.

6. Using a ruler, mark the location of the endpoint mounting holes on the wall. (The centers of the two perpendicular mounting holes on the back of the endpoint are four inches apart.)

7. Drive a screw into the center of each mounting hole marking. Allow the head of the screw to protrude approximately ¼ inch.

8. To hold the handset in place while the endpoint is wall-mounted, slide the reversible cradle hook out, rotate it 180°, and reinsert it as shown on the right.

9. Position the endpoint mounting holes over the screws and slide the endpoint into position on the wall. (If necessary, adjust the screws to ensure the endpoint is held firmly in place.)
Eclipse IP PhonePlus

10.22 To wall mount the Eclipse IP PhonePlus:

1. Remove the endpoint baseplate from the top half of the back of the endpoint.
2. Rotate the baseplate 180° and attach it to the bottom half of the back of the endpoint.
3. Using a ruler, mark the location of the endpoint mounting holes on the wall. (The centers of the two perpendicular mounting holes on the back of the endpoint are four inches apart.)
4. Drive a screw into the center of each mounting hole marking. Allow the head of the screw to protrude approximately ¼ inch.
5. To hold the handset in place while the endpoint is wall-mounted, slide the reversible cradle hook out, rotate it 180°, and reinsert it as shown on the right.
6. Position the endpoint mounting holes over the screws and slide the endpoint into position on the wall. (If necessary, adjust the screws to ensure the endpoint is held firmly in place.)
Model 8600 Series Endpoints

**NOTE:** Wall mounting the Model 8600 series endpoints is not recommended if the user will be connecting and disconnecting cords (handset, headset, line) and/or cables (Ethernet, USB, power supply) frequently. To connect and disconnect these cords and cables from a wall-mounted endpoint, the user will need to remove the endpoint from the wall.

10.23 Because there are two types of bases used on the Model 8600 series endpoints, two sets of instructions for wall mounting the endpoints are included here. Determine which type of base the endpoint has and follow the appropriate instructions.

10.24 For best results when wall mounting the Model 8600 series endpoints, Inter-Tel strongly recommends that you use the two plastic rivets shipped with the endpoint. Once installed, the plastic rivets lock the components into place, providing additional stability for wall-mounted endpoints.

10.25 Model 8600 series endpoints are shipped with a plastic adhesive label that covers the rectangular wall-mount knockout on the base of the endpoint. A portion of the adhesive label must be removed to use the wall-mount knockout.

10.26 To wall mount the Model 8600 series endpoints, you need an industry-standard wall-mount bracket (sometimes called a wall jack assembly) and a four-inch line cord. Both of these items are available through the Inter-Tel CommSource® division.

10.27 To prepare the endpoint for wall mounting (regardless of base type):

1. Remove the metal plate from the base of the endpoint as follows:
   c Remove the two plastic rivets to unlock it from the base.
   d Slide the plate off.
   The two plastic rivets are not included on endpoints built prior to May 2005.

2. Use a sharp blade to cut out the rectangular portion of the adhesive label covering the wall-mount knockout.
10.28 To wall mount the Model 8600 series endpoints that have a support mechanism:

**NOTE:** The following instructions apply to endpoints that have a support mechanism (see illustration below) that fits into holes in the base.

1. Collapse the support mechanism completely and secure it against the bottom housing of the endpoint, as shown below.

2. Close the base completely so that it lies flat against the endpoint. (The two rivet holes on the base align with the two rivet holes on the bottom housing of the endpoint.)

3. Plug the four-inch line cord into the jack on the back of the endpoint and thread the line cord through the wall-mount knockout on the base.

4. Insert the two plastic rivets through the base and press them firmly into the holes on the bottom housing of the endpoint. This locks the base to the endpoint.

5. Test the base to verify that it is securely locked to the endpoint.

6. Re-attach the metal plate to the endpoint base.

7. Insert the two plastic rivets, if applicable, through the metal plate and press them firmly into the holes on the base of the endpoint. This locks the metal plate to the base.

8. Plug the line cord into the jack on the wall-mount bracket and position the endpoint securely on the wall-mount bracket.

9. Flip the handset hanger down to the horizontal position and lock it into place. This will hold the handset in place.
10.29 To wall mount the Model 8600 series endpoints that have release buttons located on the bottom housing:

**NOTE:** The following instructions apply to endpoints that have release buttons located on the bottom housing of the endpoint. To disengage the locking mechanism in the base, push in both buttons. To lock the base in position, release the buttons.

1. Close the base completely so that it lies flat against the endpoint. (Rivet hole 1 on the base aligns with the rivet hole on the bottom housing of the endpoint.)

   ![Diagram of Model 8600 series endpoint showing rivet holes and release buttons.]

2. Plug the four-inch line cord into the jack on the back of the endpoint and thread the line cord through the wall-mount knockout on the base.

3. Insert one of the plastic rivets in rivet hole 1 on the base (see illustration above) and press it into the rivet hole on the endpoint. This locks the base to the endpoint.

4. Test the base to verify that it is securely locked to the endpoint.

5. Re-attach the metal plate to the endpoint base.

6. Insert the two plastic rivets through the metal plate and press them firmly into the holes on the base of the endpoint. This locks the metal plate to the base.

7. Insert the remaining plastic rivet through rivet hole 3 (as shown at right) in the metal plate and press it firmly into rivet hole 2 in the base. This locks the metal plate to the base.

8. Plug the line cord into the jack on the wall-mount bracket and position the endpoint securely on the wall-mount bracket.

9. Flip the handset hanger down to the horizontal position and lock it into place. This will hold the handset in place.
### E. IP ENDPOINT STATUS DISPLAYS

**10.30** While the boot code is loading, you will see the displays shown below. In the displays, the top lines change, as shown in the chart, and the bottom lines always contain the IP address and the Ethernet address.

**NOTE:** Several displays have a "/" character at the end that is a rotating bar to indicate that the device is working.

For IP PhonePlus and Model 8660

<table>
<thead>
<tr>
<th>DISPLAY</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAITING FOR DOWNLOAD</td>
<td><strong>Awaiting Download:</strong> The boot code is waiting for a code download.</td>
</tr>
<tr>
<td>ERASING FLASH</td>
<td><strong>Programming State - Erasing Flash Memory:</strong> The boot code is receiving object code and programming the flash memory. The endpoint first erases the flash memory and then displays this message.</td>
</tr>
<tr>
<td>PROGRAMMING CODE</td>
<td><strong>Programming State - Programming Flash Memory:</strong> After erasing the flash, the endpoint programs the flash memory.</td>
</tr>
<tr>
<td>DOWNLOAD COMPLETED</td>
<td><strong>Completed State:</strong> The download completed successfully.</td>
</tr>
<tr>
<td>HARDWARE FAILURE FLASH ERASURE</td>
<td><strong>Error State - Flash Erasure:</strong> The boot code encountered an error in erasing the flash chips. If this occurs, try two or three downloads before returning the endpoint for repair.</td>
</tr>
<tr>
<td>HARDWARE FAILURE FLASH PROGRAM</td>
<td><strong>Error State - Flash Program:</strong> The boot code encountered an error while programming the flash chips. If this occurs, try two or three downloads before returning the endpoint for repair.</td>
</tr>
<tr>
<td>HARDWARE FAILURE MEMORY MAP</td>
<td><strong>Error State - Memory Map:</strong> The hardware memory-map functions are not working properly. After two or three failed attempts, you should send in the endpoint for repair.</td>
</tr>
<tr>
<td>DOWNLOAD ABORTED FILE TOO BIG</td>
<td><strong>Error State - File Too Big:</strong> This display appears if you attempt to download a file that is too large for the flash memory. This error condition might indicate an incorrect or corrupted file.</td>
</tr>
<tr>
<td>DOWNLOAD ABORTED FILE CORRUPTED</td>
<td><strong>Error State - File Corrupted:</strong> This display appears if you attempt to download a file that is corrupted or that gets corrupted during the transmission. This error condition might occur during poor network conditions.</td>
</tr>
</tbody>
</table>

**10.31** For status displays for Models 8620/8622, 8662, and 8690, see page 71.
10.32 While the application code is executing, you will see the following displays as it moves through several states. After the endpoint is connected to the IP card, the default display appears on the LCD.

NOTE: Several displays have a “/” character at the end that is a rotating bar to indicate that the device is working.

For IP PhonePlus and Model 8660/8620/8622/8662/8690

NOTE: The following information does not apply to a non-LCD endpoint, such as the Model 8600. Also, because the Model 8620/8622 has a two-line LCD, this endpoint displays only the first two lines of the status.

<table>
<thead>
<tr>
<th>DISPLAY</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>INITIALIZING</td>
<td>Initializing: The application code is initializing the IP stack. For the majority of the initialization time, the IP endpoint is waiting for a BOOTP or DHCP response. If the IP endpoint receives a BOOTP or DHCP response, the IP endpoint uses the IP address, subnet mask, and gateway address from the response. If the IP endpoint times out, the IP endpoint uses its default IP address, subnet mask, and gateway address from its internal database. For each enabled option (BOOTP, DHCP, or both), an LCD shows a message indicating that the endpoint is attempting to receive that type of response. If at least one of these options is enabled and the endpoint is not able to receive an IP address, it will show “NO RESPONSE” for five seconds. If the endpoint tries BOOTP and fails, but then tries DHCP and succeeds, the display will not pause in order to reduce waiting time.</td>
</tr>
<tr>
<td>TRYING BOOTP... NO RESPONSE TRYING DHCP... SUCCESSFUL /</td>
<td></td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX MY IP ADDRESS: XXX.XXX.XXX.XXX FINDING LOCAL IP CARD ON UDP PORT XXXXX /</td>
<td>Finding IP Card Address: The application code is attempting to find a local IP card by broadcasting on the LAN. The first line contains the hexadecimal Ethernet address of the endpoint, while the second and third lines inform the user of the endpoint’s IP address. The rest of the LCD informs the user that the endpoint is attempting to find a local IP card by using the reply from the LAN broadcast. The first line contains the hexadecimal Ethernet address of the endpoint, while the second and third lines inform the user of the endpoint’s IP address. The rest of the LCD display informs the user that the endpoint is attempting to find the IP card and its port number.</td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX MY IP ADDRESS: XXX.XXX.XXX.XXX FINDING IP CARD: XXX.XXX.XXX.XXX UDP PORT XXXXX /</td>
<td></td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX MY IP ADDRESS: XXX.XXX.XXX.XXX CONNECTING TO: XXX.XXX.XXX.XXX TCP PORT XXXXX /</td>
<td>Connecting to IP Card: The application code is attempting to connect to an IP card. The first line contains the hexadecimal Ethernet address of the endpoint. The second line contains the IP endpoint’s current IP address. The fourth line contains the IP address to which the IP endpoint is attempting to connect. The sixth line indicates the number of unsuccessful connection attempts.</td>
</tr>
<tr>
<td>DISPLAY</td>
<td>STATUS (Continued)</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------</td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX XXX.XXX.XXX.XXX CONNECTED TO: XXX.XXX.XXX.XXX WAITING FOR CALL PROCESSING/</td>
<td>Connected to IP Card: The application code has made an IP connection to an IP card. The IP endpoint maintains this display until it receives a confirmation from call processing. Some possible problems are that call processing is not running yet, the board or circuit is not programming in call processing’s database correctly, or the endpoint is connected to the wrong type of system. The first line contains the hexadecimal Ethernet address of the endpoint. The second line contains the IP endpoint’s current IP address. The fourth line contains the IP address to which the IP endpoint is connected.</td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX LOCAL IP CARD NOT FOUND REMOTE IP CARD NOT PROGRAMMED /</td>
<td>IP-Card-Not-Found Error Message: After an attempt to find the local IP card through broadcast messages, the endpoint would normally attempt to contact the Remote IP card’s IP address. However, the endpoint does not have this field programmed; you can program this field through the Self-Programming Mode or the Web/Telnet interfaces. The display will show this error message for five seconds.</td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX COULD NOT CONTACT IP CARD XXX.XXX.XXX.XXX USING UDP PORT XXXXX /</td>
<td>UDP-Failed Error Message: If the endpoint did not receive a response via UDP after attempting to contact the IP card, the display will show this error message for five seconds.</td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX COUNT NOT CONTACT IP CARD XXX.XXX.XXX.XXX USING TCP PORT XXXXX /</td>
<td>TCP-Failed Error Message: If the endpoint did not receive a response via TCP after attempting to connect to the IP card, the display will show this error message for five seconds.</td>
</tr>
<tr>
<td>ID: XXXXXXXXXXXX XXX.XXX.XXX.XXX DUPLICATE IP ADDRESS AT MAC ADDRESS: XXXXXXXXXXXX</td>
<td>Duplicate-IP Error Message: If the endpoint determined that some other device is using the IP address that it is trying to use, the display will show the error message for thirty seconds. The display shows the IP address the endpoint is trying to use, that the address is in use by another device, and the MAC address of that device.</td>
</tr>
<tr>
<td>DSP FAILURE</td>
<td>DSP Failure: The application code displays the DSP Failure message if there was an error (bus error) while accessing the DSP. If this occurs, try two or three downloads before returning the endpoint for repair. After two or three failed attempts, send in the endpoint for repair.</td>
</tr>
<tr>
<td>DSP NOT RUNNING DSP NOT RUNNING</td>
<td>DSP Not Running: The application code displays the DSP Not Running message if the endpoint was able to access the DSP but has not received any response from the DSP (no online interrupt). If this occurs, try two or three downloads before returning the endpoint for repair. After two or three failed attempts, send in the endpoint for repair.</td>
</tr>
<tr>
<td>WAITING FOR ETHERNET ADDRESS /</td>
<td>Waiting for Ethernet Address: The application code has detected that the endpoint does not have a valid Ethernet address. If this occurs, try two or three downloads before returning the endpoint for repair. After two or three failed attempts, send in the endpoint for repair.</td>
</tr>
</tbody>
</table>
F. HARDWARE REVISION IDENTIFICATION

10.33 Check the following areas to identify endpoint hardware types:

- **Endpoint Web Interface** — The hardware type is displayed in the Firmware Information field under Status - Firmware - Hardware Type (see page 155).
- **LCD (Liquid Crystal Display)** — The hardware type is displayed on the bottom line of the LCD on startup.
- **Product ID and Revision** — The part number and revision are displayed on the labels on the bottom of the endpoint.
- **Message Lamp LED (Light-Emitting Diode) Pattern** — The hardware type is identified by the message lamp LEDs during startup. The user must reset the endpoint first.
- **Ethernet Ports** — The number of Ethernet interfaces can be used to identify the hardware type.

The following table lists the endpoint hardware types and identification methods.

**Table 5: Hardware Revision Identification**

<table>
<thead>
<tr>
<th>ENDPOINT</th>
<th>HARDWARE TYPE</th>
<th>LCD</th>
<th>PRODUCT ID (P/N)</th>
<th>LED PATTERN</th>
<th>ETHERNET PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model 8600 — original</td>
<td>8600</td>
<td>Not Available</td>
<td>550.8600</td>
<td>The endpoint LEDs flash in a left-right alternative blinking pattern.</td>
<td>1 Port</td>
</tr>
<tr>
<td>Model 8620 — original</td>
<td>8620</td>
<td>8620</td>
<td>550.8620</td>
<td>Not Available</td>
<td>1 Ports</td>
</tr>
<tr>
<td>Model 8622 — original</td>
<td>8622</td>
<td>8622</td>
<td>550.8622</td>
<td>Not Available</td>
<td>2 Ports</td>
</tr>
<tr>
<td>Model 8662 — original</td>
<td>8662</td>
<td>8662</td>
<td>550.8662</td>
<td>Not Available</td>
<td>2 Ports</td>
</tr>
<tr>
<td>Model 8662 — enhanced</td>
<td>8662</td>
<td>8662</td>
<td>550.8662E</td>
<td>Not Available</td>
<td>2 Ports</td>
</tr>
<tr>
<td>Model 8662 — noise-reduced*</td>
<td>8662i</td>
<td>8662i</td>
<td>550.8662E</td>
<td>Not Available</td>
<td>2 Ports</td>
</tr>
<tr>
<td>Model 8622 — enhanced, redesigned</td>
<td>8622v2</td>
<td>8622v2</td>
<td>550.8622</td>
<td>Not Available</td>
<td>2 Ports</td>
</tr>
<tr>
<td>Model 8662 — enhanced, redesigned</td>
<td>8662v2</td>
<td>8662v2</td>
<td>550.8662E</td>
<td>Not Available</td>
<td>2 Ports</td>
</tr>
</tbody>
</table>

* Available in a future release.
G. INTER-TEL PROTOCOL (ITP) MODE VS. SIP MODE

10.34 The Models 8600, 8620/8622, 8662, and 8690 multi-protocol endpoints support ITP or SIP mode. Details about each of the modes is described below. For complete information about supported features, buttons, and light-emitting diode (LED) indications for multi-protocol endpoints in ITP or SIP mode, refer to the Multi-Protocol Endpoints: Supported Features, Buttons, and LED Indications (document part no. 835.2840).

ITP Mode

10.35 When the multi-protocol endpoints are in ITP mode, the endpoints operate like traditional Inter-Tel endpoints. The endpoint connects to the Axxess system via a TCP/IP stream to the IPRC 32-Device card running an Inter-Tel proprietary protocol. This is the same protocol that the Model 8660 uses, which is a modified version of the protocol that the Model 8500 series endpoints use. The main difference is that the multi-protocol endpoints connect to the system via IP.

10.36 The advantage of ITP mode over SIP mode is that ITP mode allows you to use the Axxess features and functionality that the system provides for a traditional endpoint. The disadvantage of ITP mode over SIP mode is that when the endpoint is in ITP mode, it cannot connect to another vendor’s switch. All of the multi-protocol endpoints are configured to use ITP by default.

10.37 To support multi-protocol endpoints in ITP mode, a Call Processing software license is required.

10.38 Endpoint IP and MAC Address in ITP Mode

10.39 Unlike endpoints in SIP mode, an endpoint in ITP mode does not support the Show IP feature code (300) to display the endpoint IP address (see page 54). V2.0.06 or later endpoint firmware allows an endpoint in ITP mode to display the IP address and MAC address on the LCD, as shown on the right.

10.40 To display the IP and MAC addresses, press the Special button (∞) twice followed by the MUTE button promptly.

SIP Mode

10.41 When the multi-protocol endpoints are in SIP mode, the endpoints use SIP to connect to the Inter-Tel SIP Server (v1.1 or later). The advantage of running in SIP mode on an Axxess system is the use of the Shared Extension feature. A shared extension allows up to five SIP endpoints to use the same extension number on the Axxess system. Incoming calls to a shared extension are sent to SIP endpoints simultaneously. Once one of the endpoints answers the call, the SIP Server cancels the call to all other endpoints. This provides you with mobility so that you do not miss any calls when you are away from your main desk. For details about the Shared Extension feature, refer to the SIP Server Installation and Configuration Manual. Another advantage of SIP mode is that the endpoint can run on another vendor’s switch that supports SIP. The disadvantage of SIP mode on an Axxess system is the reduced feature set. The following features are currently supported on multi-protocol endpoints in SIP mode:

- Answer (Ringing Call)
- Attendant
- Call Forward All Calls
- Conference
- Do-Not-Disturb On/Off
- Emergency Call
• Group Listen
• Headset On/Off
• Hold (Individual)
• LCD Contrast Adjustment
• Message
• Microphone Mute
• Outgoing Calls
• Redial
• Redirect Call
• Reverse Transfer (Call Pick-Up)
• Ring Tone Selection
• Show IP (see below)
• Show Version (see below)
• Transfer to Ring

10.42 The features, listed in the table below, function differently depending on the mode.

<table>
<thead>
<tr>
<th>FEATURE NAME</th>
<th>DEFAULT FEATURE CODE</th>
<th>SIP MODE</th>
<th>ITP MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show IP (or Display Time/Date)</td>
<td>300</td>
<td>Displays the IP address of the endpoint.</td>
<td>Displays the system date and time, username, and extension.</td>
</tr>
<tr>
<td>Show Version (or Diagnostics - Show Version)</td>
<td>9928</td>
<td>Displays the firmware version on the endpoint.</td>
<td>Displays the version and date of the call processing software.</td>
</tr>
</tbody>
</table>

10.43 The multi-protocol endpoints in SIP mode use the feature codes that are programmed in the Axxess node.

**NOTE:** When configuring a SIP endpoint via Database Programming, the endpoint station flag “Handsfree Mode on/off” must be set to “no” (under System\Devices and Feature Codes\stations<extension>\flags).

10.44 For details about system features, refer to the appropriate endpoint *User Guide for SIP mode*.

10.45 To support multi-protocol endpoints in SIP mode, a SIP Server software license is required.
10.46 To change the modes on Models 8600, 8620/8622, and 8662, do one of the following:

- **Dialpad:** To switch to SIP mode, power up the endpoint with 1 and 2 pressed on the dialpad. To switch back to ITP mode, hold down 5 and 6 on the dialpad while powering up.
- **Web Interface:** Change the operation mode through the Web interface (see page 145).
- **TFTP Server:** Change the configuration files using the TFTP server (see page 63).

10.47 The recommended method to change from SIP to ITP mode is via the endpoint’s Web page and then reset the endpoint via the Web page (see page 145). If the endpoint has registered with the SIP Server, resetting the endpoint and pressing 5 and 6 to change from SIP mode to ITP mode will change the endpoint to ITP mode. Call Processing, however, will not allow the endpoint to register until the SIP Server relinquishes its connection on behalf of the endpoint.

10.48 To change the modes on the Model 8690: Change the operation mode through the Web interface (see page 145).
11. INSTALLING THE IP SLA

11.1 The IP SLA provides an interface between the standard single-line telephone and a 10Base-T network. It allows you to make phone calls through the IP network to the IPRC on the Axxess system. The IP SLA operates like a standard Axxess SLA. However, its interface to Axxess system is replaced by the Ethernet IEEE 802.3 10Mbps UTP interface. The IP SLA uses flash memory and its software can be updated over the LAN.

11.2 The installation of an IP SLA is very similar to that of an IP PhonePlus. The IP SLA connects to an AC power source and to the LAN.

11.3 To install all IP SLAs and the associated single-line endpoints:

1. Ensure the IPRC is connected to the LAN or hub and the Online LED is lit.

   NOTE: If using a hub, be aware that some hubs have a straight-through/crossover switch. The switch must be selected for straight-through operation.

2. Using the CAT5 cable, connect the 10BASE-T jack on the IP SLA to the KS/SLA jack on the 24VDC adapter.

3. Using another CAT5 cable, connect the LAN jack on the 24VDC adapter to the LAN.

4. Connect the 24VDC adapter to a 120V wall socket.

   CAUTION

   Only use the appropriate power adapter with the IP SLA. Also, no devices (e.g., hubs) should be inserted between the KS/SLA jack on the adapter and the 10BASE-T jack on the IP SLA because power is supplied through the cable.

5. Using the single-line endpoint’s line cord, connect the single-line endpoint to the SL PHONE jack. Within a few moments, the single-line endpoint will have dial tone from the system.

6. While the IP SLA is connecting to the IPRC, the following LEDs show information about its connection state. An illustration of the LEDs is shown below.

   - **ON-LINE**: Indicates a connection between the IP SLA and system call processing.
   - **SL STATUS**: Flashes in time with ringing voltage and is lit when the endpoint is off-hook (idle).
   - **IP STATUS**: Lights when there is a valid Ethernet connection to the device.
11.4 The DEFAULT button, shown below, has been added to the IP SLA (revision level -AC or later). This button allows you to perform the two functions as described below.

**DEFAULT**

**SL**

**PHONE 10 BASE-T**

**POWER**

**24V d.c. 0.3A**

**DEFAULT BUTTON**

- **Default the IP SLA Settings**: Allows you to change the IP SLA configuration (such as an IP address) to its default settings.

  **NOTE**: The default button is not a reset button.

  **To default the IP SLA**:

  1. Press and hold the DEFAULT button using a pinhole tool (such as a bent paper clip). The SL STATUS LED flutters for five or six seconds.
  2. When the ON-LINE LED is lit, remove the pinhole tool from the DEFAULT button. The ON-LINE LED turns off.

- **Place the IP SLA in the Download Mode**: Allows you to place the IP SLA into the download mode.

  **To change the mode**:

  1. Power down the IP SLA by either removing the cable from the power jack, if present, or removing the cable from the 10BASE-T jack.
  2. Press and hold the DEFAULT button using a pinhole tool while reconnecting power to the IP SLA. The ON-LINE and SL STATUS LEDs start flashing alternately.
  3. Remove the pinhole tool from the DEFAULT button. The IP SLA is now in the download mode.

  **NOTE**: To change the mode using an older IP SLA (revision level earlier than -AC), remove and reconnect the cable from/into the 10BASE-T jack six times within three seconds. The ON-LINE and SL STATUS LEDs start flashing alternately. If the LEDs do not flash alternately, repeat this procedure until the LEDs start flashing.
12. UPDATING Firmware

12.1 This section describes how to update firmware onto the IPRC and IP devices. The first two sections describe how to update the firmware onto the IPRC and IP devices using the following applications:

- **Upload Utility** (previously called Board Utility) — Comes with Axxess/Eclipse system Database Programming v5.1 or later (see below).

- **Trivial File Transfer Protocol (TFTP) Download** — Comes with the IP devices CD-ROM, or you can download it from the Inter-Tel Web site (www.inter-tel.com/software). See page 58 for details.

12.2 The IPRC firmware is not automatically updated by Call Processing. If the system is Axxess v5.0 or earlier, which does not include the Board Utility (or Upload Utility), use the TFTP Download application.

12.3 The third section describes how to update firmware onto Models 8600, 8620/8622, 8662, and 8690. These new endpoints use a **TFTP server** to update their firmware. The TFTP server allows the endpoints to pull firmware updates from a TFTP server automatically, rather than push firmware updates to individual endpoints (see page 66).

A. UPLOAD UTILITY APPLICATION

NOTE: The Upload Utility application is not applicable to the Models 8600, 8620/8622, 8662, and 8690 endpoints. To update firmware onto these endpoints, you must use a TFTP server (see page 66).

12.4 The Upload Utility program, supplied with the system Database Programming software, can be used for loading different versions of software on the IPRC and IP devices. The Upload Utility supports a network connection as well as a direct connection (RS-232 method) for uploading the firmware onto the IPRC. Inter-Tel recommends using the network connection for uploading the firmware.

12.5 The latest version of the Upload Utility allows you to upgrade multiple IP devices at once. This feature was implemented to assist installers who need to upgrade the IP devices to take advantage of the new 8.1 features (i.e., peer-to-peer audio). You can also save your settings so that you do not have to configure information for every upload. For example, you can create an entry used strictly for IPRCs on Node 2. Or, you can create one for all hard IP endpoints, such as the Model 8660, in your network.
Network Connection

12.6 To upload firmware onto IP devices or IP cards via a network connection:

1. Select Start - Programs - Inter-Tel DB Programming - Upload Utility.

2. Click New or select New from the File menu to create an entry.

3. Complete the following fields:
   - **Settings For:** Enter a description, up to 40 characters, that allows you to identify
     the connection type. For example, if creating a setting for the IP devices on node 2,
     enter **Node 2 IP Devices**.
   - **Device Type:** Select **IPP+/IP SLA - (IP Phones)** for IP devices or **IPRC/IPC - (IP Cards)**
     for IP cards. The Username field is automatically populated (IPT or IPC, respectively)
     in the Network tab.
   - **Connection Type:** Select the Network tab.

4. Click **Browse** in the Network tab. The Upload Utility queries the network for a list of
   IP addresses for Inter-Tel devices on the network. This information is then displayed
   in the Browse IP Address screen and includes the following:
   - **IP Address:** The IP address of the board or device found on the network.
   - **Hostname:** The hostname assigned to the board or device.
   - **Description:** The description used to identify the board or device in Database Pro-
     gramming. For IP endpoints, this is the station description.

5. Highlight the IP address of the desired device and click **Add**. To add all IP addresses or
   hostnames, click **Add** without highlighting any items. The selected IP addresses are
   added to the list box in the main screen.

   **NOTE:** To add multiple addresses/hostnames, use the standard Windows **SHIFT +
   click** or **CTRL + click** method.

6. Click **Save** to save the settings. At the prompt, click **Yes** to confirm the save.
7. Specify the filename to upload in the Upload File field, or click the ellipsis (...) button to select a file from the dialog box. The source file names differ based on the device. In general, the file names for IP devices are as follows:

- `ipp+.hex` for the IP PhonePlus
- `ipp8660.bin` for the Model 8660 Endpoint
- `ip_sla.hex` for the IP SLA

The file names for IP cards are as follows:

- `iprc_<version>.hex` for a device or networking IPRC
- `ipc.hex` for the IPC

**NOTE:** The IPRC files include the version. For example, if uploading a version 8.1 networking IPRC, the source file would be `iprc_8_1_x.hex`.

8. Enter the password. By default, this is `iptpassw` (case-sensitive).

9. If necessary, enter the port number that corresponds to the Web listening port number assigned to the IP card/device. The Port value must match the Web listening port number; otherwise, the upload will fail. By default, this is 80.

10. Click **Start** or select **Start** from the File menu. If you entered the correct IP address(es), username, and password, the upload process begins, and an Upload Progress screen is displayed. This screen indicates the IP address or hostname of the affected devices and the status of the upload.

While in this screen, you have the following options:

- **Close:** Closes the screen.
- **Retry:** Allows you to attempt the upload again for failed operations. To retry the upload, highlight the IP address or hostname of the devices that did not get upgraded and click **Retry**. To attempt the upload again for all devices that did not get upgraded, do not select any IP addresses or hostnames before clicking **Retry**.
- **Save Log:** Saves the log information to a text file (.txt).
- **Cancel:** Terminates the upload operation.

11. Click **Close** when the upload is complete.
12.7 Once the device accepts the file, the device indicates this change of state. The IPRC will flash the green Card On-Line LED and the yellow Circuit Busy LED once per second while it erases and programs its flash memory. The LCD on the IP PhonePlus will display ERASING FLASH, followed by PROGRAMMING CODE, and then DOWNLOAD COMPLETE. The IP SLA will flash the On-Line LED and the SL Status LED once per second while it erases and programs its flash memory.

**Direct Connection (RS-232 Method)**

**NOTE:** This method applies to IPRC and IP SLAs only.

**12.8 To upload firmware via an RS-232 connection:**

1. Make sure the IPRC is connected and online.
2. Connect a programming PC to the IPRC serial port jack as follows (refer to the diagram below). The necessary connectors can be purchased separately or as part of the Universal RS-232 Kit (part no. 828.1282). This RS-232 connection is the same as the RS-232 connection to the CPU cards used for Database Programming.
   a. Attach one end of an 8-wire reversing mod-to-mod line cord (part no. 813.1682) to the serial port jack on the IPRC.
   b. Attach the other end of the line cord to a DB9F-to-8P/8C modular adapter with RTS/CTS flow control (part no. 804.2545).
   c. If the PC does not have an available DB9M COM port, but does have an available DB25M COM port, attach the DB9M-to-DB25F converter to the DB9F end of the modular adapter.
   d. Connect the cable to the appropriate COM port on the programming PC.
3. Select Start - Programs - Inter-Tel DB Programming - **Upload Utility**.
4. Specify the board type and filename that you wish to upload, as described in step 7 on page 60.
5. Select **Direct Cable** as the connection type, and select the communications port and set the bit rate speed. Use the list boxes to scroll to the proper settings.

![Image of upload utility interface]

6. Click **Start** (or select Start from the File menu). The upload process begins. A progress bar will appear to show the progress of the upload.

**12.9** Once the device accepts the file, the device indicates this change of state as follows:

- The IPRC will flash the green Card On-Line LED and the yellow Circuit Busy LED once per second while it erases and programs its flash memory.
- The IP SLA will flash the On-Line LED and the SL Status LED once per second while it erases and programs its flash memory.
B. TFTP DOWNLOAD APPLICATION

**NOTE:** The TFTP Download application is not applicable to the Models 8600, 8620/8622, 8662, and 8690 endpoints. To update firmware onto these endpoints, you must use a TFTP server (see [page 66](#)).

**12.10** The TFTP Download application allows you to download object code to update the firmware in the IP devices whenever necessary. The application uses TFTP and is a client of TFTP.

**12.11** The TFTP Download application has two modes of download: immediate download and placing the device in download state before downloading to the device. Inter-Tel TFTP Download is a pop-up dialog box that contains five fields. The first three fields, Filename, IP Address, and Timeout, are used by the application to download object code. The next two fields are hidden unless the “Place the device in download state” option is selected.

**NOTE:** The TFTPDownload.exe program is available on the CD. To obtain a copy, order part number 827.9162. Current flash upgrade files are located on Inter-Tel’s Web site ([www.inter-tel.com/software](http://www.inter-tel.com/software)).

### Placing the Devices in Download State

**12.12** Before you can start downloading code to the IPRC or IP device, you must first get the device into the download state. You can do this in a number of different ways:

**12.13** **HTTP/Web Interface Method:**

1. Make sure the IP device is powered up, connected, and online. Then point a Web browser to the IP address of the device. The default IP address for the IP card and IP devices is 192.168.200.201.

2. Log in with your username and password. The default usernames and passwords are shown below.

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>USERNAME</th>
<th>PASSWORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPRC</td>
<td>IPRC</td>
<td>itpassw</td>
</tr>
<tr>
<td>IP Devices</td>
<td>IPT</td>
<td>iptpassw</td>
</tr>
</tbody>
</table>

3. When the Welcome page appears (as shown on [page 84](#)), select **Command - Download**. You will see a warning that a download will drop any calls that are in progress.

4. Select **OK** to place the device in download state.

**IP Device Alternative Methods**

**12.14** **Method 1:** While powering up the IP device, simultaneously hold down the 5 and 6 buttons on the dialpad until the display shows WAITING FOR DOWNLOAD.

**12.15** **Method 2:** Power down the IP device. Power up the device exactly six times, leaving the device powered up about one to two seconds and powered down about one second each time. Following the sixth cycling of power, the device should be in the download state (the IP endpoint will display WAITING FOR DOWNLOAD, and the IP SLA Online LED and the SL Status LED will alternate flashing once per second). If the device does not change to the download state, repeat this entire power-cycle process.
12.16 Method 3: Remove the IPRC from the phone system. While reinserting the IPRC into the system, hold in the MAKE BUSY SWITCH until the green Card On-Line LED and the yellow Circuit Busy LED alternate flashing once per second indicating that the device is in the download state. If you have a 9600-baud terminal emulator connected to the RS-232 port on the IPRC, you will see the IP address the card is using.

12.17 To download firmware:

1. Run **TFTPDownload.exe** and enter the information as described below.

![TFTP Download Application](image)

2. Specify the filename that you wish to download in the Filename field, or click **Browse** to select a file from the dialog box. In general, the file names are shown as follows:
   - `iprc_device_X_X_X.hex` for the IPRC where the `X_X_X` represents the version number (e.g., for version 1.3.0, the file is `iprc_device_1_3_0.hex`)
   - `ipp+.hex` for the IP PhonePlus
   - `ipp8660.bin` for the Model 8660 endpoint
   - `ip_sla.hex` for the IP SLA
3. Enter the target device’s current IP address.
4. The timeout field specifies the expiration time, in seconds, that the target device will have to respond to the application. If the timeout expires, the application aborts the download. The range is 30 - 5000 seconds. Enter the desired timeout value.
5. If you wish to remove the IP address from the local ARP cache before downloading the object code to the device, check the **Remove IP Address from the local ARP cache** check box. This function is useful when downloading code to devices that use the same IP address one after another.
6. **Immediate download to the device**: To download object code only to the target device, make sure the “Place the device in download state” check box is not checked.

**To place the device in Download State and then download to the device**: *(This feature is available only when the Web server is enabled on the target device.)* Check the “Place the device in download state” check box. Two additional fields appear, as shown below. After you click **Download**, the client authenticates the username with the target device before placing the target device in download mode by sending these fields. If the authentication process fails, the download process aborts and an error message is displayed. If the authentication is successful, the download process begins.

![TFTP Download Application](image)

**NOTE**: If the device is already in the download state before you check the box, and you start the download, the download will fail. Use the immediate download method, described above, for devices already in the download state. The download will not work unless the “Place the device in download state” check box is unchecked.

7. After entering all of the fields, click **Download**. A progress bar appears to show the progress of the download. You may click **Abort** to abort the download or **Close** to abort the download and quit the application.

8. Once the device accepts the file, the device indicates this change of state. The IPRC will flash the green Card On-Line LED and the yellow Circuit Busy LED once per second while it erases and programs its flash memory. The LCD on the IP PhonePlus or Model 8660 endpoint will display ERASING FLASH, followed by PROGRAMMING CODE, and then DOWNLOAD COMPLETE. The IP SLA will flash the On-Line LED and the SL Status LED once per second while it erases and programs its flash memory.

12.18 Common download error messages during software loading include the following:

- **Bad Header Record or Unknown Code ID**: When downloading the boot code, if the device already contains the same version of production boot code, it returns this error message to let you know that you do not need to download new boot code because it already contains the exact same version. You can verify the version of the boot code through the Telnet (or RS-232) online monitor’s “V” command or through the Web interface’s Firmware Version page (see page 118).
C. TFTP SERVER

NOTICE
It is strongly recommended that you upgrade all multi-protocol IP endpoints to the latest firmware release. This will minimize potential conflicts when installing new endpoints at an existing site. The multi-protocol IP endpoint firmware is available at Inter-Tel’s edGe Web site (www.inter-tel.com/software). For instructions about how to upgrade the firmware, see page 58.

12.19 Unlike previous IP endpoints, the Model 8600 series endpoints (does not include the Model 8660) can use a TFTP server to update their firmware. This allows the endpoints to pull firmware updates from a TFTP server automatically, rather than push firmware updates to individual endpoints. Freeware TFTP servers are widely available. The following description focuses on the Jounin TFTPD32 TFTP server (http://tftpd32.jounin.net).

Configuration Files

12.20 When the endpoints are connected to a PC that has the firmware update, the endpoints start downloading two configuration files through the TFTP server in the order listed below:

- **Global configuration file** (*globalcfg.cfg*): Contains the default configuration of all configuration parameters. This file is used to update firmware onto multiple endpoints simultaneously. Use the global configuration file to set system-wide settings such as the DHCP enable option, the TFTP server address, the SIP or ITP mode option, and if the endpoints connect to the same server, the IPRC or SIP Server port and address.

- **Device-specific configuration file** (*xxxxxxxxxxxxxxx.cfg - where the x indicates the endpoint Ethernet address*): Contains a subset of the configuration parameters specific to the device. This file is used to update firmware onto an endpoint individually. Use this file for device-specific settings such as static IP settings, the ITP logon password, the SIP extension and authentication information, or anything else that is specific to this particular endpoint.

**NOTE:** The device-specific configuration file overwrites any configuration information that is in the global configuration file.

12.21 The endpoints then download the configuration files from the server periodically (defaults to one hour).

12.22 When the configuration file detects that the endpoint does not have the latest firmware, the endpoint also downloads the **firmware update file** (e.g., *8600_1_001.bin*) from a TFTP server. This file contains the updated firmware information.

**NOTE:** You do not have to use the same TFTP server to download the firmware update and the configuration files. In other words, you can download the files from anywhere.

12.23 To update firmware onto Models 8600, 8620/8622, 8662, and 8690, see page 68.

12.24 If the endpoint is unable to contact the TFTP server, it continues to use the last configuration stored in its flash or the configuration that the endpoint receives from the Axxess system when in ITP mode.
NOTE: For the Model 8600 that has no display, use a DHCP server to assign the network settings and the TFTP server IP address to the endpoints. To do so, you must program the 66 and 67 option tags, described in the table below, in the DHCP server. Without programming these options, the endpoint cannot use the TFTP IP address and path from DHCP. Note that the DHCP options can be used for all multi-protocol endpoints, not just the 8600.

<table>
<thead>
<tr>
<th>DHCP OPTION TAG</th>
<th>DESCRIPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>Specifies the TFTP server IP address. The value of this option tag cannot contain the TFTP server domain name.</td>
</tr>
<tr>
<td>67</td>
<td>Specifies the TFTP server path where the configuration resides. If this tag is not provided, the endpoint assumes that the configuration files are located in the root of the TFTP server path.</td>
</tr>
</tbody>
</table>

Determine the IP address of a Model 8600

12.25 This section provides recommended methods to determine the IP address of an Model 8600 that does not have a display.

NOTE: The following methods work for the other Model 8600 series endpoints as well, but the other endpoints have a display to show their IP address.

12.26 If there is no DHCP server on the LAN:

1. Hold 4 and 7 to power up the endpoint. Release the buttons when the lamps turn off and the tone sounds. The endpoint is in self-test mode and uses the Inter-Tel default IP address of 192.168.200.201.

2. Configure a PC on the same LAN with a similar IP address (for example, 192.168.200.202), and web to the device to complete the configuration of the endpoint.

12.27 If there is a DHCP server on the LAN:

1. Hold 7 and 8 during power up to default its configuration. This step ensures that the endpoint will attempt to retrieve an IP address from a DHCP server.

2. Program the endpoint’s MAC address on an IPRC on the same LAN as the endpoint. When the endpoint connects to the IPRC from ITP mode, check the IPRC or Axxess Database Programming to determine the IP address of the endpoint.
Update Firmware onto Models 8600 Series Endpoints

**CAUTION**

**Device Inoperability.** To successfully update the firmware on a Model 8690 endpoint, you must use a TFTP server client that is capable of file transfers greater than 32 MB. (One of the three Model 8690 firmware update files is greater than 32 MB.) Currently, the only known TFTP client with this capability is a freeware application called Jounin TFTP32 (http://tftpd32.jounin.net). If another TFTP client is used, and it cannot transfer files greater than 32 MB, the partially downloaded file will be corrupted and render the Model 8690 inoperable. There is no restore procedure other than to return the endpoint to Inter-Tel for repair or replacement.

12.28 To update firmware onto Models 8600, 8620/8622, 8662, and 8690:

1. Run `tftpd32.exe`. The following screen appears.

![TFTP Server Screen](Image)

2. The Current Directory field should be automatically populated. If not, enter (or browse to) the directory path that contains the firmware update (e.g., `192.168.200.201\sip_configs\8690_2_3_2\bin`). The Server interfaces field is automatically populated and does not need to be changed.

**NOTE:** If you are entering a directory path manually, use backslash (`\`) for the 8690 User Interface Image and Windows CE Image URLs, and use forward slash (`/`) for the Models 8600, 8620/8622, and 8662 Image URLs and the 8690 Call Control Image URL. For details about images, see the following page.
3. Click **Settings** and check **Allow ‘\’ As virtual root** and **Translate UNIX Filenames** from the Advanced TFTP Options. Then click **OK**.

Once a connection is established, the connection log appears in the display, as shown below.

![TFTP Client Screen](image)

4. When the endpoint pulls its configuration files from a TFTP server, update one of the configuration files as described below. Sample configuration files are shown on the following pages. For complete information about configuration parameters, see page 158.

   For Models 8600, 8620/8622, and 8662, update the following fields (under Software Image) in the configuration files.

   - **xxxx_image_ver**: (where the xxxx indicates the model name, such as the 8622): 
     Change or add the new version number as follows:
     - With versions 1.0.x, change the file name to “xxxx_image_ver: v.v.v” where the v.v.v indicates the version number, such as 1.0.33.
     - With versions 1.1.x, change the file name to “xxxx_image_ver: HWID 1 v.v.v” where the v.v.v indicates the version number, such as 1.1.5.

     **NOTE:** Updating to versions 1.1.x, if the “HWID 1” portion of the version string is missing, the endpoint will flash the error message “ERROR WRONG VERSION” when attempting to download the image (see page 201 for details).

   - **xxxx_image_url** (where the xxxx indicates the model name, such as the 8662): 
     Change or add the URL of your TFTP server; e.g., “8600_image_url: 10.0.0.11/8600_updates/8600_1_001.bin.” Be sure to include any paths from the TFTP root to the software update.
Firmware Update Changes: When upgrading an 8620, 8622, or 8662 endpoint, use the following version strings.

From 1.01S to 1.0.31
86xx_image_ver: 1.0.31 (where the 86xx indicates the model type, such as 8622)
86xx_image_url: 192.168.200.202/86xx/86xx_1_0_31.bin

From 1.01S or 1.0.31 to 1.0.33
86xx_image_ver: 1.0.33
86xx_image_url: 192.168.200.202/86xx/86xx_1_0_33.bin

From 1.0.33 and earlier to 1.1.5
86xx_image_ver: HWID 1 1.1.5
86xx_image_url: 192.168.200.202/86xx/86xx_1_1_5.bin

NOTE: If upgrading an 8622 from 1.01S to 1.1.5, use the following image version string: 8620_image_ver: 8620 HWID 1 1.1.5.

From 1.1.5 and earlier to 2.0.06
86xx_image_ver: HWID 2 2.0.06
86xx_image_url: 192.168.200.202/86xx/86xx_2_0_06.bin

For future releases (2.0 and later)

iphone_image_ver: v.v.vv (where the v.v.vv indicates the firmware version, such as 2.0.06)

iphone_image_url: 192.168.200.202/iphone/iphone_v_v_vv.bin (where the v_v_vv indicates the firmware version, such as 2_0_06)

NOTE: After an endpoint is updated to the v2.0.06 or later firmware, the 86xx_image_ver and _url strings are no longer necessary. There are only two lines in the configuration files that need to be modified (iphone_image_ver and iphone_image_url), and there is only one image to be put on the TFTP server to update all of the multi-protocol endpoints (excluding the Model 8690).

For the Model 8690, update the following three software components (six fields total), as described above.

- **Call Control Image** (8690 dsp_image_ver and 8690 dsp_image_url): Indicates the version or URL of the call control. The dsp indicates digital signal processing.
- **Windows CE Image** (8690 os_image_ver and 8690 os_image_url): Indicates the version or URL of the Windows CE .NET. The os indicates an operating system.
- **User Interface Image** (8690 gui_image_ver and 8690 gui_image_url): Indicates the version or URL of the user interface. The gui indicates a graphical user interface.

NOTE: If the gui or os image version string does not match the version of the file specified by image url, then the endpoint will continually prompt you to upgrade.

You could also change the “xxxx_image_ver” and “xxxx_image_url” fields through the Web interface on the endpoint. See page 145 for information about the IP Phone Web Client.
**NOTE:** If the endpoint pulls configuration files from a TFTP server in addition to updating the Web interface, then the configuration files on the TFTP server will overwrite any change you make through the Web interface on the endpoint.

5. Wait for the endpoint to re-synchronize its configuration or force it to re-synchronize through the Web interface on the endpoint (see page 157).

### Firmware Download Progress Displays

**12.29** Several changes have been made to the firmware image update process.

**NOTE:** These changes only apply when the endpoint is running version 2.0.06 or later firmware (not when upgrading from 1.1.5 to 2.0.06, for example).

- Two copies of the firmware image are kept in case one gets corrupted during a failed download attempt (this does not apply to the Model 8600 endpoints). This may cause the firmware update process to take more time than before.

- Additional messages are displayed on the LCD during the firmware download process so the user knows the current firmware download state and does not accidentally interrupt the process (i.e., unplug the endpoint thinking that it has hung up). The table on the next page lists the updated progress displays.

**Table 6: Firmware Download Progress Displays**

<table>
<thead>
<tr>
<th>DISPLAY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOWNLOAD IN PROGRESS</td>
<td>The endpoint is downloading the image from the TFTP server.</td>
</tr>
<tr>
<td>ERASING PRIMARY FLASH</td>
<td><em>(New)</em> The endpoint is erasing primary flash. The endpoint is preparing to program the primary flash with the new software image. This message is usually only shown briefly.</td>
</tr>
<tr>
<td>WRITING IMAGE TO PRIMARY FLASH</td>
<td><em>(New)</em> The endpoint is programming the image to the primary flash.</td>
</tr>
<tr>
<td>ERASING BACKUP FLASH</td>
<td><em>(New)</em> The endpoint is erasing backup flash. The endpoint uses the backup flash as a place holder when downloading the image or as a backup storage to restore the image in case the primary flash is corrupted. This message is usually shown briefly.</td>
</tr>
<tr>
<td>WRITING IMAGE TO BACKUP FLASH</td>
<td><em>(New)</em> The endpoint is programming the image to the backup flash.</td>
</tr>
<tr>
<td>FIRMWARE DOWNLOAD SUCCESS</td>
<td>The endpoint has successfully updated the firmware. The endpoint will reset.</td>
</tr>
</tbody>
</table>

**NOTE:** If an error occurs during the firmware download process, the endpoint displays an error message described on page 73.

### Firmware Download Startup

**12.30** An endpoint with v2.0.06 or later firmware is disconnected from Call Processing while downloading an image. This prevents any incoming or outgoing calls from taking place.
D. AUTOMATED BOOT CODE UPDATE

12.31 The Models 8620, 8622, and 8662 endpoints with v2.0.06 or later firmware can now use a TFTP server to update their boot code. This works very similar to the firmware updates. The endpoint checks configuration from the TFTP server and reads new parameters either on startup, by user request, or from periodic timeout. If the boot version in the configuration file is different from the version currently on the endpoint, then the endpoint initiates the boot update procedure and downloads the new boot code. Note that the endpoint will delay this action if there is an audio stream, such as when on a call or music on hold is enabled.

12.32 The following parameters must be set in the global configuration file.

Boot Image Updates

iphone_boot_ver: v.v.vv (where the v.v.vv indicates the version number, such as 2.0.06)

iphone_boot_url: 192.168.200.202/iphone/iphone_v.v.vv_boot.bin (where the v_v_vv indicates the version number, such as 2_0_06)

Boot Code Download Progress Displays

12.33 The following table lists the progress displays that appear on the endpoint during the boot update procedure.

Table 7: Boot Code Download Progress Displays

<table>
<thead>
<tr>
<th>DISPLAY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT DOWNLOAD IN PROGRESS</td>
<td>(New) The endpoint is downloading the specified boot image from the TFTP server.</td>
</tr>
<tr>
<td>FORMATTING BOOT IMAGE</td>
<td>(New) The endpoint formats the boot image area.</td>
</tr>
<tr>
<td>WRITING BOOT TO FLASH</td>
<td>(New) If the image passes all tests, then the endpoint writes the image to flash.</td>
</tr>
<tr>
<td>VERIFYING WRITE</td>
<td>(New) This message is displayed when the endpoint reads and performs a checksum check of the boot image on flash. If the check fails, then the endpoint returns to the Writing the boot to flash state.</td>
</tr>
<tr>
<td>BOOT DOWNLOAD SUCCESS</td>
<td>(New) If the boot is successfully written, then the endpoint will reset.</td>
</tr>
</tbody>
</table>

NOTE: If an error occurs during the boot code download process, the endpoint displays an error message described on page 73.

CAUTION

Unlike firmware updates, if the boot code download procedure is interrupted by a power outage or human intervention (for example, unplugging the endpoint power cord), the endpoint will become inoperable and cannot be recovered. If this occurs, you must return the endpoint for repair.

Boot Image Changes

12.34 The boot image requires that the boot image version, including the hardware ID and platform type be stored in the last x bytes of the boot image. For example:

...<NULL>ITPHONE:2:2.0.06<NULL>9219b198ce21bd806796fddf98f74f2e<EOF>

12.35 The checksum is a 32-character (128 bit or 16 byte) MD5 checksum. The checksum evaluates the image and image version, but not the last NULL and the checksum itself.
E. DOWNLOAD ERROR MESSAGE DISPLAYS

12.36 The endpoint now displays error information concerning the status of the last TFTP application image update (firmware or boot code) not only on the LCD but also on the Web interface. The error message is displayed under Status - Image Upgrade - Last Download Error (see page 157). The following table lists the possible error messages.

Table 8: Image Download Error Message Displays

<table>
<thead>
<tr>
<th>DISPLAY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| ERROR TFTP FAIL                | The image download process failed because of one of the following problems:  
  • The endpoint cannot contact the TFTP server.  
  • The TFTP server does not have the software image file.  
  • The TFTP image URL contains the wrong path.  
  • The TFTP server does not have the permission to read the software image file. |
| ERROR TFTP FAIL START          | The endpoint failed to start TFTP client. This problem could be due to an insufficient file descriptor for TFTP, etc.                          |
| ERROR BAD FLASH                | The image download process failed because of a faulty flash memory device or the flash file system is corrupted. If the user encounters this error, replace the device. |
| ERROR TFTP TIME-OUT            | The endpoint failed to communicate with the TFTP server. This error could be due to bad network connectivity.                                   |
| ERROR WRONG VERSION            | The image contains an unexpected software version.                                                                                         |
| ERROR WRONG PLATFORM           | The image contains an unexpected platform identifier.                                                                                       |
| ERROR MISC ERROR               | Miscellaneous errors include a corrupted file system, unrecognized error by the TFTP library, etc.                                           |
| ERROR NOT GZIP                  | The image is not in GZIP format.                                                                                                             |
| ERROR INVALID FILE ID          | The image does not contain the appropriate file identifier.                                                                                   |
| ERROR INCOMPATIBLE HW          | The image contains the wrong hardware ID.                                                                                                     |
| ERROR FILE TOO BIG             | (New) The file that the endpoint downloaded for upgrade is too large.                                                                          |
| ERROR BOOT IMAGE CORRUPT       | (New) The boot image downloaded is corrupt.                                                                                                   |
| ERROR ALLOCATE FAILURE         | (New) The endpoint was unable to allocate enough memory to download the image.                                                                |
| ERROR FAILED VERIFY            | (New) The image written to flash does not match the file downloaded (i.e. there was a write error).                                             |
FIGURE 6. Sample Global Configuration File

```plaintext
# Any settings that the phone does not find in its
# device-specific configuration file, the phone will use
# the global configuration equivalent. If the setting is
# not in the device-specific file or the global file, the
# phone will not change its local setting.
#
# A line beginning with # denotes a comment.
#
# Comments lines are commented because we would rather
# pull the settings from the device-specific config file
# or let the phone keep its local setting.

# Network Settings

# DHCP -- 0 = disabled; 1 = enabled
dhcp: 1

# Put static IP in the device-specific config file.
#static_ip: 192.168.200.201
#subnet_mask: 255.255.255.0
#default_gw: 192.168.200.1

# The IP of the FTP server.
# Could also include a path from the FTP root.

# The FTP port number for the phone's web server.
http_port: 9000

# Operation mode -- 0 = SIP; 1 = ITF
open_mode: 1

# Phones will pull this config file every 3600 seconds
update_interval: 3600

# IIF Mode Settings

# DPC's IP address
ccsrv_ip: 192.168.200.100

# SIP mode settings

# SIP names should be in the device-specific config.
sip_name: 1000
sip_display_name: 1000

# SIP ID and ports can be in the global config.
sip_reg_ip: 192.168.200.100
sip_reg_port: 5060
sip_proxy_ip: 192.168.200.100
sip_proxy_port: 5060

# SIP Authentication name and password, if needed.
# Normally not set in device-specific config file.
sip_authname: 1000
sip_authpassw: 1000

Continued on the next page...
```
$ Register with the SIP server every 3000 seconds.
    sip_reg_period: 3000

$ Dial this string to retrieve messages.
$ Inter-Tel SIP Server requires "VOICEMAIL".
    sip_voicemail: VOICEMAIL

$ SIP Dial Plan

$ Dial plans are for SIP mode only!
    in_dial_plan: 1xxx
trunk_dial_plan: 9xxx

$ SIP Audio Settings

$ These audio settings are for SIP mode only!
$ Audio compression; see manual for other values.
    trn_code: 9

$ Audio frames per IP packet.
    audio_frm: 9

$ UDP port for audio
    audio_port: 5004

$ This is the 8500 version
    8500_image_ver: 1.01R
    8500_image_url: 152.158.200.202/8500_1_01R.bin

$ This is the 8520 version
    8520_image_ver: 1.01R
    8520_image_url: 152.158.200.202/8520_1_01R.bin

$ This is the 8562 version
    8562_image_ver: 1.01R
    8562_image_url: 152.158.200.202/8562_1_01R.bin

$ This is the 8590 DSP/Call-control version
    8590_dsp_image_ver: 1.01R
    8590_dsp_image_url: 152.158.200.202/8590_dsp_1_01R.bin

$ This is the 8590 WinCE version
    8590_os_image_ver: 1.020
    8590_os_image_url: 152.158.200.202/8590_os_1_020.bin

$ This is the 8590 GUI version
    8590_gui_image_ver: 1.001R
    8590_gui_image_url: 152.158.200.202/8590_gui_1_001R.cab

Update Required

Continued on the next page...
FIGURE 6. Sample Global Configuration File (Continued)

```
# This would upgrade an 0820/8822 endpoint from 1.0.31 or 1.0.32 to 1.0.33.
#8820_image_url: ip182.188.200.302/8820_f_0_33.bin

# This would upgrade an 0820/8822 endpoint from 1.0.31, 1.0.32, or 1.0.33 to 1.1.5.
#8820_image_url: ip182.188.200.302/8820_f_1_5.bin

# This would upgrade an 0820/8822 endpoint from 1.0.31, 1.0.32, or 1.0.33 to 2.0.0.
#0820_image_url: ip182.188.200.302/820_f_2_0_0.bin

# This upgrades all versions 1.0.00 endpoints and later.
# It is recommended that users leave this line uncommented along with the above two lines.
# This overwrites the information in the endpoint’s internal database (it will
# be set as specified in the above lines). Otherwise, the endpoint may display a
# “READING PLATFORM TYPE” error when it reboots.

#iphone_image_url: ip182.188.200.302/iphone_f_2_0_0.bin

# This upgrades the boot image for all endpoints running version 2.0.00 firmware and later.
#iphone_boot_url: ip182.188.200.302/iphone_f_2_0_0_boot.bin
```
FIGURE 7. Sample Device-Specific Configuration File

Continued on the next page...
FIGURE 7. Sample Device-Specific Configuration File (Continued)

```
# SIP Authentication name and password, if needed.
# Normally set in device-specific config file.
sip_authname: 1000
sip_authpassword:

# Reregister with the SIP server every 3600 seconds.
# Normally set in the global config file.
#sip_reg_period: 3600

# Dial this string to retrieve messages.
# Inter-Tel SIP Server requires "VOICEMAIL".
# Normally set in the global config file.
sip_voicemail: VOICEMAIL

Update Required
(Only if not configured in the global config file)

Continued on the next page...
```
FIGURE 7. Sample Device-Specific Configuration File (Continued)

```
@ This would upgrade an 8810/8822 endpoint from 1.0.31 or 1.0.32 to 1.0.33
8810_image_url: 181.188.200.202/8822_1.0_33.bin

@ This would upgrade an 8810/8822 endpoint from 1.0.31, 1.0.32, or 1.0.33 to 1.1.5
8820_image_url: 181.188.200.202/8820_1.1.5.bin

@ This would upgrade an 8810/8822 endpoint from 1.0.31, 1.0.32, or 1.1.5 to 1.0.00
8820_image_url: 181.188.200.202/8820_1.0.00.bin

@ This upgrades all version 1.0.00 endpoints and later
@ It is recommended that users leave this line unaltered along with the above two lines.
@ This overwrites the information in the endpoint’s internal database (it will
@ be set as specified in the above lines). Otherwise, the endpoint may display a
@ "UNKNOWN PLATFORM TYPE" error when it reboots.
iphone_image: 1.0.00
iphone_image_url: 182.188.200.202/iphone_1.0.00.bin

@ This upgrades the boot image for all endpoints running version 1.0.00 firmware and later
iphone_boot_url: 182.188.200.202/iphone_1.0.00_boot.bin
```
13. PROGRAMMING THE IP DEVICES ON A V1.5.X FIRMWARE IPRC

NOTE: This section describes IP devices programming on a v1.5.x firmware IPRC. For information about IP devices programming on a v8.2.x firmware IPRC, see page 141.

13.1 The v1.5.x firmware IPRC and IP devices can be programmed using the following methods:

- Learn Mode (see below)
- Self-Programming Mode (see page 82)
- HTTP/Web Interface (see page 84)
- RS-232 Serial Connection — IPRC Only (see page 130)
- Telnet Session (see page 131)

NOTE: Do not change the IP card’s database while a call is active; it may drop all calls in progress.

13.2 To upgrade a v1.5.x or earlier firmware to a v1.5.x firmware:

1. Make sure the software license supports the number of multi-protocol endpoints that will terminate on the IPRC.

2. Make sure it does not reside behind a firewall or NAT (see page 13 for details).

3. From the IPRC Administrative Session Web page, save the existing database in the event it needs to be restored.

4. Remove the card from the cabinet and remove the PAL (located in slot U22).

5. If necessary, install the daughter card.

6. Place the card in the correct slot in the cabinet.

7. Run the Upload Utility and upload the 8.x firmware to the IPRC and the IP devices that terminate at the card. For details about updating firmware, see page 58.

8. Under System\Cabinets, change the card type to Internet Protocol Resource Card (32-Device).

NOTE: If you have a v8.2 or later Axxess system, refer to the Addendum to the Axxess v8.0 Installation and Maintenance Manual or the latest version of the Inter-Tel Axxess Installation and Maintenance Manual for details.

9. Under System\Cabinets\<IPRC>, program the card settings using the IPRC Web page as a guide.

10. Under System\Cabinets\<IPRC>\Devices, program the IP devices, using the IPRC Web page as a guide.

13.3 You can now program the IP devices to terminate at the card in Database Programming.
A. LEARN MODE

13.4 The IP devices have a mode that allows the IP card to “learn” the Ethernet address of an IP device. When power is applied to an IP device, the device first attempts to connect locally using broadcast messages on the LAN. If a local IP card does not respond, the IP device attempts to connect to its default IP card address. If the default IP card does not respond, the IP device broadcasts a Learn Mode message and then begins the cycle over.

13.5 Setting the Ethernet Address field of a circuit to 000000000000 puts the circuit into Learn Mode. The circuit’s device type in the Device Flags field must also be set to the correct type or Any Device in the RS-232/Telnet Device Programming. If an IP card receives a Learn Mode message from an IP device, the IP card programs the IP device’s Ethernet address into the first circuit on the IP card that is in Learn Mode. The IP card also updates the circuit’s device type to match the new device.

NOTE: A single IP card may have multiple circuits in Learn Mode, but multiple IP cards must not have circuits in Learn Mode at the same time.
B. SELF-PROGRAMMING MODE

13.6 The self-programming mode allows you to program the IP endpoints, such as the IP PhonePlus and Model 8660, through the dialpad.

13.7 To use the self-programming mode:

1. While pressing 7 and 8 together on your endpoint, unplug and replace the endpoint power cord. The endpoint enters the self-programming mode and the following screen appears on the endpoint display.

2. Select one of three options: Program Database, Default Database, or Exit using the menu selection button next to the LCD.

   The PROGRAM DATABASE option allows you to program the database through a series of screens that follow. The DEFAULT DATABASE option allows you to use predefined defaults for the database. The EXIT option allows you to exit the self-programming mode without making any changes.

Program Database

13.8 Follow the displays below and complete the programming. For details about REVERT, EXIT, <<, and >>, see paragraph 13.9 on the next page.

<table>
<thead>
<tr>
<th>DISPLAY</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATIC IP xxx.xxx.xxx.xxx</td>
<td>Static IP: Enter the static IP address (defaults to 192.168.200.201).</td>
</tr>
<tr>
<td>STATIC SUBNET xxx.xxx.xxx.x</td>
<td>Default Static Subnet Mask: Enter the default static subnet mask (defaults to 255.255.255.0).</td>
</tr>
<tr>
<td>DEFAULT GATEWAY xxx.xxx.xxx.xxx</td>
<td>Default Static Gateway: Enter the default static gateway address (defaults to 192.168.200.201).</td>
</tr>
<tr>
<td>REMOTE IPC IP xxx.x.xxx.xxx</td>
<td>Remote IPC IP Address: Enter the remote IPRC IP address (defaults to 172.16.15.152).</td>
</tr>
<tr>
<td>HOSTNAME Hostname:</td>
<td>This option allows you to program a hostname (up to 15 characters). To program the hostname, follow the instructions above.</td>
</tr>
<tr>
<td>BOOTP? xxxxxxxxxx</td>
<td>BOOTP: This option allows you to program the option to use BOOTP. The second line from the top indicates the current status (either ENABLED or DISABLED). To program this option: Select either ENABLED or DISABLED. The endpoint updates the display to reflect the new change.</td>
</tr>
<tr>
<td>DHCP? xxxxxxxxxx</td>
<td>DHCP: This option allows you to program the option to use DHCP. The second line from the top indicates the current status (either ENABLED or DISABLED). To program this option: Select either ENABLED or DISABLED. The endpoint updates the display to reflect the new change.</td>
</tr>
</tbody>
</table>
13.9 To program the IP address:

1. Press a dialpad button to enter the IP address. The entire second line, except the dots, disappears, and the number you entered appears in the first space. **MUTE** serves as a backspace button, and **FWD** or **#** moves the cursor to the next space after the dot.

**NOTE:** Pressing **MUTE** deletes the numbers without deleting the dots.

You have the following options:

- **Revert:** Reverts to the old value found in the current database, and the endpoint updates the display accordingly.
- **Exit:** Exits to the confirmation screen (last screen) without scrolling through all the other options. Refer to page 83 for more details on the confirmation screen.
- **>>:** Continues to the next screen in the series.
- **<<:** Returns to the previous screen in the series. Note that this option does not appear on the Static IP Programming screen.

2. Once you have finished programming, select either **EXIT**, **>>**, or **<<**. The endpoint will check the field for errors.

- **If there are no errors,** the endpoint displays the next programming screen.
- **If there are errors,** the endpoint displays **INVALID ENTRY.** Correct the error by either selecting **REVERT** or modifying the incorrect entry.

Default Database and Exit

13.10 When you have scrolled through all the options, selected **EXIT** from any of the screens, or selected **DEFAULT DATABASE** from the initial screen, the following screen appears to confirm the changes.

```
| S | A | V | E | C | H | A | N | G | E | S | ? |
|---|---|---|---|---|---|---|---|---|---|---|
| Y | E | S |
| N | O |
<<<<
```

13.11 You have the following options:

- **Yes:** Overwrites the database. If you select this option, the **CHANGES SAVED** screen will appear to notify you that the changes have been saved. To continue initializing the endpoint, press any button.
- **No:** Leaves the database as it was. If you select this option, the **NO CHANGES SAVED** screen appears to notify you that the changes have been discarded. To continue initializing the endpoint, press any button.
- **<<:** Returns to the previous screen in the series.
C. HTTP/WEB INTERFACE METHOD

**NOTE:** Unlike prior versions of IPRC firmware, the v8.1 IPRCs cannot be programmed through the IPRC Administrative Session Web page. The HTTP/Web Interface for the IPRC v8.2.x firmware is only used for diagnostics and troubleshooting purpose (see page 205). You must program the v8.1 IPRCs and IP devices through Axxess system Database Programming. For details about programming a v8.1 IPRC and IP devices, refer to the *Addendum to the Axxess v8.0 Installation and Maintenance Manual*.

13.12 The HTTP/Web interface called the IPRC Administration Session allows you to use a Web browser to connect to the IPRC v1.5.x firmware or any of the IP devices for Database Programming. Each IP card and IP device contains an embedded Web server. For information about the Networking IPRC Administrative Session, refer to the v8.0 or later *Axxess Installation and Maintenance Manual*.

**NOTE:** Your Web browser must be Internet Explorer v4.0 or later or Netscape v4.0 or later.

13.13 To use the IPRC Administration Session:

1. Make sure the IP device is powered up, connected, and online. Then point a Web browser to the IP address of the device. The default IP address for the IPRC and IP devices is 192.168.200.201. The screen shown below appears.

2. Log in with your username and password. The default usernames and passwords are shown below. To prevent unauthorized access, you should change the password of the IP card and its devices as soon as possible. To change the login passwords, see page 97 for the IP card and page 106 for IP devices.

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>USERNAME</th>
<th>PASSWORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPRC</td>
<td>IPRC</td>
<td>itpassw</td>
</tr>
<tr>
<td>IP Devices</td>
<td>IPT</td>
<td>iptpassw</td>
</tr>
</tbody>
</table>

**NOTE:** The usernames and passwords are case-sensitive. Also, if you have trouble connecting to the IP card using your usual Database Programming password while using Microsoft Internet Explorer 4.0 or later, disable the "connect with proxy server" option.
3. The programming options, shown in the table below, are displayed along the left edge of the screen. Select the desired programming option and follow the instructions given in the following pages.

<table>
<thead>
<tr>
<th>CARD CONFIGURATION (IP Card Programming)</th>
<th>REF. PAGE</th>
<th>DEVICE CONFIGURATION (IP Devices Programming)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Setup</td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td>• Card</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>• Device</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>Card Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Network</td>
<td>93</td>
<td>Device Configuration</td>
</tr>
<tr>
<td>• Audio and Call Control</td>
<td>95</td>
<td>• Network</td>
</tr>
<tr>
<td>• Change Login Password</td>
<td>97</td>
<td>• Audio and Call Control</td>
</tr>
<tr>
<td>Circuit Configuration</td>
<td></td>
<td>• Change Login Password</td>
</tr>
<tr>
<td>• Device Type</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td>• Device Information</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>• Network</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>• Advanced Network</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>• Call Control</td>
<td>103</td>
<td></td>
</tr>
<tr>
<td>• Audio Settings</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>• Advanced Audio Settings</td>
<td>106</td>
<td></td>
</tr>
<tr>
<td>• Device Login Password</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>• Device Specific</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Firmware Version</td>
<td>118</td>
<td>Status</td>
</tr>
<tr>
<td>• Network</td>
<td>118</td>
<td>• Firmware Version</td>
</tr>
<tr>
<td>• Receive Audio</td>
<td>119</td>
<td>• Network</td>
</tr>
<tr>
<td>• Circuits</td>
<td>121</td>
<td>• Receive Audio</td>
</tr>
<tr>
<td>Command</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Reset</td>
<td>122</td>
<td>Command</td>
</tr>
<tr>
<td>• Reset Circuits</td>
<td>123</td>
<td>• Reset</td>
</tr>
<tr>
<td>• Download</td>
<td>125</td>
<td>• Download</td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Save</td>
<td>125</td>
<td>Database</td>
</tr>
<tr>
<td>• Restore</td>
<td>126</td>
<td>• Not Available</td>
</tr>
<tr>
<td>• Default</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>Not Available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/100 Switch (for Model 8660 only)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Program Switch</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>• Default Switch</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Date &amp; Time</td>
<td>129</td>
<td>Miscellaneous</td>
</tr>
</tbody>
</table>

**NOTE:** For details about SIP-specific configuration, refer to the latest version of the *SIP Server Installation and Configuration Manual.*
Quick Setup — Card

13.14 When you select Card, the following page appears.

Card Internet Protocol(IP) Settings

You can get IP setting assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for appropriate network settings.

We strongly recommend that the IP Resource Card does not obtain its IP address automatically.

- Obtain IP Address automatically
- Using the following IP address

| IP Address | 192.168.200.201 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 0.0.0.0 |

| The IP Resource Card is behind the firewall, NAT or proxy server. |
| If the IP Resource Card is behind a firewall, NAT or proxy server you need to enter the IP Resource Card public IP address. This IP address can be used by the IP device located outside the firewall or proxy server to communicate with the IP Resource Card. You need to ask your network administrator for the IP Address. |

| IP Address | 0.0.0.0 |

13.15 Program the fields as described below. When finished, click OK to save your changes or Cancel to exit without changing the settings.

- **Obtain IP Address automatically (DHCP):** Select this option to set the IP address automatically.

**NOTE:** It is recommended that you do not obtain an IP address for the IP card automatically. If the address changes, the IP endpoint will no longer know what address to use.

- **Using the following IP address:** Enter the IP address, subnet mask, and default gateway in the text boxes. The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address (192.168.200.201)</td>
<td>Defines the default IP address for the IPRC. If the card does not receive a BOOTP or DHCP response, it uses this IP address. If 0.0.0.0 is entered, the server reports an error. IP addresses 0.0.0.0 and 255.255.255.255 are invalid IP addresses.</td>
</tr>
<tr>
<td>Subnet Mask (0.0.0.0)</td>
<td>Defines the default network subnet mask for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this subnet mask.</td>
</tr>
<tr>
<td>Default IP Gateway (0.0.0.0)</td>
<td>Defines the default IP gateway or router address for the IPRC. If the card does not receive a BOOTP or DHCP response, it uses this IP gateway address.</td>
</tr>
</tbody>
</table>

- **The IP Card is behind the firewall, NAT or proxy server:** If the IP card is behind the firewall, NAT, or proxy server, check this option and enter the IPRC public address that is located outside the firewall or proxy server. For more information, see “Operation Behind Firewalls or Proxies” on page 13.
13.16 When you click OK, the following page appears. Click Circuit Installation to continue installing the circuits, or click Back to go back and change the Internet protocol settings of the card.

**Network Settings Updated**

Press the "Circuit Installation" button to continue installing the circuits.

Click Circuit Installation

Press the "<Back" button to go back and change the Internet Protocol Settings of the card.

Click Back
Quick Setup — Device

NOTE: Before using the Device Quick Setup page, ensure that the browser has cookies enabled. To enable the cookies:

— For Internet Explorer v4.x: Select View - Internet Options - Advanced. Scroll down to Cookies in the Security section. Enable Always accept cookies. Then, click OK.

— For Internet Explorer v5.x and later: Select Tools - Internet Options - Security. Click Custom Level. Then, scroll down to Cookies and enable both Allow cookies that are stored on your computer and Allow per-session cookies (not stored). Then, click OK.

— For Netscape Navigator v4.x and later: Select Preferences from the Edit menu. Select Advanced (or Privacy and Security) from the tree selection on left of the screen. Then, under the Cookies section, check Accept All cookies (or Enable all cookies). Then, click OK.

13.17 To configure a device:

1. **Device Type:** When you select Device, the following page appears. Select the circuit number you would like to configure, and select the device type you are using.

   **Device Type**

   Please select the circuit number and device type.
   Circuit Number: [1]

   Device Type:
   - IP PhonePlus
   - IP Single-Line Adapter
   - IP Softphone
   - IPP+, IPSLA, IPSOFT
   - MGCP Gateway Device + Endpoint
   - MGCP Gateway Additional Endpoint

   If you are configuring an IP PhonePlus (or Model 8660 endpoint), IP Single-Line Adapter, IP softphone, or IPP+/IPSNA/IPSOF, skip to step 3
   If you are configuring an MGCP Gateway Device with Endpoint, skip to step 4
   If you are configuring an MGCP Gateway Additional Endpoint, skip to step 5

2. Click Next> to continue configuring the device or Cancel to exit without changing the settings.
3. For an IP PhonePlus (or Model 8660 endpoint), IP Single-Line Adapter, IP softphone, or IPP+/IPSRA/IPSOFT:

e. IP Device Internet Protocol Settings: Program the network settings for the device. Check **Obtain IP Address automatically (DHCP)** to obtain an IP address automatically. Otherwise, enter the IP address, subnet mask, and default gateway address to be used as static network settings on the device. When finished, click **Next**.

**IP Device Internet Protocol Settings**

You can get IP settings for the IP device assigned automatically if your network where the IP device is located supports this capability. Otherwise, you need to ask the network administrator where the IP device is located for appropriate network settings.

- **Configuring device:** 1
  -  Obtain IP Address automatically (DHCP)
  -  Using the following IP Address

<table>
<thead>
<tr>
<th>FIELD (DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong> (192.168.200.201)</td>
<td>Defines the default IP address for the IPRC. If the card does not receive a BOOTP or DHCP response, it uses this IP address. If 0.0.0.0 is entered, the server reports an error. IP address 0.0.0.0 and 255.255.255.255 are invalid IP addresses.</td>
</tr>
<tr>
<td><strong>Subnet Mask (0.0.0.0)</strong></td>
<td>Defines the default network subnet mask for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this subnet mask.</td>
</tr>
<tr>
<td><strong>Default IP Gateway (0.0.0.0)</strong></td>
<td>Defines the default IP gateway or router address for the IPRC. If the card does not receive a BOOTP or DHCP response, it uses this IP gateway address.</td>
</tr>
</tbody>
</table>

f. **IP Device Configuration:** Program the device mode, device ID, and the remote IP card IP address. By default, the remote IP card IP address is the current IP address of the IP card. When finished, click **Next**.

**IP Device Configuration**

You will need to enter the device identification number for the device. For the IP Single-Line Adapter and IP PhonePlus, the device identification number is the Ethernet address of the device.

- **Configuring device:** 1
- **Device mode:**
  - Unused
  - Learn Mode
  - Normal

Enter the device identification number (12 characters hexadecimal values [0-9, A-F or a-f])

| Device ID | 09-18:36:6206:0072:28 |

Enter the IP address of the IP Resource Card for the IP device to communicate with the IP Resource Card:

| IP Resource Card | 1.1.1.1 |

**NOTE:** If the IP card has a public IP address, you can select either the current IP address or the public IP address.
The device mode contains the following options:

- **Unused**: If the current circuit is unused, the device ID address field is set to FF:FF:FF:FF:FF:FF. If the resulting configuration is updated, the effect will be to disable the circuit.

- **Learn Mode**: Sets the device ID address to 00:00:00:00:00:00 and puts the circuit into Learn Mode.

- **Normal**: If the current circuit is set to normal, the device ID reflects the device ID in the system database.

**g. IP Device Configuration Continued**: If you click **Learn Mode** or if you select the IP card public IP address as the remote IPRC IP address, the following page appears. This page creates a temporary IP address. This way, the IP device can connect to the IP card during the installation before being deployed at a different network segment, WAN, or somewhere in the Internet. Click **Yes** or **No** to determine if the network segment that contains the IPRC has a DHCP server. When finished, click **Next>**.

**IP Device Configuration Continued...**

- **Configuring Device**: 1
- **If you are configuring the IP device in the same network segment as the IP Resource Card, the device needs a temporary IP address.**
- **Does the network segment that contains the IP Resource Card have a MGCP server?**
  - **Yes**
  - **No**

**h. Skip to step 6**

4. **For an MGCP Gateway Device + Endpoint:**

a. **MGCP Gateway Configuration**: Select **AudioCodes MP100**. The MGCP manufacturer type is used to assign a default endpoint name to the first MGCP gateway endpoint name. If the MGCP gateway device is not AudioCode, select **Other**. Then, enter the IP address of the MGCP gateway device. When finished, click **Next>**.

**MGCP Gateway Configuration**

- **You will need to enter the manufacturer type and the IP address of the MGCP gateway device. If you don't know the manufacturer type, please select Other.**
- **Configuring Device**: 1
- **MGCP Gateway Device Manufacturer type**: **AudioCodes MP100**
- **Other**
- **Enter the IP address of the MGCP Gateway device for the IPRC to identify the device:** [0.0.0.0]
b. **MGCP Endpoint Name Setting**: By default, each gateway device must have an endpoint. The default endpoint name is shown based on the gateway manufacture type. For instance, the default endpoint name for the AudioCode first endpoint is ACgw0. This field cannot be blank. When finished, click **Next**.

**MGCP Endpoint Name Setting**

You will need to enter the endpoint name. The endpoint name is used to identify the endpoint on the MGCP gateway device.

 Configuring Device: 1
Enter the Endpoint name (9 characters) to identify the endpoint:  

| ACgw0 |

5. **For an MGCP Gateway Additional Endpoint:**

a. **MGCP Endpoint Setting**: Select the MGCP gateway device number to which the endpoint belongs. When finished, click **Next**.

**MGCP Endpoint Setting**

You will need to select the gateway device number that the endpoint belongs.

 Configuring Device: 1
Select the MGCP gateway device number:  

| 12 |

b. **MGCP Endpoint Name Setting**: By default, each gateway device must have an endpoint. The default endpoint name is based on the gateway manufacture type. For instance, the default endpoint name for the AudioCodes first endpoint is ACgw1. This field cannot be blank. When finished, click **Next**.

**MGCP Endpoint Name Setting**

You will need to enter the endpoint name. The endpoint name is used to identify the endpoint on the MGCP gateway device.

 Configuring Device: 1
Enter the Endpoint name (9 characters) to identify the endpoint:  

| |

6. **Preparing to Connect**: Plug in the IP device to the network before the final stage of the installation. When finished, click **Next**.

**Preparing to Connect**

 Configuring Device: 1
Plug the IP device into the network now and select Next to wait for the IP device to connect to the IP Resource Card.

**Device Summary**

 Device Type: IP PhonePlus
7. **Connecting Device:** Wait for two minutes for the IP device to connect to the IP card. At this point, all the database changes made from the previous pages are committed to the database.

### Connecting Device

<table>
<thead>
<tr>
<th>Device Identification number</th>
<th>000000000000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Device</td>
<td>1</td>
</tr>
</tbody>
</table>

Please wait while the IP device connects to the IP Resource Card or click here to abort this operation.

118 seconds remaining

Waiting for the IP device to connect...
Card or Device Configuration — Network

**NOTE:** This page contains the same fields for both card and device programming.

13.18 When you select **Network**, the following page (or one similar to this) appears.

### Network Configuration

<table>
<thead>
<tr>
<th>Field (AND Default Value)</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static (Default) IP Address (192.168.200.201)</td>
<td>Defines the default IP address for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this IP address. If you enter 0.0.0.0, the server defaults to 192.168.200.201.</td>
</tr>
<tr>
<td>Default Network Subnet Mask (0.0.0.0)</td>
<td>Defines the default network subnet mask for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this subnet mask.</td>
</tr>
<tr>
<td>Default IP Gateway Address (0.0.0.0)</td>
<td>Defines the default IP gateway or router address for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this IP gateway address.</td>
</tr>
<tr>
<td>WINS Server (0.0.0.0)</td>
<td>Indicates the IP address that the device should use to find the Windows Internet Name Service (WINS) server to register its hostname. The default is 0.0.0.0, which indicates no WINS server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Identifies the device on the network. This string can be up to 15 characters.</td>
</tr>
<tr>
<td>IP Address Assignment (DHCP)</td>
<td>Place checks in the appropriate box(es) to determine the method(s) in which the IP device obtains its IP Address. <strong>NOTE:</strong> If both check boxes are selected during initialization, the IP device performs a BOOTP request first. If it fails to get an IP address by BOOTP, it sends the DHCP request. If DHCP fails, the IP device uses the IP address in the Default IP Address field. If none of the check boxes are selected, the IP device uses the address in the Default IP Address field after boot up. Changes will take effect after the device resets.</td>
</tr>
</tbody>
</table>

13.19 Program the fields as described below. When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

13.20 The following table describes the information required for each field.
<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server (Enabled)</td>
<td>Defines whether the Web server and/or Telnet server is enabled. Changing these fields will take effect immediately; you do not have to reset the IP device.</td>
</tr>
<tr>
<td>Telnet Server (Enabled)</td>
<td>NOTE: Do not disable both the Web server and the Telnet server, unless you only want to allow access to configuration settings by using one of the IPRC's serial ports. Unlike an IPRC, the IP devices (IP PhonePlus, IP SLA, and Model 8660 endpoint) do not have serial ports. However, you can still access to configuration settings using the self-programming mode.</td>
</tr>
</tbody>
</table>
Card or Device Configuration — Audio & Call Control

NOTE: This page contains the same (or similar) fields for both card and device programming.

13.21 When you select **Audio & Call Control**, the following page (or one similar to this) appears.

### Audio and Call Control

- **TCP Call Control Port**: 5566
- **UDP General Purpose Port**: 5567
- **Audio Stream Receive Port**: 5004
- **Backplane Transmit Signal Gain (dB)**: 0
- **Backplane Compinging Type**: No-Law
- **RTP IP Precedence**: Enable
- **Country**: US

NOTE: For Device Configuration, be sure to change these values on the IP card before changing them on the IP device. Otherwise, when the device connects to the IP card, it will receive the old database values from the IP card.

13.22 Program the fields as described below. When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.

NOTE: If there is a call in progress, ensure to refresh this page to get the latest information.

- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page

13.23 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Call Control Port (5566)</td>
<td>Receives call control messages from IP devices. The port number should only be changed for extremely rare circumstances.</td>
</tr>
<tr>
<td>UDP General Purpose Port (5567)</td>
<td>Sends and receives connection messages to and from IP devices. The port number should only be changed for extremely rare circumstances. The IP devices use this port number to find and connect to the IP card.</td>
</tr>
<tr>
<td>Audio Stream Receive Port (5004)</td>
<td>Receives RTP audio data from all IP devices. The port number should only be changed for extremely rare circumstances.</td>
</tr>
</tbody>
</table>

NOTE: With IPRC v1.5 firmware, you must change this setting to 2427 to connect to the MGCP.

The following fields are available in card configuration only.

| Backplane Transmit Signal Gain (0dB)            | Decreases the IP card transmit signal to the backplane. This could be useful in some cases to reduce echo. However, excessive negative values (attenuation) could result in a decreased audio volume. The range for this value is 0dB to -15dB. |
Backplane Compingding Type (Mu-Law) | Indicates the system backplane type (Mu-law or A-law).
---|---
RTP IP Precedence (Enabled) | Defines whether the IP packet in the RTP stream uses the IP precedence feature. IP precedence allows some routers to apply priority queuing on the RTP packets.
Country (US) | Can be set to US, UK, or Japan to control the single-line termination settings in the IP Single-Line Adapter and to control the DTMF levels on all devices. Changes will take effect after the device resets.

The following fields are available in device configuration only.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote IPRC IP Address (0.0.0.0)</td>
<td>The IP devices first attempt to connect to a local IP card by broadcasting messages on the LAN. If a local IP card does not respond to the IP device, the IP device attempts to connect to the default IP card address. This field must be programmed for the IP device to connect across a router. Changes to this field take effect after the device resets.</td>
</tr>
<tr>
<td>Audio Stream Send/Receive Port (5004)</td>
<td>Shows the port number to send/receive RTP audio data from all IP devices that is programmed in the IPRC. <strong>NOTE:</strong> With IPRC v1.5 firmware, you must change this setting to 2427 to connect to the MGCP.</td>
</tr>
<tr>
<td>Vocoder Type (Default)</td>
<td>Shows the vocoder type that the IP device will attempt to use that is programmed in the IPRC.</td>
</tr>
<tr>
<td>Audio Frames/IP Packet (Default)</td>
<td>Shows the maximum number of RTP packets to stack in a single UDP packet that is programmed in the IPRC.</td>
</tr>
<tr>
<td>DTMF Encoding Setting (Default - 1-way):</td>
<td>Shows the encoding of DTMF tones that the IP device detects in the audio that it encode that is programming in the IPRC.</td>
</tr>
<tr>
<td>Voice Activity Detection (Disabled)</td>
<td>Shows the Voice Activity Detection setting that is programming in the IPRC. If this option is enabled, the system reduces bandwidth requirements by not sending voice packets when the user is not speaking. However, it is necessary for some calls, such as modem and fax calls, to turn off this detection.</td>
</tr>
</tbody>
</table>
Card or Device Configuration — Change Login Password

**NOTE:** This page contains the same fields for both card and device programming.

### 13.24 When you select Change Login Password, the following page appears.

### 13.25 Enter the current password in the **Current Password** field, if there is one. Then enter the new password once in the **New Password** field and again in the **Confirm New Password** field.

**Change Password**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Password</td>
<td></td>
</tr>
<tr>
<td>New Password</td>
<td></td>
</tr>
<tr>
<td>Confirm New Password</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Passwords are case-sensitive. The New Password and Confirm New Password fields must match exactly.

### 13.26 Program the fields as described below. When finished, click one of the following buttons:

- **Update:** Saves your changes.
- **Reset Fields:** Restores the fields to the values that were displayed when you opened the page.

**NOTE:** Changing the password is not a secure process. The new passwords submitted to the server are not encrypted and, therefore, may be susceptible to password snooping.

*For IPRC passwords*, you can use the RS-232 Card Programming for more security (see page 133 for more details).

*For device passwords*, because IPRCs overwrite the device's local password every time the device connects, it is recommended that you change the device password only in the IPRC Web page.
### Circuit Configuration — Device Type

13.27 When you select **Device Type**, the following page appears. Program the fields for each circuit on the IP card or for the IP device as described below.

#### Device Type

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>Device Type</th>
<th>MGCP Endpoint’s Gateway Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MGCP Add’l Endpoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IP PhonePlus, IPSLA, IPSOFT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>IP PhonePlus, IPSLA, IPSOFT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>IP PhonePlus, IPSLA, IPSOFT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IP PhonePlus, IPSLA, IPSOFT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13.28 When finished, click one of the following buttons:
- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

13.29 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that will allow you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Is programmed in the Device Information (see page 99) or Device Specific (see page 111) page.</td>
</tr>
</tbody>
</table>
| Device Type (IP PhonePlus)| Identifies the type of IP device that can be connected to the circuit. The device types include the following:   
  - IP PhonePlus (or Model 8660)   
  - IP Single-Line Adapter   
  - IP SoftPhone   
  - IPP+, IPSLA, IPSOFT   
  - MGCP Gateway Device + Endpoint   
  - MGCP Add’l Endpoint |
| MGCP Endpoint’s Gateway Device (0) | Indicates the gateway device number to which this gateway endpoint belongs. |

**NOTE**: This field only appears if the device type is an MGCP Add’l Endpoint.
Circuit Configuration — Device Information

13.30 When you select **Device Information**, the following page appears. Program the fields for each circuit on the IP card or for the IP device as described below.

### Device Information

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>Device ID or Ethernet Address</th>
<th>Host/Endpoint Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>ACqvd</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>Learn Mode Unused Reset Field</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>Learn Mode Unused Reset Field</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>Learn Mode Unused Reset Field</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>Learn Mode Unused Reset Field</td>
</tr>
</tbody>
</table>

13.31 When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

13.32 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Enter a description of up to 16 characters to help you identify the device on this circuit. This description also appears in the other programming pages.</td>
</tr>
</tbody>
</table>
| Device ID or Ethernet Address (FF:FF:FF:FF:FF) | Contains the Ethernet address of the IP device that will connect to this circuit. The IP card uses the IP device’s Ethernet address as a unique identifier for the device. You can also use the following buttons:  
  - **Learn Mode**: Sets the Ethernet address to 00:00:00:00:00:00 and puts the circuit into Learn Mode (as described on page 81).  
  - **Unused**: If the current circuit is unused, the Ethernet address field is set to FF:FF:FF:FF:FF:FF. If the resulting configuration is updated, the effect will be to disable the circuit.  
  - **Reset Field**: Returns the field to its original value. |
| Host/Endpoint Name         | Identifies the device on the network. This string can be up to 15 characters. If the device is an MGCP gateway or endpoint, this string identifies the endpoint. Changing this field takes effect immediately; you do not have to reset the IP device. |
### Circuit Configuration — Network

13.33 When you select **Circuit Configuration — Network**, the following page appears.

#### Network Configuration

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>Static (Default) IP Address</th>
<th>Default Network Subnet Mask</th>
<th>Default IP Gateway Address</th>
<th>DHCP</th>
<th>BOOTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>sdhas</td>
<td>192.168.200.201</td>
<td>0.0.0.1</td>
<td>0.0.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>192.168.200.201</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>3</td>
<td>MGCP Gateway Device</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>MGCP Endpoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>192.168.200.201</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

**13.34** Program the fields as described below. When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

**13.35** The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Is programmed in the Device Information (see page 99) or Device Specific (see page 111) page.</td>
</tr>
<tr>
<td>Static (Default) IP Address (192.168.200.201)</td>
<td>Defines the static (default) IP address for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this address. Changes to this field take effect after the device is reset.</td>
</tr>
<tr>
<td>Default Network Subnet Mask (0.0.0.0)</td>
<td>Defines the default subnet mask for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this subnet mask. Changes to this field take effect after the IP device is reset.</td>
</tr>
<tr>
<td>Default IP Gateway Address (0.0.0.0)</td>
<td>Defines the default IP gateway or router address for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this IP gateway address. Changes to this field take effect after the IP device is reset.</td>
</tr>
<tr>
<td>DHCP (Enabled)</td>
<td>Defines the method(s) in which the IP device obtains its IP address. Changes will take effect after the device resets.</td>
</tr>
<tr>
<td>BOOTP (Enabled)</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE**: If both the BOOTP and DHCP check boxes are selected, the IP device performs a BOOTP request first during bootstrap. If it fails to get an IP address by BOOTP, it sends the DHCP request. If DHCP fails, the IP device will use the IP address in the Default IP Address field. If none of check boxes are selected, the IP device uses the address in the Default IP Address field after boot up.
Circuit Configuration — Advanced Network

13.36 When you select Circuit Configuration — Advanced Network, the following page appears.

Advanced Network Configuration

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>WINS Server</th>
<th>BOOTP Client IP Address</th>
<th>Enable Web Server</th>
<th>Enable Telnet Server</th>
<th>Overwrite Device’s Local Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>sdfs</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>0.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>0.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>MGCIP endpoint</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

13.37 Program the fields as described below. When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

13.38 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Is programmed in the Device Information (see page 99) or Device Specific (see page 111) page.</td>
</tr>
<tr>
<td>WINS Server (0.0.0.0)</td>
<td>Indicates the IP address that the device should use to find the WINS server to register its hostname. The default is 0.0.0.0, which indicates no WINS server.</td>
</tr>
<tr>
<td>BOOTP Client IP Address (0.0.0.0)</td>
<td>The IP card contains a BOOTP server. If the IP card receives a BOOTP request from the Ethernet address in the Ethernet Address field, the IP card sends the BOOTP IP address to the device. If this field is set to 0.0.0.0, the IP card will not send a BOOTP reply.</td>
</tr>
<tr>
<td>Enable Web Server (Enabled)</td>
<td>Define whether the Web server and/or Telnet server is enabled. Changing these fields will take effect immediately; you do not have to reset the IP device.</td>
</tr>
<tr>
<td>FIELD (AND DEFAULT VALUE)</td>
<td>FIELD DESCRIPTION (Continued)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Overwrite Device’s Local Settings (Enabled)</td>
<td>Determines whether the IP card will overwrite the network settings on the IP PhonePlus, Model 8660 endpoint, or IP SLA. If the check box is disabled, the IP card does not overwrite the device’s local network settings, and the user must program the device correctly through the IP PhonePlus or Model 8660 endpoint’s Self-Programming Mode or through the device’s Web or Telnet interfaces. The device never changes the IP card’s database. The network settings include only the following fields: Static (Default) IP Address, Default Network Subnet Mask, Default IP Gateway Address, Remote IPRC IP Address, UDP General Purpose Port, Hostname, BOOTP, and DHCP. Changes will take effect the next time the device attempts to connect to the IP card.</td>
</tr>
</tbody>
</table>

**NOTE:** Both endpoints, the IP card and the IP PhonePlus, Model 8660 endpoint, or IP SLA, must be running version 1.2 or later for this feature to work.
Circuit Configuration — Call Control

13.39 When you select Circuit Configuration — Call Control while programming a device, the following page appears.

Call Control

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>Remote IPRC IP Address</th>
<th>MGCP Gateway Device IP Address</th>
<th>Max Keepalive Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>s/das</td>
<td>1.1.1</td>
<td></td>
<td>Default(3)</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>0.0.0.0</td>
<td></td>
<td>Default(3)</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>0.0.0.0</td>
<td></td>
<td>Default(3)</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>MGCP Endpoint</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>0.0.0.0</td>
<td></td>
<td>Default(3)</td>
</tr>
</tbody>
</table>

13.40 Program the fields as described below. When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

**NOTE**: Be sure to change these values on the IP card before changing them on the IP device. Otherwise, when the device connects to the IP card, it will receive the old database values from the IP card.

13.41 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Is programmed in the Device Information (see page 99) or Device Specific (see page 111) page.</td>
</tr>
<tr>
<td>Remote IPRC IP Address (0.0.0.0)</td>
<td>The IP devices first attempt to connect to a local IP card by broadcasting messages on the LAN. If a local IP card does not respond to the IP device, the IP device attempts to connect to the default IP card address. This field must be programmed for the IP device to connect across a router. Changes to this field take effect after the device resets.</td>
</tr>
<tr>
<td>MGCP Gateway Device IP Address (0.0.0.0)</td>
<td>Indicates the IP address of the gateway device, which the IP card uses to authenticate the MGCP gateway device.</td>
</tr>
</tbody>
</table>
Circuit Configuration — Audio Settings

13.42 When you select **Circuit Configuration — Audio Settings**, the following page appears.

### Circuit Audio and Call Control

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>Audio Stream Send Port</th>
<th>Audio Frames/IP Packet</th>
<th>Vocoder Type</th>
<th>Minimum Playback Buffer Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>sofis</td>
<td>5005</td>
<td>Default(3)</td>
<td>Default</td>
<td>Default(80)</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>5004</td>
<td>Default(3)</td>
<td>Default</td>
<td>Default(80)</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>5004</td>
<td>Default(3)</td>
<td>Default</td>
<td>Default(80)</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>5005</td>
<td>3</td>
<td>G.711 A-Law</td>
<td>80</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>5004</td>
<td>Default(3)</td>
<td>G.711 Mu-Law</td>
<td>Default(80)</td>
</tr>
</tbody>
</table>

13.43 Program the fields as described below. When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

13.44 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Is programmed in the Device Information (see page 99) or Device Specific (see page 111) page.</td>
</tr>
</tbody>
</table>
| Audio Stream Send Port (5004) | Contains the UDP port number that the IP card uses to send RTP packets to the IP device. Do not change this field while the IP device is connected to the IP card.  
**NOTE**: With IPRC v1.5 firmware, you must change this setting to 2427 to connect to the MGCP. |
<p>| Audio Frames/IP Packet (3) | Indicates the maximum number of RTP packets to stack in a single UDP packet. Increasing the number increases the audio delay but reduces the bandwidth and CPU load. This value should normally be 2 through 4. The default value allows the IP device to automatically choose a value. Changes to this field take effect when the IP device starts a new call. (This should be set to 1 for fax operation.) |
| Vocoder Type (Default)     | Defines the vocoder type that the IP device on this circuit will attempt to use. Possible values are: G.711 Mu-Law, G.711 A-Law, G.729, and Default. The Default option allows the IP device to automatically choose a value. Changes to this field take effect when the IP device starts a new call. (This should be set to G.711 for fax operation.) |</p>
<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Playback Buffer Time (ms) (80)</td>
<td>Indicates the amount of audio that the device buffers before playing. Available settings are 0, 20, 40, 60, 80, 100, 120, 140, 160, 180, or 200 ms. Increasing this field increases the amount of audio that the device buffers before playing. Doing this will increase the audio delay, but may improve the audio quality in some circumstances. If you enter a value that is too small for the IP device to use, the IP device will use the smallest value that it can. Optimum setting for the IP softphone is 200 ms and for fax operations the best setting is 160 ms.</td>
</tr>
</tbody>
</table>
Circuit Configuration — Advanced Audio Settings

13.45 When you select **Circuit Configuration — Advanced Audio Settings**, the following page appears.

---

**Advanced Audio Settings**

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>DTMF Encoding Setting</th>
<th>Voice Activity Detection</th>
<th>Echo Suppression</th>
<th>Echo Suppression Sensitivity Level</th>
<th>Echo Saturation Blocker</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default(1-way)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Default(1-way)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Default(1-way)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Out-Of-Band</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Default(1-way)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13.46 Program the fields as described below. When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Refresh**: Restores all fields to the current values stored in the database.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

13.47 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Is programmed in the Device Information (see page 99) or Device Specific (see page 111) page.</td>
</tr>
</tbody>
</table>
| DTMF Encoding Setting (1-way) | Controls the encoding of DTMF tones that the IP card and IP SLA detect in the audio that they encode. (IP PhonePlus and Model 8660 endpoint always use an “Out-Of-Band” encoding for DTMF tones pressed on its dialpad.) The DTMF encoding must be one of the following:  
  - **1-way**: The IP card uses a “None” setting, while the IP SLA, IP PhonePlus, and Model 8660 endpoint use an “Out-Of-Band” setting. This setting uses less bandwidth while DTMF tones are encoded. This setting has the benefit of pure, clean, DTMF tones in the “Out-Of-Band” setting from the IP SLA to the IP card (just like the IP PhonePlus or Model 8660 IP endpoint to the IP card). However, from the IP card to the devices has no DTMF encoding because the IP user typically does not need to hear pure, clean, DTMF tones. This setting sometimes leads to false DTMF detections on the IP SLA just as described in the “Out-Of-Band” setting on the next page. |
### Field (And Default Value) | Field Description (Continued)
--- | ---
(continued) DTMF Encoding Setting
- **None**: The IP card and the IP SLA use the same encoding for DTMF and voice. This setting requires no additional bandwidth. This setting will not continue to play the DTMF tone when audio packets are lost on the network which may lead to the other endpoint hearing duplicate digits. However, this setting does not suffer from the DTMF tone burst on false DTMF detections because the original audio stream is still encoded with the same vocoder as normal voice, rather than an out-of-band DTMF tone. Note that the DTMF tone will be distorted through the highly compressed G.729 vocoder, and some DTMF receivers may not see distorted audio as a DTMF tone. Try the G.711 DTMF encoding setting if problems exist with dialing when the voice vocoder is G.729 and the DTMF encoding is “None.”
- **Out-Of-Band**: The IP card and the IP SLA send DTMF tones through a special path outside of the normal G.729 and G.711 encodings. This setting uses less bandwidth while DTMF tones are encoded. This setting continues to play the DTMF tone even if the audio packets are lost on the network. This setting also reproduces the duration of the tone within 10 milliseconds accuracy. However, this setting sometimes leads to false DTMF tone detections. For example, sometimes during normal speech, the device falsely detects a DTMF digit. The other IP endpoint will reproduce at least a 10 millisecond pure, clean, DTMF tone in response to this false detection.
- **G.711**: The IP card and the IP SLA use G.711 to encode DTMF tones. (The Mu-Law or A-Law companding of G.711 depends on the backplane companding setting.) This setting requires additional bandwidth while tones are encoded. This setting will not continue to play the DTMF tone when audio packets are lost on the network which may lead to the other endpoint hearing duplicate digits. This setting also shortens the duration of the G.711 tone by about 40 to 60 milliseconds, forcing the user to hold each digit longer. However, this setting does not suffer from the DTMF tone burst on false DTMF detections because the original audio stream is still encoded, just as G.711, rather than an out-of-band DTMF tone.

| Voice Activity Detection (Disabled) | Reduces bandwidth requirements by not sending voice packets when the user is not speaking. However, it is necessary for some calls, such as modem and fax calls, to turn off this detection.

**NOTE:** Do not adjust the **Echo Suppression**, **Echo Suppression Sensitivity Level**, and **Echo Saturation Blocker** settings unless you have verified that you are on a good network receiving almost all of your audio packets (see “Status — Receive Audio (or Call Statistics)” on page 119). In addition, do not adjust the Advanced Audio settings until you reduce the echo as much as possible by correctly adjusting the hybrid balance on your analog trunks, and adjusting the backplane transmit signal gain (see “Card or Device Configuration — Audio & Call Control” on page 95). These settings will not eliminate echo, and, in suppressing or blocking the echo, they may introduce half-duplex conditions. See details on page 198 for troubleshooting.

| Echo Suppression (Enabled) | **When to use it**: Enable Echo Suppression when the IP user complains of a low-volume, clean, clear echo during the beginning of the audio session. With Echo Suppression enabled, adjust the Echo Suppression Sensitivity Level during the beginning of an audio session to find the balance between the IP user hearing a slight echo and hearing a half-duplex condition on the handset. The Echo Suppression Sensitivity Level does nothing if Echo Suppression is disabled. Disable Echo Suppression when using the circuit for fax operations or as a last resort to eliminate the half-duplex condition on the handset during the beginning of the audio session. Remember to eliminate echo and verify that you are on a good network receiving almost all of your audio packets [see “Status — Receive Audio (or Call Statistics)” on page 119] before adjusting these values.
What the trade offs are: The trade off between the settings is that with Echo Suppression disabled, the IP user may hear low-volume, clean, clear echo during the beginning of the audio session. With Echo Suppression enabled and the Echo Suppression Sensitivity Level at 0%, the Echo Suppression essentially does nothing, and, again, the IP user may hear low-volume, clean, clear echo during the beginning of the audio session. With Echo Suppression enabled and the Echo Suppression Sensitivity Level at 100%, the Echo Suppression creates a condition most like half duplex during the beginning of the audio session. Tests show a value near 25% is a good starting point if the system has only digital trunks (T1/E1, PRI, and/or BRI), and a value near 75% is a good starting point for systems with analog trunks (LSC and/or LGC) or analog stations (SLC and/or SLA). Note that the IP card automatically turns off Echo Suppression when the echo canceller can completely cancel the echo; therefore, make any tests of the Echo Suppression Sensitivity Level during the beginning of the audio session before the IP card automatically turns off Echo Suppression.

What it really does: Echo Suppression can be thought of as a wall that comes up to suppress or block audio bound for the IP user whenever the IP user is talking. Echo Suppression is designed to suppress echo while the echo canceller adapts to the echo during the beginning of the audio session. Any received audio bound for the IP user must be loud enough to rise above this suppression wall before the IP card allows the IP user to hear that received audio. The Echo Suppression Sensitivity Level can be thought of as the height of that wall based on a percentage of the IP user’s speech volume; 100% is essentially a wall of maximum height, and 0% is the minimum height. As the IP user talks louder, the height of the wall automatically rises to suppress or block the louder echo. Adjust the percentage so normal audio that must be louder than any echo is able to clear this suppression wall and be heard by the IP user. The IP card automatically turns off Echo Suppression after the echo canceller has fully adapted to the echo and can cancel the echo completely; the time it takes the echo canceller to adapt varies greatly depending upon the echo it must cancel. With the Echo Suppression off, either automatically with a fully adapted echo canceller or manually through the database, there is no suppression wall, no blocking, and the IP card allows the IP user to hear all received audio. Note that the echo canceller must adapt at the start of every audio session, no matter if it was a transition from handset to speaker phone (or vice versa) a hold operation, a conference, etc., all on the same call to the same destination. Disable Echo Suppression when using the circuit for fax operations because fax machines need full-duplex communication and do not have as much of a problem with any remaining echo as humans do.
### Echo Saturation Blocker (Enabled)

**When to use it:** Enable the Echo Saturation Blocker when the IP user complains of raspy or distorted echo as the IP user speaks quite loudly or holds the handset close to their mouth. Disable the Echo Saturation Blocker when the IP user complains of choppiness or a half-duplex condition on the handset as the IP user speaks quite loudly or holds the handset close to their mouth. Remember to verify that you are on a good network receiving almost all of your audio packets [see “Status — Receive Audio (or Call Statistics)” on page 119] before adjusting this value.

**What the trade offs are:** With the Echo Saturation Blocker enabled, there is a potential for a half-duplex condition on the handset, or choppiness. With the Echo Saturation Blocker disabled, there is a potential for raspy or distorted echo. Because it does more good than harm, leave the Echo Saturation Blocker enabled except for extremely rare cases.

**What it really does:** The Echo Saturation Blocker is similar to the previously described Echo Suppression; therefore, make any tests of the Echo Saturation Blocker with Echo Suppression disabled and the echo canceller fully adapted to cancel the echo so that it does not interfere. The Echo Saturation Blocker differs from Echo Suppression in that the Echo Saturation Blocker applies only when the IP user’s transmitted speech is at or near saturation levels; therefore, it applies only when the IP user speaks quite loudly or holds the handset close to their mouth. With the IP user’s speech saturating the IP card’s transmission to the backplane, the echo canceller cannot cancel the distorted echo. Therefore, the IP user has the potential to hear raspy or distorted echo. If the Echo Saturation Blocker is enabled, it will temporarily block all audio including this echo from reaching the IP user. The IP user might think this audio blocking is choppy or even similar to a half-duplex condition.

### Country (US)

Can be set to US, UK, or Japan to control the DTMF levels on all devices. Changes will take effect after the device resets.
Circuit Configuration — Device Login Password

13.48 When you select **Device Login Password**, the following page appears.

### Device Password Change

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>Update</th>
<th>New Login Password</th>
<th>Confirm New Login Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>s1fas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13.49 When finished, click one of the following buttons:

- **Update**: Saves your changes.
- **Reset Fields**: Restores the fields to the values that were displayed when you opened the page.

13.50 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates which circuit on the IP card you are programming. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Is programmed in the Device Information (see page 99) or Device Specific (see page 111) page.</td>
</tr>
<tr>
<td>Update</td>
<td>Changes any password.</td>
</tr>
<tr>
<td><strong>NOTE</strong>: If you leave the New Login Password and Confirm New Login Password fields blank and update the password for a circuit, that circuit's password will be erased.</td>
<td></td>
</tr>
<tr>
<td>New Login Password</td>
<td>Enter the new password. Changing this password affects the login password for IP PhonePlus, Model 8660 endpoint, or IP Single-Line Adapter. The default login passwords are listed on page 84.</td>
</tr>
<tr>
<td>Confirm New Login Password</td>
<td>Enter the new password again. Passwords are case-sensitive.</td>
</tr>
</tbody>
</table>

**NOTE**: Changing the password is not a secure process. The new passwords submitted to the server are not encrypted and, therefore, may be susceptible to password snooping. For more security, you can use the RS-232 Card Programming for programming passwords (see page 133 for more details).
Circuit Configuration — Device Specific

13.51 When you select Device Specific, the following page appears. This page contains the programming fields per device. The fields are categorized into six sections. Program the fields as described on the following pages.

Device Specific Configuration

When you select Device Specific, the following page appears. This page contains the programming fields per device. The fields are categorized into six sections. Program the fields as described on the following pages.

13.52 When finished, click one of the following buttons:

- Update: Saves your changes.
- Refresh: Restores all fields to the current values stored in the database.
- Reset Fields: Restores the fields to the values that were displayed when you opened the page.

13.53 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD AND DEFAULT VALUE</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td></td>
</tr>
<tr>
<td>Device Number (1)</td>
<td>Select the circuit number that you are programming.</td>
</tr>
<tr>
<td>Device Description</td>
<td>Enter a description of up to 16 characters to help you identify the device on this circuit. This description also appears in the other programming pages.</td>
</tr>
</tbody>
</table>
### Device ID or Ethernet Address (FF:FF:FF:FF:FF:FF)

This field can also be programmed in the “Circuit Configuration — Device Information” on page 99. Contains the Ethernet address of the IP device that will connect to this circuit. The IP card uses the IP device’s Ethernet address as a unique identifier for the device. You can also use the following buttons:

- **Learn Mode**: Sets the Ethernet address to 00:00:00:00:00:00 and puts the circuit into Learn Mode (as described on page 81).
- **Unused**: If the current circuit is unused, the Ethernet address field is set to FF:FF:FF:FF:FF:FF. If the resulting configuration is updated, the effect will be to disable the circuit.
- **Reset Field**: Returns the field to its original value.

### Device Type (IP PhonePlus)

This field can also be programmed in the “Circuit Configuration — Device Type” on page 98. Identifies the type of IP device that can be connected to the circuit. The device types include the following:

- IP PhonePlus (or Model 8660)
- IP Single-Line Adapter
- IP SoftPhone
- IPP+, IPSLA, IPSOFT
- MGCP Gateway Device + Endpoint
- MGCP Add’l Endpoint

### Host/Endpoint Name

This field can also be programmed in the “Circuit Configuration — Device Information” on page 99. Identifies the device on the network. This string can be up to 15 characters. If the device is an MGCP gateway or endpoint, this string identifies the endpoint. Changing this field takes effect immediately; you do not have to reset the IP device.

### Call Control

**Remote IPRC IP Address (0.0.0.0)**

This field can also be programmed in the “Circuit Configuration — Call Control” on page 103. The IP devices first attempt to connect to a local IP card by broadcasting messages on the LAN. If a local IP card does not respond to the IP device, the IP device attempts to connect to the default IP card address. This field must be programmed for the IP device to connect across a router. Changes to this field take effect after the device resets.

### Network Configuration

**Static (Default) IP Address (192.168.200.201)**

This field can also be programmed in the “Circuit Configuration — Network” on page 100. Defines the static (default) IP address for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this address. Changes to this field take effect after the device is reset.

**Default Network Subnet Mask (0.0.0.0)**

This field can also be programmed in the “Circuit Configuration — Network” on page 100. Defines the default subnet mask for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this subnet mask. Changes to this field take effect after the IP device is reset.

**Default IP Gateway Address (0.0.0.0)**

This field can also be programmed in the “Circuit Configuration — Network” on page 100. Defines the default IP gateway or router address for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this IP gateway address. Changes to this field take effect after the IP device is reset.
<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address Assignment (DHCP)</td>
<td>(This field can also be programmed in the &quot;Card or Device Configuration — Network&quot; on page 93) Defines the method(s) in which the IP device obtains its IP address. Changes will take effect after the device resets.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If both the BOOTP and DHCP check boxes are selected, the IP device performs a BOOTP request first during bootstrap. If it fails to get an IP address by BOOTP, it sends the DHCP request. If DHCP fails, the IP device will use the IP address in the Default IP Address field. If none of check boxes are selected, the IP device uses the address in the Default IP Address field after boot up.</td>
</tr>
</tbody>
</table>

**Audio Settings**

| Audio Stream Send Port (5004) | (This field can also be programmed in the "Circuit Configuration — Audio Settings" on page 104) Contains the UDP port number that the IP card uses to send RTP packets to the IP device. Do not change this field while the IP device is connected to the IP card. |
| Audio Frames/IP Packet (3) | (This field can also be programmed in the "Circuit Configuration — Audio Settings" on page 104) Indicates the maximum number of RTP packets to stack in a single UDP packet. Increasing the number increases the audio delay but reduces the bandwidth and CPU load. This value should normally be 2 through 4. The default value allows the IP device to automatically choose a value. Changes to this field take effect when the IP device starts a new call. (This should be set to 1 for fax operation.) |
| Vocoder Type (Default) | (This field can also be programmed in the "Circuit Configuration — Audio Settings" on page 104) Defines the vocoder type that the IP device on this circuit will attempt to use. Possible values are: G.711 Mu-Law, G.711 A-Law, G.729, and Default. The Default option allows the IP device to automatically choose a value. Changes to this field take effect when the IP device starts a new call. (This should be set to G.711 for fax operation.) |
| Minimum Playback Buffer Time (ms) (80) | (This field can also be programmed in the "Circuit Configuration — Audio Settings" on page 104) Indicates the amount of audio that the device buffers before playing. Available settings are 0, 20, 40, 60, 80, 100, 120, 140, 160, 180, or 200 ms. Increasing this field increases the amount of audio that the device buffers before playing. Doing this will increase the audio delay, but may improve the audio quality in some circumstances. If you enter a value that is too small for the IP device to use, the IP device will use the smallest value that it can. Optimum setting for the IP softphone is 200 ms and for fax operations the best setting is 160 ms. |

**Advanced Network Configuration**

| WINS Server (0.0.0.0) | (This field can also be programmed in the “Circuit Configuration — Advanced Network” on page 101) Indicates the IP address that the device should use to find the WINS server to register its hostname. The default is 0.0.0.0, which indicates no WINS server. |
| BOOTP Client IP Address (0.0.0.0) | (This field can also be programmed in the “Circuit Configuration — Advanced Network” on page 101) The IP card contains a BOOTP server. If the IP card receives a BOOTP request from the Ethernet address in the Ethernet Address field, the IP card sends the BOOTP IP address to the device. If this field is set to 0.0.0.0, the IP card will not send a BOOTP reply. |
### Circuit Configuration — Device Specific

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server (Enabled)</td>
<td>(This field can also be programmed in the “Card or Device Configuration — Network” on page 93) Defines whether the Web server and/or Telnet server is enabled. Changing these fields will take effect immediately; you do not have to reset the IP device.</td>
</tr>
<tr>
<td>Telnet Server (Enabled)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Do not disable both the Web server and the Telnet server, unless you only want to allow access to configuration settings by using one of the IPRC’s serial ports. Unlike an IPRC, the IP devices (IP PhonePlus, IP SLA, and Model 8660 endpoint) do not have serial ports. However, you can still access to configuration settings using the self-programming mode.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Overwrite Device’s Local Settings (Enabled)</td>
<td>(This field can also be programmed in the “Circuit Configuration — Advanced Network” on page 101) Determines whether the IP card will overwrite the network settings on the IP PhonePlus, Model 8660 endpoint, or IP SLA. If the check box is disabled, the IP card does not overwrite the device’s local network settings, and the user must program the device correctly through the IP PhonePlus or Model 8660 endpoint’s Self-Programming Mode or through the device’s Web or Telnet interfaces. The device never changes the IP card’s database. The network settings include only the following fields: Static (Default) IP Address, Default Network Subnet Mask, Default IP Gateway Address, Remote IPRC IP Address, UDP General Purpose Port, Hostname, BOOTP, and DHCP. Changes will take effect the next time the device attempts to connect to the IP card.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Both endpoints, the IP card and the IP PhonePlus, Model 8660 endpoint, or IP SLA, must be running version 1.2 or later for this feature to work.</td>
</tr>
<tr>
<td>Advanced Audio Settings</td>
<td></td>
</tr>
<tr>
<td>DTMF Encoding Setting (1-way)</td>
<td>(This field can also be programmed in the “Circuit Configuration — Advanced Audio Settings” on page 106) Controls the encoding of DTMF tones that the IP card and IP SLA detect in the audio that they encode. (IP PhonePlus and Model 8660 endpoint always use an “Out-Of-Band” encoding for DTMF tones pressed on its dialpad.) The DTMF encoding must be one of the following:</td>
</tr>
<tr>
<td></td>
<td><strong>1-way:</strong> The IP card uses a “None” setting, while the IP SLA, IP PhonePlus, and Model 8660 endpoint use an “Out-Of-Band” setting. This setting uses less bandwidth while DTMF tones are encoded. This setting has the benefit of pure, clean, DTMF tones in the “Out-Of-Band” setting from the IP SLA to the IP card (just like the IP PhonePlus or Model 8660 endpoint to the IP card). However, from the IP card to the devices has no DTMF encoding because the IP user typically does not need to hear pure, clean, DTMF tones. This setting sometimes leads to false DTMF detections on the IP SLA just as described in the “Out-Of-Band” setting below.</td>
</tr>
</tbody>
</table>
**DTMF Encoding Setting (1-way)**

- **None:** The IP card and the IP SLA use the same encoding for DTMF and voice. This setting requires no additional bandwidth. This setting will not continue to play the DTMF tone when audio packets are lost on the network which may lead to the other endpoint hearing duplicate digits. However, this setting does not suffer from the DTMF tone burst on false DTMF detections because the original audio stream is still encoded with the same vocoder as normal voice, rather than an out-of-band DTMF tone. Note that the DTMF tone will be distorted through the highly compressed G.729 vocoder, and some DTMF receivers may not see distorted audio as a DTMF tone. Try the G.711 DTMF encoding setting if problems exist with dialing when the voice vocoder is G.729 and the DTMF encoding is “None.”

- **Out-Of-Band:** The IP card and the IP SLA send DTMF tones through a special path outside of the normal G.729 and G.711 encodings. This setting uses less bandwidth while DTMF tones are encoded. This setting continues to play the DTMF tone even if the audio packets are lost on the network and also reproduces the duration of the tone within 10 milliseconds accuracy. However, this setting sometimes leads to false DTMF tone detections. For example, sometimes during normal speech, the device falsely detects a DTMF digit, the other IP endpoint will reproduce at least a 10 millisecond pure, clean, DTMF tone in response to this false detection.

- **G.711:** The IP card and the IP SLA use G.711 to encode DTMF tones. (The Mu-Law or A-Law companding of G.711 depends on the backplane companding setting.) This setting requires additional bandwidth while tones are encoded. This setting will not continue to play the DTMF tone when audio packets are lost on the network which may lead to the other endpoint hearing duplicate digits. This setting also shortens the duration of the G.711 tone by about 40 to 60 milliseconds, forcing the user to hold each digit longer. However, this setting does not suffer from the DTMF tone burst on false DTMF detections because the original audio stream is still encoded, just as G.711, rather than an out-of-band DTMF tone.

**Voice Activity Detection (Disabled)**

(This field can also be programmed in the “Circuit Configuration — Advanced Audio Settings” on page 106) Reduces bandwidth requirements by not sending voice packets when the user is not speaking. However, it is necessary for some calls, such as modem and fax calls, to turn off this detection.
Circuit Configuration — Device Specific

**NOTE:** Do not adjust the *Echo Suppression*, *Echo Suppression Sensitivity Level*, and *Echo Saturation Blocker* settings unless you have verified that you are on a good network receiving almost all of your audio packets (see “Status — Receive Audio (or Call Statistics)” on page 119). In addition, do not adjust the Advanced Audio settings until you reduce the echo as much as possible by correctly adjusting the hybrid balance on your analog trunks, and adjusting the backplane transmit signal gain (see “Card or Device Configuration — Audio & Call Control” on page 95). These settings will not eliminate echo, and, in suppressing or blocking the echo, they may introduce half-duplex conditions. See details on page 198 for troubleshooting.

<table>
<thead>
<tr>
<th><strong>FIELD (AND DEFAULT VALUE)</strong></th>
<th><strong>FIELD DESCRIPTION (Continued)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo Suppression (Enabled)</td>
<td>When to use it: Enable Echo Suppression when the IP user complains of a low-volume, clean, clear echo during the beginning of the audio session. With Echo Suppression enabled, adjust the Echo Suppression Sensitivity Level during the beginning of an audio session to find the balance between the IP user hearing a slight echo and hearing a half-duplex condition on the handset. The Echo Suppression Sensitivity Level does nothing if Echo Suppression is disabled. Disable Echo Suppression when using the circuit for fax operations or as a last resort to eliminate the half-duplex condition on the handset during the beginning of the audio session. Remember to eliminate echo and verify that you are on a good network receiving almost all of your audio packets [see “Status — Receive Audio (or Call Statistics)” on page 119] before adjusting these values.</td>
</tr>
<tr>
<td>Echo Suppression Sensitivity Level (0)</td>
<td>What the trade offs are: The trade off between the settings is that with Echo Suppression disabled, the IP user may hear low-volume, clean, clear echo during the beginning of the audio session. With Echo Suppression enabled and the Echo Suppression Sensitivity Level at 0%, the Echo Suppression essentially does nothing, and, again, the IP user may hear low-volume, clean, clear echo during the beginning of the audio session. With Echo Suppression enabled and the Echo Suppression Sensitivity Level at 100%, the Echo Suppression creates a condition most like half duplex during the beginning of the audio session. Tests show a value near 25% is a good starting point if the system has only digital trunks (T1/E1, PRI, and/or BRI), and a value near 75% is a good starting point for systems with analog trunks (LSC and/or LGC) or analog stations (SLC and/or SLA). Note that the IP card automatically turns off Echo Suppression when the echo canceller can completely cancel the echo; therefore, make any tests of the Echo Suppression Sensitivity Level during the beginning of the audio session before the IP card automatically turns off Echo Suppression.</td>
</tr>
<tr>
<td></td>
<td>What it really does: Echo Suppression can be thought of as a wall that comes up to suppress or block audio bound for the IP user whenever the IP user is talking. Echo Suppression is designed to suppress echo while the echo canceller adapts to the echo during the beginning of the audio session. Any received audio bound for the IP user must be loud enough to rise above this suppression wall before the IP card allows the IP user to hear that received audio. The Echo Suppression Sensitivity Level can be thought of as the height of that wall based on a percentage of the IP user’s speech volume; 100% is essentially a wall of maximum height, and 0% is the minimum height. As the IP user talks louder, the height of the wall automatically rises to suppress or block the louder echo. Adjust the percentage so normal audio that must be louder than any echo is able to clear this suppression wall and be heard by the IP user.</td>
</tr>
<tr>
<td>FIELD (AND DEFAULT VALUE)</td>
<td>FIELD DESCRIPTION (Continued)</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>(Continued) Echo Suppression (Enabled)</td>
<td>The IP card automatically turns off Echo Suppression after the echo canceller has fully adapted to the echo and can cancel the echo completely; the time it takes the echo canceller to adapt varies greatly depending upon the echo it must cancel. With the Echo Suppression off, either automatically with a fully adapted echo canceller or manually through the database, there is no suppression wall, no blocking, and the IP card allows the IP user to hear all received audio. Note that the echo canceller must adapt at the start of every audio session, no matter if it was a transition from handset to speaker phone (or vice versa) a hold operation, a conference, etc., all on the same call to the same destination. Disable Echo Suppression when using the circuit for fax operations because fax machines need full-duplex communication and do not have as much of a problem with any remaining echo as humans do.</td>
</tr>
<tr>
<td>Echo Suppression Sensitivity Level (0)</td>
<td></td>
</tr>
</tbody>
</table>
| Echo Saturation Blocker (Enabled)         | **When to use it:** Enable the Echo Saturation Blocker when the IP user complains of raspy or distorted echo as the IP user speaks quite loudly or holds the handset close to their mouth. Disable the Echo Saturation Blocker when the IP user complains of choppiness or a half-duplex condition on the handset as the IP user speaks quite loudly or holds the handset close to their mouth. Remember to verify that you are on a good network receiving almost all of your audio packets [see “Status — Receive Audio (or Call Statistics)” on page 119] before adjusting this value.  

**What the trade offs are:** With the Echo Saturation Blocker enabled, there is a potential for a half-duplex condition on the handset, or choppiness. With the Echo Saturation Blocker disabled, there is a potential for raspy or distorted echo. Because it does more good than harm, leave the Echo Saturation Blocker enabled except for extremely rare cases.  

**What it really does:** The Echo Saturation Blocker is similar to the previously described Echo Suppression; therefore, make any tests of the Echo Saturation Blocker with Echo Suppression disabled and the echo canceller fully adapted to cancel the echo so that it does not interfere. The Echo Saturation Blocker differs from Echo Suppression in that the Echo Saturation Blocker applies only when the IP user’s transmitted speech is at or near saturation levels; therefore, it applies only when the IP user speaks quite loudly or holds the handset close to their mouth. With the IP user’s speech saturating the IP card’s transmission to the backplane, the echo canceller cannot cancel the distorted echo. Therefore, the IP user has the potential to hear raspy or distorted echo. If the Echo Saturation Blocker is enabled, it will temporarily block all audio including this echo from reaching the IP user. The IP user might think this audio blocking is choppy or even similar to a half-duplex condition. |
| Country (US)                              | (This field can also be programmed in the “Circuit Configuration — Advanced Audio Settings” on page 106) Can be set to US, UK, or Japan to control the DTMF levels on all devices. Changes will take effect after the device resets. |
**Status — Firmware Version**

*NOTE: This page is used for both card and device programming.*

13.54 When you select **Firmware Version**, the following page (or one similar to this) appears. This page shows the device type, software version number, build date and time, boot code version, boot build date and time, and maximum allowed channels.

### Firmware Version

- **Device:** IPRC (DWS-16 emulation)
- **Version:** 1.3
- **Build Date and Time:** Wed Aug 14 2002 15:21:46
- **Boot Version:** 1.2.3
- **Boot Build Date and Time:** Mon Oct 21 2002 16:23:11
- **Maximum Allowed Channels:** 4

Part of the software embedded in this product is eCos - Embedded Configurable Operating System, a trademark of Red Hat. Portions created by Red Hat are Copyright (C) 1998, 1999, 2000 Red Hat, Inc. [http://www.redhat.com], All Rights Reserved.

**THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY RED HAT AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**

**Status — Network**

*NOTE: This page is used for both card and device programming.*

13.55 When you select **Network**, the following page (or one similar to this) appears. It shows a summary of the network information currently in use, including the Ethernet address, current IP address, device subnet mask, and IP gateway address. It also shows the BOOTP or DHCP server IP address if the device receives its IP address from one of these servers. The primary WINS server is acquired through a BOOTP or DHCP response. The secondary WINS server is the pre-programmed address on the “Circuit Configuration — Network” on page 100. The IP devices also show the IP Address of the IP card to which they are connected.

### Network

- **Physical Address:** 00:10:36:09:59:1C
- **IP Address:** 172.16.9.37
- **Subnet Mask:** 255.255.240.0
- **Default Gateway:** 172.16.8.99
- **DHCP Server:** 172.16.6.49
- **Primary WINS Server:** 172.16.6.49
- **Secondary WINS Server:** 0.0.0.0
- **Hostname:** IPRC
Status — Receive Audio (or Call Statistics)

NOTE: This page is used for both card and device programming.

13.56 When you select Receive Audio (or Call Statistics), the following page (or one similar to this) appears.

Receive Session Information

<table>
<thead>
<tr>
<th>Circuit Description</th>
<th>Playback Buffer (ms)</th>
<th>Intime Frames (%)</th>
<th>Total Number of Adjustments</th>
<th>Total Number of Resynchs</th>
<th>Average Network Jitter (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>500</td>
<td>100</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>No Associated Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>No Associated Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>No Associated Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>No Associated Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>No Associated Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>No Associated Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>No Associated Channel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Call Quality

- Good
- Moderate
- Critical

Refresh Interval: 50 seconds

13.57 It shows the current status of all the circuits in the IP card. If desired, click one of the following buttons:

- **Set Interval**: Sets the refresh rate of this page with the value in “Refresh Interval.” The value of the Refresh Interval is in second(s).
- **Stop**: Stops refreshing the page.
- **Refresh**: Restores all fields to the current values stored in the database.
Device status information includes the following:

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit (or Audio Channel)</td>
<td>Clicking on an entry in the Circuit (Audio Channel) column will bring up the Intime Frame Graph, similar to the one shown below, in a separate window. This graph shows the intime frames percentage values of the last 30 seconds.</td>
</tr>
<tr>
<td>Description</td>
<td>Indicates the description of the device.</td>
</tr>
<tr>
<td>Playback Buffer (ms) (500)</td>
<td>Measures the current playback buffer time. This value should correspond to the Minimum Playback Buffer Time (ms) field in the Circuit Configuration — Audio Settings Page (see page 104). When there are no calls present, it uses 500 ms by default.</td>
</tr>
<tr>
<td>Intime Frames (%) (100%)</td>
<td>Displays the percentage of audio frames that were successfully played in the last second. When there are no calls present, it uses 100% by default.</td>
</tr>
<tr>
<td>Total Number of Adjustments (0)</td>
<td>Shows the total number of playback adjustments made by the device to maintain a consistent end-to-end delay during a call. Every time the device adjusts, the audio quality may degrade slightly.</td>
</tr>
<tr>
<td>Total Number of Resynchs (0)</td>
<td>Shows the total number of frame resynchronizations. Resynchronizations should only occur with large changes in network latency. Every time the device resynchronizes, the audio quality will degrade tremendously.</td>
</tr>
<tr>
<td>Average Network Jitter (ms) (0)</td>
<td>Shows an estimate of the average variance of the interarrival delay between network packets in milliseconds.</td>
</tr>
</tbody>
</table>
Status — Circuits

13.59 When you select Circuits, the following page appears.

## Circuit Status Information

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Description</th>
<th>Device ID</th>
<th>IP Address</th>
<th>Device Type</th>
<th>Connected</th>
<th>Send</th>
<th>Receive</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>MGCP Add'l Endpoint</td>
<td>NO</td>
<td>No Channel</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Unused</td>
<td></td>
<td>0.0.0.0</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td>NO</td>
<td>No Channel</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Unused</td>
<td></td>
<td>0.0.0.0</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td>NO</td>
<td>No Channel</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Unused</td>
<td></td>
<td>0.0.0.0</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td>NO</td>
<td>No Channel</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Unused</td>
<td></td>
<td>0.0.0.0</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td>NO</td>
<td>No Channel</td>
<td></td>
</tr>
</tbody>
</table>

13.60 It shows the current status of all the circuits in the IP card. If desired, click one of the following buttons:

- **Set Interval**: Sets the refresh rate of this page with the value in “Refresh Interval.” The value of the Refresh Interval is in second(s).
- **Stop**: Stops refreshing the page.
- **Refresh**: Restores all fields to the current values stored in the database.

13.61 Device status information includes the following:

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Slot (Unknown)</td>
<td>Indicates the card’s location in relation to the CPU in slot 8 (add 16 to this value if the card resides in the second cabinet of a dual-cabinet system).</td>
</tr>
<tr>
<td>Circuit</td>
<td>Indicates the circuit on the IP card. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Description</td>
<td>Shows the description of the device.</td>
</tr>
<tr>
<td>Device ID (Unused)</td>
<td>Shows the device ID of the IP device that will connect to this circuit.</td>
</tr>
<tr>
<td>IP Address (0.0.0.0)</td>
<td>Shows the Ethernet address of the IP device that will connect to this circuit.</td>
</tr>
<tr>
<td>Device Type (IP PhonePlus)</td>
<td>Shows the type of IP device that is connected to the circuit. The device types include the following:</td>
</tr>
<tr>
<td></td>
<td>• IP PhonePlus (or Model 8660)</td>
</tr>
<tr>
<td></td>
<td>• IP Single-Line Adapter</td>
</tr>
<tr>
<td></td>
<td>• IP SoftPhone</td>
</tr>
<tr>
<td></td>
<td>• IPP+, IPSLA, IPSOFT</td>
</tr>
<tr>
<td></td>
<td>• MGCP Gateway Device + Endpoint</td>
</tr>
<tr>
<td></td>
<td>• MGCP Add'l Endpoint</td>
</tr>
<tr>
<td>Connected (NO)</td>
<td>Shows the status of the connection.</td>
</tr>
<tr>
<td></td>
<td>• YES: Indicates the device is connected to the IP card.</td>
</tr>
<tr>
<td></td>
<td>• NO: Indicates the device is not connected to the IP card</td>
</tr>
<tr>
<td></td>
<td>• RECV IP: Indicates UDP communication is established, but TCP has not connected.</td>
</tr>
<tr>
<td></td>
<td>• RECONNECT: Indicates the devices is connecting to the IP card after a minor reset.</td>
</tr>
</tbody>
</table>
Command — Reset

**NOTE:** This command is used in both card and device programming.

13.62 When you select **Reset**, the following page appears. Clicking **Reset** forces the device to perform a major reset.

13.63 After you click **Reset**, the subsequent page waits for 20 seconds before trying to reload the main menu page of the device.

**Reset**

Press the "Reset" button to reset.

**Warning!!** The reset will drop all calls connected to this card.
Command — Reset Circuits

13.64 When you select **Reset Circuits**, the following page appears.

**Reset Circuits**

*Warning*: Resetting the circuit will drop the call on that circuit.

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Device Description</th>
<th>Device Type</th>
<th>Device ID or Ethernet Address</th>
<th>Device IP Address</th>
<th>Send (OFF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MGCP Add'l Endpoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td></td>
<td>Unused</td>
<td>Not Connected</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td></td>
<td>Unused</td>
<td>Not Connected</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td></td>
<td>Unused</td>
<td>Not Connected</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IPP+, IPSLA, IPSOFT</td>
<td></td>
<td>Unused</td>
<td>Not Connected</td>
<td></td>
</tr>
</tbody>
</table>

13.65 It shows the current status of all the circuits in the IP card. If desired, click one of the following buttons:

- **Set Interval**: Sets the refresh rate of the above page with the value in “Refresh Interval.” The value of the Refresh Interval is in second(s).
- **Stop**: Stops refreshing the page.
- **Refresh**: Restores all fields to the current values stored in the database.

**Device status information includes the following:**

<table>
<thead>
<tr>
<th>FIELD</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit</td>
<td>Indicates the circuit on the IP card. It is also a hyperlink that allows you to jump to the Device Specific page for that circuit (see page 111).</td>
</tr>
<tr>
<td>Device Description</td>
<td>Shows the description of the device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Shows the type of IP device that is connected to the circuit. The device types include the following:</td>
</tr>
<tr>
<td></td>
<td><strong>IP PhonePlus</strong> (or Model 8660)</td>
</tr>
<tr>
<td></td>
<td><strong>IP Single-Line Adapter</strong></td>
</tr>
<tr>
<td></td>
<td><strong>IP SoftPhone</strong></td>
</tr>
<tr>
<td></td>
<td><strong>IPP+, IPSLA, IPSOFT</strong></td>
</tr>
<tr>
<td></td>
<td><strong>MGCP Gateway Device + Endpoint</strong></td>
</tr>
<tr>
<td></td>
<td><strong>MGCP Add’l Endpoint</strong></td>
</tr>
<tr>
<td>Device ID or Ethernet Address</td>
<td>Shows the device ID or Ethernet address of the IP device that is connected to this circuit.</td>
</tr>
<tr>
<td>Device IP Address</td>
<td>Shows the device IP address that is connected to this circuit.</td>
</tr>
<tr>
<td>Send (OFF)</td>
<td>Shows the sending status of the device. The status options include the following:</td>
</tr>
<tr>
<td></td>
<td><strong>ON</strong>: IP card is sending audio packets to the device.</td>
</tr>
<tr>
<td></td>
<td><strong>OFF</strong>: IP card is not sending audio packets to the device.</td>
</tr>
</tbody>
</table>
### FIELD DESCRIPTION (Continued)

<table>
<thead>
<tr>
<th>FIELD</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Receive (OFF)** | Shows the receiving status of the device. The status options include the following:  
  - **OFF**: IP card is not expecting to receive audio packets on that circuit.  
  - **READY**: IP card is ready to receive audio packets.  
  - **RUNNING**: IP card is currently receiving audio packets.  
| **Reset**     | To reset one or more circuits:  
  5. Place a check mark next to each circuit you want to reset. (You can click Check All to select all of the circuits on the board, or click Clear All to erase all the check marks.)  
  6. Click **Reset**. The devices on the selected circuits performs a major reset. |
Command — Download

**NOTE:** This command is used in both card and device programming.

**13.67** When you select **Download**, the following page appears. To download software to the device, click **Download**. The device becomes in the Download state (see page 133).

### Download

Press the "Download" button to place the device in the download state.

*Warning!! The download procedure will drop all calls.*

**Database — Save**

**13.68** When you select **Save**, the following page appears. Click **Save**. The Web interface then begins a download procedure and allows you to select the destination. The entire database, with the exception of the password, is downloaded to the specified destination. The downloaded file contains only data in ASCII text format.

### Save Database

Press the "Save" button to start downloading the database.

*NOTE:* The downloaded file also contains a database version number. The version number prevents you from restoring a newer database to an older version IP card. The IP card will automatically update older databases.
Database — Restore

13.69 When you select **Restore**, the following page appears. Enter a file name or click **Browse** to select the file to be restored. Click **Restore Now** to complete the upload.

- *If the Browse button does not appear on this page*, your Web browser needs to be updated. For restore database to work, you have to use Internet Explorer or Netscape version 4.0 or later.
- *If the database restore fails*, the server generates the same page with an error message, stating the reason of the failure.
- *If the database restore is successful*, a success message appears and asks you to reset the device to allow the changes to take effect.

### Restore Database

If you do not see the "BROWSE" button, you may need to install Internet Explorer 4.0 or later, or Netscape Navigator 4.0 or later.

**File to upload:**

- **Browse**
- **Restore Now**

Database — Default

**NOTE:** This page is used for both card and device programming.

13.70 When you select **Default**, the following page appears. Clicking **Default Database** overwrites the database with default values and resets the card.

**NOTE:** The Default Database command also defaults the IP card password and the IP devices password.

### Default Database

Press the "Default Database" button to overwrite the database with default values and reset the card.

*Warning! Defaulting the database will result in the loss of the entire database.*

*The subsequent reset will drop all cells connected to this card.*

- **Default Database**
### 10/100 Switch — Program Switch

**NOTE:** This page is used for Model 8660 endpoint programming only.

13.71 When you select **Program Switch**, the following page appears.

#### 10/100 Switch Configuration

- **Update:** Saves your changes.
- **Refresh:** Restores all fields to the current values stored in the database.
- **Reset Fields:** Restores the fields to the values that were displayed when you opened the page.

13.72 The following table describes the information required for each field.

<table>
<thead>
<tr>
<th>FIELD (DEFAULT)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOS (Type of Service) Prioritization for PC1-3 (Disabled)</td>
<td>Allows TOS-based priority to the 10/100 ports.</td>
</tr>
<tr>
<td>Prioritize Assured Forwarding DSCP (Diffserv Cord Point Values (Disabled)</td>
<td>Allows all Assured Forwarding values indicating low drop precedence to have high priority.</td>
</tr>
<tr>
<td>Support Old-Style IP Precedence (Disabled)</td>
<td>Allows all values other than the Routine within the IP Precedence field to have high priority. Otherwise, only specific DSCP values are high priority.</td>
</tr>
</tbody>
</table>

**NOTE:** If too much traffic through the switch is considered high priority, the audio quality may degrade.
10/100 Switch — Default Switch

NOTE: This page is used for Model 8660 endpoint programming only.

13.73 When you select Default Switch, the following page appears. Clicking Default 10/100 Switch overwrites the switch settings with default values and resets the card.

**Default 10/100 Switch**

Press the "Default Switch" button to overwrite the switch settings with default values and reset the device.

*Warning! Defaulting the switch will result in the loss of customized switch settings.*

The subsequent reset will drop all calls connected to this device.

Default 10/100 Switch
NOTE: This page is used for both card and device programming.

**13.74** When you select **Date & Time**, the following page appears. Currently, the date and time fields are used only for debug purposes. Changing them does not change the system time or the IP device’s display.

**13.75** Program the fields that need to be changed and then click **Update** (or **Update Date** and/or **Update Time** for device configuration) to save your changes. (You can click **Refresh** to erase your changes, if necessary.)

---

### Date and Time

- **The current date:** Sun, Sep 1, 2002
- **New Date (mm-dd-yyyy):** Sep 21, 2002
- **The current time:** 19:38:34
- **New Time (hh:mm:ss):** 19:20:34

[Update] [Refresh]
D. RS-232 CONNECTION METHOD (IPRC ONLY)

NOTE: Initially, the IP addressing for the card must be done through the RS-232 port. The RS-232 connection method supports all versions of IPRCs.

13.76 To use a serial interface via an RS-232 connection:

1. Make sure the IPRC is connected and online.

2. Connect a programming PC to the IPRC serial port jack as follows (refer to the diagram below). The necessary connectors can be purchased separately or as part of the Universal RS-232 Kit (part no. 828.1282). This RS-232 connection is the same as the RS-232 connection to the CPU cards used for Database Programming.
   a. Attach one end of an 8-wire reversing mod-to-mod line cord to the serial port jack on the IPRC.
   b. Attach the other end of the line cord to a DB9F-to-8P/8C modular adapter with the proper flow control. (This application does not require flow control unless the bps rate exceeds 9600.)
   c. If the PC does not have an available DB9M COM port, but does have an available DB25M COM port, attach the DB9M-to-DB25F converter to the DB9F end of the modular adapter.
   d. Connect the cable to the appropriate COM port on the programming PC.

3. Using a terminal program (such as HyperTerminal) on the PC, press ENTER several times to establish communication. The same screen used for a Telnet session (shown below) should be displayed.

4. Follow the instructions for the Telnet session (beginning with step 4) to view the diagnostic displays.
E. TELNET CONNECTION METHOD

13.77 To use a serial interface via a Telnet connection:

1. Make sure the IPRC is connected and online.

2. Establish a Telnet connection to the IPRC’s IP address using a Telnet program (such as the Microsoft Windows Telnet program) on a PC configured to run the IPRC’s subnet. A Telnet page similar to the one shown below appears.

3. At the prompt, enter the IPRC’s password and press ENTER. The following page appears.

   NOTE: The password is case-sensitive.

4. Enter A (not case-sensitive) at the Enter selection prompt. The Programming Menu is displayed, as shown below.

The Programming Menu contains the following options:

a. **Quick Setup**: Allows you to set up the IP card network settings and speeds up the setup process. The command will ask whether you would like to use BOOTP and/or DHCP. If you answer Y (yes), the command asks you to reset the card. Otherwise, the command asks you to enter the following fields: IP Address, Subnet Mask, and IP Gateway Address.

b. **Database Programming**: Allows you to set up telnet and Web access for card and device programming. (For details, see pages 133 through 135).

c. **Network Information**: Provides the current network information, including status, Ethernet address, IP address, subnet mask, default gateway, DNS server, DNS suffix, DHCP server, primary and secondary WINS servers, and hostname, if any.

d. **Diagnostic**: Provides the following options:
   — Message Server Setup
— Connection Status (not applicable to the Model 8660 endpoint)
— Audio Receive Statistics
— Audio Send Statistics
— DSP Events Statistics
— Echo Cancellation Statistics (not applicable to the Model 8660 endpoint)
— NIC Statistics
— Thread Registry
— Crosspoint Connections (not applicable to the Model 8660 endpoint)
— Timer-Alarm Statistics
— Audio Session Send Configuration

The most important of these are the Connection Status, Audio Receive Statistics, and NIC Statistics. The Echo Cancellation Statistics may also be important in solving echo problems. A sample Echo Cancellation Statistics is shown on the next page. The others are for engineering use.

e. **Version:** Shows the software version information, including the device, version, build date and time, boot version, boot build date and time, and maximum allowed channels (maximum number of ports allowed by the security PAL).

*A Sample Echo Cancellation Statistics*

The Echo Cancellation Statistics has the following options:

— **Echo blocker switch,** **Echo blocker sensitivity level,** and **Saturation echo blocker switch:** Show the current settings that are programmed in Database Programming (located under System\Devices and Feature Codes\IP Connections\P6xxx\Backplane Call Configuration).

— **Near-end level:** Shows the energy level of audio from the IP stream.

— **Far-end level:** Shows the energy of the audio from the backplane.

— **After-cancellation level:** Shows the energy level of what the near-end will hear after echo canceller worked its magic. It should match far-end level and not follow near-end level.

— **Adapting:** If set to yes, the echo canceller adapts when only near-end speaks.

— **Echo blocker:** If set to yes, once the echo canceller believes it has adapted, it turns off this echo blocker/suppression.

— **Saturation echo blocker enabled:** Shows the current setting that is programmed in Database Programming (located under System\Devices and Feature Codes\IP Connections\P6xxx\Backplane Call Configuration).

— **Saturation echo blocker active:** Indicates when blocking is due to loud/saturated near-end.
### F. RS-232/TELNET CARD PROGRAMMING FIELDS

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static (Default) IP Address (192.168.200.201)</td>
<td>Defines the default IP address for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this IP address. If you enter 0.0.0.0, the server defaults to 192.168.200.201. It is recommend that you obtain a static IP address from the customer’s IT department for this equipment and enter it at the Static (Default) IP Address prompt. You can use a dynamic IP address from a DHCP server, but if the address changes later, the IP endpoints will no longer know what address to use. You should always use a static address for the IPRC. Use DHCP for endpoints.</td>
</tr>
<tr>
<td>Subnet Mask (255.255.255.0)</td>
<td>Defines the default subnet mask for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this subnet mask. Enter the subnet mask that was provided to you by the customer’s IT department.</td>
</tr>
<tr>
<td>IP Gateway Address (0.0.0.0)</td>
<td>Defines the default IP gateway or router address for the IP device. If the card does not receive a BOOTP or DHCP response, it uses this IP gateway address.</td>
</tr>
<tr>
<td>Message Server IP Address (0.0.0.0) Message Server Port (5568)</td>
<td>The IPRC can send error and debug information to a specified message server. These fields define the IP address and UDP port number of the message server that the IPRC will send error and debug information to. If a message server is not available, set this field to 0.0.0.0.</td>
</tr>
<tr>
<td>Password - Change (Y/N)?</td>
<td>This password protects the IPRC’s database from modifications. Whenever a user attempts to browse the Web page, connect a Telnet session, or program the database over RS-232, the IPRC will prompt the user to enter this password.</td>
</tr>
<tr>
<td>TCP Call Control Port (5566)</td>
<td>The IPRC uses this port number to receive call control messages from IP devices. The port number should only be changed for rare circumstances.</td>
</tr>
<tr>
<td>UDP General Purpose Port (5567)</td>
<td>The IPRC uses this port number to send and receive connection messages to and from IP devices. The port number should only be changed for extremely rare circumstances. The IP devices use this port number to find and connect to the IPRC.</td>
</tr>
<tr>
<td>Audio Stream Receive Port (5004)</td>
<td>The IPRC uses this port number to receive RTP audio data from all IP devices. The port number should only be changed for extremely rare circumstances.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> With IPRC v1.5 firmware, you must change this setting to 2427 to connect to the MGCP.</td>
<td></td>
</tr>
<tr>
<td>WINS Server IP Address (0.0.0.0)</td>
<td>Indicates the IP address that the device should use to find the WINS server to register its hostname. The default is 0.0.0.0, which indicates no WINS server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Identifies the device on the network. This string can be up to 15 characters. The default value is blank.</td>
</tr>
<tr>
<td>FIELD (AND DEFAULT VALUE)</td>
<td>FIELD DESCRIPTION (Continued)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Main Flags (00000100 in octal format)</td>
<td>This field is a list of flags. The bits are numbered 0-31, where the right-most bit (0) is the least-significant bit. The bits are defined below. All bits that are not listed are undefined and should always be zero.</td>
</tr>
<tr>
<td>Bit</td>
<td>Definition</td>
</tr>
<tr>
<td>0</td>
<td><strong>Companding type of the system backplane</strong>: 1=A-law, 0=Mu-law</td>
</tr>
<tr>
<td>1</td>
<td><strong>Enable IP precedence</strong>: 1=High Precedence, 0=Normal Precedence</td>
</tr>
<tr>
<td>2-3</td>
<td><strong>Country Setting</strong>: This field indicates the country of the IP card. The IP card and the IP devices use this setting for tone levels and single-line termination type. 0=USA, 1=UK, 2=Japan. The devices use this setting when sending audio toward the backplane. The devices use the setting from the Device Flags 2 when sending audio from the backplane.</td>
</tr>
<tr>
<td>4-7</td>
<td><strong>IPRC backplane signal gain</strong>: This is used as a negative value in the range from 0 dB to -15 dB.</td>
</tr>
<tr>
<td>8</td>
<td><strong>BOOTP mask</strong>: If this bit is 1, the IPRC will not do a BOOTP request during initialization.</td>
</tr>
<tr>
<td>9</td>
<td><strong>DHCP mask</strong>: If this bit is 1, the IPRC will not do a DHCP request during initialization. <em>If bits 8 and 9 are both 0</em>, the IP card will attempt BOOTP before DHCP. <em>If bits 8 and 9 are both 1</em>, the IP card will immediately use its default IP address, subnet mask, and gateway.</td>
</tr>
<tr>
<td>10</td>
<td><strong>IP Web interface mask</strong>: If this bit is 1, the IPRC will not respond to HTTP requests.</td>
</tr>
<tr>
<td>11</td>
<td><strong>Telnet interface mask</strong>: If this bit is 1, the IPRC will not accept Telnet connections.</td>
</tr>
</tbody>
</table>
### G. RS-232/TELNET DEVICE PROGRAMMING FIELDS

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Number: 01</td>
<td>Indicates the circuit number that you are programming.</td>
</tr>
</tbody>
</table>
| Ethernet Address (FF:FF:FF:FF:FF) | Contains the Ethernet address of the IP device that will connect to this circuit. The IPRC uses the IP device’s Ethernet address as a unique identifier for the device. You can also use the following:  
  - **Learn Mode**: Sets the Ethernet address to 00:00:00:00:00:00 to put the circuit into Learn Mode (as described on page 81).  
  - **Unused**: If the current circuit is unused, set the Ethernet address field to FF:FF:FF:FF:FF:FF. If the resulting configuration is updated, the effect will be to disable the circuit. |
| BOOTP IP Address (0.0.0.0) | The IPRC contains a BOOTP server. If the IPRC receives a BOOTP request from the Ethernet address in the Ethernet Address field, the IPRC sends the BOOTP IP address to the device. If this field is set to 0.0.0.0, the IPRC will not send a BOOTP reply. |
| Remote IPRC/MGCP Gateway Device IP Address (255.255.255.0) | The IP devices first attempt to connect to a local IPRC by broadcasting messages on the LAN. If a local IPRC does not respond to the IP device, the IP device attempts to connect to the default IP card address. This field must be programmed for the IP device to connect across a router. Changes to this field take effect after the device resets. |
| Static IP Address (192.168.200.201) | Defines the default IP address for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this address. Changes to this field take effect after the device is reset. |
| Static Subnet Mask (0.0.0.0) | Defines the default subnet mask for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this subnet mask. Changes to this field take effect after the IP device is reset. |
| Static IP Gateway (0.0.0.0) | Defines the default IP gateway or router address for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this IP gateway address. Changes to this field take effect after the IP device is reset. |
| Message Server IP Address (0.0.0.0) Message Server Port (5568) | The IP device can send error and debug information to a specified message server. These fields define the IP address and UDP port number of the message server that the IP device will send error and debug information to. If a message server is not available, set this field to 0.0.0.0. |
| Audio Stream Send Port (5004) | Contains the UDP port number that the IPRC uses to send RTP packets to the IP device. Do not change this field while the IP device is connected to the IPRC.  
  **NOTE**: With IPRC v1.5 firmware, you must change this setting to 2427 to connect to the MGCP. |
<p>| Vocoder Type (FF - Default) | Defines the vocoder type that the IP device on this circuit will attempt to use. Possible values are: 00 - G.711 Mu-Law, 08 - G.711-A-Law, 12 - G.729 Mu-Law, FF - Default. The Default option allows the IP device to automatically choose a value. Changes to this field take effect when the IP device starts a new call. (This should be set to G.711 for fax operation.) |</p>
<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Frames/IP Packet; FF is default: FF</td>
<td>Indicates the maximum number of RTP packets to stack in a single UDP packet. Increasing the number increases the audio delay, but reduces the bandwidth and CPU load. This value should normally be 2 through 4. The default value allows the IP device to automatically choose a value. Changes to this field take effect when the IP device starts a new call. (This should be set to 1 for fax operation.)</td>
</tr>
<tr>
<td>WINS Server IP Address (0.0.0.0)</td>
<td>Indicates the IP address that the device should use to find the WINS server to register its hostname. The default is 0.0.0.0, which indicates no WINS server.</td>
</tr>
<tr>
<td>Host name/Endpoint name: ACgw0 - Change (Y/N)?</td>
<td>Identifies the device on the network. This string can be up to 15 characters. The default value is blank.</td>
</tr>
<tr>
<td>Device Description: - Change (Y/N)?</td>
<td>You can enter a description of up to 16 characters to help you identify the device on this circuit. This description also appears in the Network, Status, and Device Specific screens.</td>
</tr>
<tr>
<td>Device Password: - Change (Y/N)?</td>
<td>This password protects the IP device’s database from modifications. Whenever a user attempts to browse the Web page, connect a Telnet session, or program the database over RS-232, the IP device prompts the user to enter this password.</td>
</tr>
<tr>
<td>Gateway Device (00)</td>
<td>Represents the zero-based circuit number of the MGCP gateway to which an MGCP Endpoint belongs. For the “Gateway Device and Endpoint,” this field must contain the device’s own zero-based circuit number. For example, if the gateway was on circuit 14, the additional MGCP endpoint would show a “Gateway Device” of 13.</td>
</tr>
<tr>
<td>Device Flags (00000206 in octal format)</td>
<td>This field is a list of flags. The bits are numbered 0-31, where the rightmost bit (0) is the least-significant bit. The bits are defined below. All bits that are not listed are undefined and should always be zero.</td>
</tr>
<tr>
<td>Bit</td>
<td>Definition</td>
</tr>
<tr>
<td>0-7</td>
<td>Device type that is to connect to this circuit: 0=Any Device, 2=IP Terminal, 3=IP-SLA, 5=IP SoftPhone, 6=MGCP Gateway Device and Endpoint, 7=Additional MGCP Endpoint. Changes to this field take effect immediately.</td>
</tr>
<tr>
<td>8</td>
<td>BOOTP mask: If this bit is 1, the IP device will not do a BOOTP request during initialization.</td>
</tr>
<tr>
<td>9</td>
<td>DHCP mask: If this bit is 1, the IP device will not do a DHCP request during initialization. If bits 8 and 9 are both 0, the IP device will attempt BOOTP before DHCP. If bits 8 and 9 are both 1, the IP device will immediately use its default IP address, subnet mask, and gateway.</td>
</tr>
<tr>
<td>10</td>
<td>IP Web interface mask: If this bit is 1, the IP device will not respond to HTTP requests.</td>
</tr>
<tr>
<td>11</td>
<td>Telnet Interface Mask: If this bit is 1, the IP device will not accept Telnet connections.</td>
</tr>
<tr>
<td>12-13</td>
<td>DTMF Encoding Setting: 0=Default 1-way, 1=None, 2=Out-of-band, 3=G.711. See the HTTP/Web Interface Method (page 106) or the online help for more details.</td>
</tr>
<tr>
<td>14</td>
<td>G.729B Voice Activity Detector Enable: 1=Enabled, 0=Disabled. Setting this bit allows this circuit to use the G.729 Annex B voice activity detector.</td>
</tr>
<tr>
<td>Bit</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>15</td>
<td><strong>Echo suppression/blocker mask:</strong> 1=Disabled, 0=Enabled. Setting this bit disables the echo suppression/blocker function on this circuit.</td>
</tr>
<tr>
<td>16-22</td>
<td><strong>Echo suppression sensitivity level:</strong> 0=Most sensitive (100%), 100 ($64)=least sensitive (0%). Increasing this value reduces the sensitivity of echo suppression, changing from a condition most like half-duplex to a condition most like no echo suppression at all.</td>
</tr>
<tr>
<td>23</td>
<td><strong>Saturation echo blocker mask:</strong> 1=Disabled, 0=Enabled. Setting this bit disables the saturation echo blocker function on this circuit.</td>
</tr>
<tr>
<td>24-31</td>
<td><strong>Minimum playback buffer time (ms):</strong> Increasing this field increases the amount of audio that the device buffers up before playing it. Doing this will increase the audio delay but may improve the audio quality in some circumstances. If the user enters a value that is too small for the IP device to use, the IP device will use the smallest value that it can. If the user enters a zero value, the device will use a default value (80 ms).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Use the IP device’s self-programming settings. If this bit is 0, the IP device connected to this circuit updates all fields in its own database from the IPRC’s database. Otherwise, the IP device will use its own settings for network-related fields such as IP address, subnet mask, gateway, remote IPRC IP, UDP port number, hostname, DHCP, and BOOTP.</td>
</tr>
<tr>
<td>2-3</td>
<td><strong>Country setting:</strong> This field indicates the country of the IP device connected to this port. The IPRC and the IP devices use this setting for tone levels and single-line termination type. 0=USA, 1=UK, 2=Japan. The devices use this setting when sending audio away from the backplane. The devices use setting from the Main Flags when sending audio toward the backplane.</td>
</tr>
</tbody>
</table>
H. RS-232/TELNET IP DEVICES PROGRAMMING FIELDS

13.78 The IP PhonePlus and IP SLA use the Database Main Entries (DBMN) command to program the device-specific fields, shown in the table below. The Model 8660 endpoint uses the menu-based interface as previously described.

13.79 To program these fields using the DBMN command:

1. When the Enter Password prompt is displayed in a terminal program (such as HyperTerminal) or Telnet screen, as shown in step 2 on page 131, enter the IP device password and press **ENTER**.

   **NOTE:** The passwords are case-sensitive.

2. The IP device should display a OLMN> prompt, as shown below. (If necessary, type “?” or “HELP” to display a list of available online monitor (OLMN) commands.)

3. Type **dbmn** and press **ENTER**. This command allows you to set up the IP device network settings.

   — The IP device prompts you to enter several values. When the IP device displays the field name and the current value, you may either enter a new value or press **ENTER** to accept the current value. The fields and sample values are shown on the next several pages. Modify the values to match the network to which the IP device is connected.

   — Answer **Y** (yes) or **N** (no) when the IP device asks if you would like to accept the shown values.

   — When prompted, reset the IP device so that the changes take effect.

   **NOTE:** It is recommended that you do not obtain an IP address for the IP card automatically. If the address changes, the IP endpoint will no longer know what address to use.

<table>
<thead>
<tr>
<th>FIELD (AND DEFAULT VALUE)</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Password - Change (Y/N)?</td>
<td>The IP device can accept a Telnet connection for remote configuration. Whenever a user opens a Telnet or Web interface session to the IP device, the IP card prompts the user for this nine-character password. If you select Yes (Y), you will be prompted to enter the new password.</td>
</tr>
<tr>
<td>Remote IPRC IP Address: 0.0.0.0</td>
<td>The IP devices first attempt to connect to a local IP card by broadcasting messages on the LAN. If a local IP card does not respond to the IP device, the IP device attempts to connect to the default IP card address. This field must be programmed for the IP device to connect across a router.</td>
</tr>
<tr>
<td>FIELD (AND DEFAULT VALUE)</td>
<td>FIELD DESCRIPTION (Continued)</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Static IP Address: 192.168.200.201</td>
<td>Defines the default IP address for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this IP address. Changes to this field take effect when the IP device resets.</td>
</tr>
<tr>
<td>Static Subnet Mask: 255.255.255.0</td>
<td>Defines the default subnet mask for the IP device on this circuit. If the device does not receive a BOOTP or DHCP response, it uses this subnet mask. Changes to this field take effect when the IP device resets.</td>
</tr>
<tr>
<td>Static IP Gateway: 0.0.0.0</td>
<td>Defines the default IP gateway or router address for the IP device. If the device does not receive a BOOTP or DHCP response, it uses this IP gateway address. Changes to this field take effect when the IP device resets.</td>
</tr>
<tr>
<td>Message Server IP Address: 0.0.0.0</td>
<td>The IP devices can send error and debug information to a specified message server. These fields define the IP address and UDP port number of the message server that the IP device will send error and debug information to. If a message server is not available, set the message server IP address to 0.0.0.0. Changes to this field take effect immediately.</td>
</tr>
<tr>
<td>Message Server Port Number: 5568</td>
<td>The IP device uses this port number to send and receive connection messages to and from the IP card. The IP devices must use this port number to find and connect to the IP card. The port number should only be changed for extremely rare circumstances.</td>
</tr>
<tr>
<td>UDP General-Purpose Port Number: 5567</td>
<td>This field is a list of flags. The bits are numbered 0-31, where the rightmost bit (0) is the least-significant bit. The bits are defined below. All bits that are not listed are undefined and should always be zero.</td>
</tr>
<tr>
<td>Device Flags: 0 (in octal format)</td>
<td>Bit    Definition</td>
</tr>
<tr>
<td></td>
<td>0-7  <strong>Device type that is to connect to this circuit:</strong> 0=Any Device, 2=IP Terminal, 3=IP-SLA, 5=IP SoftPhone, 6=MGCP Gateway Device and Endpoint, 7=Additional MGCP Endpoint. Changes to this field take effect immediately.</td>
</tr>
<tr>
<td></td>
<td>8     <strong>BOOTP mask:</strong> If this bit is 1, the IP device will not do a BOOTP request during initialization.</td>
</tr>
<tr>
<td></td>
<td>9     <strong>DHCP mask:</strong> If this bit is 1, the IP device will not do a DHCP request during initialization. If bits 8 and 9 are both 0, the IP device will attempt BOOTP before DHCP. If bits 8 and 9 are both 1, the IP device will immediately use its default IP address, subnet mask, and gateway.</td>
</tr>
<tr>
<td></td>
<td>10    <strong>IP Web interface mask:</strong> If this bit is 1, the IP device will not respond to HTTP requests</td>
</tr>
<tr>
<td></td>
<td>11    <strong>Telnet Interface Mask:</strong> If this bit is 1, the IP device will not accept Telnet connections.</td>
</tr>
<tr>
<td></td>
<td>12-13 <strong>DTMF Encoding Setting:</strong> 0=Default 1-way, 1=None, 2=Out-of-band, 3=G.711. See the HTTP/Web Interface Method (page 106) or the online help for more details.</td>
</tr>
<tr>
<td></td>
<td>14    <strong>G.729B Voice Activity Detector Enable:</strong> 1=Enabled, 0=Disabled. Setting this bit allows this circuit to use the G.729 Annex B voice activity detector.</td>
</tr>
<tr>
<td></td>
<td>15    <strong>Echo suppression/blocker mask:</strong> 1=Disabled, 0=Enabled. Setting this bit disables the echo suppression/blocker function on this circuit.</td>
</tr>
<tr>
<td>FIELD (AND DEFAULT VALUE)</td>
<td>FIELD DESCRIPTION (Continued)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>(Continued) Device Flags: 0</td>
<td>Bit Definition</td>
</tr>
<tr>
<td>16-22 <strong>Echo suppression sensitivity level:</strong> 0=Most sensitive (100%), 100 ($64)=least sensitive (0%). Increasing this value reduces the sensitivity of echo suppression, changing from a condition most like half-duplex to a condition most like no echo suppression at all.</td>
<td></td>
</tr>
<tr>
<td>23 <strong>Saturation echo blocker mask:</strong> 1=Disabled, 0=Enabled. Setting this bit disables the saturation echo blocker function on this circuit.</td>
<td></td>
</tr>
<tr>
<td>24-31 <strong>Minimum playback buffer time (ms):</strong> Increasing this field increases the amount of audio that the device buffers up before playing it. Doing this will increase the audio delay but may improve the audio quality in some circumstances. If the user enters a value that is too small for the IP device to use, the IP device will use the smallest value that it can. If the user enters a zero value, the device will use a default value (80 ms).</td>
<td></td>
</tr>
</tbody>
</table>

Device Flags 2: 0

This field is another list of flags in hexadecimal. The bits are numbered 0-3, where bit 0 is the least-significant bit. The bits are defined below. All bits that are not listed are undefined and should always be zero.

<table>
<thead>
<tr>
<th>Bit</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>Use the IP device’s self-programming settings.</strong> If this bit is 0, the IP device connected to this circuit updates all fields in its own database from the IPRC’s database. Otherwise, the IP device will use its own settings for network-related fields such as IP address, subnet mask, gateway, remote IPRC IP, UDP port number, hostname, DHCP, and BOOTP.</td>
</tr>
<tr>
<td>2-3</td>
<td><strong>Country setting:</strong> Indicates the country of the IP device connected to this port. The IPRC and the IP devices use this setting for tone levels and single-line termination type. 0=USA, 1=UK, 2=Japan. The devices use this setting when sending audio away from the backplane. The devices use setting from the Main Flags when sending audio toward the backplane.</td>
</tr>
</tbody>
</table>

**WINS Server IP Address (0.0.0.0)**

Indicates the IP address that the device should use to find the WINS server to register its hostname. The default is 0.0.0.0, which indicates no WINS server.

**Device Hostname - Change (Y/N)?**

If you select Yes (Y), you will be prompted to enter the new hostname. This string can be up to 15 characters. It identifies the device on the network. The default value is blank.
14. PROGRAMMING THE IP DEVICES ON A V8.2.X FIRMWARE IPRC

**NOTE:** For information about IP devices programming on a v1.5.x firmware IPRC, see page 80.

**14.1** This section contains information about how to configure Models 8600, 8620/8622, 8662, and 8690 on a v8.2.x firmware IPRC. To configure the existing IP endpoints, such as the Model 8660, on a v8.2.x firmware IPRC, you must program them through Axxess Database Programming. Refer to the *Addendum to the Axxess v8.0 Installation and Maintenance Manual* for details.

**14.2** The v8.2.x firmware IPRC and multi-protocol endpoints can be programmed using various methods. The following ordered list shows the various sources of configuration information:

- Self-Programming Mode - Models 8620/8622 and 8662 Only (see page 142)
- IP Phone Web Client (see page 145)
- TFTP Device-Specific Configuration (see page 158)
- TFTP Global Configuration (see page 158)
- Axxess Database Programming for IP endpoints that are in ITP Mode (see page 167)
- Setup Wizard - Model 8690 Only (see page 168)

**14.3** The configuration information from a source in the list above overwrites any configuration information from a higher priority configuration source in the list. For example, if the global configuration file enabled DHCP, but the device-specific configuration file disables it, then this specific endpoint will have DHCP disabled. The other endpoints that pull the same global configuration file will have DHCP enabled unless something higher in the list, like the device-specific configuration file, changes it for a specific endpoint.

**NOTE:** Do not change the IP card’s database while a call is active; it may drop all calls in progress.
A. SELF-PROGRAMMING MODE (MODELS 8620/8622 AND 8662 ONLY)

14.4 The self-programming mode is the easiest way to configure the Models 8620/8622 and 8662. This self-programming mode is very similar to the Model 8660 endpoint. It allows you to set all the basic settings required for ITP mode.

14.5 The following endpoints do not support self-programming mode:

- **Model 8600**: This endpoint does not have a display. Hold 7 and 8 during power up to default its configuration.

- **Model 8690**: Even though the Model 8690 has a virtual six-line display, it does not support self-programming mode because there are no physical buttons to hold during power up. Instead, you can configure the network settings through the Setup Wizard (see page 168).

14.6 To use the self-programming mode on Models 8620/8622 and 8662:

1. While pressing 7 and 8 together on your endpoint, unplug and replace the endpoint power cord. The endpoint enters the self-programming mode and the following screen appears on the endpoint display.

**Six-Line Display for the Model 8662:**

<table>
<thead>
<tr>
<th>MENU SELECTION BUTTONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROGRAMMING MODE</strong></td>
</tr>
<tr>
<td><strong>PROGRAM DATABASE</strong></td>
</tr>
<tr>
<td><strong>DEFAULT DATABASE</strong></td>
</tr>
<tr>
<td><strong>EXIT</strong></td>
</tr>
</tbody>
</table>

**Two-Line Display for the Model 8620/8622:**

<table>
<thead>
<tr>
<th>MENU SELECTION BUTTONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROGRAM</strong></td>
</tr>
<tr>
<td><strong>DATABASE = 1</strong></td>
</tr>
<tr>
<td><strong>DEFAULT</strong></td>
</tr>
<tr>
<td><strong>DATABASE = 2</strong></td>
</tr>
</tbody>
</table>

2. You have the following options:

- **Program Database**: Allows you to program the static network settings through a series of screens that follow.

- **Default Database**: Allows you to use predefined defaults for the settings.

- **Exit**: Allows you to exit the self-programming mode without making any changes.

*With a Model 8662*, select one of the options using the menu selection button next to the LCD.

*With a Model 8620/8622*, press 1 to program the database or 2 to default the database. Or you can use the lower six programmable buttons in both of the right-most rows, as shown on the right. These buttons have the same functionality that the corresponding six-line display menu button would for each of the self-programming screens.
**Program Database**

14.7 Follow the displays and complete the programming. For details about **REVERT**, **EXIT**, **<<**, and **>>**, see paragraph 13.9 on page 83.

**NOTE:** Unlike the previous endpoints, such as the Model 8600, the multi-protocol endpoints do not support some configuration fields, such as hostnames and BOOTP. These endpoints, however, have additional fields like the software image information (see page 158).

---

<table>
<thead>
<tr>
<th>DISPLAY</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STATIC IP</strong> xxx.xxx.xxx.xxx</td>
<td><strong>Static IP Address:</strong> Enter the static IP address (defaults to 192.168.200.201).</td>
</tr>
<tr>
<td><strong>STATIC SUBNET</strong> xxx.xxx.xxx.xxx</td>
<td><strong>Default Static Subnet Mask:</strong> Enter the default static subnet mask (defaults to 255.255.255.0).</td>
</tr>
<tr>
<td><strong>DEFAULT GATEWAY</strong> xxx.xxx.xxx.xxx</td>
<td><strong>Default Static Gateway:</strong> Enter the default static gateway address (defaults to 192.168.200.201).</td>
</tr>
<tr>
<td><strong>REMOTE IPC IP</strong> xxx.xxx.xxx.xxx</td>
<td><strong>(For ITP Mode Only) Remote IPC IP Address:</strong> Enter the remote IPRC IP address (defaults to 172.16.15.152).</td>
</tr>
<tr>
<td><strong>REMOTE UDP PORT</strong> xxx</td>
<td><strong>(For ITP Mode Only) Remote UDP Port:</strong> Enter the remote UDP port (defaults to 5567).</td>
</tr>
<tr>
<td><strong>REMOTE TCP PORT</strong> xxx</td>
<td><strong>(For ITP Mode Only) Remote TCP Port:</strong> Enter the remote TCP port (defaults to 5566).</td>
</tr>
<tr>
<td><strong>TFTP SERVER URL</strong> XXXXXXXXXXXXXXXXX</td>
<td><strong>TFTP Server:</strong> Enter the URL of the TFTP Server (up to 79 digits). If the URL is too long to fit on the second line, it scrolls from right to left to allow the full URL to be displayed. <strong>To program the URL:</strong> The URL can contain any characters including the period (.) and hyphen (-) (press [FWD] and [MUTE] respectively). The number of times a button is pressed determines which character is entered, as shown below. When adjoining characters are under the same button, press [FWD] to advance to the next character. For example, 1 [FWD] 11 [FWD] 11 enters “ABC.” Press [FWD] twice to leave a space and press [MUTE] if you need to backspace.</td>
</tr>
<tr>
<td><strong>PASSWORD</strong> * * * * * * * * * * * * * * *</td>
<td><strong>(For SIP Only) SIP Authentication Password:</strong> Enter the authentication password (up to nine characters) for SIP registration. To enter the password, use the table shown above. To change the case of a character, select <strong>CHANGE CASE</strong>.</td>
</tr>
<tr>
<td><strong>DHCP?</strong> xxxxxxxx</td>
<td><strong>DHCP:</strong> This option allows you to program the option to use DHCP. The second line from the top indicates the current status (either <strong>ENABLED</strong> or <strong>DISABLED</strong>). <strong>To program this option:</strong> Select either <strong>ENABLED</strong> or <strong>DISABLED</strong>. The endpoint updates the display to reflect the new change.</td>
</tr>
</tbody>
</table>

---

**NUMBER OF TIMES BUTTON IS Pressed**

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>:</td>
<td>@</td>
<td>(</td>
<td>)</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>/ or \</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td>!</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>*</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>#</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>M</td>
<td>N</td>
<td>O</td>
<td>&amp;</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>$</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>?</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
<td>9</td>
</tr>
<tr>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>

*The slash (/) is used for the URL and the backslash (\) is used for the SIP authentication password.*
14.8 To program the IP address:

1. Press a dialpad button to enter the IP address. The entire second line, except the dots, disappears, and the number you entered appears in the first space. MUTE serves as a backspace button, and FWD, 3, or 7 moves the cursor to the next space after the dot.

**NOTE:** Pressing MUTE deletes the numbers without deleting the dots.

You have the following options:

- **Revert:** Reverts to the old value found in the current database, and the endpoint updates the display accordingly.
- **Exit:** Exits to the confirmation screen (last screen) without scrolling through all the other options. Refer to page 83 for more details on the confirmation screen.
- **>>:** Continues to the next screen in the series.
- **<<:** Returns to the previous screen in the series. Note that this option does not appear on the Static IP Programming screen.

2. Once you have finished programming, select either EXIT, >>, or <<. The endpoint will check the field for errors.

- **If there are no errors,** the endpoint displays the next programming screen.
- **If there are errors,** the endpoint displays INVALID ENTRY. Correct the error by either selecting REVERT or modifying the incorrect entry.

### Default Database and Exit

14.9 When you have scrolled through all the options, select EXIT from any of the screens or select DEFAULT DATABASE from the initial screen. The following screen appears to confirm the changes.

<table>
<thead>
<tr>
<th>S</th>
<th>A</th>
<th>V</th>
<th>E</th>
<th>C</th>
<th>H</th>
<th>A</th>
<th>N</th>
<th>G</th>
<th>E</th>
<th>S</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>E</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;</td>
<td>&lt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

14.10 You have the following options:

- **Yes:** Overwrites the database. If you select this option, the CHANGES SAVED screen appears to notify you that the changes have been saved. To continue initializing the endpoint, press any button.
- **No:** Leaves the database as it was. If you select this option, the NO CHANGES SAVED screen appears to notify you that the changes have been discarded. To continue initializing the endpoint, press any button.
- **<<:** Returns to the previous screen in the series.
B. IP PHONE WEB CLIENT

14.11 The Web interface, IP Phone Web Client Administrative Session, for the multi-protocol endpoints allows you to set the most frequently-used options. The Web interface also allows you to reset the device and synchronize its configuration with the configuration files on the TFTP server.

**NOTE:** Clicking **Synch** in the Configuration page synchronizes with the TFTP server only and not with the Axxess system (see page 157).

14.12 To reach the Web page on the Model 8690, you must use a different computer than the Model 8690 endpoint. This is because the Windows CE .NET and the VPS (Voice Processing Subsystem) share an IP address and the Web pages are served from the VPS but browsed from the Windows CE .NET. Once the Windows CE .NET sees its own IP address, the request never makes it to the VPS. When an external computer requests the Web pages, the VPS receives the request first so the Web pages are properly served.

**NOTE:** The Web Client configuration can be overwritten by a higher priority configuration source, such as self-programming mode.

**NOTICE**
The passwords, usernames, and URLs of the Web interface are all case-sensitive. If you do not enter the characters in the correct case (upper or lower), the browser will not be able to find the appropriate Web page.

14.13 To use the IP Phone Web Client:

1. Make sure the IP device is powered up, connected, and online.
2. Open the Microsoft Internet Explorer and enter the IP address of the endpoint followed by \:8080 (e.g., http://172.17.158.14:8080) in the Address field.
3. Log in with your username and password. The default username is **IPT** and password is **iptpassw**. To prevent unauthorized access, you should change the password of the IP Phone Web Client as soon as possible. To change the login password, see page 152. The screen shown on the following page appears.

**NOTE:** The username is predefined and cannot be changed.
14.14 The Web client contains the fields as described in the following table.

**NOTE:** Some of the fields can also be programmed in a TFTP configuration file. See page 158 for details about TFTP configuration files.

<table>
<thead>
<tr>
<th>ITP MODE</th>
<th>PAGE#</th>
<th>SIP MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Configuration</td>
<td></td>
<td>Device Configuration</td>
</tr>
<tr>
<td>- Network</td>
<td>147</td>
<td>- Network</td>
</tr>
<tr>
<td>- Audio &amp; Call Control</td>
<td>148</td>
<td>- Audio &amp; Call Control</td>
</tr>
<tr>
<td>- Phone</td>
<td>150</td>
<td>- Phone</td>
</tr>
<tr>
<td>- Trace</td>
<td>151</td>
<td>- Trace</td>
</tr>
<tr>
<td>- Authentication</td>
<td>152</td>
<td>- Authentication</td>
</tr>
<tr>
<td>N/A</td>
<td>153</td>
<td>- SIP</td>
</tr>
<tr>
<td>N/A</td>
<td>154</td>
<td>- Feature Code</td>
</tr>
<tr>
<td>- VLAN</td>
<td>154</td>
<td>- VLAN</td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td>Status</td>
</tr>
<tr>
<td>- Network</td>
<td>155</td>
<td>- Network</td>
</tr>
<tr>
<td>- Firmware</td>
<td>155</td>
<td>- Firmware</td>
</tr>
<tr>
<td>N/A</td>
<td>156</td>
<td>- Volume</td>
</tr>
<tr>
<td>- License</td>
<td>155</td>
<td>- License</td>
</tr>
<tr>
<td>- Image Upgrade</td>
<td>157</td>
<td>- Image Upgrade</td>
</tr>
<tr>
<td>- RTP/RTCP</td>
<td>157</td>
<td>- RTP/RTCP</td>
</tr>
<tr>
<td>Command</td>
<td></td>
<td>Command</td>
</tr>
<tr>
<td>- Configuration</td>
<td>157</td>
<td>- Configuration</td>
</tr>
<tr>
<td>- Reset</td>
<td>157</td>
<td>- Reset</td>
</tr>
</tbody>
</table>

**Web Interface Changes**

14.15 The Status menu has the following new pages and/or fields:

- Network Page — Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, and DNS Server fields (see page 155)
- Firmware Page — Boot Code Version and Boot Code Date/Time fields (see page 155)
- License Page (see page 155)
- RTP/RTCP Page (see page 157)
- Image Upgrade Page — Last Download Error Page field (see page 157)
Device Configuration

14.16 The Device Configuration field allows you to configure network, audio and call control, firmware, and trace settings.

14.17 **Network**: The Network Configuration page contains the network-specific configuration information. Both SIP and ITP modes have the same fields.

14.18 This page contains the fields described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>xx-xx-xx-xx-xx-xx-xx</td>
<td>The MAC address of the endpoint.</td>
</tr>
<tr>
<td>Static (Default) IP Address</td>
<td>192.168.200.201</td>
<td>The static IP address of the endpoint (when DHCP is disabled).</td>
</tr>
<tr>
<td>Default Network Subnet Mask</td>
<td>255.255.255.0</td>
<td>The default network subnet mask for the endpoint.</td>
</tr>
<tr>
<td>Default IP Gateway Address</td>
<td>192.168.200.201</td>
<td>The default IP gateway address for the endpoint.</td>
</tr>
<tr>
<td>IP Address Assignment</td>
<td>DHCP Enabled</td>
<td>Whether the IP endpoint uses DHCP to obtain an IP address instead of using the assigned static IP address.</td>
</tr>
<tr>
<td>TFTP Server IP Address</td>
<td>192.168.200.202</td>
<td>The IP address of the TFTP server where configuration files for this endpoint reside. Required if the DHCP does not provide the TFTP address.</td>
</tr>
</tbody>
</table>

You can also include the path to the profile file, if desired. For example, if the TFTP server IP address is “192.168.200.150” and the path file is “/basic_sip,” then you can specify the URL as “192.168.200.150/basic_sip.”
14.19 To apply the changes, click Update.

14.20 Audio & Call Control: This Audio & Call Control Configuration page shows specific information about a call in progress. The information is only valid if there is a call in progress. Refreshing the page (by pressing the refresh icon on browser) while a call is in progress ensures that the information is current. Depending on the mode, the available fields are different.

14.21 ITP Mode — This page contains the fields described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Server IP Address</td>
<td>0.0.0.0</td>
<td>The IP address of the IPRC to which this IP endpoint is currently connected (the same value that is programmed in Axxess system).</td>
</tr>
<tr>
<td>IP Terminal TCP Call Control Port</td>
<td>5566</td>
<td>The port number for TCP call control packets that are transmitted from this endpoint for the current connection. This value may or may not be what is programmed in the Axxess system.</td>
</tr>
<tr>
<td>IP Terminal General Purpose UDP Port</td>
<td>5567</td>
<td>The port number for all UDP (audio) packets that are transmitted from this endpoint for the current connection. This value may or may not be what is programmed in the Axxess system.</td>
</tr>
</tbody>
</table>

14.22 This page also shows the current call control status. The status fields are described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Server IP Address</td>
<td>0.0.0.0</td>
<td>The IP address of the IPRC to which this IP endpoint is currently connected (the same value that is programmed in Axxess system).</td>
</tr>
<tr>
<td>IP Terminal TCP Call Control Port</td>
<td>5566</td>
<td>The port number for TCP call control packets that are transmitted from this endpoint for the current connection. This value may or may not be what is programmed in the Axxess system.</td>
</tr>
<tr>
<td>IP Terminal General Purpose UDP Port</td>
<td>5567</td>
<td>The port number for all UDP (audio) packets that are transmitted from this endpoint for the current connection. This value may or may not be what is programmed in the Axxess system.</td>
</tr>
</tbody>
</table>
14.23 To apply the changes, click Update.

14.24 SIP Mode — This page contains the fields described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Send State</td>
<td>OFF</td>
<td>Whether the endpoint is currently sending RTP audio packets.</td>
</tr>
<tr>
<td>RTP Receive State</td>
<td>OFF</td>
<td>Whether the endpoint is currently receiving RTP audio packets.</td>
</tr>
</tbody>
</table>
| Session Description       | 2025 (GW) 1000| A description that indicates the two endpoints on the current connection along with the connection type. Connection types include:
  - GW – gateway (using backplane)
  - PTP – peer-to-peer (not using backplane) |
| Audio Stream Transmit IP Address | xxx.xxx.xxx.xxx | The IP address of the IP device to which the endpoint is currently transmitting audio. This device may be another IP endpoint or an IPRC. |
| Audio Stream Transmit Port | 5006          | The port number on the other IP device to which the IP endpoint is currently transmitting audio packets. |
| Audio Stream Receive Port | 5006          | The port number on this IP endpoint that is currently receiving audio packets. |
| Audio Frames/IP Packet    | 3             | The number of audio frames that this endpoint is currently sending per IP packet. A higher value indicates a lower bandwidth, but an increased latency. |
| RTP Profile               | A/V           | The method used to package the RTP methods. The IP endpoints support A/V only. |
| Speech Encoding Setting   | G.729         | The type of encoding that this endpoint uses when encoding DTMF tones. |
| Voice Activity Detection  | Disabled      | Whether the endpoint is currently transmitting RTP audio packets during periods of silence. |

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Audio Frames</td>
<td>3</td>
<td>The number of audio frames per output audio RTP packet.</td>
</tr>
<tr>
<td>Codec Type</td>
<td>G.729 Annex A</td>
<td>The encoding/decoding codec preference for this endpoint.</td>
</tr>
<tr>
<td>Audio Port</td>
<td>5004</td>
<td>The port where the endpoint transmits and receives RTP packets. This port must be an even number; each connection uses the next available even-numbered port.</td>
</tr>
<tr>
<td>Diffserv</td>
<td>46</td>
<td>The IP precedence value.</td>
</tr>
<tr>
<td>Suppress Silence</td>
<td>Disabled</td>
<td>Whether the endpoint sends audio packets during periods of silence.</td>
</tr>
</tbody>
</table>
14.25 To apply the changes, click Update.

14.26 Phone: The Phone Configuration page shows information that is related to the endpoint setup and whether the endpoint is currently in SIP mode.

14.27 This page contains the fields described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Out-Of-Band DTMF</td>
<td>Enabled</td>
<td>Whether the endpoint is currently sending DTMF tones &quot;out-of-band.&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Version</td>
<td>N/A</td>
<td>The image version of the endpoint-specific code (e.g., xxxx_image_ver=1-2-13 (where the xxxx indicates the model name, such as the 8662)).</td>
</tr>
</tbody>
</table>
| Image URL   | xxx.xxx.xxx.xxx/image/image-<ss>.bin. The <ss> is the image version from "xxxx_image_ver."
              |           | The IP address or URL (up to 79 digits) of the image TFTP server. Required if the DHCP does not provide the TFTP address.
              |           | You can also include the path to the profile file, if desired. For example, if the TFTP server IP address is "192.168.200.150" and the path file is "image," then you can specify the URL as "192.168.200.150/image/image-1-3-4.bin." |
## Device Configuration

### 14.28 To apply the changes, click Update.

### 14.29 Trace: The Trace Configuration page allows you to setup a remote trace capture for UDP debug information. The available fields vary depending on the mode the endpoint is in.

### 14.30 This page contains the fields described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC Dial Plan</td>
<td>xxxx</td>
<td><em>(For SIP Mode Only)</em> The dial plan mask that this endpoint uses to determine valid dial strings for end of dialing for IC, trunk, or outgoing calls. If the syntax is bad, you cannot dial calls. The acceptable symbols for a dial plan are described in the table below.</td>
</tr>
<tr>
<td>Trunk Dial Plan</td>
<td>9xxx</td>
<td></td>
</tr>
<tr>
<td>Outgoing Dial Plan</td>
<td>[2-9]xxxxxxx</td>
<td>011[1-9]xxxxxxx</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>(For SIP Mode Only)</em> Whether the endpoint will be in SIP mode or ITP mode after the next reset.</td>
</tr>
<tr>
<td>Hold Reminder Time</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>SIP Mode</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-9</td>
<td>Digit 0-9.</td>
</tr>
<tr>
<td>x</td>
<td>Any digit 0-9.</td>
</tr>
<tr>
<td>*, #</td>
<td>Dialpad entry (*, #).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Zero or more of the preceding digit(s) or [ ] expression. For example, “+#” means that a dial plan can accept any dial string that ends with “#,” such as “1234*#” or “#” (zero digits). Also “[2-9]+#” means that a dial plan can accept any dial string that begins with any digit “2” through “9” followed by “#.”</td>
</tr>
<tr>
<td>[ ]</td>
<td>Symbol inclusive OR.</td>
</tr>
<tr>
<td>-</td>
<td>Used only with [ ]. Represents a range of acceptable symbols.</td>
</tr>
</tbody>
</table>

### FIELD NAME | DEFAULT VALUE | INDICATES
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace Host</td>
<td>0.0.0.0</td>
<td>The address of the remote device where trace output should be sent.</td>
</tr>
<tr>
<td>Trace Host Port</td>
<td>0</td>
<td>The port number of the remote device where trace output should be sent.</td>
</tr>
<tr>
<td>Trace SIP</td>
<td>Disabled</td>
<td><em>(For SIP Mode Only)</em> Whether the trace output includes SIP information.</td>
</tr>
<tr>
<td>UDP Trace Log</td>
<td>Disabled</td>
<td>Whether the trace output includes UDP log information.</td>
</tr>
</tbody>
</table>
14.31 To apply the changes, click Update.

14.32 Authentication: The Authentication page allows you to change the password to access the IP Phone Web Client.

NOTE: Passwords are case-sensitive.

14.33 To change the password:

1. Enter the current password in the Current Password field, if there is one.
2. Enter the new password once in the New Password field and again in the Confirm New Password field.

14.34 When the endpoint is in SIP mode, you can also change the password to access the SIP Server.

14.35 To change the SIP authentication password:

1. Enter the authentication name that is used to access the SIP Server.
2. Enter the current password in the Current Authentication Password field, if there is one.
3. Enter the new password once in the New Authentication Password field and again in the Confirm New Authentication Password field.

14.36 To apply the new password, click Update.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet/Serial Trace Log</td>
<td>Disabled</td>
<td>Whether the trace output includes Telnet/serial log information.</td>
</tr>
</tbody>
</table>
14.37 SIP: The SIP Call Client Configuration page shows SIP-related information.

**NOTE:** This page is only available when the endpoint is in SIP mode.

14.38 This page contains the fields described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DEFAULT VALUE</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Extension/Name</td>
<td>1000</td>
<td>The name used by the endpoint for authentication with the SIP proxy server.</td>
</tr>
<tr>
<td>Display Name</td>
<td>1000</td>
<td>The user or registration name on the endpoint that is shown if the endpoint has a display.</td>
</tr>
<tr>
<td>Proxy Server IP Address</td>
<td>192.168.200.100</td>
<td>The IP address of the primary SIP proxy Server.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>5060</td>
<td>The port of the primary SIP proxy Server.</td>
</tr>
<tr>
<td>Register Server IP Address</td>
<td>192.168.200.100</td>
<td>The IP address of the primary SIP registration Server.</td>
</tr>
<tr>
<td>Register Server Port</td>
<td>5060</td>
<td>The port of the primary SIP registration Server.</td>
</tr>
<tr>
<td>Register Period</td>
<td>3600 seconds (one hour)</td>
<td>The time between synchronizations (in progress).</td>
</tr>
<tr>
<td>Voice Mail</td>
<td>VOICEMAIL</td>
<td>The voice mail string that is displayed when the MSG button is pressed or the Message feature code is entered.</td>
</tr>
</tbody>
</table>

14.39 To apply the changes, click **Update**.
14.40 Feature Code: The Feature Code page shows the setting for the SIP mode feature codes. The available features and their default feature codes are shown in the table below. For details about each feature, refer to the appropriate endpoint User Guide for SIP Mode.

**NOTE:** This page is only available when the endpoint is in SIP mode.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DEFAULT FEATURE CODE</th>
<th>FEATURE</th>
<th>DEFAULT FEATURE CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer</td>
<td>351</td>
<td>Hold</td>
<td>336</td>
</tr>
<tr>
<td>Attendant</td>
<td>0</td>
<td>LCD Contrast Adjustment</td>
<td>303</td>
</tr>
<tr>
<td>Conference</td>
<td>5</td>
<td>Message</td>
<td>365</td>
</tr>
<tr>
<td>Do-Not-Disturb On</td>
<td>370</td>
<td>Mute</td>
<td>314</td>
</tr>
<tr>
<td>Do-Not-Disturb On/Off</td>
<td>372</td>
<td>Outgoing</td>
<td>8</td>
</tr>
<tr>
<td>Do-Not-Disturb Off</td>
<td>371</td>
<td>Redial</td>
<td>380</td>
</tr>
<tr>
<td>Emergency</td>
<td>911</td>
<td>Redirect Call</td>
<td>331</td>
</tr>
<tr>
<td>Forward All</td>
<td>355</td>
<td>Reverse Transfer</td>
<td>4</td>
</tr>
<tr>
<td>Group Listen</td>
<td>312</td>
<td>Ring Tone Select</td>
<td>398</td>
</tr>
<tr>
<td>Headset On</td>
<td>315</td>
<td>Show IP*</td>
<td>300</td>
</tr>
<tr>
<td>Headset On/Off</td>
<td>317</td>
<td>Show Version*</td>
<td>9928</td>
</tr>
<tr>
<td>Headset Off</td>
<td>316</td>
<td>Transfer</td>
<td>345</td>
</tr>
</tbody>
</table>

* For details about the Show IP and Show Version features, see page 54.

14.41 To apply the changes, click Update.

14.42 To default the feature codes, click Default.

14.43 VLAN: The VLAN Configuration page allows you to specify the VLAN IDs of the downlink (PC) ports and endpoint (IP Phone) port. It also allows you to enable LAN QoS if the endpoint is connected to a switch that supports 802.1P. See page 22 for details.

14.44 To specify the VLAN ID, enter the VLAN ID for each port.

**NOTE:** The available ports vary depending on the IP endpoint (see page 23).

14.45 To enable the LAN QoS feature, check Enable LAN QoS. See page 25 for details.

**NOTE:** The values of the QoS are pre-defined and cannot be changed.

14.46 To apply the changes, click Update.
Status

14.47 Network: The Network Status page shows network information. Both SIP and ITP modes have the same fields. The page contains the following fields.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Address</td>
<td>The MAC address of the endpoint.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the endpoint.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The network subnet mask.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The network gateway.</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>The IP address of the DHCP server that the end-point obtains.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>The IP address of the DNS server that the end-point uses.</td>
</tr>
<tr>
<td>Link Status</td>
<td>The link status of the network ports.</td>
</tr>
<tr>
<td>Negotiation</td>
<td>The negotiation status of the network ports.</td>
</tr>
<tr>
<td>Speed</td>
<td>The connection speed of the network ports.</td>
</tr>
<tr>
<td>Duplex</td>
<td>The connection mode of the network ports.</td>
</tr>
</tbody>
</table>

14.48 Firmware: The Firmware Information page shows current firmware information. Both SIP and ITP modes use the same page. This page contains the fields described in the following table.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>The endpoint application type, such as the Model 8600, 8660, 8662.</td>
</tr>
<tr>
<td>Image Version</td>
<td>The version of the application.</td>
</tr>
<tr>
<td>Phonex Version</td>
<td>The version of the Broadcom Phonex (PhoneExchange) software.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>The current date and time.</td>
</tr>
<tr>
<td>Boot Code Version</td>
<td>The version of boot image version number.</td>
</tr>
<tr>
<td>Boot Code Date/Time</td>
<td>The current boot code date and time.</td>
</tr>
<tr>
<td>Hardware Type</td>
<td>The model type (see page 52 for details).</td>
</tr>
<tr>
<td>Tool Information</td>
<td>The versions of the tools (e.g., gcc, GNU assembler, etc.).</td>
</tr>
</tbody>
</table>

14.49 License: Displays the end user license agreement.
14.50 Volume: The Volume Status page shows current firmware information. This page contains the fields described in the following table.

**NOTE:** This page is only available when the endpoint is in SIP mode.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ringer</td>
<td>The volume level for the ring tone. The range is 1-8.</td>
</tr>
<tr>
<td>Speakerphone Call</td>
<td>The volume level for the speakerphone call. The range is 1-8.</td>
</tr>
<tr>
<td>Speakerphone Tone</td>
<td>The volume level for the speakerphone tone. The range is 1-8.</td>
</tr>
<tr>
<td>Handset Call</td>
<td>The volume level for the handset call. The range is 1-8.</td>
</tr>
<tr>
<td>Handset Tone</td>
<td>The volume level for the handset tone. The range is 1-8.</td>
</tr>
<tr>
<td>Headset Call</td>
<td>The volume level for the headset call. The range is 1-8.</td>
</tr>
<tr>
<td>Headset Tone</td>
<td>The volume level for the headset tone. The range is 1-8.</td>
</tr>
</tbody>
</table>
14.51 **Image Upgrade:** The Image Upgrade page shows current image version information and download status. This page contains the fields described in the following table. Both ITP and SIP modes have the same fields.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>INDICATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Version</td>
<td>The image version of the endpoint-specific code.</td>
</tr>
<tr>
<td>Configuration Image Version</td>
<td>The version of the configuration image.</td>
</tr>
<tr>
<td>Download Status</td>
<td>The status of the TFTP download.</td>
</tr>
<tr>
<td>Last Download Error Page</td>
<td>The additional error information concerning the status of the last TFTP application image update (see page 73 for details).</td>
</tr>
</tbody>
</table>


**Command**

14.53 **Configuration:** The Configuration page allows you to synchronize the configuration.

14.54 **To synchronize the configuration**, click **Synch**.

14.55 **To default the configuration**, click **Default**.

14.56 **Reset:** The Reset Hardware page allows you to reset the endpoint.

14.57 **To reset the endpoint**, click **Reset**.
C. TFTP CONFIGURATION FILES

14.58 This section describes all of the parameters that are available in the global and device-specific configuration files. You may add or edit any of the parameters in the configuration files. The files contain the following areas:

- Network Settings (see page 159)
- ITP Mode Settings (see page 161)
- SIP Mode Settings (see page 162)
- SIP Dial Plan (see page 163)
- SIP Audio Settings (see page 164)
- Software Images (see page 165)
- Trace Settings (see page 166)

14.59 For details about how to download the configuration files from a TFTP server, see page 66.

NOTE: The configuration files overwrite any information that are programmed in the Axxess system when the endpoint is in ITP mode (see page 167) or in the Setup Wizard on the Model 8690 (see page 168).

ALSO: An endpoint in ITP mode receives configuration information from the Axxess system only after the endpoint comes online. The endpoint ignores any of the basic settings as if the “overwrite local settings” was permanently set to “disabled” for this circuit on the Axxess system.

14.60 The format of the configuration files is the Windows .ini format, “field name: value”. Although both the device-specific and global configuration files can contain any subset or all of the configuration fields, you only have to include the fields needed to configure the device.

14.61 In SIP mode, you can program all of the configuration options in the configuration files because there is no central configuration authority (not controlled by the Axxess system). In ITP mode, you can only program the basic settings and the software image information. All other configuration information is received from the Axxess system once the endpoint is connected.

14.62 For the endpoint to function in ITP mode, the following basic settings are required:

- The endpoint’s network settings (IP address, subnet mask, default gateway) including DHCP enable/disable
- IP address and TCP port number of the IPRC to which the endpoint belongs if not on the same LAN
- Logon password (not the same as the station password)

14.63 For the endpoint to function in SIP mode, the following basic settings are required:

- The endpoint’s network settings (IP address, subnet mask, default gateway) including DHCP enable/disable
- IP address and UDP port number of the SIP proxy server to which the endpoint belongs
- IP address and UDP port number of the SIP registrar server to which the endpoint belongs
- Endpoint extension or registration name
- Authentication name and password
Network Settings

14.64 The configuration files contain the network parameters as described in the following table. Some of the parameters can also be programmed in the IP Phone Web Client Administrative Session. The IP Phone Web Client field names and their reference pages that correspond to the parameters are also shown in this table.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFAULT</th>
<th>INDICATES</th>
<th>IP PHONE WEB CLIENT (PG#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>1</td>
<td>Whether to contact the DHCP server to obtain values for network-related parameters such as IP address, network gateway IP address, subnet mask, NTP, TFTP, domain name, DNS, VLAN ID, and more. The options are: 0 – There is no DHCP server. Use static values. 1 – Contact the DHCP server to obtain the values</td>
<td>IP Address Assignment (p147)</td>
</tr>
<tr>
<td>static_ip</td>
<td>192.168.200.201</td>
<td>The static IP address of the endpoint (when DHCP is disabled).</td>
<td>Static (Default) IP Address (p147)</td>
</tr>
<tr>
<td>static_snm</td>
<td>255.255.255.0</td>
<td>The default network subnet mask for the endpoint.</td>
<td>Default Network Subnet Mask (p147)</td>
</tr>
<tr>
<td>static_gw</td>
<td>192.168.200.201</td>
<td>The default IP gateway address for the endpoint.</td>
<td>Default IP Gateway Address (p147)</td>
</tr>
<tr>
<td>tftp_url</td>
<td>192.168.200.202</td>
<td>The IP address of the TFTP server where configuration files for this endpoint reside. Required if the DHCP does not provide the TFTP address. You can also include the path to the profile file, if desired. For example, if the TFTP server IP address is “192.168.200.150” and the path file is “/basic_sip,” then you can specify the URL as “192.168.200.150/basic_sip.”</td>
<td>TFTP Server IP Address (p147)</td>
</tr>
<tr>
<td>http_port</td>
<td>8080</td>
<td>The TCP port number of the Web server. A zero value disables the HTTP server.</td>
<td>N/A</td>
</tr>
<tr>
<td>operm_mode</td>
<td>1</td>
<td>Whether the endpoint will be in SIP mode or ITP mode after the next reset. 0 – SIP Mode 1 – ITP Mode</td>
<td>SIP Mode (p151)</td>
</tr>
<tr>
<td>update_interval</td>
<td>3600 seconds (one hour)</td>
<td>The time, in seconds, between automatic configurations updates from the TFTP server. The interval should vary among endpoints to prevent massive simultaneous updates. The range of the values are 0-4294967295. A zero value disables the automatic update.</td>
<td>N/A</td>
</tr>
<tr>
<td>static_domain</td>
<td>0</td>
<td>The static domain name of the network if DHCP is not used.</td>
<td>N/A</td>
</tr>
<tr>
<td>static_dns_ip</td>
<td>0.0.0.0</td>
<td>The IP address of the DNS server if DHCP is not used.</td>
<td>N/A</td>
</tr>
<tr>
<td>PARAMETER</td>
<td>DEFAULT</td>
<td>INDICATES (Continued)</td>
<td>IP PHONE WEB CLIENT (PG#)</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>static_ntp_ip</td>
<td>0.0.0.0</td>
<td>The IP address of the NTP server if DHCP is not used. DHCP may also supply a NTP server. If this parameter has an IP address, it overwrites the DHCP’s NTP server IP address.</td>
<td>N/A</td>
</tr>
<tr>
<td>tftp_update_enable</td>
<td>1</td>
<td>Whether to perform the configuration updates from the TFTP server. The options are:</td>
<td>Enable TFTP Configuration Update (p148)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 – Disable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 – Enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If this flag is disabled (set to 0) and the DHCP server provides the TFTP IP address and path, the endpoint would not start the update.</td>
<td></td>
</tr>
<tr>
<td>tftp_url_dhcp</td>
<td>1</td>
<td>Whether to overwrite the TFTP URL in the TFTP Server IP Address field, listed above, with the TFTP server IP address and path from the DHCP server. The options are:</td>
<td>Use DHCP for TFTP Server and Path (p148)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 – Ignore the TFTP server IP address and path from the DHCP server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 – Program the TFTP server IP address and path from the DHCP server to the tftp_url configuration parameter on the endpoint.</td>
<td></td>
</tr>
<tr>
<td>lan_pq_port</td>
<td>0x0000</td>
<td>Specifies which of the Ethernet ports support 802.1P/Q.</td>
<td>VLAN Configuration (p154)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> This parameter does not apply to endpoints with v1.1.x or later firmware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the Model 8690:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x0001 – LAN/PWR Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x0002 – P1 Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x0004 – P2 Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x0008 – P3 Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the Models 8620/8622 and 8662:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x0001 – LAN/PWR Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x0002 – PC Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Models 8600:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x0001 – LAN/PWR Port</td>
<td></td>
</tr>
<tr>
<td>telnet_port</td>
<td>23</td>
<td>The port number of the Telnet server. A zero value disables the Telnet server.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### ITP Mode Settings

**14.65** The configuration files contain the ITP mode-related parameters as described in the following table. Some of the parameters can also be programmed in the IP Phone Web Client Administrative Session. The IP Phone Web Client field names and their reference pages that correspond to the parameters are also shown in this table.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFAULT</th>
<th>INDICATES</th>
<th>IP PHONE WEB CLIENT (PG#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlanid</td>
<td>0</td>
<td>Specifies the VLAN ID of the phone port.</td>
<td>VLAN Configuration (p154) For details about VLAN ID, see page 22</td>
</tr>
<tr>
<td>dwnlnk_vlanid_1</td>
<td>0</td>
<td>Specifies the VLAN ID of the PC downlink port.</td>
<td></td>
</tr>
<tr>
<td>dwnlnk_vlanid_2</td>
<td>0</td>
<td>Specifies the VLAN ID of the PC downlink port 2 of the Model 8690.</td>
<td></td>
</tr>
<tr>
<td>dwnlnk_vlanid_3</td>
<td>0</td>
<td>Specifies the VLAN ID of the PC downlink port 3 of the Model 8690.</td>
<td></td>
</tr>
<tr>
<td>network_flags</td>
<td>0x00000000</td>
<td>Specifies whether the LAN QoS feature is enabled.</td>
<td>VLAN Configuration (p154) For details about LAN QoS, see page 25</td>
</tr>
<tr>
<td>cc_srv_ip</td>
<td>xxx.xxx.xxx.xxx</td>
<td>The IP address of the IPRC to which this IP endpoint is currently connected (the same value that is programmed in Axxess system).</td>
<td>Remote Server IP Address (p148)</td>
</tr>
<tr>
<td>cc_srv_tcp_port</td>
<td>5566</td>
<td>The port number for TCP call control packets that are transmitted from this endpoint for the current connection. This value may or may not be what is programmed in the Axxess system.</td>
<td>IP Terminal TCP Call Control Port (p148)</td>
</tr>
<tr>
<td>cc_srv_udp_port</td>
<td>5567</td>
<td>The port number for all UDP (audio) packets that are transmitted from this endpoint for the current connection. This value may or may not be what is programmed in the Axxess system.</td>
<td>IP Terminal General Purpose UDP Port (p148)</td>
</tr>
</tbody>
</table>
### SIP Mode Settings

When the endpoint is in SIP mode, the parameters described in the following table are available. Some of the parameters can also be programmed in the IP Phone Web Client Administrative Session. The IP Phone Web Client field names and their reference pages that correspond to the parameters are also shown in this table.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFAULT</th>
<th>INDICATES</th>
<th>IP PHONE WEB CLIENT (PG#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip_name</td>
<td>1000</td>
<td>The number used when registering. For example, 21295.</td>
<td>N/A</td>
</tr>
<tr>
<td>sip_display_name</td>
<td>1000</td>
<td>The user or registration name on the endpoint that is shown if the endpoint has a display.</td>
<td>Display Name (p153)</td>
</tr>
<tr>
<td>sip_reg_ip</td>
<td>192.168.200.100</td>
<td>The IP address of the primary SIP registration Server.</td>
<td>Register Server IP Address (p153)</td>
</tr>
<tr>
<td>sip_reg_port</td>
<td>5060</td>
<td>The port of the primary SIP registration Server.</td>
<td>Register Server Port (p153)</td>
</tr>
<tr>
<td>sip_proxy_ip</td>
<td>192.168.200.100</td>
<td>The IP address of the primary SIP proxy Server.</td>
<td>Proxy Server IP Address (p153)</td>
</tr>
<tr>
<td>sip_proxy_port</td>
<td>5060</td>
<td>The port of the primary SIP proxy Server.</td>
<td>Proxy Server Port (p153)</td>
</tr>
<tr>
<td>sip_authname</td>
<td>1000</td>
<td>The name used by the endpoint for authentication with the SIP proxy server.</td>
<td>Phone Extension/Name (p153)</td>
</tr>
<tr>
<td>sip_authpassw</td>
<td>N/A</td>
<td>The password for SIP authentication (up to nine digits) if the proxy server challenges the registration.</td>
<td>Authentication (p152)</td>
</tr>
<tr>
<td>sip_reg_period</td>
<td>3600 seconds (one hour)</td>
<td>The time between synchronizations (in progress).</td>
<td>Register Period (p153)</td>
</tr>
<tr>
<td>sip_voicemail</td>
<td>VOICEMAIL</td>
<td>The voice mail string that is displayed when the MSG button is pressed or the Message feature code is entered.</td>
<td>Voice Mail (p153)</td>
</tr>
</tbody>
</table>
SIP Dial Plan

14.67 When the endpoint is in SIP mode, the parameters described in the following table are available. Some of the parameters can also be programmed in the IP Phone Web Client Administrative Session. The IP Phone Web Client field names and their reference pages that correspond to the parameters are also shown in this table.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFAULT</th>
<th>INDICATES</th>
<th>IP PHONE WEB CLIENT (PG#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ic_dial_plan</td>
<td>1xxx</td>
<td>The dial plan mask that this endpoint uses to determine valid dial strings for end of dialing</td>
<td>IC Dial Plan (p151)</td>
</tr>
<tr>
<td>trunk_dial_plan</td>
<td>9xxxx</td>
<td>for IC, trunk, or outgoing calls. If the syntax is bad, you cannot dial calls. The acceptable</td>
<td>Trunk Dial Plan (p151)</td>
</tr>
<tr>
<td>out_dial_plan</td>
<td>[2-9]xxxx [-]{1}[2-9]xxxxxx[011][1-9]xxxxx</td>
<td>symbols for a dial plan are described in the table below.</td>
<td>Outgoing Dial Plan (p151)</td>
</tr>
</tbody>
</table>

SYMBOL | MEANING
--- | ---
0-9 | Digit 0-9.
\* | Any digit 0-9.
\#, \* | Dialpad entry (*, #).
| | Expression inclusive OR.
+ | Zero or more of the preceding digit(s) or [ ] expression. For example, “+\#” means that a dial plan can accept any dial string that ends with “\#,” such as “1234\#” or “\#” (zero digits). Also “[2-9]+\#” means that a dial plan can accept any dial string that begins with any digit “2” through “9” followed by “\#.”
| | Symbol inclusive OR.
- | Used only with [ ]. Represents a range of acceptable symbols.
SIP Audio Settings

14.68 The configuration files contain the audio parameters as described in the following table. Some of the parameters can also be programmed in the IP Phone Web Client Administrative Session. The IP Phone Web Client field names and their reference pages that correspond to the parameters are also shown in this table.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFAULT</th>
<th>INDICATES</th>
<th>IP PHONE WEB CLIENT (PG#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tx_codec</td>
<td>0</td>
<td>The encoding/decoding codec preference for this endpoint. The available decoder options are:</td>
<td>Codec Type (p149)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 – G.711 u-law</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 – G.711 A-law</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 9 – G.729a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> Currently, Option 13 (Broadvoice Wideband 32 Kbps) is not supported.</td>
<td></td>
</tr>
<tr>
<td>audio_frm</td>
<td>3</td>
<td>The number of audio frames per output audio RTP packet.</td>
<td>Number of Audio Frames (p149)</td>
</tr>
<tr>
<td>audio_port</td>
<td>5004</td>
<td>The port where the endpoint transmits and receives RTP packets. This port must be an even number; each connection uses the next available even-numbered port.</td>
<td>Audio Port (p149)</td>
</tr>
<tr>
<td>differcnt</td>
<td>46</td>
<td>The IP precedence value.</td>
<td>Diffserv (p149)</td>
</tr>
<tr>
<td>audio_mode</td>
<td>0x00000001</td>
<td>Specifies whether the endpoint sends audio packets during periods of silence.</td>
<td>Suppress Silence (p149)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x01 - Enables silence suppression (i.e. do not send packets during periods of silence)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x02 - Uses RFC 2833 for the DTMF transmission method (default is to send DTMF in band in the codec)</td>
<td></td>
</tr>
</tbody>
</table>
Software Images

14.69 The configuration files contain the endpoint parameters as described in the following table. Some of the parameters can also be programmed in the IP Phone Web Client Administrative Session. The IP Phone Web Client field names and their reference pages that correspond to the parameters are also shown in this table.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFAULT</th>
<th>INDICATES</th>
<th>IP PHONE WEB CLIENT (PG#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxx_image_ver</td>
<td>xx-yy-zz</td>
<td>The image version of the endpoint-specific code (e.g., xxxx_image_ver=1-2-13 (where the xxxx indicates the model name, such as the 8662).</td>
<td>Image Version (p150)</td>
</tr>
<tr>
<td>xxxx_image_url</td>
<td>xxx.xxx.xxx.xxx/image/image-&lt;ss&gt;.bin. The &lt;ss&gt; is the image version from &quot;xxxx_image_ver.&quot;</td>
<td>The IP address or URL (up to 79 digits) of the image TFTP server. Required if the DHCP does not provide the TFTP address. You can also include the path to the profile file, if desired. For example, if the TFTP server IP address is &quot;192.168.200.150&quot; and the path file is &quot;image,&quot; then you can specify the URL as &quot;192.168.200.150/image/image-1-3-4.bin.&quot;</td>
<td>Image URL (p150)</td>
</tr>
<tr>
<td>8690_dsp_image_ver</td>
<td>N/A</td>
<td><em>(For the Model 8690 Only)</em> The call control firmware version string.</td>
<td>N/A</td>
</tr>
<tr>
<td>8690_dsp_image_url</td>
<td>N/A</td>
<td><em>(For the Model 8690 Only)</em> The IP address or URL of the image TFTP server of the call control firmware image. Required if the DHCP does not provide the TFTP address. You can also include the path to the profile file, if desired. For example, if the TFTP server IP address is &quot;192.168.200.150&quot; and the path file is &quot;image,&quot; then you can specify the URL as &quot;192.168.200.150/image/image-1-3-4.bin.&quot;</td>
<td>N/A</td>
</tr>
<tr>
<td>8690_os_image_ver</td>
<td>N/A</td>
<td><em>(For the Model 8690 Only)</em> The Windows CE firmware version string.</td>
<td>N/A</td>
</tr>
<tr>
<td>8690_os_image_url</td>
<td>N/A</td>
<td><em>(For the Model 8690 Only)</em> The IP address or URL of the image TFTP server of the Windows CE firmware image. Required if the DHCP does not provide the TFTP address. You can also include the path to the profile file, if desired. For example, if the TFTP server IP address is &quot;192.168.200.150&quot; and the path file is &quot;image,&quot; then you can specify the URL as &quot;192.168.200.150/image/image-1-3-4.bin.&quot;</td>
<td>N/A</td>
</tr>
<tr>
<td>8690_gui_image_ver</td>
<td>N/A</td>
<td><em>(For the Model 8690 Only)</em> The user interface firmware version string.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Trace Settings

14.70 The configuration files contain the trace parameters as described in the following table. Some of the parameters can also be programmed in the IP Phone Web Client Administrative Session. The IP Phone Web Client field names and their reference pages that correspond to the parameters are also shown in this table.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFAULT</th>
<th>INDICATES (Continued)</th>
<th>IP PHONE WEB CLIENT (PG#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>trace_ip</td>
<td>0.0.0.0</td>
<td>The address of the remote device where trace output should be sent.</td>
<td>Trace Host (p151)</td>
</tr>
<tr>
<td>trace_port</td>
<td>0</td>
<td>The port number of the remote device where trace output should be sent.</td>
<td>Trace Host Port (p151)</td>
</tr>
</tbody>
</table>
| trace_flags       | 0x00000000 | Enable specific trace features.  
• 0x01 - Turn on SIP traces  
• 0x02 - Turn on UDP traces  
• 0x10 - Turn on serial and telnet logs  
To turn all of the trace features on, use the following value: 0x13.  
                                                                 | Trace SIP (p151)  
                                                                 | UDP Trace Log (p151)  
                                                                 | Telnet/Serial Trace Log (p152)           |
D. AXXESS DATABASE PROGRAMMING

14.71 When the IP endpoint is in ITP mode, the Axxess system sends down configuration information when the IP endpoint powers up. However, the only fields that the Axxess system can update are as follows:

- MAC Address
- Telnet Server
- Password (changes the password on the IPRC-side, not the endpoint-side).
- Audio RTP Type of Service
- Audio Stream Receive Port
- Call Control Timeout
- IP Terminal TCP Call Control Port
- IP Terminal General Purpose UDP Port

14.72 These fields are located under System\Devices and Feature Codes\Stations\<IP station>\IP Settings\Network Configuration in Axxess Database Programming. Refer to the Addendum to the Axxess v8.0 Installation and Maintenance Manual for details.

**NOTE:** The rest of the fields must come from the areas that are programmed in a higher priority configuration source, such as the internal database, the self-programming mode, the configuration files, etc.
E. WINDOWS CE .NET PROGRAMMING (MODEL 8690 ONLY)

14.73 This section provides information about Model 8690 programming using the Model 8690 client application on Windows CE .NET. For complete information about how to use the 8690 client application, refer to the Model 8690 Administrator’s Guide (document part no. 550.8120) and the appropriate Model 8690 User Guide (ITP or SIP mode). The following issues are discussed in this section:

- Running the Setup Wizard (see page 168)
- Upgrading the Model 8690 (see page 169)
- Reformatting the Model 8690 Flash File System (see page 172)
- Installing the Model 8690 (see page 173)
- Configuring Phone Ports for a VLAN (see page 174)

Running the Setup Wizard

14.74 The first time the 8690 client application runs, the Setup Wizard launches. Once you successfully complete the Setup Wizard, it will not run again.

NOTE: The Default Configuration option on the Advanced menu resets the endpoint to its default state. If the Default Configuration option is run, the Setup Wizard will run automatically the next time the client application starts.

14.75 To run the Setup Wizard:

1. EITHER, Press Network and Dial-up Connections (under Windows CE .NET\Control Panel).
   OR, Press the Unified Communicator® Tray Client icon ( ), then press Advanced – Run Setup Wizard from the menu. Press Next at the opening screen.
   
   NOTE: Unified Communicator is included in the Model 8690 client application package. This application provides simplified access to endpoint functionality, advanced endpoint features, and presence management options. For more details, refer to the latest version of the Unified Communicator Installation and Configuration Manual.

2. Select a network adapter from the drop-down list or accept the default adapter. Press Properties.

3. Press the option Obtain an IP address via DHCP. If the endpoint is not using DHCP, then specify the hostname or IP address of the endpoint, the subnet mask, the default gateway, and the DNS server. Then press Next.

4. In the Phone Configuration Download screen, enter the hostname or IP address of the computer hosting the endpoint configuration file in the format: 172.34.56.78.

5. At the Unified Communicator screen, enter the following information:

   NOTE: If you do not enter this information now, you will be prompted for it each time you log on or power on the endpoint.

   - Web Address: Enter the URL for the UC computer where your account is located.
   - Username: Enter your account username.
   - Password: Enter your account password.
• **Automatically log on:** Enable this option and you will not be prompted for logon information each time the endpoint starts or you select Log on from the Tray Client icon menu. Press **Next**.

6. Enable or disable the option to log on to UC upon completing the Setup Wizard. Press **Finish**.

**Upgrading the Model 8690**

14.76 The 8690 client application can be upgraded automatically or manually.

**NOTE:** If an upgrade fails, or if the application is partially installed, you must reformat the flash file system on the endpoint. See page 172 for instructions on how to reformat the Model 8690 flash file system.

14.77 **Upgrade the Model 8690 Automatically**

14.78 The 8690 periodically checks for the following upgrades:

- **Firmware:** You are notified that the upgrade is starting, and the client application continues to run. You can monitor the progress of the upgrade on the six-line display. When the upgrade is complete, the endpoint resets.

- **Client Application:** The client application exits and the upgrade application launches. The upgrade application downloads the new version of the client application from the TFTP server, and you can monitor the download progress. When the download completes, the upgrade application launches the Windows CE .NET installation mechanism and installs the new client application version. At this point, you are prompted for where you would like to install the new files (the default is `\Mounted Volume\8690 Phone`). Press **OK** to continue with the installation. Press **Yes** when prompted to overwrite existing files. You are notified when the upgrade is complete. The upgrade application launches the new version of the client application and then exits.

- **Operating System:** The client application exits, and the upgrade application launches. The upgrade application erases the existing version of the operating system from the persistent memory. Upon completion, the upgrade application downloads the new version of the operating system from the TFTP server. As the new version of the operating system is downloaded, it is simultaneously written to persistent memory, and you can monitor the progress. When the download and installation completes, you are notified and the endpoint resets. The registry settings are lost when the operating system is upgraded. This means that certain client application settings stored in the registry are lost as well. These include the session and diagnostic options.

---

**CAUTION**

Do not press **Cancel** when the installation dialog box prompts you to select a directory for the new files. At this point the previous client application has been deleted and if you cancel the upgrade, you will have to manually reinstall the client application. Also, do not change the default location (`\Mounted Volume\8690 Phone`) specified in the installation dialog box. The client application must be installed in the Mounted Volume folder to survive a reset or an upgrade to the operating system.
7. When an upgrade is available, the Software Upgrade dialog box opens, and you are prompted to install the upgrade. To install the upgrade immediately, press **OK**. To install the upgrade later, you can set a reminder (1 hour, 1 day, or 3 days). When the reminder timer has expired, the Software Upgrade dialog box automatically prompts you to install the pending upgrade.

**14.79 Upgrade the Model 8690 Manually**

**14.80** Although the Model 8690 automatically checks for upgrades, you can manually upgrade the Model 8690 by running the Auto Upgrade feature. If there are no new upgrades available, you will not be notified, and your endpoint will function normally. If there is an upgrade available, the Software Upgrade dialog box opens, and you are prompted to install the upgrade. You can choose to install the upgrade immediately by pressing **OK** or set a reminder to install it later.

**14.81 To run the Auto Upgrade feature:**

1. Press the System Tray icon, then press Advanced – Auto Upgrade – **Check for New Versions**. The upgrade search dialog box opens.

2. Press **OK** to allow the system to search for software upgrades. You are not informed if upgrades are not available.

**14.82** In addition to running the Auto Upgrade feature, you can view, install, or cancel pending upgrades using the Advanced options.

**14.83 To view and install pending upgrades:**

1. Press the System Tray icon, then press Advanced – Auto Upgrade – **Pending Upgrades**. The Pending Upgrades dialog box opens and displays the status for the following:
   - Firmware
   - Client Application
   - Operating System

**NOTE:** The **Upgrade Now** option indicates a pending software upgrade.

2. Press **Upgrade Now** next to the upgrade you want to install. There is one button for each upgrade type.

3. When the Software Upgrade dialog box opens, press **OK** to install the upgrade.
14.84 To cancel pending upgrades:

1. Press the System Tray icon, then press Advanced – Auto Upgrade – **Pending Upgrades**. The Pending Upgrades dialog box opens and displays the status for the following:
   - Firmware
   - Client Application
   - Operating System

2. Press **Cancel** next to the upgrade that you want to cancel. There is one button for each upgrade type.

3. Press **OK**.
Reformatting the Model 8690 Flash File System

14.85 Installing the client application on the Model 8690 may fail if the endpoint does not have sufficient memory resources or if the endpoint loses power before the upgrade is complete. If the upgrade fails, or if the application is partially installed (see the dialog boxes below), it is strongly recommended that you reformat the flash file system on the endpoint.

14.86 To reformat the flash file system:

1. Press Start - Settings - Control Panel.
2. Double-press Storage Manager.
3. Press Dismount, and then press Format. The following dialog box appears.

4. Press Yes to erase all data.
5. Press OK to close the Format store succeeded dialog box.
6. In the Storage Properties dialog box, press New to create a new partition.
7. Enter a name for the partition, and then press OK.
10. Verify that the Quick Format option is selected and press Start.
11. Press Yes to format.
12. Press OK to close the Format dialog box.
13. In the Partition Properties dialog box press Mount and then OK.
14. Close the Storage Properties dialog box and then exit the Control Panel.
15. Reinstall the client application as described on the following page.

CAUTION

Any data or files saved in the Mounted Volume folder will be lost. To avoid loss of data, the data should be saved to a host, a memory card, or a location on the network.
Installing the Model 8690

14.87 The following lists the system requirements for installing the 8690 client application:

- Windows CE .NET v4.2

**NOTE:** For details about Windows CE .NET Operating System, refer to the latest version of the Axxess Administrator’s Guide.

- 400 MHz Processor, 128 MB RAM
- 5 MB Persistent Storage

14.88 The 8690 client application is distributed in a single CAB (cabinet) file. A CAB file contains one or more application files compressed into a single archive file (just like a WinZip® file).

14.89 To install the client application on the Model 8690:

1. Obtain the latest CAB file, `8690Phone.8690_CEDOTNET_MIPSII.CAB`, from the Inter-Tel Web site.
2. Copy the CAB file onto your Model 8690 endpoint.
3. Double-click on the CAB file to launch the installation program.
4. The display shows the default location, `\Mounted Volume\8690 Phone`, where the application will be installed. Click **OK** to accept the default location.

**NOTE:** If you choose to install the product in some location other than the default, you must make sure that you install it in the flash file system (somewhere in the Mounted Volume folder). This insures that the files will persist in the event that the endpoint is reset. When the installation completes, launch `8690Phone.exe` to start the client application.

**ALSO:** If an installation or update fails, or if the application is partially installed, you must reformat the flash file system on the endpoint. See page 172 for instructions on how to reformat the Model 8690 flash file system.
Configuring Phone Ports for a VLAN

14.90 You can place VLAN tags to improve voice quality and security (see page 22 for details).

14.91 To specify VLAN IDs:

1. Press Start - Settings - Control Panel.
3. Double-press AUMAC1. The following screen appears.

4. Press the VLAN tab.
5. Press the VLAN ID (1-4094) for the Phone Port and the Downlink Ports using the associated scroll buttons.
6. Press OK.
7. Save the registry.
15. IP LOCAL LOOP SUPPORT

15.1 System v7.0 or later support IP-based solutions for providing local Public Switched Telephone Network (PSTN) connectivity using the IPRC and a third-party Media Gateway Control Protocol (MGCP) gateway. The system requires software v7.0 or later and IPRC firmware v1.5.1 or later. The firmware expands the support of 32 IP endpoints/SLAs/SoftPhones to include Loop Start Adapters (LSAs). Support for IP-based local loop requires no new premium feature units.

**NOTE:** You must manually upload firmware to the IPRC using the Upload Utility program. There is no auto-download for the IPRC software from call processing. The utility supports an RS-232 method as well as a network connection for getting the firmware onto the IPRC. See page 58 for details on how to upload firmware to the IPRC.

15.2 Up to 32 ports of an IPRC can be programmed to be loop start adapter ports (MGCP gateway trunks). The IPRC statically maps Voice over IP (VoIP) resources on a one-to-one, non-blocking basis for each loop start port within the MGCP device.

15.3 Inter-Tel currently supports the following MGCP gateways:

- **AudioCodes MP-100 Foreign Exchange Office (FXO) MGCP Gateway:** Supports up to four loop start line (FXO) ports. For configuration instructions, see page 178.

- **AudioCodes MP-104 FXO MGCP Gateway:** Supports up to four loop start line (FXO) ports. Although the MP-104 is similar to the MP-100, each gateway uses a different switch type for configuring the device. The MP-100 uses DIP switches, and the MP-104 uses a command line switch (-fb). For configuration instructions, see page 189. See page 189 for details.

15.4 With system v9.0, the system supports SIP (Session Initiated Protocol) trunks to reach the CO in addition to MGCP trunks. SIP trunks allow the system to communicate with the CO via SIP-enabled gateways. As the SIP protocol becomes more and more popular, it is important to be able to communicate to SIP gateways in the IP-centric world. Inter-Tel currently supports the **AudioCodes™ MP-104 SIP gateway (with software version 4.2)**. See page 189 for details.

---

**CAUTION**

If an IP or SIP device user dials 911 from a remote location and an MGCP or SIP gateway is not present and/or functioning properly, the call will be placed from where the telephone system is located. Because 911 services use caller ID to help locate the caller, emergency service could be misdirected or delayed. Also, the 911 service contacted may be local to the system, but not to the IP or SIP device. All IP and SIP device users should be alerted to this situation and instructed to use a local telephone line for placing emergency calls if an MGCP or SIP gateway is not present and/or functioning properly. Also note that IP and SIP devices will not function in the event of a power failure at either the local site or the system location. Inter-Tel will not be held responsible for any problems resulting from an unavailable line that is connected to the MGCP or SIP gateway. Inter-Tel also recommends that users regularly test the MGCP or SIP gateway for dial tone.

15.5 When configured with an MGCP or SIP gateway, you can program the system so that when 911 is dialed from an IP device, the calling name and number associated with the IP device, not the system, is sent to the 911 operators. See page 177 for details.
15.6 The following diagrams illustrate a remote site without or with an MGCP gateway.

**FIGURE 8. Example of a Remote Site without an MGCP Gateway Application**

![Diagram of a remote site without an MGCP gateway.]

**FIGURE 9. Example of a Remote Site with an MGCP Gateway Application**

![Diagram of a remote site with an MGCP gateway.]

**NOTE:** The MGCP gateway is intended to connect to the PSTN. Connecting the MGCP gateway to single-line ports on other phone systems is currently not supported.

**WARNING**

**Positive Disconnect** - Signaling a call termination from the CO over an analog loop start line differs from CO to CO. Because the MGCP gateways detect this call event differently, you must pay particular attention to how the CO and the MGCP gateway detect far-end call termination. If the MGCP gateway you are installing relies on the CO to detect dial tone to signal a call termination, then a user could possibly hookflash and place a second call before the phone system realizes that a new call is being made. If this occurs, the appropriate toll restrictions are not applied to the new call. If the CO detects dial tone to indicate a terminated call, Inter-Tel recommends that the CO line used with the MGCP gateway be restricted to local calls.

Also, if the CO caller hangs up before the user, the user may still be connected to the CO until the user either hangs up or the MGCP gateway detects dial tone. The user may eventually hear reorder tone or a message that says, “If you would like to make a call...” until they hang up.
A. SYSTEM DATABASE PROGRAMMING

15.7 The following describes the brief instructions on how to program an LSA in Axxess Database Programming.

**NOTE:** For information about how to program an MGCP gateway on an IPRC v8.2.x firmware, refer to the *Addendum to the v8.0 Axxess Installation and Maintenance Manual*.

1. Program the cabinet slot where the IPRC is installed as a **DKSC-16**.

   **NOTE:** The “Amps Required” field will show that the card requires the 0.64 amps needed by a DKSC-16. However, an IPRC only requires 0.34 amps.

2. Program the port as **Single-Port LSA** (under System\Cabinets \Digital Keyset 16 Card).

3. Program the following fields that are specific to IPRC LSA. Program rest of the fields as you normally program standard loop start trunks.

   **NOTE:** Unless otherwise stated, all functionality of a standard loop start trunk is supported with the LSA.

   — **Service Type:** Call processing supports Caller ID on the LSA. The LSA has built-in Caller ID receivers and does not use shared Caller ID resources within the system. The resource manager within call processing is modified to have Caller ID receivers as an attribute for this device type and to use the local Caller ID receiver. If the service type is set to Caller ID, Caller ID messages are passed up through the IPRC to call processing. By default, it is set to None.

     **NOTE:** Caller ID receivers are not available on all MGCP gateways. Consult the device’s documentation for information on Caller ID support.

   — **DTMF Signaling:** LSA trunks can be set for dual-tone multi frequency (DTMF) signals. The IPRC provides for several delivery methods of DTMF, call progress tone information, and audio. DTMF dialing can be done from anywhere, and the digits will be correctly passed to the LSA (and vice versa). By default, it is set to Yes.

   **NOTE:** LSA timers and flags in Database Programming have no effect on the MGCP devices. Some of these settings can be directly programmed on the gateways. Consult the manuals provided by the manufacturer for more information.
B. AUDIOCODES MP-100 MGCP GATEWAY

15.8 This section describes how to install and configure the AudioCodes MP-100 gateway, shown below.

15.9 AudioCodes MP-100 FXO gateway supports up to four loop start line (FXO) ports. For details, refer to the *MP-100 User’s Manual & Installation Guide*.

Quick Start Installation Outline

15.10 The following steps outline the MP-100 installation. For details, refer to the pages shown in parentheses in each step.

15.11 To install the MP-100:

1. Unpack the box, and set up the MP-100 gateway device through the AudioCodes BootP/TFTP Server program (see page 179).

2. Configure the MP-100 application through the AudioCodes MP-100 Web administrator (see page 184).

3. Verify that the Call Agent IP address in the MGCP Client Settings page is the IPRC IP address (see page 185).

4. Configure the IPRC ports through the IPRC Web page, and verify the following:
   - The gateway is configured as an MGCP gateway and endpoint (the first circuit) and each additional endpoint is attached to the correct circuit. (See page 187.)
   - All information is correct (MAC address, IP address, etc.). (See page 84).
   - The connection is active in the Circuit Status page (see page 121).

15.12 The AudioCodes MP-100 Gateway is now ready for connection to the CO.
Setting Up the MP-100

15.13 To set up the MP-100:

1. Create a new directory (e.g., Audiocodes MP_100) in the Windows Explorer on your PC.

2. Detach and unpack the BootP and mp-100 zip files that were provided in the Inter-Tel AudioCodes MP-100 CD (part no. 827.9920) into this folder. You may want to create a subfolder for the BootP zip file within the same folder. The folder should look like the one shown below.

3. Verify that you have the following files in the directory.

   **NOTE:** The file names may be different depending on the version and date when the files were created.

   - **BOOT file** (e.g., ramMP100.cmp) — Contains a compressed, downloadable software image file.
   - **INI file** (e.g., mp100-2.ini) — Contains the default settings for the MP-100.
   - **Call Progress Tone file** (e.g., CPUSA.dat or CPUK.dat) — Contains all the tone and cadence definitions for US and European systems.

4. Open the mp100-2.ini file by using a word processor, such as Notepad, Microsoft® Word, etc. Add the IPRC IP address in the CallAgentIP field as shown below.
5. *If you are using Caller ID receivers,* you must also manually add a caller ID definition to the `mp100-2.ini` file. Enter `CallerIdTransportType = 3` at the end of the row in the Channel Params field, as shown below.

![New Definition for Caller ID](image)

6. Save and close the file.

7. Double-click on `Setup.exe` (in the BootP folder) to install the BootP Server.

8. Double-click on `bootp.exe` to launch the AudioCodes BootP/TPTF Server program. The following screen appears.

![AudioCodes BootP/TFTP Server](image)

**NOTE:** Ensure the AudioCodes BootP/TFTP Server application is the only BootP server running. If another server, such as the IPRC, is running at the same time, it may cause problems with the download.
9. Select **Preferences** from the Edit menu. The following dialog box appears. Enter (or browse to) the directory path, where three MP-100 configuration files and BootP files were unpacked, in the Directory text box. Once the correct directory path is displayed, click **OK**. The dialog returns to the main screen.

![Preferences dialog box](image)

10. Ensure the Dip Switch 3 in the up position and all others are down, as shown below.

![Dip Switch](image)
11. In the main BootP/TFTP Server screen, select **Clients** from the Services menu or click ![Add New Client Icon](image). The following dialog appears. The Client Configuration dialog allows the client (AudioCodes MP-100 gateway) to connect to the server application for code and configuration updates.

![Client Configuration](image)

12. Click the Add New Client icon ![Add New Client Icon](image). Highlight the desired client (if you have more than one client) in the list on the left, and configure the settings as described below.

- **Client MAC**: Enter the MAC address, which can be found on the bottom of the MP-100 device.
- **Client Name**: Enter the desired name (e.g. mp100).
- **Template**: Select `<none>`.
- **IP**: Enter the IP address of the MP-100.
- **Subnet**: Enter the subnet mask of the MP-100.
- **Gateway**: Enter the gateway IP address of the MP-100.
- **TFTP Server IP**: Enter the TFTP Server IP address, if applicable.
- **Boot File**: Select `ramMP100.cmp` from the drop-down list.
- **INI File**: Select `mp100-2.ini` from the drop-down list.
- **Call Agent**: Enter the IPRC IP address.

13. Click **Apply & Reset** and close the Client Configuration dialog. Make sure the Pause icon ![Pause Icon](image) is not pressed in the main screen.

**NOTE**: If you have more than one AudioCodes MP-100 gateway, repeat steps 8 and 9.
14. Attach up to four loop start lines to the RJ-11 connectors. The back view of an MP-100 is shown below.

![Back view of MP-100](image)

**NOTE:** Up to 200 m (660 ft) of 24AWG line cord can be used on loop start lines.

15. Attach the Ethernet cable to the ETH-1 RJ-45 connector to connect to your LAN. To determine the configuration of the MP-100, connect the DC power supply and observe the front panel LEDs. For more details on LED indicators, refer to the *MP-100 User’s Manual & Installation Guide*.

16. The BootP status in the BootP/TFTP Server should show “Client Found” and “100% OK” on all three files. If not, there is a problem with the file location. Verify that the file location is accurate and reconfigure the Client Configuration dialog, if necessary.

17. If the status is “100% OK,” then change the Dip Switch 3 to the down position.

**15.14** Once the device is configured, the yellow lamps on the “Line” and “Tel” LEDs and the green lamps on the “Link” and “Ready” LEDs light. Follow the instructions on the following pages to launch the MP-100 Web administrator and configure the application.
Configuring the MP-100

15.15 Once the BootP Client is set up, configure the MP-100 in the AudioCodes Web administrator.

15.16 To configure the MP-100:

1. Open the Web browser and enter the IP address of your MP-100 gateway in the Address field. Then, press ENTER. The following home page appears.

   **NOTE:** The IP address can be found in the IP field in the Client Configuration dialog, shown on page 182.

2. When the logon dialog box appears, enter the username and password. The default username is **User** and the password is **12345**. If you are unable to login, verify that the Client Configuration is set up correctly (see page 182).

3. Click **Configuration Menu**. This menu has the following options. Click any of the options on the Web page and configure the settings as needed.

   **NOTE:** Make sure the Call Agent IP address in the MGCP Client Settings matches the IPRC IP address (see page 185).

   - **Software Version:** Make sure you have version number 3.80.024.0 or later.
     
     **The Version Id:** 3.80.024.0

   - **Network Settings:** Select **Network Settings** from the Configuration Menu. The following page appears.

     | Base UDP Port:        | 4000 |
     |-----------------------|------|
     | Default Gateway Address: | 0.0.0.0 |
     | Board IP Address:     | 10.1.1.46 |
     | Board Subnet Mask:    | 255.255.255.0 |
Configuring the MP-100

— **Base UDP Port:** The base User Datagram Protocol (UDP) voice port is **4000**. Do not change this number unless you are using other ports at or around this number. Each voice channel or endpoint uses two UDP ports: one for Real-Time Transport Protocol (RTP) and one for Real-time Transport Control Protocol (RTCP). Using lines 1 through 4 will use ports 4000 through 4050, inclusively.

— **Default Gateway Address:** If you need to change the subnet mask or gateway address, it can be done here. Ensure these values match those on the IPRC Device Configuration page (see page 93) if using static IP addressing.

— **Board IP Address:** Enter the IP address of the MP-100.

— **Board Subnet Mask:** Enter the subnet mask of the MP-100.

- **MGCP Client Settings:** Select **MGCP Client Settings** from the Configuration Menu. The following page appears.

<table>
<thead>
<tr>
<th>Call Agent IP</th>
<th>192.168.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Agent Port</td>
<td>2427</td>
</tr>
<tr>
<td>Call Agent Domain Name</td>
<td></td>
</tr>
<tr>
<td>Redundant Agent IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Redundant Agent Port</td>
<td>2427</td>
</tr>
<tr>
<td>Redundant Call Agent Domain Name</td>
<td></td>
</tr>
<tr>
<td>Gateway Name</td>
<td>MP100v1</td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>ACgw</td>
</tr>
<tr>
<td>MGCP Communication Layer Timeout</td>
<td>60</td>
</tr>
</tbody>
</table>

— **Call Agent IP:** Should match the IPRC IP address.

— **Call Agent Port:** Should be set to **2427**.

— **Call Agent Domain Name:** Leave this field blank.

— **Redundant Agent IP:** Should be set to **0.0.0.0**.

— **Redundant Agent Port:** Should be set to **2427**.

— **Redundant Call Agent Domain Name:** Leave this field blank. Inter-Tel currently does not support this feature.

— **Gateway Name:** Enter the name you wish to identify this gateway with on the network, such as MP100v1 (case-sensitive with no spaces or special characters).

**NOTE:** With a v8.2.x firmware IPRC, ensure the names match those in Axxess Database Programming (under System\Cabinets\IPRC (32-Device)\Devices\MGCP Gateway and Endpoint).

— **Endpoint Name:** The default endpoint name is **ACgw** (case-sensitive) and should not be changed to avoid hostname resolution complications. Each endpoint has a number appended to it. For example, line 1 is assigned the name “ACgw0,” line 2 is “ACgw1,” and line 4 is “ACgw3.”

**NOTE:** With a v1.5.x firmware IPRC, ensure the names match those on the MGCP Endpoint Name Settings page in the IPRC Web page. With a v8.2.x firmware IPRC, ensure the names match those in Axxess Database Programming (under System\Cabinets\IPRC (32-Device)\Devices\MGCP Endpoint).

— **MGCP Communication Layer Timeout:** Should be set to **60** seconds.
• **MGCP Channel Settings:** Select **MGCP Channel Settings** from the Configuration Menu. The following dialog appears.

<table>
<thead>
<tr>
<th>Voice Volume (31 - 31 dB)</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Gain (31 - 31 dB)</td>
<td>1</td>
</tr>
<tr>
<td>Test Mode</td>
<td>No Loop Back</td>
</tr>
<tr>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>RTP Redundancy Depth</td>
<td>0</td>
</tr>
<tr>
<td>Dynamic Jitter Buffer Minimum Delay (0 - 150 ms)</td>
<td>70</td>
</tr>
<tr>
<td>Dynamic Jitter Buffer Optimization Factor (0 - 12)</td>
<td>7</td>
</tr>
<tr>
<td>DTMF Transport Type</td>
<td>Transparent</td>
</tr>
<tr>
<td>MF Transport Type</td>
<td>Relay MF</td>
</tr>
<tr>
<td>DTMF Volume (31 - 0 dB)</td>
<td>-11</td>
</tr>
<tr>
<td>Fax Transport Mode</td>
<td>Relay</td>
</tr>
<tr>
<td>Use T30 or FRF11</td>
<td>T.36</td>
</tr>
<tr>
<td>T30 Protection Mode</td>
<td>Redundancy Packets</td>
</tr>
<tr>
<td>Fax Relay Redundancy Depth</td>
<td>0</td>
</tr>
<tr>
<td>Fax Relay ECM Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>Fax Relay Max Rate (BPS)</td>
<td>14400</td>
</tr>
<tr>
<td>BELL Modem Transport Type</td>
<td>Transparent</td>
</tr>
<tr>
<td>V21 Modem Transport Type</td>
<td>Transparent</td>
</tr>
<tr>
<td>V22 Modem Transport Type</td>
<td>Transparent</td>
</tr>
<tr>
<td>V23 Modem Transport Type</td>
<td>Transparent</td>
</tr>
<tr>
<td>V32 Modem Transport Type</td>
<td>Transparent</td>
</tr>
<tr>
<td>V34 Modem Transport Type</td>
<td>Transparent</td>
</tr>
<tr>
<td>Modem Relay Redundancy Depth</td>
<td>0</td>
</tr>
<tr>
<td>Modem Relay Max Rate (BPS)</td>
<td>14400</td>
</tr>
<tr>
<td>Fax/Modem Relay Volume (18.5 - 3.5 dBm)</td>
<td>9</td>
</tr>
<tr>
<td>Fax/Modem Bypass Coder Type</td>
<td>G711MuLaw_64</td>
</tr>
<tr>
<td>Fax/Modem Bypass M</td>
<td>1</td>
</tr>
</tbody>
</table>

All settings, except the following, should remain as shown above. For more details, refer to the *AudioCodes MP-100 User’s Manual.*

— **DTMF Transport Type:** Should match the DTMF Encoding Setting (see page 106) on the IPRC device page.

If **G711** is selected in the Audio Settings page on the IPRC (see page 104), the DTMF Encoding Setting on the IPRC must be either **None** or **Out-Of-Band** and the DTMF Transport Type must be set to **Transparent.**

If **G729** is selected in the Audio Settings page on the IPRC (see page 104), the DTMF Encoding Setting on the IPRC must be **Out-Of-Band** and the DTMF Transport Type must be set to **RFC2833 Relay DTMF.**

**NOTE:** If **G711** is selected in the Audio Settings page on the IPRC (see page 104), all transport types (DTMF, MF, Fax, BELL Modem, and V21/22/23/32/34 Modem) must be set to **Transparent.** If **G729** is selected on the IPRC, set the DTMF Transport Type to **RFC2833 Relay DTMF** and set the Fax Transport Type to **Transparent.**

— **Fax/Modem Bypass Coder Type:** Select **G711MuLaw_64** for US systems and **G711ALaw_64** for European systems.
Configuring the IPRC

15.17 Once the MP-100 is configured, configure the ports for the MP-100 in the IPRC Web page.

15.18 To configure the ports:
   1. Open the Web browser and enter the IP address of the IPRC in the Address field.
   2. Press ENTER. The IPRC Administrative Session page appears (see page 84 for more details).
   3. Select one of the following fields depending on how you want to setup the ports:
      - **Quick Setup — Device**: Gives you step by step instructions on how to configure the ports. This is the quickest method (see page 88 for details).
      - **Circuit Configuration — Device Type and Device Information**: Allows you to manually configure the ports (see pages 98 and 99 for details).
   4. Select the port (a.k.a. circuit) to configure and follow the instructions below:
      - *For port 1*, select **MGCP Gateway Device + Endpoint** as the device type.
      - *For ports 2, 3, and 4*, select **MGCP Add’l Endpoint** as the device types.
      
      **NOTE**: The same rule applies even when you have more than one gateway device installed in a network system. Configure the device type as **MGCP Gateway Device+Endpoint** for port 1 and as **MGCP Add’l Endpoint** for ports 2-4.

      Then follow the instructions on page 88 for the Quick Setup field or pages 98 and 99 for the Circuit Configuration field.

   5. Make sure the connection(s) are active in the Circuit Status page (see page 121).

15.19 The AudioCodes MP-100 Gateway is now ready for connection to the CO.
C. AUDIOCODES MP-104 MGCP GATEWAY

15.20 The AudioCodes MP-104 FXO MGCP gateway supports up to four loop start line (FXO) ports. Although the MP-104 is similar to the MP-100, each gateway uses a different switch type for configuring the device. The MP-100 uses DIP switches (see page 181), and the MP-104 uses a command-line switch (-fb). For details about command line switches, refer to the MP-104 User’s Manual & Installation Guide.

15.21 The MP-104 on a v8.2.x or later IPRC firmware supports the peer-to-peer (P2P) audio feature. This feature allows certain IP and SIP devices to transmit and receive audio directly with each other. With this feature, the audio is not transmitted or received through the system cabinet. This reduces delay and removes the audio stream from the Time Division Multiplex (TDM) highway.

15.22 The MP-104 on a v8.2.x or later IPRC firmware does not support the following features:

- Tick Tone as an audio source for CO calls. This is normally used for features that require audio sources, such as the Music-On-Hold feature.
- Pause digits. These digits are normally used to program a speed-dial or other digit string.

**NOTE:** The MP-104 MGCP gateway must be running software version 4.2 or later when connected to an IPRC running version 8.2.x firmware.

15.23 For information about how to install and configure the AudioCodes MP-104 MGCP gateway, refer to the AudioCodes MP-104 Gateway Installation Guide (document part number 835.2741)
D. AUDIOCODES MP-104 SIP GATEWAY

15.24 With v9.0, the system supports SIP (Session Initiated Protocol) trunks to reach the CO. SIP trunks allow the system to communicate with the CO via SIP-enabled gateways. As the SIP protocol becomes more and more popular, it is important to be able to communicate to SIP gateways in the IP-centric world. Inter-Tel currently supports the AudioCodes MP-104 SIP gateway (with software version 4.2).

NOTE: Inter-Tel does not provide technical support for any SIP gateway other than the AudioCodes MP-104 SIP gateway.

15.25 SIP trunks support the following functionality:
- They are transparent to the system user because SIP trunks act like any other CO trunk in the system.
- They support transferring trunks, putting trunks on hold, and connecting trunks to conferences similar to other CO trunks in the system.
- They support making and receiving calls by any endpoint.
- They support peer-to-peer audio by IP endpoints.
- They reside in CO trunk groups just like other trunks so that SIP trunk calls can be routed using Automatic Route Selection (ARS).
- They support 911 calls just like MGCP trunks.

15.26 The MP-104 on a v8.2.x or later IPRC firmware does not support the following features:
- Pause digits. These digits are normally used to program a speed-dial or other digit string.
- SIP registration which is used for authentication purposes.

15.27 If you are updating an existing AudioCodes MP-104 MGCP gateway to support SIP trunks, once the SIP software is installed you can no longer use MGCP. The MP-104 cannot support both MGCP and SIP simultaneously. To support MGCP, you must install the appropriate software using the BootP/TFTP process or by using the MP-104’s Web interface (see page 58 for details).

15.28 For information about how to install and configure the AudioCodes MP-104 SIP gateway, refer to the *AudioCodes MP-104 SIP Installation Guide* (document part number 835.2884)
16. IP SOFTPHONE

16.1 The IP softphone is software that runs on your PC. The user interface is a virtual representation of an Executive or Professional endpoint, or IP PhonePlus. You can use it exactly as you would the IP PhonePlus when connected to the IP card. You can also customize the display by changing the fonts and colors. The available IP softphone are Axxess IP SoftPhone, Eclipse IP SoftPhone, and Model 8602. See below for illustrations and system requirements of each softphone. For installation and operation instructions, refer to the document provided with the IP softphone.

A. AXXESS IP SOFTPHONE

16.2 Below is an illustration of the Axxess IP SoftPhone. The Axxess IP SoftPhone also has optional DSS maps with 20, 40, or 60 buttons.

16.3 Minimum PC requirements for IP SoftPhone are:

- For v1.101 - Microsoft Windows 98, 2000, NT, ME, and XP
- For v1.003 - Microsoft Windows 95, 98, 2000, and NT

**NOTE:** IP SoftPhone v1.003 uses an older version of the Java Runtime Environment (JRE) which may not work properly with Intel® Pentium® 4 processors. If there is a problem starting the application on a machine with a Pentium 4 processor, delete the SYMCJIT.DLL file from the JRE directory (e.g., C:\Program Files\JavaSoft\JRE\1.1\bin).

- IBM-compatible PC
- Modem (56K or higher) or Ethernet Card
- 200 MHz or faster microprocessor
- 32 MB RAM
- 20 MB available hard disk space
- Network card with TCP/IP configured (or Dial-up Adapter via TCP/IP if via modem)
- Full-duplex sound card
- Headset with microphone (or speaker and microphone, but headset is recommended)
B. ECLIPSE IP SOFTPHONE

16.4 Below is an illustration of the Eclipse IP SoftPhone.

16.5 Minimum PC requirements for IP SoftPhone v1.000 are:

- Microsoft Windows 95, 98, 2000, and NT
- IBM-compatible PC
- Modem (56K or higher) or Ethernet Card
- 200 MHz or faster microprocessor
- 32 MB RAM
- 20 MB available hard disk space
- Network card with TCP/IP configured (or Dial-up Adapter via TCP/IP if via modem)
- Full-duplex sound card
- USB or Parallel port (for security key)
- Headset with microphone (or speaker and microphone, but headset is recommended)
C. MODEL 8602

The Model 8602 is a new Internet Protocol (IP) softphone that is used with the Inter-Tel® Axxess® Converged Communications Platform versions 9.1 and later. It requires IPRC firmware v9.0.0 or later. The Model 8602 is a softphone application that enables Voice over IP (VoIP) telephone calls from laptops or desktop computers. The Model 8602 connects to the Inter-Tel® telephone system through an existing IP network. The Model 8602 operates like a Model 8662 endpoint and supports Inter-Tel Protocol (ITP) mode. After a connection is established, Model 8602 users can converse with the other party via a headset connected to their PC. Below is an illustration of the 8602 IP softphone.

Model 8602 has the following features:

- Integration with the Plantronics CS50-USB Wireless Headset
- Control and user-configurable options
- Control of audio and volume settings for the microphone and speaker
- Tray Client feature access
- Tray Client status indication
- Retractable dialpad
- User-friendly, modern look and feel
- Mouse and keyboard activated feature control

Like other endpoints, the IP softphone is identifiable in System Monitor and appears in:

- System Monitor dumps as an 890 device type
- Message Print as “IP Softphone Port”

Refer to the Model 8602 User Guide, part no. 835.3019, which provides the installation procedures for the Model 8602 and highlights the basic features for making and receiving calls and checking voice mail messages. For more details on basic or advanced features of the Model 8602, refer to the Model 8602 online help. Or, refer to the Inter-Tel Model 8662 User Guide (part no. 550.8117), which includes details of features not included in the Model 8602 User Guide or online help. You can find this user guide on Inter-Tel’s Web site at www.inter-tel.com/techpublications.
17. TROUBLESHOOTING

17.1 This section provides troubleshooting procedures for the following categories:

- Connection issues (see page 193)
- Audio issues (see page 195)
- Echo issues (page 198)
- Multi-protocol endpoint issues (page 199)
- VLAN tagging issues (page 205)

A. CONNECTION ISSUES

Table 9: Connection Issues

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>General connection issues</td>
<td>The Link LEDs are not lit</td>
<td>Verify the following settings:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Link LED is lit on the IP card and/or device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Link LED is lit on the switch or hub to which these devices connect.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The IP card or device has a unique IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You can ping the IP address from another PC on the same subnet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• From the IP card’s RS-232 or Telnet OLMN, you can ping the IP address of the problem device or IP card, and also you can ping in the other direction from the problem device or IP card to the first card.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Appropriate ports for IP devices and IP card are opened on a firewall, router, and/or NAT. To verify the port connection, use the Port Test in the Network Qualifier software application.</td>
</tr>
<tr>
<td>Cannot connect a device to the IPRC</td>
<td>The endpoint does not have the latest firmware</td>
<td>Verify the endpoint has the latest firmware by viewing the latest version in the endpoint Web interface. Refer to the Multi-Protocol Endpoint Firmware Compatibility Matrix on page 5.</td>
</tr>
<tr>
<td></td>
<td>The debug output is not normal</td>
<td>Check the debug output using RS-232 or Telnet (type <code>msgp</code> in the Debug Session) (see page 131). Normal output appears as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;&lt;UDP Broadcast Range/LAN ONLY&gt;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>Find server for 00:10:36:00:07:01 from 172.16.10.171:5567 -- port 13</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;&lt;UDP PART&gt;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>IP ID for 00:10:36:00:07:01 from 172.16.10.171:5567 -- port 13</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;&lt;TCP PART&gt;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>Connection from 172.16.10.171 on port 13</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the output is not normal, contact Inter-Tel Technical Support.</td>
</tr>
</tbody>
</table>
Connection Issues (Continued)

Table 9: Connection Issues (Continued)

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| (Continued) Cannot connect a device to the IPRC                   | Endpoint is not programmed                  | Check the status in the Connected field in the Circuit Status page on the Web interface (see page 121) or the Network Status field in the Network Information on the Telnet (see page 131). If the device is connected, but not operational, then it is a call processing problem. Verify that the System Database is programed as follows:  
  - The MAC address of the device is programed in DB programming under System – Devices and Feature Codes – <endpoints>  
  - The card slot is programed for **DKSC16** (even for the 8-circuit IPCs).  
  - The circuit port is programed for **Keyset, Dual Single Line**, or **Single-Port LSA** (requires system v7.0 or later).  
  - The call processing has the correct security PAL for the system.  
If the device not connected, ensure the Device Type, Device ID, and/or Ethernet Address match the device. The following describes where the Ethernet address or device ID is located on each IP device type.  
  - IP PhonePlus displays its Ethernet address as it cycles through its power up screens.  
  - IP SLA has a sticker with the Ethernet address.  
  - IP SoftPhone controls the device ID under the settings option on startup.  
  - MGCP Gateway needs the device IP address, instead of the Ethernet address.  
  - MGCP endpoint needs the endpoint name, instead of the Ethernet address.  
  - Verify no network address translation is being used on the IP scheme (NAT/PAT). |

|connection Issues |  |  |
## B. AUDIO ISSUES

### Table 10: Audio Issues

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio quality is poor</td>
<td>The network cannot support VoIP calls.</td>
<td><strong>Pre-Installation:</strong> Verify the network’s ability to support a VoIP call or calls using the Network Test in the Network Qualifier software application.</td>
</tr>
<tr>
<td></td>
<td>An IP endpoint does not receive audio packets properly</td>
<td><strong>NOTE:</strong> The Network Qualifier requires a PC on each site. The PCs should not be used for any other purpose because other Windows applications could cause jitter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Post-Installation:</strong> Verify the intime frames percentage using the Intime Packet Graph in the Receive Audio Status page (see page 119) on the Web interface. You can also watch live values through the Audio Receive Statistics on the Telnet interface. Be sure to watch the percentages on both the IP card and device. Note that the percentages will be quite low with Voice Activity Detection (VAD) enabled. These low values give some indication of the bandwidth saved by not transmitting silent audio packets.</td>
</tr>
</tbody>
</table>
### Audio Issues (Continued)

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| Audio quality is poor (Continued) | Network related issues: there is heavy traffic contending for bandwidth, a hardware problem with switch or router, or defective cabling. | To improve audio quality, try any of the following:  
- Increase playback (jitter) buffer; however, adds delay or latency.  
- Use G.729B (B = VAD); does not send silent packets.  
- Increase Audio Frames/IP packet (see page 104) to reduce bandwidth needed; however, increases latency.  
- Use switches not hubs.  
- Prioritize the packets through routers; most simply prioritize the audio port (typically UDP 5004), but could also use DiffServ or TOS.  
- Add more bandwidth.  
- Paging and background music consume bandwidth; if a site has low bandwidth, they probably should not put all IP endpoints in the page zone.  
- Do not use the hub or switch on the IP endpoint for a PC or other device that will consume a large amount of bandwidth in bursts or constantly. |
| Not enough bandwidth to support voice and data. |  |  |

To test the best-case scenario:  
- To eliminate any network problems, use a cross-over cable between an IPRC and an IP endpoint, or simply plug the cable from the IP card into the hub on the endpoint. Remove the LAN cable from the IP endpoint’s power brick.  
- Test a DKSC16 with a normal digital endpoint. If it sounds okay, then the backplane slot is okay; otherwise, switch slots.  

Run the Network Qualifier to assess your bandwidth.

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>An IP endpoint lost audio suddenly while on a muted call</td>
<td>IP endpoints are behind a firewall</td>
<td>When the Voice Activity Detection option (page 107) is enabled and if any IP endpoints are behind a firewall, the IP endpoints may suddenly lose audio (while on a muted call) or lose background music. If this occurs, disable the Voice Activity Detection flag. When the flag is enabled, the IP endpoint does not send silent audio packets to the IP card; however, the IP card continues to send non-silent audio packets to the IP endpoint. Eventually, most firewalls block this unsolicited IP audio stream from the IP card to the IP endpoint. (see page 13 for details about firewalls)</td>
</tr>
</tbody>
</table>
A call was established between two IP endpoints, but there is no audio.

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP endpoints are programmed for P2P audio, but they do not support the same vocoder.</td>
<td>Remove the IP devices from the Network Group. Consider adding them to a Network Group that contains IP devices that support the vocoder.</td>
<td></td>
</tr>
<tr>
<td>The IP endpoints are programmed for P2P audio, but they do not support the same number of audio frames per IP packet.</td>
<td>Remove the IP devices from the Network Group. Consider adding them to a Network Group that contains IP devices that support the same number of audio frames per IP packet.</td>
<td></td>
</tr>
<tr>
<td>There is a firewall or NAT between the two devices.</td>
<td>Place the devices into different Network Groups or disable the Use Peer-To-Peer Audio flag for the group. Make sure the correct IP ports are open. Refer to the PROGRAMMING or the Web interface for the current available ports that can be used, Run Network Qualifier to test the ports to make sure they are not blocked.</td>
<td></td>
</tr>
</tbody>
</table>

The endpoint received the following alarm: A032 ALARM Ext. <xxxx> Received Insufficient Bandwidth.

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IPRC [b.p.d] detected that the audio-receive timer has expired without receiving the first audio packet or the average-in-time-frame percentage has fallen below the threshold specified in the Voice Audio Session Configure Command.</td>
<td>This indicates a network problem. Poor network condition could cause packet loss or a firewall prevents the callers to receive audio packets. There is a system flag that can disable this alarm. The “Insufficient Bandwidth” alarm is displayed when the average number of In Time frames falls below the Average In Time Frame Percentage Threshold (in System\IP-Related Information\Call Configuration), and the average number of In Time frames stays below that threshold for the time given by the Average In Time Frame Timer (in seconds) in System\IP-Related Information\Call Configuration. To change the percentage, click the current Value and use the scroll box to select the new value. Then press ENTER or click another field to save the change. The range for Average In Time Frame Percentage Threshold is 0-100%, and the default is 60%. The range for Average In Time Frame Timer is 0-255 seconds, and the default is 5 seconds.</td>
<td></td>
</tr>
</tbody>
</table>
## C. ECHO ISSUES

### Table 11: Echo Issues

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| IP endpoint users hear echo on their endpoint while talking to an analog trunk (like SLC, SLA, or trunk) | Hybrid balance is not on the correct setting | To reduce echo, first test echo and verify the following settings. Then, follow the instructions on the following page.  

**NOTE:** When testing echo, make sure you dial the same phone number using the same trunk. Seize the trunk directly, and do not use the trunk group or ARS. Different trunks have different characteristics.  
Verify the hybrid balance setting. If the trunk does not connect to a public CO, or if the CO is relatively close, then the hybrid balance should be set to “Short.” No matter what the current setting is, try the other setting and dial the same number through the same trunk. One setting should be dramatically worse than the other. You should disable the Echo Suppression option (see page 107) so you can actually hear the echo from the beginning of the call, or use the Echo Canceller Statistics (see page 132) on Telnet to measure the echo. Refer to the Echo Troubleshooting Guide (document part no. 835.2844) that is located on the Inter-Tel edGe at [www.inter-tel.com/techpublications](http://www.inter-tel.com/techpublications). |
| The audio volume for the IP device is too high | To reduce echo from an analog circuit, reduce the audio volume the IP card drives on to the backplane. This will help the echo canceller adapt quicker. Follow the instructions below:  
1. Adjust the Backplane Transmit Signal Gain option (see page 95) on the Web interface. The default setting is 0dB (without any reduction). Any change you make will reduce the volume.  
2. After the adjustment, dial the same number through the same trunk. You should disable the Echo Suppression option (see page 107) so you can actually hear the echo from the beginning of the call. The side effect is that the person on the other end of the call may have a hard time hearing the IP user because the volume is reduced. |
Troubleshooting

Table 11: Echo Issues (Continued)

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP endpoint users hear echo on their endpoint while on a digital trunk</td>
<td>The echo canceller is designed to cancel echo from the cabinet, not the echo from the CO because it takes too long for echo to return to IP card. In an attempt to reduce echo from a digital CO trunk, do any of the following: • Reduce T1 gain on Transmit to CO if your system supports it. • Reduce T1 gain on Receive from CO if the echo is quite low in volume and if your system supports it. <strong>NOTE:</strong> System v5.1 or later is required to support T1/E1 or T1/E1/PRI gain control. Reducing T1 gain will affect all users, not just the VoIP users. • Adjust the Backplane Transmit Signal Gain option (see page 95) on the Web interface, as described above in the troubleshooting for analog circuits. The Backplane Transmit Signal Gain setting can be applied to T1 or any circuit, not just analog circuits.</td>
<td></td>
</tr>
<tr>
<td>IP users hear a low-volume, clean, clear echo during the beginning of the audio session</td>
<td>Echo Suppression Sensitivity Level is not balanced</td>
<td>Enable the Echo Suppression option (see page 108). With this option enabled, adjust the Echo Suppression Sensitivity Level during the beginning of an audio session to find the balance between the IP user hearing a slight echo and hearing a half-duplex condition on the handset. The Echo Suppression Sensitivity Level does nothing if the Echo Suppression is disabled. Disable the Echo Suppression when using the circuit for fax operations or as a last resort to eliminate the half-duplex condition on the handset during the beginning of the audio session.</td>
</tr>
<tr>
<td>An IP user hears raspy or distorted echo as he speaks quite loudly or holds the handset close to his mouth</td>
<td>The Echo Saturation Blocker option is not enabled</td>
<td>Enable the Echo Saturation Blocker option (see page 109).</td>
</tr>
<tr>
<td>An IP user hears choppiness or a half-duplex condition on the handset as she speaks quite loudly or holds the handset close to her mouth</td>
<td>The Echo Saturation Blocker option is enabled</td>
<td>Disable the Echo Saturation Blocker option (see page 109).</td>
</tr>
</tbody>
</table>

D. MULTI-PROTOCOL ENDPOINT-RELATED ISSUES
### Table 12: Multi-Protocol Endpoint-Related Issues

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The multi-protocol endpoint powers up and all the lamps remain lit</td>
<td>The endpoint software is corrupt</td>
<td>The voice processing software is corrupt, and the multi-protocol endpoint must be recovered using the following steps:</td>
</tr>
<tr>
<td>permanently.</td>
<td></td>
<td>1. Set up a PC on the same LAN as the endpoint.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Make sure the PC has a TFTP server and the correct software image file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Rename the software image from 86xx_x_x_x.bin (where the _x_x_x represents the version number) to 86xx.bin. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Rename 8600_1_1_5.bin to 8600.bin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Rename 8620_1_1_5.bin to 8620.bin (note that the Models 8620 and 8622 share the same binary image)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Rename 8662_1_1_5.bin to 8662.bin (note that the Models 8622 and 8622 share the same binary image)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Rename 8690_1_1_5.bin to 8690.bin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Point the TFTP server at the directory that contains this software image file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Configure the IP address of the PC as 192.168.200.202. The endpoint starts pulling this file from the TFTP server. When finished, the endpoint resets on its own.</td>
</tr>
<tr>
<td>The Model 8622 or 8662 endpoints are not uploading new firmware images</td>
<td>The image strings have not been</td>
<td>Make sure that these strings have been updated. For example,</td>
</tr>
<tr>
<td>as specified in the TFTP configuration files.</td>
<td>updated</td>
<td><strong>From 1.1.5 and earlier to 2.0.06:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>66xx_image_ver: HWID 2.0.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td>86xx_image_url: 192.168.200.202/86xx/86xx_2_0_06.bin</td>
</tr>
<tr>
<td>OR The TFTP configuration files have been modified with new image</td>
<td></td>
<td><strong>NOTE:</strong> If upgrading an 8622 from 1.01S to 1.1.5, use the following image version string: 8620_image_ver: 8620 HWID 1.1.5.</td>
</tr>
<tr>
<td>versions, but the Model 8622 or 8662 endpoints have not uploaded the new</td>
<td></td>
<td><strong>For future releases (2.0 and later):</strong></td>
</tr>
<tr>
<td>firmware.</td>
<td></td>
<td>iphone_image_ver: 2.0.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iphone_image_url: 192.168.200.202/iphone/iphone_2_0_06.bin</td>
</tr>
<tr>
<td>The endpoint may have background music enabled</td>
<td></td>
<td>Turn off the background music feature (default feature code: 313).</td>
</tr>
</tbody>
</table>
### Multi-Protocol Endpoint-Related Issues (Continued)

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>While installing the client application on the Model 8690, an error</td>
<td>The endpoint does not have sufficient memory resources or the endpoint</td>
<td>The client application installation on the Model 8690 has failed. You must</td>
</tr>
<tr>
<td>message indicating that the setup failed appears.</td>
<td>has lost power before the upgrade is complete</td>
<td>reformat the flash file system on the endpoint. See page 172 for details.</td>
</tr>
<tr>
<td>The Windows CE.Net stops during the firmware upgrade.</td>
<td>This may be caused by using most of the system resources (processor and RAM)</td>
<td>Try doing one of the following:</td>
</tr>
<tr>
<td></td>
<td>during an upgrade.</td>
<td>• Restart the Windows CE upgrade by going into Pending Upgrades. Windows CE will</td>
</tr>
<tr>
<td></td>
<td></td>
<td>still show up as “Pending” because it has not completed copying, which results</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in a reset of the Model 8690. Press “OK” to restart the upgrade and eventually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>this causes the original upgrade time out and display the dialog box to restart</td>
</tr>
<tr>
<td></td>
<td></td>
<td>that upgrade. Press “No” to cancel the original upgrade and continue with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>second download that is in progress (usually still erasing flash at this point).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Launch the 8690 manually by using a USB mouse. The USB mouse does not require</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a lot of memory in the CPU. With the USB mouse attached the user can perform</td>
</tr>
<tr>
<td></td>
<td></td>
<td>some basic functions and still see the Model 8690 endpoint responding. The mouse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>should be attached before the upgrade is started.</td>
</tr>
<tr>
<td>The Model 8622 or 8662 endpoint flashes the error message “ERROR WRONG</td>
<td>The image that the Model 8622 or 8662 endpoint is attempting to download does</td>
<td>Use a more recent image, preferably at or above the version shipped with the</td>
</tr>
<tr>
<td>HWID” when attempting to download a new image.</td>
<td>not support the endpoint’s hardware.</td>
<td>endpoint.</td>
</tr>
<tr>
<td>A multi-protocol endpoint flashes the error message “ERROR WRONG VERSION” when attempting to download a new image.</td>
<td>The version number in the xxxx_image_ver string may not match up with the image’s version.</td>
<td>Correct the xxxx_image_ver image version number or the image name (if pointing at the wrong image file).</td>
</tr>
</tbody>
</table>

**NOTE:** When an upgrade is in progress, avoid using the Model 8690 endpoint.
### Multi-Protocol Endpoint-Related Issues (Continued)

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| The Model 8622 endpoint flashes the error message “ERROR WRONG VERSION” when attempting to download a new image. | The endpoint does not have the latest firmware.                            | The Model 8622 endpoints running firmware version 1.01S will display the error “ERROR WRONG VERSION” when attempting to download new firmware. To upload the new firmware to the 8622, first use one of the following version strings to upgrade to either versions 1.0.33 or 1.1.5:  
  
  8620_image_ver: 8620 1.0.33  
  or  
  8620_image_ver: 8620 HWID 1 1.1.5  
  
  Once the newer firmware has been loaded on the Model 8622 endpoint, change the image version string back to one of the following:  
  
  8620_image_ver: 1.0.33  
  or  
  8620_image_ver: HWID 1 1.1.5  
  or  
  iphone_image_ver: 2.v.vv (the v.vv indicates the firmware version, such as 2.0.06) |

**NOTE:** After the firmware has been upgraded, the endpoint will again display the error “ERROR WRONG VERSION” every time it attempts to upgrade until the configuration version line is returned to the normal state noted above in either the TFTP file or the Web page (i.e., “8620_image_ver: 1.0.33”).

---

**Table 12: Multi-Protocol Endpoint-Related Issues (Continued)**
When the multi-protocol endpoints reset, network connectivity on the downlink (i.e., the LAN port labeled “PC” on the back on the endpoint) is temporarily lost.

The endpoints generally reset for one of the following reasons:

1. Endpoint setting or firmware updates - the endpoints may require a reset for certain configuration changes to take place and will reset if the firmware is updated.
2. Telephony system updates - the endpoints will reset when the Call Processing system disconnects their connection for updates on the Call Processing side. The endpoint will continue to reset every several minutes until the telephony system recovers and the endpoint can re-connect.
3. Loss of network connectivity - the endpoints will reset when network congestion or loss of network connectivity prevents necessary keepalive packets from being exchanged between Call Processing and the endpoint.

Work-arounds for this issue are as follows:

- Minimize endpoint resets due to system updates - Schedule telephony system and endpoint updates for non-peak hours when endpoint and network connectivity outages are less service affecting.
- Isolate and eliminate any network issues - Isolate and eliminate any network congestion issues that may cause the endpoint to lose communication with Call Processing and thus reset.
- For critical applications that cannot tolerate any interruptions in LAN service, use an external switch in place of the downlink port for network connectivity until resets due to external factors can be minimized.

In the case of (3) loss of network connectivity, make sure that the network in question meets the minimum requirements specified in the Inter-Tel’s VoIP Data Network Requirements (document part no. 835.2885). This document can be found on the Inter-Tel eDge Web site, under Online Manuals & Guides – IP Telephony Online Manuals (www.inter-tel.com/techpublications).

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work-arounds for this issue are as follows:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Minimize endpoint resets due to system updates - Schedule telephony system and endpoint updates for non-peak hours when endpoint and network connectivity outages are less service affecting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Isolate and eliminate any network issues - Isolate and eliminate any network congestion issues that may cause the endpoint to lose communication with Call Processing and thus reset.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- For critical applications that cannot tolerate any interruptions in LAN service, use an external switch in place of the downlink port for network connectivity until resets due to external factors can be minimized.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the case of (3) loss of network connectivity, make sure that the network in question meets the minimum requirements specified in the Inter-Tel’s VoIP Data Network Requirements (document part no. 835.2885). This document can be found on the Inter-Tel eDge Web site, under Online Manuals & Guides – IP Telephony Online Manuals (www.inter-tel.com/techpublications). |
Troubleshooting
AXXESS® IP DEVICES MANUAL – Revised, April 2006

Multi-Protocol Endpoint-Related Issues

Table 12: Multi-Protocol Endpoint-Related Issues (Continued)

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Probable Cause</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The HP (Hewlett-Packard) POE (Power over Ethernet) network appliances may cause an issue with the Inter-Tel IP endpoints (Models 8600, 8620, 8622 or 8662) where the endpoint will fail to activate (power up).</td>
<td>The HP POE equipment is influencing the pins 4, 5, 7 and 8 when applying power on pins 1, 2, 3 and 6 thus preventing the Inter-Tel endpoint from working.</td>
<td>If using an HP POE network appliance with the Inter-Tel endpoints remove the unused set of power leads 4, 5, 7 and 8 by un-terminating them for each endpoint or purchase network splitters that split 1, 2, 3 and 6 from 4, 5, 7 and 8. These are available through Inter-Tel’s Commsource or Telecom suppliers. The following are the pin outs for Power over Ethernet.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conductor</th>
<th>Alternative A (MDI-X)</th>
<th>Alternative A (MDI)</th>
<th>Alternative B (All)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Negative V Port</td>
<td>Positive V Port</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Negative V Port</td>
<td>Positive V Port</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Positive V Port</td>
<td>Negative V Port</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>Positive V Port</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>Positive V Port</td>
</tr>
<tr>
<td>6</td>
<td>Positive V Port</td>
<td>Negative V Port</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>Negative V Port</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>Negative V Port</td>
</tr>
</tbody>
</table>

Inter-Tel’s Hardware engineering is continuing to work with Hewlett-Packard on a long-term solution. Once this is completed this information will be updated.
E. VLAN TAGGING-RELATED ISSUES

Table 13: VLAN Tagging-Related Issues

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>PROBABLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user cannot connect to the Web interface for a multi-protocol endpoint.</td>
<td>The PC that the user uses may not be in the same VLAN group as the endpoint.</td>
<td>The PC that the user uses may not be in the same VLAN group as the endpoint. Make sure that the PC and endpoint are in the same VLAN group. If not, set the endpoint VLAN ID to match the PC or disable the VLAN feature for the endpoint (see page 23).</td>
</tr>
<tr>
<td>The user cannot connect to the Model 8690 Web interface but could connect to the Model 8622 or 8662 Web interface. The VLAN ID of the phone port is disabled but the VLAN ID of the downlink port is enabled (not zero).</td>
<td>The VLAN ID of the endpoint is disabled</td>
<td>This is a limitation of the 8690 internal phone Ethernet switch. The 8690 Ethernet switch inserts the default VLAN ID which is 1 if the frames from the endpoint are untagged. Connect the PC to one of the downlink ports which has VLAN ID set to zero.</td>
</tr>
<tr>
<td>The user powers up the endpoint with the correct VLAN ID, but the endpoint receives the wrong IP settings from the wrong DHCP from another VLAN.</td>
<td>The network switch may not support VLAN or wrong VLAN ID is programmed at the switch port of the core switch network.</td>
<td>Make sure that the core network switch is programmed correctly.</td>
</tr>
<tr>
<td>The user powers up 8690 but the network settings still show the settings with the old VLAN values.</td>
<td>The endpoint application may not be updated so the new VLAN settings may not have been propagated to the VPS. If the endpoint application is up to date, then the new VLAN IDs may not have been sent down to the VPS in time.</td>
<td>Make sure that the endpoint application is up to date, and reset the endpoint after the VLAN ID in the phone port has been changed from the networking control panel of Windows CE.</td>
</tr>
</tbody>
</table>

F. IPRC DIAGNOSTICS

17.2 The IPRC v7.0 or later firmware has many diagnostic tools used for troubleshooting purposes. These tools are separate from Call Processing and display only information local to the IPRC. There are also limited programming displays to control the card. For details about diagnostics information, refer to the TROUBLESHOOTING section in the Inter-Tel Axxess Installation and Maintenance Manual (document part no. 550.8000).
18. PART NUMBERS

18.1 The part numbers associated with IP cards and IP devices are listed in the following table.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>PART NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td></td>
</tr>
<tr>
<td>IP Resource Card (IPRC)</td>
<td>550.2265</td>
</tr>
<tr>
<td>Axxess IP PhonePlus with 10Base-T Hub</td>
<td>770.4500</td>
</tr>
<tr>
<td>Eclipse IP PhonePlus with 10Base-T Hub</td>
<td>560.4401</td>
</tr>
<tr>
<td>Model 8660</td>
<td>550.8660</td>
</tr>
<tr>
<td>Model 8664 Wireless IP Endpoint</td>
<td>550.8664</td>
</tr>
<tr>
<td>Model 8665 Wireless IP Endpoint</td>
<td>550.8665</td>
</tr>
<tr>
<td>Model 8600 Multi-Protocol Endpoint</td>
<td>550.8600</td>
</tr>
<tr>
<td>Model 8620</td>
<td>550.8620</td>
</tr>
<tr>
<td>Model 8622</td>
<td>550.8622</td>
</tr>
<tr>
<td>Model 8662</td>
<td>550.8662 (8 MB)</td>
</tr>
<tr>
<td></td>
<td>550.8662E (16 MB)</td>
</tr>
<tr>
<td>Model 8690</td>
<td>550.8690</td>
</tr>
<tr>
<td>Model 8601 SoftPhone for Pocket PC</td>
<td>827.9901</td>
</tr>
<tr>
<td>IP Single-Line Adapter</td>
<td>770.3000</td>
</tr>
<tr>
<td>MP-100 MGCP Gateway 4-Port FXO</td>
<td>901.3915</td>
</tr>
<tr>
<td>MP-104 MGCP Gateway 4-Port FXO</td>
<td>901.3916</td>
</tr>
<tr>
<td>Device IPRC PALs</td>
<td></td>
</tr>
<tr>
<td>8-Port Station PAL for IPRC</td>
<td>827.9449</td>
</tr>
<tr>
<td>16-Port Station PAL for IPRC</td>
<td>827.9450</td>
</tr>
<tr>
<td>IPRC PAL Upgrade</td>
<td>828.1637</td>
</tr>
<tr>
<td>32-Device IPRC Software License</td>
<td></td>
</tr>
<tr>
<td>Category A Endpoint License: 8 Ports</td>
<td>840.0132</td>
</tr>
<tr>
<td>Category A Endpoint License: 16 Ports</td>
<td>840.0133</td>
</tr>
<tr>
<td>Category A Endpoint License: 32 Ports</td>
<td>840.0134</td>
</tr>
<tr>
<td>Category B Endpoint License (for the Model 8602)</td>
<td>840.0633</td>
</tr>
<tr>
<td>IP Networking Ports: 4 Ports</td>
<td>840.0115</td>
</tr>
<tr>
<td>IP Networking Ports: 8 Ports</td>
<td>840.0116</td>
</tr>
<tr>
<td>IP Networking Ports: 16 Ports</td>
<td>840.0117</td>
</tr>
<tr>
<td>IP Networking Ports: 32 Ports</td>
<td>840.0118</td>
</tr>
<tr>
<td>Power Supply Parts</td>
<td></td>
</tr>
<tr>
<td>US Power Supply — AC Input: 120V 0.2A, DC Output: 24V 0.5A</td>
<td>806.1113</td>
</tr>
<tr>
<td>US Power Supply — AC Input: 120V 0.12A, DC Output: 48V 0.15A</td>
<td>806.1114</td>
</tr>
<tr>
<td>UK Power Supply — AC Input: 240V 0.12A, DC Output: 48V 0.15A</td>
<td>806.1117</td>
</tr>
<tr>
<td>DESCRIPTION (Continued)</td>
<td>PART NUMBER</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>UK Power Supply — AC Input: 240V 0.12A, DC Output: 24V 0.5A</td>
<td>806.1118</td>
</tr>
<tr>
<td>Universal Power Supply — AC Input: 100-240V 1.2A, DC Output: 24V 1.0A</td>
<td>806.1119</td>
</tr>
<tr>
<td>Red Hawk PowerSense Single-Port Module for Multi-port Hub (24V Protocol)</td>
<td>901.0403</td>
</tr>
<tr>
<td>Red Hawk PowerSense Single-Port Module for Multi-port Hub (IEEE 802.3af Protocol)</td>
<td>901.0404</td>
</tr>
<tr>
<td>Red Hawk PowerSense Single-Port Module (24V Protocol)</td>
<td>901.0406</td>
</tr>
<tr>
<td>Red Hawk PowerSense Single-Port Module (IEEE 802.3af Protocol)</td>
<td>901.0407</td>
</tr>
<tr>
<td>US Power Supply Kit</td>
<td>828.1642</td>
</tr>
<tr>
<td>- US power supply (P/N 806.1113)</td>
<td></td>
</tr>
<tr>
<td>- Network cable (P/N 813.1790)</td>
<td></td>
</tr>
<tr>
<td>Universal Power Supply Kit</td>
<td>828.1660</td>
</tr>
<tr>
<td>- Universal power supply (P/N 806.1119)</td>
<td></td>
</tr>
<tr>
<td>- Network cable (P/N 813.1790)</td>
<td></td>
</tr>
<tr>
<td>System Software</td>
<td></td>
</tr>
<tr>
<td>AudioCodes MP-100/104 CD-ROM</td>
<td>827.9920</td>
</tr>
<tr>
<td>IP Devices CD-ROM</td>
<td>827.9162</td>
</tr>
<tr>
<td>Documentation</td>
<td></td>
</tr>
<tr>
<td>Inter-Tel Axxess Installation Maintenance Manual</td>
<td>550.8000</td>
</tr>
<tr>
<td>Addendum to Issue 8.0 of the Inter-Tel Axxess Installation and Maintenance Manual</td>
<td>550.8023</td>
</tr>
<tr>
<td>Model 8690 Administrator’s Guide</td>
<td>550.8120</td>
</tr>
<tr>
<td>Multi-Protocol Endpoints: Supported Features, Buttons, and LED Indications</td>
<td>835.2840</td>
</tr>
<tr>
<td>SIP Server Installation and Configuration Manual</td>
<td>835.2605</td>
</tr>
<tr>
<td>Model 8601 SoftPhone for Pocket PC Installation Manual</td>
<td>835.2736</td>
</tr>
<tr>
<td>NetLink SVP Server and Model 8664/8665 Installation Manual</td>
<td>935.4521</td>
</tr>
<tr>
<td>Red Hawk PowerSense Power over Ethernet Installation Manual</td>
<td>935.0400</td>
</tr>
<tr>
<td>AudioCodes MP-104 Quick Start Guide</td>
<td>835.2740</td>
</tr>
</tbody>
</table>
19. FCC INFORMATION

19.1 The IP SLA complies with UL1950/CSA950 and EN 60950 standards and complies with EN 55022 and Part 15 of the FCC Rules.

19.2 The IP PhonePlus has a hearing-aid compatible handset that is in compliance with section 68.316 of the FCC Rules.

19.3 The IP devices comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
   • This device may not cause harmful interference.
   • This device must accept any interference received, including interference that may cause undesired operation.

19.4 The AudioCodes MP-100 and MP-104 FXO comply with Part 68 of the FCC Rules.

19.5 For further FCC information, refer to the Inter-Tel Axxess Installation and Maintenance Manual (document part no. 550.8000).

20. GLOSSARY

• **BOOTP (Bootstrap Protocol):** A protocol that lets a network user be automatically configured (receive an IP address) and have an operating system booted or initiated without user involvement.

• **Circuit:** Crosspoint connection on the IPRC.

• **Cookie:** Refers to the state information that passes between a Web server and user agent (Web client). This information is stored by the user agent.

• **DHCP (Dynamic Host Configuration Protocol):** Allows a network administrator to supervise and distribute IP addresses from a central point and automatically send a new IP address when a computer is plugged into a different place in the network.

• **Firewall:** A set of related programs, located at a network gateway server, that protects the resources of a private network from users on other networks.

• **Frame Relay:** A telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and end-points in a wide area network (WAN).

• **Gateway:** A network point that acts as an entrance to another network.

• **IE:** Microsoft Internet Explorer.

• **IP (Internet Protocol):** The method or protocol by which data is sent from one computer to another on the Internet.

• **IPT (Internet Protocol Terminal):** IP PhonePlus or Model 8660 endpoint (IP PhonePlus), IP Single-Line Adapter (IPSLA), or IP SoftPhone (IPSOFT).

• **LAN (Local Area Network):** A network of interconnected workstations sharing the resources of a single processor or server within a relatively small geographic area.

• **MGCP (Media Gateway Control Protocol):** A protocol for controlling telephony gateways from external call control elements called media gateway controllers or call agents.

• **MGCP Gateway:** Network device that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks using MGCP.
• **MGCP Gateway Endpoint:** MGCP endpoints are physical/virtual sources or sinks of data that reside in an MGCP gateway.

• **NAT (Network Address Translation):** The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.

• **Network:** A series of points or nodes interconnected by communication paths.

• **OLMN:** Online Monitor.

• **Ports:** A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.

• **Packet:** A packet is the unit of data that is routed between an origin and a destination on the Internet or an any other packet-switched network.

• **Proxy Server:** A server that acts as an intermediary device between a workstation user and the Internet to ensure security, administrative control, and caching service capabilities. A proxy server is associated with or is part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

• **Router:** A device or, in some cases, software in a computer that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is located at any juncture of networks. A router is often included as part of a network switch.

• **RTP (Real-time Transport Protocol):** A protocol that ships real-time packets, such as voice packets, from one endpoint to another endpoint.

• **SIP (Session Initiation Protocol):** A text-based, standards protocol, similar to Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP).

• **Subnet:** An identifiably separate part of an organization’s network. Typically, a subnet may represent all of the machines at one geographic location, in one building, or on the same local area network (LAN).

• **TCP (Transmission Control Protocol):** A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet.

• **UDP (User Datagram Protocol):** A communications method that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet. UDP is an alternative to the Transmission Control Protocol (TCP). It also provides port numbers to help distinguish different user requests.

• **WAN (Wide Area Network):** A geographically dispersed telecommunications network, distinguishing a broader telecommunication structure from a local area network (LAN).
Index

Numerics

0 144
10/100 Switch
default switch 128
program switch 127
10/100 Switch — Default Switch 128
10/100 Switch — Program Switch 127
10Base-T Module 33, 34
16 MB RAM, 4 MB flash memory, enhanced 5
16 MB RAM, 4 MB flash memory, enhanced, redesigned 5
16 MB RAM, 4 MB flash memory, noise-reduced 5
16 MB RAM, 4 MB flash memory, original 5
16-Port Station PAL for IPRC 206
32-Device IPRC Software License 206
8 MB RAM, 2 MB flash memory, original 5
8 MB RAM, 4 MB flash memory, original 5
8690 Client Application 173
8-Port Station PAL for IPRC 206

A

ADDRESS 51
Address 51
ADDRESS AT 51
Advanced Audio Settings 114
Advanced Network Configuration 113
Application Name 155
Application Programming 20
Audio & Call Control 148
  card configuration 95
  circuit configuration 101
  device configuration 103
Audio Channel 120
Audio Frames per IP Packet 10
Audio Frames/IP Packet 96, 104, 113, 136, 149
Audio Frames/IP Packet (3) 104, 113
Audio Frames/IP Packet (Default) 96
Audio Issues 195
Audio Port 149
Audio Quality 196
Audio quality is poor 195
Audio quality is poor (Continued) 196
Audio Settings 113, 164
Audio Stream 96
  receive port 95, 96, 133, 149
  send port 96, 104, 113, 135
  transmit IP address 149
  transmit port 149
Audio Stream Receive Port 149
Audio Stream Receive Port (5004) 95, 133
Audio Stream Send Port (5004) 104, 113, 135
Audio Stream Send/Receive Port (5004) 96
Audio Stream Transmit IP Address 149
Audio Stream Transmit Port 149
AudioCodes
configuration 184
gateway device 178, 188, 189
MP-100 175
MP-100/104 CD-ROM 207
MP-104 188, 189
AudioCodes MP-100 Gateway 178
AudioCodes MP-100 MGCP Gateway 178
AudioCodes MP-100/104 CD-ROM 207
AudioCodes MP-104 Gateway 188, 189
AudioCodes MP-104 MGCP Gateway 188
AudioCodes MP-104 Quick Start Guide 207
AudioCodes MP-104 SIP Gateway 189
Automated Boot Code Update 72
Average Network Jitter 120
Average Network Jitter (ms) (0) 120
Awaiting Download 49
Axxess Database Programming 167
Axxess Database Programming in ITP mode 167
Axxess IP PhonePlus 44
  with 10Base-T Hub 206
Axxess IP PhonePlus with 10Base-T Hub 206
Axxess IP SoftPhone 190

B

Backplane
  companding type 96
  transmit signal gain 95
Backplane Companding Type(Mu-Law) 96
Backplane Transmit Signal Gain (0dB) 95
Bandwidth Utilization 8
Barrel Jack 34
Base UDP Port 185
Board
  IP address 185
  subnet mask 185
Boot Code Date/Time 155
Boot Code Download Progress Displays 72
Boot Code Version 155
Boot File 182
Boot Image Changes 72
BOOTP 82, 100
  Client IP Address 101, 113
  client IP address 113
  IP Address 135
  IP address 135
  BOOTP (Enabled) 100
BOOTP Client IP Address (0.0.0.0) 101, 113
BOOTP IP Address (0.0.0.0) 135
BOOTP? 82
Burst Rate (BR) 7

C

Calculations
  latency 10
  voice over IP 8
  VoIP across frame relay 9
Call Agent
domain name 185
Index
AXXESS® IP DEVICES MANUAL – Revised, April 2006

IP 185
IP address 182
Call Control 112
CALL PROCESSING 51
Card or Device Configuration
audio & call control 95
change login password 97
network 93
Card or Device Configuration — Audio & Call Control 95
Card or Device Configuration — Change Login Password 97
Card or Device Configuration — Network 93
Card Slot 121
Card Slot (Unknown) 121
CF (Compact Flash) 39
CHANGE CASE 143
Change Login Password 97
Changes and New Features 3
CIR (Committed Information Rate) 7
Circuit 98, 99, 100, 101, 103, 104, 106, 110, 120, 121, 123
Circuit (or Audio Channel) 120
Circuit Configuration
  circuit login password 106
  device information 98
  device specific 111
  network 100
Circuit Configuration — Advanced Audio Settings 106
Circuit Configuration — Advanced Network 101
Circuit Configuration — Audio Settings 104
Circuit Configuration — Call Control 103
Circuit Configuration — Device Information 99
Circuit Configuration — Device Login Password 110
Circuit Configuration — Device Specific 111
Circuit Configuration — Device Type 98
Circuit Configuration — Network 100
Client
  MAC 182
  name 182
Codec Type 149
Command 157
  configuration 157
  download 125
  reset 122, 157
  reset circuits 123
Command — Download 125
Command — Reset 122
Command — Reset Circuits 123
Committed Information Rate (CIR) 7
Compact Flash (CF) 39
Completed State 49
Computer Science Roots 4
Configuration 157
Configuration Files 66
Configuration Image Version 157
Configuration Parameters
  audio settings 164
  ITP mode settings 161
  network settings 159
  SIP mode settings 162
  SIP settings 163
Configuring the IPRC 187
Configuring the MP-100 184
Confirm New Login Password 110

Confiuring Phone Ports for a VLAN 174
Connected (NO) 121
Connecting
  the IP device 92
  to the IPRC 50
CONNECTING TO 50
Connection Issues 193
CONTACT IP CARD 51
COULD NOT 51
COUNT NOT 51
Country 96, 109, 117
Country (US) 96, 109, 117

D

Database
  default 126
  programming 131
  restore 126
  save 125
Database — Default 126
Database — Restore 126
Database — Save 125
Date/Time 155
DBDS (Database Device Specific) 138
DBMN (Database Main Entries) 138
Default
  database 83, 126, 144
  database and exit 83, 144
  gateway 82, 143
  gateway address 185
  IP gateway 86, 89
  IP gateway address 93, 100, 112, 147
  network subnet mask 93, 100, 112, 147
Default Database and Exit 83, 144
DEFAULT GATEWAY 82, 143
Default Gateway 155
Default IP Gateway (0.0.0.0) 86, 89
Default IP Gateway Address 147
Default IP Gateway Address (0.0.0.0) 93, 100, 112
Default Network Subnet Mask 147
Default Network Subnet Mask (0.0.0.0) 93, 100, 112
Description 120, 121
Determine the IP address of a Model 8600 67
Device
  description 98, 99, 100, 101, 103, 104, 106, 110, 111, 123, 136
  flags 136, 137, 139, 140
  hostname 140
  ID 99, 112, 121, 123
  information 98, 99, 111
  IP address 123
  IPRC PALs 206
  number 111, 135
  password 136, 138
  quick setup 88
  specific 111
  type 98, 112, 121, 123
Device Configuration 147
  feature code 154
  SIP 152
Device Description 98, 99, 100, 101, 103, 104, 106, 110, 111, 123
- Change (Y/N)? 136
Device Flags
 0 (in octal format) 139
Device Flags (00000206 in octal format) 136
Device Flags 2
 0 140
Device Flags 2 (00000000) 137
Device Hostname - Change (Y/N)? 140
Device ID 121
Device ID (Unused) 121
Device ID or Ethernet Address 99, 112, 123
Device Information 111
Device IP Address 123
Device IPRC PALs 206
Device Number
 01 135
Device Number (1) 111
Device Password
  - Change (Y/N)? 136
Device Password - Change (Y/N)? 138
Device Type 123
Device Type (IP PhonePlus) 98, 112, 121
Devices 206
Device-Specific Configuration File 66
DHCP 93, 113
DHCP (Dynamic Host Configuration Protocol) 26, 82, 100, 143
on the alternate subnet 12
  on the subnet 11
DHCP (Enabled) 100
DHCP Server 155
DHCP? 82, 143
 Diagnostic 131
  audio receive statistics 132
  audio send statistics 132
  audio session send configuration 132
  connection status 132
  crosspoint connections 132
  DSP events statistics 132
  echo canceller statistics 132
  message server setup 131
  NIC statistics 132
  thread registry 132
  timer-alarm statistics 132
DiffServ 149
Direct Connection (RS-232 Method) 61
DISABLE 144
Display Name 153
DNS Server 155
Documentation 207
Download
  completed 49
  firmware 64, 125
  status 157
Download Aborted
  file corrupted 49
  file too big 49
DOWNLOAD ABORTEDFILE CORRUPTED 49
DOWNLOAD ABORTEDFILE TOO BIG 49
DOWNLOAD COMPLETED 49
Download Error Message Displays 73
Download Status 157
DSCP (DiffServ Cord Point) 127
DSP (Digital Signal Processor) 27, 28
  failure 51
  not running 51
DSP FAILURE 51
DSP NOT RUNNING 51
DTMF (Dual-Tone Multifrequency) 177
  encoding setting 96, 106, 114
  signaling 177
  transport type 186
DTMF Encoding Setting (1-way) 106, 114
DTMF Encoding Setting (Default - 1-way) 96
Duplex 155
DUPLICATE IP 51
Duplicate IP 51
Duplicate-IP Error Message 51

E

Echo
  issues 198
    saturation blocker 117
    saturation blocker 109, 117
    suppression 107, 116
    suppression sensitivity level 116
Echo Issues 198
Echo Saturation Blocker (Enabled) 109, 117
Echo Suppression (Enabled) Echo Suppression Sensitivity Level (0) 107, 116
Echo Suppression Sensitivity Level is not balanced 199
Eclipse IP PhonePlus 34, 45
Eclipse IP PhonePlus with 10Base-T Hub 206
Eclipse IP SoftPhone 191
Emergency
  extension 30
    outgoing access 30
Enable Telnet Server 101
Enable Telnet Server (Enabled) 101
Enable TFTP Configuration Update 148
Enable Web Server 101
Enable Web Server (Enabled) 101
Endpoint is not programmed 194
Endpoint Name 185
Endpoints and Phones 4
ERASING FLASH 49
Erasing Flash 49
Error Messages
  duplicate IP 51
  TCP failed 51
  UDP failed 51
Error State
  file corrupted 49
  file too big 49
  flash erase 49
  flash program 49
  memory map 49
ETHERNET 51
Ethernet 51
Ethernet Address 99, 112, 123, 135
Exit 83, 144
Fax/Modem Bypass Coder Type 186
FCC Information 208
Feature Code 154
FF is default
Finding
   IP card 50
   IP card address 50
FINDING IP CARD 50
Firewall 13, 86
Firmware 5, 155
   update file 66
   version 118
Firmware Download Progress Displays 71
Firmware Download Startup 71
For IP PhonePlus and Model 8660 49
For IP PhonePlus and Model 8660/8620/8662/8690 50
For IP PhonePlus and Model 8660/8620/8662/8690 50
Frame Size 10

Gateway
device 136
   IP address 182
   name 185
Gateway Device (00) 136
General Connection Issues 193
General connection issues 193
Global Configuration File 66
Glossary 208

Handset Call 156
Handset Jack 34, 35
Handset Tone 156
Hard Multi-Protocol Endpoints 1
Hardware Failure
   flash erasure 49
   flash program 49
   memory map 49
HARDWARE FAILUREFLASH ERASURE 49
HARDWARE FAILUREFLASH PROGRAM 49
HARDWARE FAILUREMEMORY MAP 49
Hardware Revision Identification 52
Hardware Type 155
Headset Call 156
Headset Tone 156
Hold Reminder Time 151
Hops 7
Host name/Endpoint name
   ACgw0 - Change (Y/N)? 136
Host/Endpoint Name 99, 112, 136
HOSTNAME 82
Hostname 82, 93, 133
HTTP/Web Interface Method 63, 84
Hybrid balance is not on the correct setting 198

IC Dial Plan 151
IEC (International Electrical Cord) 42
Image URL 150
Image Version 150, 155, 157
INI File 182
INITIALIZING 50
Initializing 50
Installation 41
Installing
   the IP and Multi-Protocol Endpoints 32
   the IP devices 26
   the IP PhonePlus 32
   the IP SLA 56
   the IPRC 27, 28, 29
   the Model 8690 173
Installing the IP and Multi-Protocol Endpoints 32
Installing the IP SLA 56
Installing the IPRC 27, 29
Inter-Tel Axxess Installation Maintenance Manual 207
Inter-Tel Protocol (ITP) Mode vs. SIP Mode 53
Intime Frames 120
Intime Frames (%) (100%) 120
Introduction 1
IP 182
IP Address 86, 89, 121, 155
IP Address (0.0.0.0) 121
IP Address (192.168.200.201) 86, 89
IP Address Assignment 93, 113, 147
IP Address Assignment (DHCP) 93, 113
IP Device
   alternative methods 63
   CD-ROM 207
   configuration 89, 90
IP Devices CD-ROM 207
IP Endpoint Status Displays 49
IP Endpoints
   Axxess IP PhonePlus 44, 206
   Axxess IP SoftPhone 44, 190
   Eclipse IP PhonePlus 45, 206
   Eclipse IP SoftPhone 191
   IP SLA 56
   Model 8660 206
   Model 8664 206
   Model 8665 206
IP endpoints are behind a firewall 196
IP Gateway Address 133
IP Gateway Address (0.0.0.0) 133
IP Local Loop Support 175
IP Network
   bandwidth utilization 8
   performance 6
IP Network Specifications 6
IP Networking Ports
   16 Ports 206
   32 Ports 206
   4 Ports 206
8 Ports  206
IP Phone Status Displays  49
IP Phone Web Client  145
IP PhonePlus with 10Base-T Module  33, 34
IP Resource Card (IPRC)  206
IP Single-Line Adapter  206
IP SoftPhone  190
IP Terminal General Purpose UDP Port  148
IP Terminal TCP Call Control Port  148
IPRC (IP Resource Card)  28
diagnostics  205
firmware compatibilities  5
PAL upgrade  206
v1.5.x firmware  80
v8.2.x firmware  141
web page  209
IPRC Diagnostics  205
IPRC Firmware Compatibilities  5
IPRC PAL Upgrade  206
IPRCs and Firewalls  13
ITP Mode  53, 55
Axess Database Programming  167
settings  161
ITP Mode Settings  161
ITP PhonePlus  33

J

Jitter  7

L

LAN QoS  154
LAN QoS for VLAN Tagging  25
LAN/POWER Jack  33, 34, 35, 37, 39
Last Download Error Page  157
Latency  6, 10
Learn Mode  81
LED (Light-Emitting Diode) Indicators  27
LEDs  33, 34, 35, 38, 40
Link Status  155
LOCAL IP CARD  51
Local IP Card  51

M

MAC ADDRESS  51
MAC Address  51, 147
Main Flags  134
Main Flags (00000001 in octal format)  134
Make-Busy Switch  27
Managed Private Network  6
Message Server
  IP address  133, 135, 139
  port  133, 135
  port number  139
Message Server IP Address  133, 135, 139
  0.0.0.0Message Server Port Number  5568  139
Message Server IP Address (0.0.0.0)  133, 135
Message Server Port  133, 135
Message Server Port (5568)  133, 135
Message Server Port Number  139
MGCP (Media Gateway Control Protocol)  175
  channel settings  186
  client settings  185
  communication layer timeout  185
  endpoint name setting  91
  gateway  175
  gateway additional endpoint  91
  gateway device + endpoint  90
  gateway device IP address  103, 135
  MGCP Endpoint’s Gateway Device (0)  98
  MGCP Gateway Device IP Address (0.0.0.0)  103
  Minimum Playback Buffer Time  10, 113
  Minimum Playback Buffer Time (ms)  105, 113
  Minimum Playback Buffer Time (ms) (80)  105, 113
  Miscellaneous — Date & Time  129
  Miscellaneous Date & Time  129
Model 8600  36, 206
Model 8600 — original  52
Model 8600 (8600)  5
Model 8600 Multi-Protocol Endpoint  206
Model 8600 Series Endpoints  46
Model 8601 SoftPhone for Pocket PC  206, 207
Model 8601 SoftPhone for Pocket PC Installation Manual  207
Model 8602  192
Model 8620  36, 206
Model 8620 — original  52
Model 8620 (8620)  5
Model 8622  206
Model 8622 — enhanced, redesigned  52
Model 8622 — original  52
Model 8622 (8622)  5
Model 8622 (8622v2)  5
Model 8660  35, 206
Model 8660 Endpoint  206
Model 8662  36, 206
Model 8662 — enhanced  52
Model 8662 — enhanced, redesigned  52
Model 8662 — noise-reduced*  52
Model 8662 — original  52
Model 8662 (8662)  5
Model 8662 (8662i)  5
Model 8662 (8662v2)  5
Model 8664 Wireless IP Endpoint  1, 206
Model 8665 Wireless IP Endpoint  1, 206
Model 8690  39, 206
  installation  173
  running the Setup Wizard  168
  upgrade  169
Model 8690 Administrator’s Guide  207
Models 8600, 8620, and 8662  36
MP-100 MGCP Gateway 4-Port FXO  206
MP-104 MGCP Gateway 4-Port FXO  206
Multi-Protocol Endpoint Firmware Compatibilities  5
Multi-Protocol Endpoint  36
Index

AXXESS® IP DEVICES MANUAL – Revised, April 2006

Multi-Protocol Endpoint-Related Issues 199, 205
Multi-Protocol Endpoints
  Model 8600 36
  Model 8620 36, 206
  Model 8662 36
  Model 8690 39
Supported Features, Buttons, and LED Indications 207
MY IP ADDRESS 50

N

NAT (Network Address Translation) 11, 86
Negotiation 155
NetLink SVP Server and Model 8664/8665 Installation Manual 207
Network 93, 100, 147, 155
  configuration 175
  information 131
  status 118
Network Configuration 112
Network Parameters 159
Network Settings 159
New Login Password 110
NO RESPONSE 50
Normal 90
NOT FOUND 51
NOT PROGRAMMED / 51
Number of Audio Frames 149

O

Obtain IP Address automatically (DHCP) 86
Operation Behind Firewalls and Proxies 13
Operation Behind Firewalls or Proxies 13
Outgoing Dial Plan 151
Overwrite Device’s Local Settings 102, 114
Overwrite Device’s Local Settings (Enabled) 102, 114

P

Packet Loss 6
Part Numbers 206
PASSWORD 143
Password 84, 133, 143
Password - Change (Y/N)? 133
PC Ports 35, 38
PCMCIA (Personal Computer Memory Card International Association) 40
Peer-to-Peer (P2P) Audio 188
Phone 150
Phone Extension/Name 153
PHONE VLAN ID 144
Phonex Version 155
Physical Address 155
Placing the Devices in Download State 63
Playback Buffer (ms) 120
Playback Buffer (ms) (500) 120
Port 1-3 (OUT TO PC Jack) 34
Port Configuration 16
Positive Disconnect 176
Power Jack 33, 35
Power over Ethernet (PoE) Hub 42
Power Supply compatibilities 43
  UK 206, 207
  universal 42, 207
  US 206
Power Supply Compatibilities 43
Power Supply Parts 206
Preparing to Connect 91
Prioritize Assured Forwarding DSCP (DiffServ Cord Point) Values 127
Prioritize Assured Forwarding DSCP (DiffServ Cord Point) Values (Disabled) 127
Prioritize Assured Forwarding DSCP Values 127
Private Network 6
Processing Latency 10
Program Database 82, 143
Programming
  an emergency extension for IP devices 30
  database 82, 143
  the IP address 83, 144
PROGRAMMING CODE 49
Programming Code 49
Programming Fields
  RS-232/Telnet card 133
  RS-232/Telnet device 135
Programming State
  erasing flash memory 49
  programming flash memory 49
Programming the IP Devices
  on a v1.5.x firmware IPRC 80
  on a v8.2.x firmware IPRC 141
Programming the IP Devices on a v1.5.x Firmware IPRC 80
Programming the IP Devices on a v8.2.x Firmware IPRC 141
Proxies 13
Proxy Server IP Address 153
Proxy Server Port 153
QoS (Quality of Service) 154
QoS Settings 20
Quick Setup 131
  card 86
  device 88
Quick Setup — Card 86
Quick Setup — Device 88
Quick Start Installation Outline 26, 178

R

Real-Time Transport Protocol (RTP) 185
Receive 122, 124
Receive (OFF) 122, 124
Red Hawk PowerSense Power over Ethernet Installation Manual 207
Red Hawk PowerSense Single-Port Module
  24V Protocol 207
IEEE 802.3af Protocol 207
Red Hawk PowerSense Single-Port Module (24V Protocol) 207
Red Hawk PowerSense Single-Port Module (IEEE 802.3af Protocol) 207
Red Hawk PowerSense Single-Port Module for Multi-port Hub
24V Protocol 207
IEEE 802.3af Protocol 207
Red Hawk PowerSense Single-Port Module for Multi-port Hub (24V Protocol) 207
Red Hawk PowerSense Single-Port Module for Multi-port Hub (IEEE 802.3af Protocol) 207
Redundant
agent IP 185
agent port 185
call agent domain name 185
Reformatting the Model 8690 Flash File System 172
Register
period 153
server IP address 153
server port 153
Register Period 153
Register Server IP Address 153
Register Server Port 153
Remote
IP card 51
IPC IP 82, 143
IPRC IP address 96, 103, 112, 135, 138
IPRC/MGCP Gateway Device IP Address 135
server IP address 148
TCP port 143
UDP port 143
REMOTE IP CARD 51
REMOTE IPC IP 82, 143
Remote IPRC IP Address
0.0.0.0 138
Remote IPRC IP Address (0.0.0.0) 96, 103, 112
Remote IPRC/MGCP Gateway Device IP Address (255.255.255.0) 135
Remote Server IP Address 148
REMOTE TCP PORT 143
REMOTE UDP PORT 143
Reset 122, 124, 157
Reset Circuits 123
Restore Database 126
Ringer 156
RJ-45 10/100Base-T LAN Connection Port 27
RS-232 Connection Method (IPRC Only) 130
RS-232 Ports 27
RS-232/Telnet
card programming fields 133
device programming fields 135
IP device DBMN programming fields 138
RS-232/Telnet Card Programming Fields 133
RS-232/Telnet Device Programming Fields 135
RS-232/Telnet IP Devices Programming Fields 138
RTCP (Real-time Transport Control Protocol) 185
RTP (Real-Time Transport Protocol) 185
IP precedence 96
profile 8, 149
receive state 149
send state 149
RTP IP Precedence (Enabled) 96
RTP Profile 149
RTP Receive State 149
RTP Send State 149
Running the Setup Wizard 168
S
Save Database 125
Self-Programming Mode 82
for IP PhonePlus and Model 8660 82
for Models 8620 and 8662 142
Send 122, 123
Send (OFF) 122, 123
Service Type 177
Session Description 149
Setting Up the MP-100 179
SIP 152
SIP Audio Settings 164
SIP Dial Plan 163
SIP Mode 53, 55, 151
SIP Mode Settings 162
SIP Parameters 162, 163
SIP Server Installation and Configuration Manual 207
SIP Settings 162, 163
Soft SIP Endpoints 1
Software Images 165
Software Version 184
Speakerphone Call 156
Speakerphone Tone 156
Speech Encoding Setting 149
Speed 155
Static (Default) IP Address 93, 100, 112, 133, 147
Static (Default) IP Address (192.168.200.201) 93, 100, 112, 133
STATIC IP 82, 143
Static IP 82, 143
Static IP Address 135, 139
192.168.200.201 139
on the alternate subnet 12
on the subnet 11
Static IP Address (192.168.200.201) 135
Static IP Gateway 135, 139
0.0.0.0 139
Static IP Gateway (0.0.0.0) 135
STATIC SUBNET 82, 143
Static Subnet 82, 143
Static Subnet Mask 135, 139
255.255.255.0 139
Static Subnet Mask (0.0.0.0) 135
Status 155
call statistics 119
circuits 121
firmware version 118
network 118, 119
receive audio 119
volume 156
Status — Circuits 121
Status — Firmware Version 118
Status — Network 118
Status — Receive Audio (or Call Statistics) 119
Subnet
IP address 182
Index

V

Version 132
Virtual Local Area Network (VLAN) Tagging Support 22
VLAN IDs 23
VLAN Tagging-Related Issues 205
Vocoder Type 96, 104, 113, 135
Vocoder Type (Default) 96, 104, 113
Vocoder Type (FF - Default) 135
Vocoders (Voice Codec) 8
Voice Activity Detection 96, 107, 115, 149
Voice Activity Detection (Disabled) 96, 107, 115
Voice Mail 153
Voice Over IP
  across frame relay bandwidth calculation 9
  bandwidth calculation 8
Volume 156

W

WAITING FOR 51
WAITING FOR DOWNLOAD 49
Waiting for Ethernet Address 51
Wall Mounting 44
  the Axxess IP PhonePlus 44
  the Eclipse IP PhonePlus 45
  the IP PhonePlus 44
  the Model 8600 series endpoints 46
Web Interface 145
Web Interface Changes 146
Web Server 94, 114
Web Server (Enabled) 94, 114
Windows CE .NET Programming (Model 8690 Only) 168
WINS Server 93, 101, 113
WINS Server (0.0.0.0) 93, 101, 113
WINS Server IP Address 133, 136, 140
WINS Server IP Address (0.0.0.0) 133, 136, 140