Avaya Voice Priority Processor
Avaya 3641/3645 Wireless IP Telephones
Handset Administration Tool

Installation, Configuration, and Administration
For CCMS Protocol
© 2007 Avaya Inc.  
All Rights Reserved.  

Notice  
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full support information, please see the complete document, Avaya Support Notices for Hardware Documentation, document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer  
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer  
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty  
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Copyright  
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support  
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support.
About This Document
Part A explains how to configure and maintain one or more Avaya Voice Priority Processors (AVPP) (models AVPP, AVPP 20, AVPP 10) within IP telephony environments.

Part B explains how to configure and maintain the Avaya 3641/3645 Wireless IP Telephone with an Avaya Communication Manager (such as an Avaya™ MultiVantage™ on a DEFINITY® Server SI or an Avaya™ S8100 Media Server with CMC1 Media Gateway).

Part C explains how to install and use the Handset Administration Tool, a software utility that automates the configuration of multiple Avaya 3641/3645 Wireless IP Telephones.

Part D is the Appendix which contains troubleshooting information and lists status messages that may appear on the handset display.

Part E is the Index.

Hotline
If you have questions please contact Avaya Technical Support at 1-800-242-2121 (USA only) or your local authorized Avaya dealer.

Icons and Conventions
This manual uses the following icons and conventions:

- **Caution!** Follow these instructions carefully to avoid danger.

- **Note** these instructions carefully.

- **NORM** This typeface indicates a key, label, or button on the AVPP, Wireless IP Telephone or Handset Administration Tool.
Contents

A. Avaya Voice Priority Processor ................................................................. 7
1. Avaya Voice Priority Processor Overview ................................................. 8
  1.1 SpectraLink Voice Priority (SVP), QoS and Security ............................. 8
  1.2 Avaya Voice Priority Processor Models .............................................. 9
  1.3 The Timing Function ........................................................................ 9
  1.4 Multiple Avaya Voice Priority Processors/Master Avaya Voice Priority Processor ... 9
  1.5 Multiple Avaya Voice Priority Processor Capacities .......................... 10
  1.6 Notes on System Configuration ......................................................... 11
  1.7 System Diagram ........................................................................... 12
  1.8 System Components ................................................................... 13
  1.9 The Front Panel of the Avaya Voice Priority Processor ...................... 15
2. Installing the Avaya Voice Priority Processor ........................................... 16
  2.1 Required Materials ..................................................................... 16
  2.2 Locate the Avaya Voice Priority Processor ...................................... 16
  2.3 Install the Avaya Voice Priority Processor ....................................... 16
3. Configuring the Avaya Voice Priority Processor ....................................... 18
  3.1 Connecting to the Avaya Voice Priority Processor ............................ 18
  3.2 The NetLink SVP-II System Menu .................................................. 19
  3.3 Network Configuration .................................................................. 20
  3.4 AVPP Configuration ....................................................................... 23
  3.5 Change Password .......................................................................... 27
4. Swapping/Add/Deleting AVPPs ................................................................. 28
5. Software Maintenance ............................................................................ 29
6. Troubleshooting via System Status Menu ................................................ 30
  6.1 Error Status ............................................................................... 31
  6.2 Network Status ........................................................................... 32
  6.3 Software Version ......................................................................... 34

B. Avaya 3641/3645 Wireless IP Telephones .............................................. 35
1. Avaya 3641/3645 Wireless IP Telephone Overview ............................... 36
  1.1 Quick Start Guide ....................................................................... 37
2. The Avaya 3641/3645 Wireless IP Telephones ....................................... 38
  2.1 Specifications ............................................................................ 38
  2.2 Handset Display ......................................................................... 39
  2.3 Startup Sequence ....................................................................... 40
  2.4 Wireless IP Telephone Modes ...................................................... 41
3. Avaya Communication Manager Configuration ....................................... 42
  3.1 Configuring a Standalone Station ................................................... 42
  3.2 Configuring an Associated Station ............................................... 42
4. Avaya 3641/3645 Wireless IP Telephone Configuration .......................... 43
  4.1 The Admin Menu ....................................................................... 43
  4.2 Configuration (Config) Menu ........................................................... 53
Contents

5. Software License and Protocol Management ............................................................. 55
   5.1 Requirements .................................................................................................. 55
   5.2 Configuration Process .................................................................................. 55
6. Avaya Communication Manager Integration Factors ....................................... 57
7. Feature Programming ......................................................................................... 60
   7.1 Softkey Assignment ..................................................................................... 61
   7.2 Function Assignment .................................................................................. 61
8. Testing a Wireless IP Telephone ........................................................................ 63
9. Diagnostic Tools .................................................................................................. 64
   9.1 Run Site Survey .......................................................................................... 64
   9.2 Diagnostics Enabled ................................................................................... 66
   9.3 Syslog Mode ............................................................................................... 69
10. Certifying the Wireless IP Telephones ............................................................ 71
   10.1 Conducting a Site Survey ......................................................................... 71
11. Software Maintenance ....................................................................................... 72
   11.1 Upgrading Wireless IP Telephones ......................................................... 72
C. Handset Administration Tool .............................................................................. 75
   1. Handset Administration Tool Installation ..................................................... 76
      1.1 Installing the USB Driver ....................................................................... 76
      1.2 Install the Handset Administration Tool .............................................. 79
   2. Using the Handset Administration Tool Console ........................................ 84
      2.1 Connecting the Handset ....................................................................... 84
      2.2 Password Configuration ...................................................................... 86
      2.3 Error Information ................................................................................. 87
      2.4 Software Updates ............................................................................... 88
      2.5 Version ............................................................................................... 89
   3. Configuring Admin Menu Settings .................................................................. 90
D. Appendix ............................................................................................................. 95
   Troubleshooting Wireless IP Telephone Problems ........................................... 95
   Access Point Problems ...................................................................................... 95
   Configuration Problems .................................................................................... 95
   Wireless IP Telephone Status Messages ......................................................... 96
E. Index ..................................................................................................................... 107
A. Avaya Voice Priority Processor

AVPP
AVPP 20
AVPP 10

Installation, Configuration, and Administration
For CCMS
1. **Avaya Voice Priority Processor Overview**

The Avaya Voice Priority Processor is an Ethernet LAN device that works with access points (APs) to provide QoS on the wireless LAN. Voice packets to and from the Avaya Wireless IP Telephones are intercepted by the Avaya Voice Priority Processor and encapsulated for prioritization as they are routed to and from an IP telephony server.

1.1 **SpectraLink Voice Priority (SVP), QoS and Security**

The Avaya Voice Priority Processor (AVPP) is an Ethernet LAN device that works with the AP to provide quality of service QoS on the wireless LAN. Voice packets to and from the Avaya 3641/3645 Wireless IP Telephones are intercepted by the Avaya Voice Priority Processor and encapsulated for prioritization as they are routed to and from an IP telephony server or gateway.

The Avaya 3641/3645 Wireless IP Telephone supports Wired Equivalent Privacy (WEP) as defined by the 802.11 specification. Avaya offers the product with both 40-bit and 128-bit encryption.

Avaya 3641/3645 Wireless IP Telephones support basic WMM™ as part of the 802.11e protocol. If the AP supports WMM, the Wireless IP Telephone automatically discovers and uses it. WMM does not replace the Avaya Voice Priority Processor as described in the following paragraph. WMM settings must be configured on the AVPP.

Avaya 3641/3645 Wireless IP Telephones also support the 802.11i protocol including Wi-Fi Protected Access (WPA™ and WPA2™)—PSK. Please see the Avaya Access Point references for information about compatible systems.

The latest software versions are required to support the features described in this document.

SpectraLink Voice Priority (SVP) is the quality of service (QoS) mechanism that is implemented in the Wireless IP Telephone and access point (AP) to enhance voice quality over the wireless network. SVP gives preference to voice packets over data packets on the wireless medium, increasing the probability that all voice packets are transmitted efficiently and with minimum delay. SVP is fully compatible with the IEEE 802.11b standards.

Avaya Wireless IP Telephones support basic WMM (Wi-Fi Multimedia) if also supported by the AP as part of the 802.11e protocol. If the AP supports WMM, the Wireless IP Telephone automatically discovers and uses it. WMM does not replace the Avaya Voice Priority Processor.
1.2 **Avaya Voice Priority Processor Models**

The AVPP is available in three models. Which model is selected for your facility depends on current and expected capacity. All AVPPs within a subnet must be the same model type.

- AVPP – Serves 80 calls simultaneously.
- AVPP 20 – Serves 20 powered-on handsets.
- AVPP 10 – Serves 10 powered-on handsets.

See the following capacity tables for multiple AVPP system capacities.

All AVPP models are installed, configured and administered according to the instructions in this document. The model information is available on the Software Version screen. See section 7.3 *Software Version*.

1.3 **The Timing Function**

Avaya Voice Priority Processors provide the connection or "gateway" to the IP PBX for the Wireless IP Telephones and the "timing" function for active calls. This "gateway" function is distributed across the AVPPs.

The number of active AVPPs is determined dynamically. Whenever AVPPs are added to or removed from the system, the distribution of the "timing" function for active calls is affected.

1.4 **Multiple Avaya Voice Priority Processors/Master Avaya Voice Priority Processor**

Multiple AVPP environments are those which have more than one Avaya Voice Priority Processor. Up to four AVPP 10 models or up to two AVPP 20 models may be installed in any one subnet. Up to 16 models of AVPP Servers may be installed in any one subnet. All AVPPs must be in the same subnet.

In a system comprised of multiple AVPPs, a master AVPP must be identified. The master AVPP must have a static IP address. The Wireless IP Telephones and the other AVPPs locate the master by using a static IP address, DHCP, or DNS.

The master AVPP performs important coordinating functions. The loss of a non-master AVPP does not significantly affect the operation of the remaining AVPPs but results in the reboot of all handsets. However, the loss of the master AVPP results in a loss of all communication between all of the AVPPs. This also means that the loss of the master AVPP results in the loss of all active calls and Wireless IP Telephones cannot check-in until communication with the master is reestablished.
Part A: Avaya Voice Priority Processor

1.5 Multiple Avaya Voice Priority Processor Capacities

The system capacity of each AVPP model is shown in the below tables. Note that AVPP models may not be combined within one subnet.

**AVPP 10 and AVPP 20 Server Capacity**

The system capacity of the AVPP 10 and AVPP 20 is measured by number of powered-on handsets. If this number exceeds the maximum, the handset that cannot be served will display an error and will not connect to the AVPP. Other handsets will not be affected.

<table>
<thead>
<tr>
<th>Number of AVPPs</th>
<th>AVPP 10</th>
<th>AVPP 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>3</td>
<td>30</td>
<td>NA</td>
</tr>
<tr>
<td>4</td>
<td>40</td>
<td>NA</td>
</tr>
</tbody>
</table>

**AVPP Server Capacity**

The capacity of the AVPP Server is determined by active calls. The table below shows the capacity of an IP gateway in a multiple-AVPP environment.

<table>
<thead>
<tr>
<th>AVPPs</th>
<th>Calls per server</th>
<th>Total Calls</th>
<th>Erlangs</th>
<th>10% use</th>
<th>15% use</th>
<th>20% use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>80</td>
<td>80</td>
<td>65</td>
<td>500</td>
<td>433</td>
<td>325</td>
</tr>
<tr>
<td>2</td>
<td>64</td>
<td>128</td>
<td>111</td>
<td>1000</td>
<td>740</td>
<td>555</td>
</tr>
<tr>
<td>3</td>
<td>60</td>
<td>180</td>
<td>160</td>
<td>1500</td>
<td>1067</td>
<td>800</td>
</tr>
<tr>
<td>4</td>
<td>58</td>
<td>232</td>
<td>211</td>
<td>2000</td>
<td>1407</td>
<td>1055</td>
</tr>
<tr>
<td>5</td>
<td>57</td>
<td>285</td>
<td>262</td>
<td>2500</td>
<td>1747</td>
<td>1310</td>
</tr>
<tr>
<td>6</td>
<td>56</td>
<td>336</td>
<td>312</td>
<td>3000</td>
<td>2080</td>
<td>1560</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
<td>392</td>
<td>367</td>
<td>3500</td>
<td>2447</td>
<td>1835</td>
</tr>
<tr>
<td>8</td>
<td>55</td>
<td>440</td>
<td>415</td>
<td>4000</td>
<td>2767</td>
<td>2075</td>
</tr>
<tr>
<td>9</td>
<td>55</td>
<td>495</td>
<td>469</td>
<td>4500</td>
<td>3127</td>
<td>2345</td>
</tr>
<tr>
<td>10</td>
<td>55</td>
<td>550</td>
<td>524</td>
<td>5000</td>
<td>3493</td>
<td>2620</td>
</tr>
<tr>
<td>11</td>
<td>55</td>
<td>605</td>
<td>578</td>
<td>5500</td>
<td>3853</td>
<td>2890</td>
</tr>
<tr>
<td>12</td>
<td>54</td>
<td>648</td>
<td>621</td>
<td>6000</td>
<td>4140</td>
<td>3105</td>
</tr>
<tr>
<td>13</td>
<td>54</td>
<td>702</td>
<td>674</td>
<td>6500</td>
<td>4493</td>
<td>3370</td>
</tr>
<tr>
<td>14</td>
<td>54</td>
<td>756</td>
<td>728</td>
<td>7000</td>
<td>4853</td>
<td>3640</td>
</tr>
<tr>
<td>15</td>
<td>54</td>
<td>810</td>
<td>782</td>
<td>7500</td>
<td>5213</td>
<td>3910</td>
</tr>
<tr>
<td>16</td>
<td>54</td>
<td>864</td>
<td>836</td>
<td>8000</td>
<td>5573</td>
<td>4180</td>
</tr>
</tbody>
</table>
1.6 Notes on System Configuration

In an IP system using subnets to differentiate telephony areas, each subnet must have its own access points. Each subnet may require an AVPP to maintain voice quality, but this depends on traffic volume and router capacity.

Multiple AVPP environments are those which have more than one AVPP. A master AVPP must be identified in a multiple-AVPP environment.

AVPP models may not be combined within one subnet. More than one AVPP model type may be used within a facility if installed on different subnets.

Wireless IP Telephones cannot roam with uninterrupted service between subnets unless specific LAN components are present. Certain AP/Ethernet switch combinations establish a layer-2 tunnel across subnets that enables the handsets to roam. Without this capability, any call in progress will be dropped when the user moves out of range and the handset must be power-cycled in order to resume functionality in the new subnet area.

Please contact your service representative for detailed configuration information when installing multiple AVPP models across several different subnets.

IP multicast addresses are used by the Avaya 3645 Wireless IP Telephone system. This requires that multicasting be enabled on the subnet used for the Avaya Wireless IP Telephones, AVPP, and Avaya Communication Manager.

The Avaya Voice Priority Processor requires a Cat. 5 cable connection between its network port and the Ethernet switch. The Avaya Voice Priority Processor auto-negotiates to the type of port on the Ethernet switch and supports 10Base-T, 100Base-T, full-duplex and half-duplex port types.
1.7 System Diagram

The following diagram shows multiple Avaya Voice Priority Processors residing on a network with an IP telephony gateway and Avaya Communication Manager, wireless LAN access points, and Ethernet switch.
1.8 System Components

**Avaya 3641/3645 Wireless IP Telephone**
The Avaya 3641 Wireless IP Telephone is a lightweight, durable handset specifically designed for mobile workplace use within a facility using the Avaya Communication Manager and 802.11 APs in a wireless LAN.

The Avaya 3645 Wireless IP Telephone offers a durable design with push-to-talk functionality.

Wireless IP Telephone functionality is provided by emulating the Avaya IP 4612 telephone. The Avaya 3641/3645 Wireless IP Telephones support six predefined feature keys and a mixture of twelve programmable line and feature keys. Among other features, the Wireless IP Telephone can receive calls directly, receive transferred calls, transfer calls to other extensions, make conference calls, and make outside and long distance calls (subject to the restrictions applied in your facility.) The Wireless IP Telephones are to be used on-premises; they are not cellular or satellite phones.

Avaya 3641/3645 Wireless IP Telephones use direct-sequence spread spectrum radio technology to transmit audio packets over wireless LAN APs that support the Avaya Wireless PC card.

**Avaya Voice Priority Processor**
The Avaya Voice Priority Processor (AVPP) is an Ethernet LAN appliance that works with the AP to provide QoS on the wireless LAN. All packets to and from the Avaya 3641/3645 Wireless IP Telephones pass through the Avaya Voice Priority Processor and are encapsulated for prioritization as they are routed to and from the Avaya Communication Manager.

SpectraLink Voice Priority (SVP) is the Quality of Service (QoS) mechanism that is implemented in the AVPP, Wireless IP Telephones and APs to enhance voice quality over the wireless network. SVP gives preference to voice packets over data packets on the wireless medium, increasing the probability that all voice packets are transmitted efficiently and with minimum or no delay. SVP is fully compatible with IEEE 802.11b standards.

**Avaya Communication Manager**
The Avaya Communication Manager is the call-processing component of the Avaya IP telephony solution.

**Access Points**
Access points (APs) provide the connection between the wired Ethernet LAN and the wireless (802.11) LAN. Access points must be positioned in all areas where Wireless IP Telephones will be used. The number and placement of access points will affect the coverage area and capacity of the wireless system. Typically, the requirements for use of Avaya 3641/3645 Wireless IP Telephones are similar to those of wireless data devices.

**Ethernet Switch**
Ethernet switches interconnect multiple network devices, including the Avaya Voice Priority Processor, Avaya Communication Manager, Avaya IP Phones and the access points. Ethernet switches provide the highest performance networks, which can handle combined voice and data traffic, and are required when using the Avaya 3641/3645 Wireless IP Telephones.
Although a single Ethernet switch network is recommended, the Wireless IP Telephones and the Avaya Voice Priority Processor can operate in larger, more complex networks, including networks with multiple Ethernet switches, routers, VLANs and/or multiple subnets. However, in such networks, it is possible for the Quality of Service (QoS) features of the Avaya Voice Priority Processor to be compromised and voice quality may suffer. Any network that consists of more than a single Ethernet switch should be thoroughly tested to ensure that any quality issues are detected.

Note that the Avaya 3641/3645 Wireless IP Telephones cannot “roam” from one subnet to another. If routers and multiple subnets are in use, the Wireless IP Telephones must only use access points attached to a single subnet, or be powered off and back on to switch to a different subnet.

**Avaya IP Phone**
The wired-LAN desk sets provided by Avaya for use with the Avaya Communication Manager.

**Router**
A router is an optional component in the wired Ethernet LAN infrastructure that separates a wired LAN into segments so that network traffic is restricted to those segments that are directly involved in the communication. Installation of a network router is recommended in larger networks, where there may be significant network traffic not related to the wireless LAN. A router will isolate the wireless LAN from the associated wired LAN so that they are not impacted by each others' traffic. The Avaya Voice Priority Processors, the APs, and their associated Ethernet switch must all be on the same “side” of the router.

**Administrative computer**
An administrative computer is required for setup and maintenance of the Avaya Voice Priority Processor. This computer may be temporarily connected directly to the component or to the network; a dedicated computer is not required. Some installations use a laptop to configure and maintain system components.

**TFTP Server**
Required in the system to distribute software to the Wireless IP Telephones. May be on a different subnet than the Avaya Communication Manager, Avaya Voice Priority Processor, APs and/or Wireless IP Telephones.

The Avaya Voice Priority Processor, all IP Wireless IP Telephones, and all access points must be on the same subnet.
1.9 The Front Panel of the Avaya Voice Priority Processor

The Avaya Voice Priority Processor’s front panel contains ports to connect to power, the LAN, and to an administrative computer via an RS-232 port. Status LEDs supply information about the Avaya Voice Priority Processor’s functioning.

RS-232 Port – male DB-9 connector (DTE) used for RS-232 connection to a terminal, terminal emulator, or modem for system administration.

Link LEDs:
- **LNKOK** – Lit when there is a network connection.
- **ACT** – Lit if there is system activity.
- **COL** – Lit if there are network collisions.

**NETWORK** – Port to wired (Ethernet) LAN.

**ERROR** – Lit when the system has detected an error.

**STATUS** – Indicate system error messages and status.
- **1** – Heartbeat, indicates gateway is running.
- **2** – If active calls.
- **3**, **4**, **5** – Currently unused.

**PWR** (power jack) – Connects to the AC adapter supplying power to the system.

Use only the Avaya-provided Class II AC Adapter with output 24VDC, 1A.

Note that the model designation may be found on the label which is on the side of the AVPP.
2. **Installing the Avaya Voice Priority Processor**

As shown in the system diagram the Avaya Voice Priority Processor is connected to the Ethernet switch. The specifications covered here allow for great flexibility in physical placement of the components within stated guidelines.

See the Configuration and Administration for Avaya 3641/3645 Wireless IP Telephones for information on IP addressing.

2.1 **Required Materials**

The following equipment must be provided by the customer.

- Power Outlet – Must accept Avaya-provided AC adapter.
- Backboard space – The Avaya Voice Priority Processor is designed to be wall mounted to $\frac{3}{4}"$ plywood securely screwed to the wall.
- Screws – Required to mount the Avaya Voice Priority Processor to the wall. Four #8 - $\frac{3}{4}"$ panhead wood screws (or similar device) are required.
- Cat. 5 Cable – RJ-45 connector at the Avaya Voice Priority Processor. Connection to Ethernet switch.

2.2 **Locate the Avaya Voice Priority Processor**

The Avaya Voice Priority Processor measures approximately $4 \times 12.5 \times 7"$, and weighs about five pounds. The unit can be wall mounted, vertically or horizontally, over $\frac{3}{4}"$ plywood. The AVPP can also be rack-mounted using a rack-mount kit (sold separately).

Locate the Avaya Voice Priority Processor in a space with:

- Sufficient backboard mounting space (for wall mount) and proximity to the LAN access device (switched Ethernet hub) and power source.
- Easy access to the front panel, which is used for cabling.
- A maximum distance of 325 feet (100 meters) from the Ethernet switch.

2.3 **Install the Avaya Voice Priority Processor**

The Avaya Voice Priority Processor may be mounted on a rack or to a wall.

**Mount the AVPP on a rack**

The rack-mount kit is designed for mounting equipment in a standard 19" rack and should contain the following equipment:

- Mounting plates – Two for each AVPP to be mounted.
- Screws – Four rack-mount screws for each AVPP to be mounted.

To rack-mount the Avaya Voice Priority Processor:

1. Remove the corner screws from the AVPP.
2. Screw the **U-shaped** end (round screw holes) of the two mounting plates to the AVPP.
3. Screw the other end of the two mounting plates (oblong screw holes) to the rack.
4. Repeat steps 1-3 for each additional AVPP. The mounting plate is designed to provide the correct minimum spacing between units. When mounting multiple units, stack the units in the rack as closely as possible.

Mount the Avaya Voice Priority Processor to a wall
The Avaya Voice Priority Processor can be mounted either horizontally or vertically.

To mount the Avaya Voice Priority Processor to a wall:
1. Using a 1/8" drill bit, drill four pilot holes, on 1.84" by 12.1" centers (approximately equivalent to 1-13/16" by 12-1/8").
2. Insert the #8 x 3/4" screws in the pilot holes and tighten, leaving a 1/8" to 1/4" gap from the wall.

Connect Avaya Voice Priority Processor to LAN
Using a Cat. 5 cable, connect the NETWORK port on the Avaya Voice Priority Processor to the connecting port on the Ethernet switch.

Connect Power
1. Connect the power plug from the AC adapter to the jack labeled PWR on the Avaya Voice Priority Processor.

⚠️ Use only the Avaya-provided Class II AC Adapter with output 24VDC, 1A.

2. Plug the AC adapter into an 110VAC outlet to apply power to the Avaya Voice Priority Processor.

3. The system will cycle through diagnostic testing and the LEDs will blink for about one minute. When the system is ready for use:
   - The ERROR LED should be off.
   - Status 1 should be blinking.
3. Configuring the Avaya Voice Priority Processor

During initial setup of the Avaya Voice Priority Processor the IP address is established and the maximum number of active calls per access point is set. Optionally, you may enter a hostname and a location for software updates via TFTP.

3.1 Connecting to the Avaya Voice Priority Processor

The initial connection to the Avaya Voice Priority Processor must be made via a serial connection to establish the Avaya Voice Priority Processor’s IP address. After the IP address is established, connection to the Avaya Voice Priority Processor may be done via the network using telnet. It is recommended that the basic setup actions occur while the serial connection is made.

Connect via the Serial Port

1. Using a DB-9 female, null-modem cable, connect the Avaya Voice Priority Processor to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration –
   - Bits per second – 9600
   - Data bits – 8
   - Parity – None
   - Stop bits – 1
   - Flow control – None
3. Press Enter to display the Avaya Voice Priority Processor login screen.
4. Enter the default login – admin and default password – admin. These are case sensitive.
5. The NetLink SVP-II System menu will display.

Connecting Via Telnet

Telnet can only be used after the Avaya Voice Priority Processor’s IP address is configured.

The telnet method of connection is used for routine maintenance of the NetLink Server for both local and remote administration, depending on your network.

To connect via telnet, run a telnet session to the IP address of the Avaya Voice Priority Processor. Once you connect and log in, the NetLink SVP-II System menu displays.
3.2 The NetLink SVP-II System Menu

The main menu displays as shown here:

```
NetLink SVP-II System
Hostname: [SU202_1], Address: 10.8.0.61

System Status
SUP-II Configuration
Network Configuration
Change Password
Exit
```

- **System Status** – Menu for viewing error messages, status of operation and software code version.
- **SUP-II Configuration** – Allows you to set the mode and reset the system.
- **Network Configuration** – Allows you to set network configuration options, including IP address and hostname.
- **Change Password** – Allows you to change the password for Avaya Voice Priority Processor access.

---

1 SVP-II is a designation used internally by Avaya Engineering.
3.3 Network Configuration

The IP address and other network settings are established via the Network Configuration screen. This is also where you may optionally establish a hostname and enter the IP address of the location of any software updates you may obtain from Avaya. See section 6, the Software Maintenance section, of this document for more information about installing software updates via TFTP.

Scroll to Network Configuration and select by pressing Enter. A screen similar to the following appears:

```
Network Configuration
Hostname: [SVPO20_1], Address: 10.8.0.61

Ethernet Address (fixed): 00:90:7A:02:8F:AB
IP Address: 10.8.0.61
Hostname: SVPO20_1
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.90
SVF-II TFTP Download Master: 10.0.0.3
Primary DNS Server: NONE
Secondary DNS Server: NONE
DNS Domain: NONE
WINS Server: 10.13.0.1
Workgroup: WORKGROUP
Syslog Server: 10.0.0.31
Disable Telnet service: N
Maintenance Lock: N

Enter=Change S=SendAll ESC=Exit Use Arrow Keys to Move Cursor
```

Note the navigation options at the bottom of the screen. Press Enter to change a value, ESC to exit the screen, and the arrow keys to move the cursor.

SendAll

In an IP system with multiple Avaya Voice Priority Processors, the SendAll option is provided to speed configuration and to ensure identical settings. The S–SendAll option allows you to send that configuration parameter to every Avaya Voice Priority Processor on the LAN. SendAll can only be used after the IP address is established on EACH Avaya Voice Priority Processor via the serial connection. If you anticipate identical settings across the LAN, set just the IP address and custom hostname (if desired) for each Avaya Voice Priority Processor using the initial serial connection. Then connect via the LAN and use SendAll to set identical configuration options for all Avaya Voice Priority Processors.

If SendAll is to be utilized in your system, all passwords must be identical. Do not change the password at the initial configuration if the SendAll option is desired. Use the default password and change it globally if desired after a LAN connection is established for all Avaya Voice Priority Processors.

If independent administration of each Avaya Voice Priority Processor is desired, the passwords may be set at initial configuration.
The following options must be configured:

**IP Address**
Enter the IP address of the Avaya Voice Priority Processor, defined by your network administrator. Enter the complete address including digits and periods. **DHCP** may be entered.

⚠️ A master AVPP must have a static IP address.

The Avaya Voice Priority Processor will automatically lock for maintenance if the IP address is changed. When this Maintenance Lock occurs, the Avaya Voice Priority Processor must be reset upon exit. All active calls are terminated during a reset.

**Hostname**
(Optional) change the default host name, if desired. This is the name of the Avaya Voice Priority Processor to which you are connected, for identification purposes only. You cannot enter spaces in this field.

**Subnet Mask**
The network administrator must define the subnet mask.

**Default Gateway**
The IP address of a router on the local subnet.

**SVP-II TFTP Download Master**
This entry indicates the source of software updates for the Avaya Voice Priority Processor. See the *Software Maintenance* section for more information. Valid source location entries are:

- **NONE** – disable.
- **IP Address** – The IP address of a network TFTP server that will be used to transfer software updates to the Avaya Voice Priority Processor.

**DNS server and DNS domain**
These settings are used to configure Domain Name services. Consult your system administrator for the correct settings. These can also be set to **DHCP**. This will cause the DHCP client in the Avaya Voice Priority Processor to attempt to automatically get the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.

**WINS servers**
These settings are used for Windows Name Services. Consult your system administrator for the correct settings. These can also be set to **DHCP**. This will cause the DHCP client in the Avaya Voice Priority Processor to attempt to automatically get the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.

When the name services are set up correctly, the Avaya Voice Priority Processor can translate hostnames to IP addresses. Using telnet, it is also possible to access the Avaya Voice Priority Processor using its hostname instead of the IP address.
Workgroup
As set in WINS.

Syslog Server
Logging can be set to Syslog or NONE. If Syslog is set, a message is sent to the syslog server when an alarm is triggered.

Disable Telnet Service
Prevents Telnet access into the AVPP. Reset the AVPP for the change to take effect.
Upon reset the Telnet protocol server is not started.

The Avaya Voice Priority Processor must be reset in order to set the configuration options. If the Avaya Voice Priority Processor is in Maintenance Lock, you must manually reset it by selecting the Reset option in the SVP-II Configuration screen and then pressing Y upon exit.
### 3.4 AVPP Configuration

The **SVP-II Configuration** screen is where you set the mode of the Avaya Voice Priority Processor. It is also where you can lock the Avaya Voice Priority Processor for maintenance and reset the Avaya Voice Priority Processor after maintenance. The type of gateway you are using determines the mode of the Avaya Voice Priority Processor.

From the main menu, scroll to **SVP-II Configuration** and select by pressing Enter.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>[SVPII_1], address: 10.8.0.52</td>
</tr>
<tr>
<td>SVF-II Mode</td>
<td>NetLink IP</td>
</tr>
<tr>
<td>Ethernet link</td>
<td>auto-negotiate</td>
</tr>
<tr>
<td>System Locked</td>
<td>N</td>
</tr>
<tr>
<td>Maintenance Lock</td>
<td>N</td>
</tr>
<tr>
<td>Inactivity Timeout (min)</td>
<td>20</td>
</tr>
</tbody>
</table>

**SVP-II Mode** – Defaults to **NetLink IP** for an IP environment. Press enter to select and the screen is immediately redrawn with additional options for the IP environment.

```
SVP-II Configuration
Hostname: [SVPII_1], Address: 10.8.0.52

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phones per Access Point</td>
<td>12</td>
</tr>
<tr>
<td>802.11 Rate</td>
<td>Automatic</td>
</tr>
<tr>
<td>SVF-II Master</td>
<td>10.8.0.52</td>
</tr>
<tr>
<td>First Alias IP Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Last Alias IP Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Enable H.323 Gatekeeper</td>
<td>N</td>
</tr>
<tr>
<td>SVF-II Mode</td>
<td>NetLink IP</td>
</tr>
<tr>
<td>Ethernet link</td>
<td>auto-negotiate</td>
</tr>
<tr>
<td>System Locked</td>
<td>N</td>
</tr>
<tr>
<td>Maintenance Lock</td>
<td>N</td>
</tr>
<tr>
<td>Inactivity Timeout (min)</td>
<td>20</td>
</tr>
</tbody>
</table>

Reset
Reset all SVP servers
```

Enter=Change  S=SendAll  ESC=Exit  Use Arrow Keys to Move Cursor
The following options must be configured:

**Phones per Access Point** – Access point specifications are detailed in the *Configuration Notes* for each brand and type. Refer to these notes when entering the number of simultaneous calls supported for your type.

**802.11 Rate** – Select **1MB/2MB** to limit the transmission rate between the Wireless IP Telephones and access points. Select **Automatic** to allow the Wireless IP Telephone to determine its rate (up to 11 Mb/s).

**SVP-II Master** – The master AVPP must be identified in an IP system. Select one of the following identification options:

- Statically configure the IP address of the master AVPP in each of the AVPPs. Enter the IP address.

  See the Overview section for an explanation of the master AVPP.

- Statically configure the IP address of the master AVPP in a DHCP server and configure each of the AVPPs to get the information from the DHCP server. Enter DHCP. If DHCP is used, the IP address of the master AVPP must be configured in the DHCP server. See the Wireless IP Telephone interface document for your IP environment for more information about DHCP integration factors.

- Statically configure the IP address of the master AVPP in a DNS server and configure each of the AVPPs to retrieve this information from the DNS server. Enter DNS. If DNS is used, the IP address of the master AVPP must be configured in the DNS server.

**First Alias IP Address/Last Alias IP Address** – The AVPP uses an IP address when acting as a proxy for the Wireless IP Telephone. Therefore, one alias IP address is required for every installed Avaya Wireless IP Telephone. These IP addresses must be entered as a range and must be assigned solely for this purpose.

When multiple AVPP Servers are installed, a different range must be configured in each AVPP. In determining how many addresses to configure per AVPP, use this formula – (# of handsets / # of AVPPs) + 30%. This formula will accommodate the possibility of unequal distribution of handsets among the available AVPPs.

Alias IP Addresses are not necessary in Avaya systems.

If used, all alias addresses must be on the same subnet as the AVPP and cannot be duplicated on other subnets or AVPPs. There is no limit to the number of addresses that can be assigned, but the capacity of each AVPP is 500 Wireless IP Telephones.

**Enable H.323 Gatekeeper** – In certain H.323 protocol systems, the AVPP may function as a gatekeeper. Enter **Y** to have the AVPP function as the gatekeeper in the H.323 protocol environment.

**Ethernet link** – The AVPP will auto-negotiate unless there is a need to specify a link speed.
System Locked – This option is used to take the system down for maintenance. The default entry is \textbf{N} (No). Set it at \textbf{Y} (Yes) to prevent any new calls from starting. Return to \textbf{N} to restore normal operation.

Maintenance Lock – The system automatically sets this option to \textbf{Y} (Yes) after certain maintenance activities that require reset, such as changing the IP address. Maintenance Lock prevents any new calls from starting. Note that the administrator cannot change this option. It is automatically set by the system. Reset the system at exit to clear Maintenance Lock.

Inactivity Timeout (min) – Set the number of minutes the administrative module can be left unattended before the system closes it. This number can be from 1 to 100. If it is set to zero (0), the administrative module will not close due to inactivity.

QoS Configuration – Select this option to set the DSCP tags. See \textit{QoS Configuration} section below.

Reset System – If this option is selected, you will be prompted to reset the Avaya Voice Priority Processor upon exiting this screen.

Reset All SVP Servers – If this option is selected, you will be prompted to reset all AVPPs upon exiting this screen. This is necessary if you have changed configurations on other AVPPs by using the SendAll option.

The Avaya Voice Priority Processor should be reset at the end of any maintenance procedure that requires a reset either via \textbf{Maintenance Lock} or manually via \textbf{Reset System}.

Note that resetting the Avaya Voice Priority Processor will terminate any calls in progress.

\textbf{QoS Configuration}
DSCP tags set packet priorities for QoS.

\begin{center}
\begin{tabular}{|c|c|}
\hline
Traffic Class & DSCP Tag \\
\hline
Administration & Default \\
\hline
WT (In call) Default & Default \\
\hline
WT (Standby) Default & Default \\
\hline
RIP Default & Default \\
\hline
PBX Default & Default \\
\hline
Inter-SVP2 Default & \\
\hline
\end{tabular}
\end{center}

\begin{center}
\textbf{QoS Configuration}
\textbf{Hostname: Islnk-03e961, Address: 10.13.0.127}
\end{center}

Enter=Change S=SendAll ESC=Exit Use Arrow Keys to Move Cursor
**DSCP Tag**
DSCP (Differentiated Services Code Point) is a QoS mechanism for setting relative priorities. Packets are tagged with a DSCP field in the IP header for type of service. The decimal value may be set as a number from 0-63 and may be different for each traffic class listed on the screen. The default for all traffic classes is 4.

**Administration** tags set the priority for telnet, TFTP, and other administrative traffic. Administrative traffic can have the lowest priority because it does not require voice quality.

**WT (In call)** traffic requires voice quality and may be set to a higher priority than **WT (Standby)** traffic.

**RTP** traffic is the audio traffic to the IP PBX. It requires voice quality.

**PBX** traffic is not audio to the PBX.

**Inter-SVP2** traffic is the information-passing protocol that SVP Servers use to communicate with each other.

When forwarding packets, the SVP Server shall always overwrite the received DSCP value. The final DSCP tag for packets in each of the traffic classes are assigned a DSCP value based on the following rules. (Please see table on next page.)

- If both **Administration** and the **Traffic Class** setting is **Default**, the **Default** value as shown in the table below will be used.

- If **Administration** is set at any number (**Value X**) other than **Default**, that setting (**Value X**) it will override the **Default** value of the **Traffic Class**.

- If any of the **Traffic Class** settings are set at any value (**Value Y**) other than **Default**, that setting (**Value Y**) will override the **Administration** setting.

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Administration</th>
<th>Default</th>
<th>Value X</th>
</tr>
</thead>
<tbody>
<tr>
<td>WT (In call)</td>
<td></td>
<td>Default</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value Y</td>
<td>X</td>
</tr>
<tr>
<td>WT (Standby)</td>
<td></td>
<td>Default</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value Y</td>
<td>X</td>
</tr>
<tr>
<td>RTP</td>
<td></td>
<td>Default</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value Y</td>
<td>Y</td>
</tr>
<tr>
<td>PBX</td>
<td></td>
<td>Default</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value Y</td>
<td>Y</td>
</tr>
<tr>
<td>Inter-SVP2</td>
<td></td>
<td>Default</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
3.5 Change Password

If desired, the password to access the Avaya Voice Priority Processor may be changed. A password must meet the following requirements:

- It must be more than four characters, but cannot exceed 16 characters.
- The first character must be a letter.
- Numbers or letters are allowed.
- No dashes, spaces, or punctuation marks, etc. are allowed.

Select Change Password from the main menu. A screen similar to the following will appear:

```
Change Password
Hostname: [SUPU2_1], Address: 10.8.8.61

Old Password ****************
New Password ***************
Confirm New Password ***************
Set Password
Set Password on all SUP servers

Enter=Select          ESC=Exit          Use Arrow Keys to Move Cursor
```

Enter the information and either select Set Password or press the S key to set the new password.

If you forget a password, call Avaya Customer Service for assistance.
4. **Swapping/Adding/Deleting AVPPs**

Whenever an AVPP is removed from the system, Wireless IP Telephones that are using the AVPP will be affected. If the removal of the AVPP is intentional, the administrator should lock and idle the system prior to removing an AVPP.

### Adding an AVPP

A new AVPP is detected within two seconds of being added to the system (booted/configured/connected). When detected, any Wireless IP Telephone not active in a call will immediately be forced to reboot and check in again. Any Wireless IP Telephone in a call will immediately switch to the AVPP that should provide its “timing” function. This switch should not be noticeable to the user since it is similar to a normal handoff between access points. When the Wireless IP Telephone ends the call, it will be forced to reboot and check in again.

### Removing an AVPP

When an AVPP is removed from the system it is detected within two seconds. Wireless IP Telephones not in calls are immediately forced to reboot and check in again. For Wireless IP Telephones active in calls, two possible scenarios can occur. If the AVPP that was removed was providing the “gateway” function for the Wireless IP Telephone, then the call is lost and the Wireless IP Telephone is forced to check-in again. If the AVPP that was removed was providing the “timing” function for the call, the call will switch to the AVPP that should now provide the “timing” function. Note that during the two seconds while the loss of the AVPP is being detected, the audio for the call will be lost.

### Changing the Master AVPP

In the event the master AVPP loses communication with the network, the Wireless IP Telephone system will fail. All AVPPs will lock, all calls will be lost, and no calls can be placed. Therefore, if the master AVPP needs to be replaced, be sure the system can be brought down with minimal call interruption. Be sure to reset all AVPPs after the master has been replaced. If the IP address of the master is changed, it must be changed in all AVPPs.
5. **Software Maintenance**

The Avaya Voice Priority Processor uses proprietary software programs written and maintained by Avaya Corporation. The software versions that are running on the system components can be displayed via the **System Status** screen.

You may obtain information about software updates from Avaya or its authorized dealer.

At startup the Avaya Voice Priority Processor uses TFTP to check the software version it is running against the version in the TFTP location. If there is a discrepancy, the Avaya Voice Priority Processor will download the version in the TFTP location.

**Software Updates**

Lock the Avaya Voice Priority Processor in the **SVP-II Configuration** screen prior to updating the software.

Downloads for the Avaya Voice Priority Processor are available you’re your service representative.

After software updates are obtained from Avaya, they must be transferred to the TFTP location in the LAN to update the code used by the Avaya Voice Priority Processor.

Note that locking the Avaya Voice Priority Processor will prevent new calls from starting. All calls in progress will be terminated when the Avaya Voice Priority Processor is reset.
6. **Troubleshooting via System Status Menu**

Information about system alarms, and network status displays on various screens accessed through the *System Status Menu* screen, which is opened from the main menu of the Avaya Voice Priority Processor. See the previous sections for directions on how to connect to the Avaya Voice Priority Processor and navigate to the *System Status Menu*.

---

**System Status Menu**

Hostname: [SU62_1], Address: 10.80.61

- **Error Status**
- **Network Status**
- **Software Versions**
- **Gatekeeper Database**

Enter=Select ESC=Exit Use Arrow Keys to Move Cursor

- **Error Status** – Displays alarm and error message information.
- **Network Status** – Displays information about the Ethernet network to which the Avaya Voice Priority Processor is connected.
- **Software Versions** – Lists the software version for each Avaya component.
- **Gatekeeper Database** – not used.

Options on the System Status menu provide a window into the real time operation of the components of the system. Use this data to determine system function and to troubleshoot areas that may be experiencing trouble.
6.1 Error Status

The Error Status screen displays any alarms that indicate some system malfunction. Some of these alarms are easily remedied and others require a call to Avaya’s Customer Support Department.

From the System Status Menu, select Error Status. The screen displays active alarms on the Avaya Voice Priority Processor.

The following table displays the list of alarms and a description of the action to take to eliminate the alarm.

<table>
<thead>
<tr>
<th>Alarm Text</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum payload usage reached</td>
<td>Reduce usage, clear alarm</td>
</tr>
<tr>
<td>Maximum telephone usage reached</td>
<td>Reduce usage, clear alarm</td>
</tr>
<tr>
<td>Maximum access point usage reached</td>
<td>Reduce usage, clear alarm</td>
</tr>
<tr>
<td>Maximum call usage reached</td>
<td>Reduce usage, clear alarm</td>
</tr>
<tr>
<td>SRP audio delayed</td>
<td>Reduce usage, clear alarm</td>
</tr>
<tr>
<td>SRP audio lost</td>
<td>Reduce usage, clear alarm</td>
</tr>
<tr>
<td>No IP address</td>
<td>Configure an IP address</td>
</tr>
</tbody>
</table>

Press C to clear all clearable alarms.
6.2 Network Status

The Avaya Voice Priority Processor is connected to the Ethernet network, referred to as the LAN or Local Area Network. The information about that connection is provided through the Network Status screen.

From the System Status Menu, select Network Status. The screen displays information about the Ethernet network. This information can help troubleshoot network problems. A sample screen is displayed here.

<table>
<thead>
<tr>
<th>Ethernet Address: 00:90:7A:00:77:15</th>
<th>Net: 100/Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Uptime: 6 days, 02:34</td>
<td>Max calls: 80</td>
</tr>
</tbody>
</table>

RX: bytes packets errors drop fifo alignment multicast
432891547 4112190 0 0 0 0 0 1321217

TX: bytes packets errors drop fifo carrier collisions
1478261799 1311194 0 0 0 0

SUP-II Sockets in Use (Last / Max): 0 / 10
SUP-II Access Points in Calls (Last / Max): 0 / 2
SUP-II Telephones in Use (Last / Max): 0 / 1
SUP-II Telephones in Calls (Last / Max): 0 / 2
SUP-II SRP Audio (Delay / Lost): 0 / 0

ESC to Exit

Ethernet Address – MAC address of the Avaya Voice Priority Processor (hexadecimal).

System Uptime – The number of days, hours and minutes since the Avaya Voice Priority Processor was last reset.

Net – The type of connection to the Ethernet switch currently utilized. See AVPP Capacity for more information.

Data is transmitted over Avaya components by proprietary technology developed by SpectraLink Corporation. The SpectraLink Radio Protocol (SRP) packets and bytes can be differentiated from other types of transmissions and are used to evaluate system functioning by Avaya customer support and engineering personnel.
RX – Ethernet statistics concerning the received packets during System Uptime.
  - **bytes** – bytes received
  - **packets** – packets received
  - **errors** – Sum of all receive errors (long packet, short packet, CRC, overrun, alignment)
  - **drop** – packets dropped due to insufficient memory
  - **fifo** – overrun occurred during reception
  - **alignment** – nonoctet-aligned packets (number of bits NOT divisible by eight)
  - **multicast** – packets received with a broadcast or multicast destination address

TX – Ethernet statistics concerning the transmitted packets during System Uptime.
  - **bytes** – bytes transmitted
  - **packets** – packets transmitted
  - **errors** – Sum of all transmit errors (heartbeat, late collision, repeated collision, underrun, carrier)
  - **drop** – packets dropped due to insufficient memory
  - **fifo** – underrun occurred during transmission
  - **carrier** – carrier lost during transmission
  - **collisions** – packets deferred (delayed) due to collision

**SVP-II Access Points in Use** – Access points in use by Wireless IP Telephones, either in standby or in a call. ‘Last’ is current, ‘Max’ is the maximum number in use at one time.

**SVP-II Access Points in Calls** – Access points with Wireless IP Telephones in a call.

**SVP-II Telephones in Use** – Wireless IP Telephones in standby or in a call.

**SVP-II Telephones in Calls** – Wireless IP Telephones in a call.

**SVP-II SRP Audio (Delay)** – SRP audio packets whose transmission was momentarily delayed.

**SVP-II SRP Audio (Lost)** – SRP audio packets dropped due to insufficient memory resources.
6.3 Software Version

The Avaya Voice Priority Processor and Wireless IP Telephones utilize SpectraLink Corporation's proprietary software that is controlled and maintained through versioning. The **Software Version** screen provides information about the version currently running on the Avaya Voice Priority Processor. This information will help you determine if you are running the most recent version and will assist Avaya engineering and/or customer support in troubleshooting software problems.

This screen also displays the model type.

From the **System Status Menu**, select **Software Version**. A sample screen is displayed here.

```
Software Version Numbers
Hostname: [SVP020_1], Address: 10.8.0.61

SVF Type: 020
Hardware Versions: 33/03
Factory Page: 213.001
Downloader: 213.004 (99cd73ee)
Table of Contents: 173.024 (4553d976)
Functional Code: 174.024 (74ae1056)
File System: 175.024 (4bfc9ac9)
```

Note that the software versions on your system may be different from the versions displayed in the above sample screen.

The table below shows the description, major version numbers, and filenames of the files that are provided when downloading updates.

<table>
<thead>
<tr>
<th>Name</th>
<th>Major version number</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of contents</td>
<td>173</td>
<td>svp100.toc</td>
</tr>
<tr>
<td>Functional code</td>
<td>174</td>
<td>zvmlinux</td>
</tr>
<tr>
<td>File system</td>
<td>175</td>
<td>flashfs</td>
</tr>
</tbody>
</table>

The minor version numbers for these three files must all match, as they do in the screen example (17x.024).
B. Avaya 3641/3645 Wireless IP Telephones

Configuration and Administration
For CCMS
1. **Avaya 3641/3645 Wireless IP Telephone Overview**

The Avaya 3641/3645 Wireless IP Telephone is a mobile handset for workplace IP telephone systems. The Wireless IP Telephone operates over an 802.11a/b/g wireless Ethernet LAN providing users a wireless voice over IP (VoIP) extension. By seamlessly integrating with an Avaya Communication Manager (such as an Avaya MultiVantage™ on a DEFINITY® Server SI or an Avaya S8100 Media Server with CMC1 Media Gateway), Wireless IP Telephone users are provided with high-quality mobile voice communications throughout the workplace. The Wireless IP Telephone gives users the freedom to roam throughout the workplace while providing all the features and functionality of an IP desk phone.

The Avaya 3641/3645 Wireless IP Telephone provides a wireless extension to the Avaya Communication Manager. The Wireless IP Telephones reside on the wireless LAN with other wireless devices using direct-sequence spread spectrum (DSSS) radio technology. The handset radio transmits and receives packets at up to 54Mb/s.

A Wireless IP Telephone must be administered on the Avaya Communication Manager for the specific features and lines to be accessed by the Wireless IP Telephone. After the handset is registered, it receives its configuration information from the Avaya Communication Manager.
1.1 Quick Start Guide

1. A wireless LAN must be properly configured and operational through the use of 802.11b wireless access points (APs).

2. A TFTP Server must be available on the network in order to load the appropriate software into the Wireless IP Telephones. See Section 6 “License Management” for detailed instructions for loading software on Wireless IP Telephones.

3. The Avaya Communication Manager must be connected to your network and completely operational.

4. The Avaya Voice Priority Processor, which controls the QoS on the wireless LAN for the Wireless IP Telephones, must be on the same subnet as the Wireless IP Telephones.

5. Download software – See your vendor for instructions about downloading the latest software. Download the correct Avaya 3641/3645 Wireless IP Telephone software per Section 6.2 Configuration Process. Download updates to the AVPP software per Part 1 of this document.

6. Add a station on the Avaya Communication Manager for each Wireless IP Telephone. You will administer each Wireless IP Telephone as an Avaya 4612 IP Telephone.

7. Configure your Wireless IP Telephone to ensure that it is associated with the Wireless LAN, has the appropriate software and is registered to the Avaya Communication Manager. See License Management for detailed instructions for loading software onto Wireless IP Telephones.

The Avaya Voice Priority Processor and all access points must be on the same subnet.

IP multicast addresses are used by the Avaya 3645 Wireless IP Telephone system. This requires that multicasting be enabled on the subnet used for the Avaya 3645 Wireless IP Telephones and AVPP Server.

Routers are typically configured with filters to prevent multicast traffic from flowing outside of specific domains. The wireless LAN can be placed on a separate VLAN or subnet to reduce the effects of broadcast and multicast traffic from devices in other network segments.
2. The Avaya 3641/3645 Wireless IP Telephones

2.1 Specifications

- **Radio mode**
  - (selectable) 802.11b, 802.11g (802.11a)
  - 2.4–2.4835 GHz
  - 5.150–5.250 GHz
  - 5.250–5.350 GHz
  - 5.470–5.725 GHz
  - 5.725–5.825 GHz

- **Transmission type**
  - Direct-sequence spread spectrum (DSSS)

- **Transmit data rate**
  - up to 54 Mb/s

- **Radio QoS**
  - SpectraLink Voice Priority (SVP)

- **Wireless security**
  - Wired Equivalent Privacy (WEP), 40-bit and 128-bit; Cisco FSR; WPA-PSK, WPA2-PSK

- **FCC certification**
  - Part 15.247

- **Management**
  - DHCP, TFTP

- **Voice encoding**
  - G.711, G.729a/ab

- **VoIP Protocols**
  - CCMS

- **Transmit power**
  - See Admin menu

- **Display**
  - Up to five lines of text plus two icon status rows and one row for softkey labels.

- **Avaya 3641 Wireless IP Telephone**
  - Dimensions: 5.4” x 2.0” x 0.9”
  - Weight: 3.9 oz. (110.6 g) with Standard Battery Pack

- **Avaya 3645 Wireless IP Telephone**
  - Dimensions: 5.7” x 2.0” x 0.9”
  - Weight: 4.2 oz. (119.1 g) with Standard Battery Pack

- **Standard Battery Pack capacity**
  - 4 hours talk, 80 hours standby

- **Extended Battery Pack capacity**
  - 6 hours talk, 120 hours standby

- **Ultra-Extended Battery Pack capacity**
  - 8 hours talk, 160 hours standby
2.2 **Handset Display**

Display information provided by the Avaya Communication Manager when the Wireless IP Telephone is off-hook will be passed directly to the Wireless IP Telephone display in an emulation of the Avaya 4612 IP Telephone display handling. Certain characters may be used by the Avaya Communication Manager that are not implemented in the Wireless IP Telephone such as definable and special characters.

There are 12 programmable keys that may be allocated to line appearances or features in any combination. Pressing the **LINE** key from the active mode displays the list of line appearances extracted from the programmable keys list. The line appearances are also mapped to corresponding line icons across the top of the Wireless IP Telephone display.

Press the **FCN** key while off-hook to scroll through system features. In this mode, the display has four lines and up to 18 characters. OAI features, if assigned, will be displayed with their shortcuts. The programmable key items that appear on this list each have a state indicator in the second column of the display that shows a plus sign if the associated feature is active. This second column is blank if the associated feature is not active. The plus sign emulates a lit or blinking LED on a Avaya 4612 IP Telephone, indicating an active feature. Press the shortcut key to activate the feature. Softkeys are programmed to the fixed feature keys of the Avaya 4612 IP Telephone.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Signal-strength icon" /></td>
<td>The signal-strength icon indicates the strength of the signal and can assist the user in determining if the handset is moving out of range.</td>
</tr>
<tr>
<td><img src="image" alt="Voicemail icon" /></td>
<td>The voicemail icon is activated when a new voicemail message is received if the feature is supported by the phone emulation.</td>
</tr>
<tr>
<td><img src="image" alt="Battery icon" /></td>
<td>The battery icon indicates the amount of charge remaining in the Battery Pack. When only one level remains, the Battery Pack needs to be charged.</td>
</tr>
<tr>
<td><img src="image" alt="Speakerphone icon" /></td>
<td>The speakerphone icon displays when the speakerphone is active.</td>
</tr>
<tr>
<td><img src="image" alt="Line indicators" /></td>
<td>The line indicators are associated with telephone line status and access.</td>
</tr>
<tr>
<td><img src="image" alt="Up and down arrows" /></td>
<td>Up and down arrows are displayed when the menu has additional options above or below.</td>
</tr>
<tr>
<td><img src="image" alt="Left or right arrows" /></td>
<td>Left or right arrows are displayed during editing when the cursor may be moved left or right.</td>
</tr>
<tr>
<td><img src="image" alt="PBX ring icon" /></td>
<td>PBX ring icon. A regular telephone call is coming in.</td>
</tr>
<tr>
<td><img src="image" alt="OAI ring icon" /></td>
<td>OAI ring icon. A call is coming in from the OAI application.</td>
</tr>
<tr>
<td><img src="image" alt="Push-to-talk (PTT) ring icon" /></td>
<td>The push-to-talk (PTT) ring icon. A PTT call is coming in.</td>
</tr>
<tr>
<td><img src="image" alt="Priority PTT ring icon" /></td>
<td>The priority PTT ring icon. A call is coming in on the priority PTT channel. This call will override any other.</td>
</tr>
<tr>
<td><img src="image" alt="Muted" /></td>
<td>The muted indicator displays after the Mute softkey has been pressed. It indicates that the microphone is not transmitting sound. Press the Mute softkey again to unmute the microphone.</td>
</tr>
<tr>
<td><img src="image" alt="Locked" /></td>
<td>Locked indicates that the keypad is locked to prevent accidental activation. Use the Unlk softkey plus the # key to unlock it.</td>
</tr>
<tr>
<td><img src="image" alt="No Service message" /></td>
<td>If warning tones are not disabled, an alarm will sound and a descriptive message displays when the handset cannot receive or place calls. You may be outside of the covered area. Walk back into the covered area. The in-service tone indicates that service is reestablished.</td>
</tr>
<tr>
<td><img src="image" alt="Download icon" /></td>
<td>The download icon indicates that the handset is downloading code. This icon only appears while the handset is running the over-the-air downloader. It appears to the right of the signal strength icon in the same location as the voicemail icon.</td>
</tr>
</tbody>
</table>
2.3 **Startup Sequence**

The Wireless IP Telephone goes through an initialization sequence at startup. The line icons 1-9 display and count down as the Wireless IP Telephone steps through this sequence. If there is difficulty at any step that prevents initialization from continuing, an error message will display and the related icon(s) will stay on. Please see the error table at the back of this document for instructions on how to handle error messages that occur during initialization.

<table>
<thead>
<tr>
<th>Icon</th>
<th>The icon(s) shown in bold turns off when:</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456789</td>
<td>The Wireless IP Telephone has located and authenticated and associated with at least one AP, and is proceeding to bring up higher-layer networking functions.</td>
</tr>
<tr>
<td>12345678</td>
<td>The Wireless IP Telephone is either configured for Static IP, or if configured for DHCP the DHCP discovery process has started.</td>
</tr>
<tr>
<td>1234567</td>
<td>If DHCP is configured, a DHCP response was received which contains a good DNS server configuration.</td>
</tr>
<tr>
<td>123456</td>
<td>Note: Only valid on non-SRP protocol. Indicates one of the following: Static IP configuration, or AVPP address found in DHCP response, or AVPP address found via DNS lookup.</td>
</tr>
<tr>
<td>12345</td>
<td>All networking functions are complete (notably, DHCP) and the Wireless IP Telephone is proceeding with establishing the SRP link to either the Gateway or AVPP.</td>
</tr>
<tr>
<td>1234</td>
<td>The SRP link is established, all network stack initialization is complete and the Wireless IP Telephone is proceeding with application-specific initialization.</td>
</tr>
<tr>
<td>123</td>
<td>The CCMS application has started.</td>
</tr>
<tr>
<td>12</td>
<td>At least one IP address for a PBX has been identified.</td>
</tr>
<tr>
<td>1</td>
<td>The Wireless IP Telephone has successfully registered with the PBX.</td>
</tr>
<tr>
<td>(no icons)</td>
<td></td>
</tr>
<tr>
<td>EXT.</td>
<td>The Wireless IP Telephone requires verification of the extension number.</td>
</tr>
<tr>
<td># – OK</td>
<td>New –</td>
</tr>
<tr>
<td>Password</td>
<td>The Wireless IP Telephone requires verification of the password.</td>
</tr>
<tr>
<td># – OK</td>
<td></td>
</tr>
<tr>
<td>Ext. xxxx</td>
<td>Initialization is complete. The Wireless IP Telephone is in standby mode ready to receive and place calls.</td>
</tr>
</tbody>
</table>

* These prompts do not appear at every startup. They appear at first initialization and when certain conditions require them as described in section 7.
### 2.4 Wireless IP Telephone Modes

**Standby** (on-hook)

In the standby mode the Wireless IP Telephone is waiting for an incoming call or for the user to place an outgoing call. The extension number is shown on the display and there is no dial tone. In this mode, the Wireless IP Telephone is conserving battery power and wireless LAN bandwidth.

When an incoming call occurs the handset will ring loudly until the call is answered by pressing the **START** key, or the **END** key is pressed to silence the ringing.

**Predial**

To place a call using predialing (cell phone dialing), dial the number while in standby mode and then press **START**. This transitions the Wireless IP Telephone to active off-hook mode and the number is immediately called.

**Active** (off-hook)

To place a call, press the **START** key. This transitions the Wireless IP Telephone to active off-hook mode. There is a dial tone, the Wireless IP Telephone is in communication with the PBX, and the display shows information as it is received from the PBX. The user may place a call or press the **FCN** or **LINE** key to access additional operations.

The Wireless IP Telephone is also in the active mode when a call is received.

When an incoming call occurs the handset will ring until the call is answered by pressing the **START** key, or the **END** key is pressed to silence the ringing. If **END** is pressed, the first call is terminated and the handset reverts to a full ring.

The active modes utilize the most bandwidth and battery power. To conserve these resources and allow the handset to receive new calls, return the Wireless IP Telephone to the standby mode when a call is completed by pressing the **END** key.

**Configuration Menu Mode**

When user preferences are being configured in the Config menu, the handset is on but is not active. It cannot receive calls while in the Config menu.

**Push-to-talk (PTT) Mode**

The Avaya 3645 Wireless IP Telephone utilizes channels for incoming and outgoing radio communication. While PTT is active, the handset is in PTT mode. It can receive regular phone calls in this mode. When a regular phone call is answered, the handset enters active mode.

**Messaging Mode**

If text messaging functions have been programmed as in a nurse call system, the handset is able to receive text messages. While these messages are being accessed, the handset is in Messaging mode. Incoming calls will ring with the second call ringing sound.

---

2 The speakerphone softkey (Spkr) may be pressed instead of **START** to initiate the calling process.
3. **Avaya Communication Manager Configuration**

You can configure the Avaya 3641/3645 Wireless IP Telephone as a stand-alone station or associate it with a desk station. When the Avaya 3641/3645 Wireless IP Telephone is associated with a desk station, the user can make and handle calls from either the Avaya 3641/3645 Wireless IP Telephone or the desk station.

3.1 **Configuring a Standalone Station**

To configure an Avaya 3641/3645 Wireless IP Telephone as a stand-alone station, you must add a station on the Avaya Communication Manager for the Avaya 3641/3645 Wireless IP Telephone.

To administer a stand-alone station on the Avaya Communication Manager for a Wireless IP Telephone:

1. From the Avaya Communication Manager administration software, add a new station.
2. Set “Type” to “4612.”
3. Administer a station security code.
4. Complete the remainder of the station form as you would for a desk station.
5. Repeat Steps 1 through 5 for each stand-alone Wireless IP Telephone.

3.2 **Configuring an Associated Station**

To configure an Avaya 3641/3645 Wireless IP Telephone as an associated station, you must add a station on the Avaya Communication Manager for the Avaya 3641/3645 Wireless IP Telephone and then associate that station with a desk station.

To administer an associated station on the Avaya Communication Manager for a Wireless IP Telephone:

1. From the Avaya Communication Manager administration software, add a new station.
2. Set “Type” to “4612.”
3. Set “Security Code” to the same security code used for the extension to which this Wireless IP Telephone will be associated (that is, the desk station). You can use a different security code, but to make it easier for the user it is recommended that you use the same security code as the desk station.
4. Set “Message Lamp Ext” to the extension of the associated desk station.
5. Set “Bridged Call Alerting” to “y.”
6. Set “Auto Select Any Idle Appearance” to “y.”
7. For Button Assignments, create bridged appearances to the line appearances on the desk station.
8. Add additional feature buttons to unassigned buttons, if desired.
9. Repeat Steps 1 through 8 for each Wireless IP Telephone.

When making changes to feature buttons, the phone must be power-cycled.
4. **Avaya 3641/3645 Wireless IP Telephone Configuration**

The Wireless IP Telephone can be automatically configured for IP address by enabling DHCP.

Each Wireless IP Telephone may be configured for site-specific requirements by opening the Admin menu and selecting options or entering specific information. Any settings entered in the Admin menu must conform to system settings. Only the Wireless IP Telephone being configured is affected by the Admin menu settings.

The Wireless IP Telephone user may select several usability options from the standby menu, described below in the *User-defined Preferences* section. This information is also provided in the end user manual.

Configuration is vastly simplified through the use of the Handset Configuration Tool. See section C in this document for more information.

4.1 **The Admin Menu**

The Admin menu contains configuration options that are stored locally (on each Wireless IP Telephone). Every Wireless IP Telephone is independent and if the default settings are not desired, the admin options must be set in each Wireless IP Telephone requiring different settings.

**Opening the Admin menu**

1. With the Wireless IP Telephone powered OFF, press and hold the **START** key. While holding the **START** key, press and release the **END** key.

2. When the Admin menu appears, release the **START** key.

If an admin password has been set, the display will require the user to enter the password before opening the Admin menu. The default password is 123456. If no password is set, the display will proceed directly into the Admin menu.

**Navigation**

The navigation keys just below the softkeys are used to navigate through and select menu options. These are referred to as **Nav ▲**, **Nav ▼**, **Nav ◄**, **Nav ►**, and **NavOK**.
Part B: Avaya 3641/3645 Wireless IP Telephone

**Toggle Options**

Some menu options that have only two possibilities operate on a toggle basis. The current setting is shown on the second row of the display, called the info line. Press **NavOK** to toggle between the settings. For example, when **PTT Enable** is the menu option, **Currently Disabled** will show on the info line. If you select **PTT Enable**, **Currently Enabled** will show on the info line and the menu option will toggle to **PTT Disable**.

**Data Entry and Editing**

An asterisk (*) next to an option on the display indicates that it is selected. Use the **Nav** keys and the softkeys to navigate and select desired options.

Enter numbers by pressing the buttons on the keypad. The blinking underscore identifies the current cursor position. When entering alphanumeric strings, the **CAPS/caps** softkey will appear and may be pressed to toggle the case. Enter letters by repeatedly pressing the corresponding key until the desired letter displays on the screen. Use the **CAPS** softkey to change the case as needed.

To edit during entry, delete the character to the left of the cursor by pressing the **Del** softkey. To replace an entry, delete it by pressing the **Clr** softkey and then enter the new data. To edit an existing entry, use **Nav◄** and **Nav►** to move the cursor position, and then press the **Del** softkey to delete the character to the left. Insert new data by pressing the buttons on the keypad.

Alphanumeric entries:

<table>
<thead>
<tr>
<th>Key</th>
<th>caps</th>
<th>CAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2 a b c</td>
<td>2 A B C</td>
</tr>
<tr>
<td>3</td>
<td>3 d e f</td>
<td>3 D E F</td>
</tr>
<tr>
<td>4</td>
<td>4 g h l</td>
<td>4 G H I</td>
</tr>
<tr>
<td>5</td>
<td>5 j k l</td>
<td>5 J K L</td>
</tr>
<tr>
<td>6</td>
<td>6 m n o</td>
<td>6 M N O</td>
</tr>
<tr>
<td>7</td>
<td>7 p q r s</td>
<td>7 P Q RS</td>
</tr>
<tr>
<td>8</td>
<td>8 t u v</td>
<td>8 T UV</td>
</tr>
<tr>
<td>9</td>
<td>9 w x y z</td>
<td>9 W X Y Z</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>*</td>
<td>* . ! $ % &amp; ' ( ) + , : ; / - @ ~</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>&lt;space&gt;</td>
<td></td>
</tr>
</tbody>
</table>
# Admin menu

<table>
<thead>
<tr>
<th>Admin Menu Options</th>
<th>2nd Level</th>
<th>3rd Level</th>
<th>4th Level</th>
<th>5th Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone Config</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephony Protocol</td>
<td>*Type 030</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type 33</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Push-to-talk</td>
<td>PTT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Enable/*Disable]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowed Channels</td>
<td></td>
<td></td>
<td>*Channel 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*Channel 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Channel 24</td>
</tr>
<tr>
<td>Name Channels</td>
<td>[list]</td>
<td></td>
<td>[Enter name]</td>
<td></td>
</tr>
<tr>
<td>Priority Channel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Priority Channel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>On/*Off</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name Channel</td>
<td></td>
<td>[Enter name]</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>[list]</td>
<td></td>
<td>*GMT</td>
<td></td>
</tr>
<tr>
<td>Daylight Savings</td>
<td></td>
<td></td>
<td>*DST No Adjust</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DST Auto &lt;USA&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DST Auto &lt;AUS&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DST Auto &lt;EUR&gt;</td>
<td></td>
</tr>
<tr>
<td>System Speed-dial</td>
<td></td>
<td></td>
<td>Enter Number</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>[Disable/*Enable]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[If Password is enabled]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speakerphone</td>
<td>[Disable/*Enable]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear Extension</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network Config</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Office</td>
<td>[Disable/Enable]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OAI</td>
<td>[Disable/Enable]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Addresses</td>
<td>*Use DHCP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default Gateway</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet Mask</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TFTP Server IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syslog Server IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time Server IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Call Server IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Call Server Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVPP IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OAI Server IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS ID</td>
<td>[enter]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>*None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WEP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td></td>
<td>*Open System</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shared Key</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WEP</td>
<td></td>
<td>[Enable/Disable]</td>
<td></td>
</tr>
</tbody>
</table>
### Admin Menu Options

<table>
<thead>
<tr>
<th>Options</th>
<th>2nd Level</th>
<th>3rd Level</th>
<th>4th Level</th>
<th>5th Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Key Information</td>
<td>Default Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Key Length</td>
<td>Key 1-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rotation Secret</td>
<td></td>
</tr>
<tr>
<td>WPA2-PSK</td>
<td></td>
<td></td>
<td>*Passphrase</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pre-Shared Key</td>
<td></td>
</tr>
<tr>
<td>WPA-PSK</td>
<td></td>
<td></td>
<td>*Passphrase</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pre-Shared Key</td>
<td></td>
</tr>
<tr>
<td>Cisco FSR</td>
<td></td>
<td></td>
<td>Username</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Reg. Domain</td>
<td>01</td>
<td>02</td>
<td>[802.11 Config]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[if 802.11(Aa)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.150–5.250</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.250–5.350 DFS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.470–5.725 DFS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.725–5.825 DFS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*b &amp; b/g mixed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>g only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[Transmit Power]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5mW (7dbm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10mW (10dbm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20mW (13dbm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*30mW (15dbm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>40mW (16dbm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50mW (17dbm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>100mW (20dbm)</td>
<td></td>
</tr>
</tbody>
</table>

### Diagnostics

- Run Site Survey
- Diagnostics (*Disable/Enable*)
- Syslog Mode: *Disabled Errors Events Full*
- [Error Handling Mode]
  - Halt on Error/Restart on Error

### Restore Defaults

*default setting*
Phone Config

Telephony Protocol
Telephony Protocol lets you select the VoIP protocol that your site is licensed to download and run. The CCMS Protocol to use for the Avaya 3641/3645 Wireless IP Telephones is 33. Any other protocol will cause the Wireless IP Telephone to malfunction.

Push-to-talk [Disable/Enable]
This option appears only on the Avaya 3645. Allowed Channels – All 24 PTT channels are allowed by default. To toggle the allowed status of any channel, scroll to the channel to be disallowed and press NavOK. Allowed channels are displayed with an asterisk (*) in the left column. Only those channels allowed in the Admin menu will appear on the config menu where they can be subscribed to by the end user. Name Channel – Allowed channels may be named. The name will appear instead of channel number when channel information is displayed on the handset. Priority Channel – The priority channel, labeled by default as channel 25, may be set and will be available to all PTT handsets. When a PTT broadcast is made on the priority channel, it will override any active PTT transmission on all other channels. The priority channel may be named.

Time Zone
Worldwide time zone options are available. Greenwich Mean Time (GMT) is the default.

Daylight Savings
The handset may be adjusted for daylight savings time.

System Speed-dial
The system speed-dial number appears as the first item on the speed-dial list and is specially marked with a greater-than symbol (>) as the first character in its name. It is usually programmed to a number that should be called in emergency situations. Enter the number to be dialed, the name (e.g. Security), and scroll to assign to a key press: 1-9, 0, *, #, ^. The carat represents the volume up and down buttons. This number must be programmed in every handset to work system-wide. It cannot be modified by the user.

Password [Disable/Enable]
The password option controls access to the Admin menu. To modify the password requirement, the default or previously set password must be entered to verify the change. The password must be set in each handset for which controlled access is desired. The Password option operates as a toggle between Enabled and Disabled. The info line will display the current state. Press NavOK to change the password protection state. Change Password will appear only if the password is enabled. The password is disabled by default.

Speakerphone
The speakerphone may be disabled when quiet handset operation is required. Disabling the speakerphone will remove the speakerphone softkey from the active mode display. The current speakerphone setting is shown on the info line. Press NavOK to toggle to the alternate setting.

Clear Extension
When the extension stored in the handset is cleared, the handset must redo the Extension and Password entry steps prior to registering with the PBX. This option is guarded with an Are you sure? query before being executed.
**IP Office [Disable/Enable]**
For proper display handling on the Wireless IP Telephone, enable the IP Office when using the IP Office system.

**OAI [Disable/Enable]**
The Open Application Interface (OAI) enables third-party computer applications to display alphanumeric messages on the Wireless IP Telephone display and take input from the Wireless IP Telephone keypad. Refer to the Open Application Interface (OAI) Specification (Version 1.2) documentation for information about administering the OAI Gateway and the services it can provide.

If you have an OAI Gateway installed in your system, OAI may be optionally enabled in each Wireless IP Telephone. You may select whether the Wireless IP Telephone should attempt to connect to the Avaya OAI Gateway by pressing `NavOK` to toggle to the alternate setting.

If OAI is enabled, and an OAI IP Address is available to the telephone (either via DHCP or Static IP configuration), the telephone will communicate with the OAI Server at START, and periodically while it is powered on. If you don’t have an Avaya OAI Gateway installed at your site, you should disable the OAI feature to preserve network bandwidth and battery life.

**Network Config**

**IP Address**
There are two modes in which the Wireless IP Telephone can operate – DHCP enabled or Static IP. Select the mode for operation from the **IP Address** menu:

* **Use DHCP** – will use Dynamic Host Configuration Protocol to assign an IP Address each time the Wireless IP Telephone is turned on. If DHCP is enabled, the Wireless IP Telephone also receives all other IP Address configurations from the DHCP server.

* **Static IP** – allows you to manually set a fixed IP Address. If selected, the Wireless IP Telephone will prompt for the IP Addresses of each configurable network component. When entering addresses, enter the digits only, including leading zeroes. No periods are required.

Regardless of the mode in which the Wireless IP Telephone is operating, the following components must be configured:

- The currently-used IP address of IP Office, the Call Server, the Call Server Port, and the AVPP may be displayed in the phone settings menu of the standby menu in the handset.

- **Phone IP** – the IP Address of the Wireless IP Telephone. This is automatically assigned if DHCP is used. If using Static IP configuration, you must obtain a unique IP Address for each phone from your network administrator.

- **Default Gateway and Subnet Mask** – used to identify subnets, when using a complex network which includes routers. Both of these must be configured either with an IP address under Static IP (not set to 000.000.000.000 or 255.255.255.255) or with DHCP for the Wireless IP Telephone to contact any network components on a different subnet. If configured on the DHCP server, use option 3 for the Default Gateway and option 1 for the Subnet Mask. Contact your network administrator for the proper settings for your network.
Note that the Wireless IP Telephones cannot “roam” across subnets, since they cannot change their IP address while operational. Ensure that all your access points are attached to the same subnet for proper operation. The Wireless IP Telephone can change subnets if DHCP is enabled and the Wireless IP Telephone is powered off then back on when within range of access points on the new subnet.

**TFTP Server IP** – the IP address of a TFTP server on your network which holds software images for updating the Wireless IP Telephones. If this feature is configured (not set to 0.0.0.0 or 255.255.255.255) with either Static IP configuration or using DHCP option 66 (TFTP Server), or the Boot server/next server (siaddr) field, the Wireless IP Telephone will check for newer software each time it is powered on or comes back into range of your network. This check takes only a second and ensures that all Wireless IP Telephones in your network are kept up-to-date with the same version of software.

**Syslog Server IP** – the IP address of the syslog server. See the Diagnostics section for more information.

**Time Server IP** – the IP address of the time server. The time server controls the date/time information that is displayed in standby mode.

**Call Server IP** – the IP address of the Avaya Communication Manager, such as the DEFINITY MultiVantage system. If using Static IP configuration, this is the IP address of the Communication Manager. If DHCP is being used, the Wireless IP Telephone will try the following, in order – DHCP Option 43 (Keyword MCIPADD), DHCP Option 176 (Keyword MCIPADD), and if DHCP Option 6 (DNS Server) and Option 15 (Domain Name) are configured, DNS lookup of server names found in the above options, and finally the DNS lookup of “AvayaCallServer.DOMAIN”.

**Call Server Port** – the IP port address of the Avaya Communication Manager. This port normally defaults to 1719, and is rarely changed. The port number entered must be coordinated with the administration of the Communication Manager, otherwise the wireless phone will not be able to register with the Communication Manager. If DHCP is being used, this can be changed via DHCP Option 43 (Keyword MCPORT) or DHCP Option 176 (Keyword MCPORT).

**AVPP IP** – the IP address of the Avaya Voice Priority Processor. Note that the Avaya Voice Priority Processor must be statically configured to have a permanent IP address. If DHCP is being used, the Wireless IP Telephone will try the following, in order: the DHCP option 151, then a DNS lookup of “SLNKSVP2” if the DHCP options 6 (DNS Server) and 15 (Domain Name) are configured.

**OAI Server IP** – the IP address of the NL OAI Gateway. If using static IP configuration, this is simply the IP address of the NL OAI Gateway. If DHCP is being used, the Wireless IP Telephone will try the DHCP option 152.

**SSID**
Enter the SSID.

**Security**
*NONE* disables any 802.11 encryption or security authentication mechanisms.

For WEP, WPA-PSK and WPA2-PSK set each of the following options to match exactly the settings in your APs.
Encryption codes display as they are entered. For security reasons codes will not display when a user returns to the Admin menu, Encryption options.

**WEP** (Wired Equivalent Privacy) is a wireless encryption protocol that encrypts data frames on the wireless medium allowing for greater security in the wireless network. If WEP is required at this site, you must configure each Wireless IP Telephone to correspond with the encryption protocol set up in the access points. Select the entries from the options below to enable the Wireless IP Telephone to acquire the system.

**Authentication**
Select either Open System or Shared Key.

**WEP [Enable/Disable]**
Select either Enable WEP or Disable WEP.

**Key Information**
- **Default Key** – Enter the key number specified for use by the Wireless IP Telephones. This will be 1 through 4.
- **Key Length** – Select either 40-bit or 128-bit depending on the key length specified for use at this location.
- **Key 1-4** – Scroll to the key option that corresponds to the Default Key that was entered above. Enter the encryption key as a sequence of hexadecimal characters. (Use the 2 and 3 keys to access hexadecimal digits A-F, use the Right Arrow key to advance to the next digit, and the Left Arrow key to backspace.) For 40-bit keys you will need to enter 10 digits; for 128-bit keys you will need to enter 26 digits. The display will scroll as needed.

**Rotation Secret** – This is used for proprietary WEP key rotation. Refer to your custom document if this feature is supported in your system.

**WPA2-PSK** – The security features of WPA2 (Wi-Fi Protected Access) using PSK (Pre-Shared Key) are available and may be used if supported by the access points in the facility. Select either Passphrase and enter a passphrase between eight and 63 characters in length or Pre-Shared Key and enter the 256-bit key code.

**WPA-PSK** – The security features of WPA (Wi-Fi Protected Access) using PSK (Pre-Shared Key) are available and may be used if supported by the access points in the facility. Select either Passphrase and enter a passphrase between eight and 63 characters in length or Pre-Shared Key and enter the 256-bit key code.

**Cisco FSR** (Fast Secure Roaming) In order to provide the highest level of security without compromising voice quality on Cisco Aironet wireless LAN access points, Avaya and Cisco Systems have cooperated to implement the Fast Secure Roaming mechanism. FSR is designed to minimize call interruptions for Avaya 3641/3645 Wireless IP Telephone users as they roam throughout a facility. Existing Aironet 350, 1100, and 1200 APs may require a firmware upgrade to support FSR. Cisco FSR requires advanced configuration of the Cisco access points in your site. See your Cisco representative for detailed documentation on configuring your access points and other required security services on
your wired network. To configure Cisco FSR in your Avaya 3641/3645 Wireless IP Telephone, you must enter a Radius Server username and password into each handset.

**Username** – Enter a username that matches an entry on your Radius server. Usernames are alphanumeric strings, and can be entered using the alphanumeric string entry technique.

**Password** – Enter the password that corresponds to this Username.

Consult the Configuration Note for the access points (APs) installed in your facility for information on which of the WPA versions are recommended by Avaya engineering. Configure the recommended version on the AP and select the corresponding option on the Admin menu.

**Regulatory Domain/802.11 Config/Transmit Power**
Regulatory domain, 802.11 configuration and transmit power are interdependent settings. Once the domain and 802.11 type are established, the transmit power may be set.

The 802.11 option(s) and the transmit power option(s) must be set to match the corresponding settings used by the APs in your facility.

FCC requirements dictate that the menu for changing the regulatory domain be available by password, which in our case is the **LINE** key. To set the domain, press **LINE** and then select the domain.

- **01** - North America
- **02** - Europe

Once the regulatory domain is established, the **802.11 Config** modes are displayed. Only one may be chosen. 802.11(b & b/g mixed) is the default. If 802.11(a) is selected, another menu opens so that you can select 802.11a transmission frequency range(s). Only those ranges which are allowed in the selected domain are displayed. Multiple ranges may be selected. Selected mode and ranges are marked with an asterisk (*). Press the **Done** softkey when you are finished specifying the 802.11 mode.

The **Transmit Power** menu opens when the **Done** softkey is pressed. Only those power levels which apply to the domain and 802.11 mode are listed. Only one level may be selected. The default will vary with the domain and 802.11 mode. The selected level is marked with an asterisk (*). Note that the bands labeled DFS may vary depending on the selected regulatory domain.

**Diagnostics**

**Run Site Survey**
The Site Survey mode is activated by selecting this option. Site survey starts running immediately upon selecting this option. See the Diagnostic Tools section for more information about site survey.

**Diagnostics [Disable/Enable]**
See the **Diagnostic Tools** section for a detailed explanation of the Diagnostics option.

**Syslog Mode**
See the **Diagnostic Tools** section for a detailed explanation of the syslog mode options.
Error Handling Mode
The error handling mode determines how the handset will behave when an error occurs. The **Halt on Error** option will cause the handset to stop operating if an error message is received. Unless the error is a fatal one, normal operation may be resumed by power-cycling the handset. The **Restart on Error** option will cause the handset to make every effort to reboot quietly and quickly to standby mode. In either scenario, a call in progress will be lost.

Error detail may be shown on the display, captured by the syslog server, and may also be available for downloading with the Handset Administration Tool.

**Restore Defaults**
The Restore Defaults option will set all user and administrative parameters to their factory defaults except **Telephony Protocol**.
## 4.2 Configuration (Config) Menu

The Avaya 3641/3645 Wireless IP Telephone features a Config (configuration) menu that allows the end user to configure user preferences and display handset information. The Config menu is opened by pressing the **Cfg** softkey from standby mode. See the end user guide 21-601633.

The diagram below shows the options on the Config menu.

<table>
<thead>
<tr>
<th>Config Menu Options</th>
<th>2nd Level</th>
<th>3rd Level</th>
<th>4th Level</th>
<th>5th Level</th>
<th>6th Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lock Keys</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Profiles</td>
<td>Silent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vibrate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Soft</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set as Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ring Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary Ring 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary Ring 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ring Cadence</td>
<td>Off</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PBX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Short Pulse</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Long Pulse</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ring Tone</td>
<td>Tones 1-10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ring Volume</td>
<td>Volume</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vibrate Cadence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PBX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Short Pulse</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Long Pulse</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ring Delay</td>
<td>No Delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 Second Delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 Second Delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Noise Mode</td>
<td>Normal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Severe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ring in Headset</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ring in Speaker</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning Tones</td>
<td>Disable/Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Tones</td>
<td>Disable/Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTT</td>
<td>Disable/Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone Settings</td>
<td>Keypad Autolock</td>
<td>Disable</td>
<td>5 seconds</td>
<td>10 seconds</td>
<td>20 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Display Contrast</td>
<td>Set Contrast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use Hearing Aid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use No Hearing Aid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Startup Song</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Play/Inhibit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Predial</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disable/Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Config Menu Options

<table>
<thead>
<tr>
<th></th>
<th>2nd Level</th>
<th>3rd Level</th>
<th>4th Level</th>
<th>5th Level</th>
<th>6th Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Push to talk</strong></td>
<td>Default Channel</td>
<td>Channel 1</td>
<td>.....</td>
<td>Channel 24</td>
<td></td>
</tr>
<tr>
<td>Subscribed Channels</td>
<td>Channel 1</td>
<td>Channel 2</td>
<td>Channel 3</td>
<td>Channel 4</td>
<td>Channel 24</td>
</tr>
<tr>
<td>PTT Audio Volume</td>
<td>Audio Volume</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTT Tone Volume</td>
<td>Tone Volume</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>Enter Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Info</td>
<td>Phone IP Address</td>
<td>AVPP IP Address</td>
<td>OAI IP Address</td>
<td>Call Server IP</td>
<td>Call Server Port</td>
</tr>
</tbody>
</table>

### Default Settings:
The profile options on the standby menu may be reset to their default values by the **Restore Defaults** option in the Admin menu. These are the default settings:

<table>
<thead>
<tr>
<th>Setting/profile</th>
<th>Silent</th>
<th>Vibrate</th>
<th>Soft</th>
<th>Loud</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring Cadence</td>
<td>Off</td>
<td>Off</td>
<td>PBX</td>
<td>PBX</td>
<td>PBX</td>
</tr>
<tr>
<td>Ring Tone</td>
<td>Tone 1</td>
<td>Tone 1</td>
<td>Tone 1</td>
<td>Tone 1</td>
<td>Tone 1</td>
</tr>
<tr>
<td>Ring Volume</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Vibrate Cadence</td>
<td>Off</td>
<td>PBX</td>
<td>Off</td>
<td>Off</td>
<td>PBX</td>
</tr>
<tr>
<td>Ring Delay</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Noise Mode</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>Headset/Speaker</td>
<td>Speaker</td>
<td>Speaker</td>
<td>Speaker</td>
<td>Speaker</td>
<td>Speaker</td>
</tr>
<tr>
<td>Key Tones</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Warning Tones</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Push-to-talk</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
</tr>
</tbody>
</table>
5. **Software License and Protocol Management**

The Avaya 3641/3645 Wireless IP Telephone System supports a number of different IP protocol integrations. All Malta series Wireless IP Telephones are shipped from Avaya with the correct software. However, it may be necessary to update the software. Please see section *Software Maintenance* for more information.

The following details the process to properly configure Avaya 3641/3645 Wireless IP Telephones and download software via over-the-air file transfer.

### 5.1 Requirements

- A wireless LAN must be properly configured and operational through the use of 802.11a/b/g wireless access points.
- The Avaya Communication Manager must also be connected to your network and completely operational.
- A TFTP Server must be available on the network in order to load the appropriate software into the Wireless IP Telephones.
- The AVPP Server is installed and properly configured.
- Software versions required:

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVPP</td>
<td>17x.028 or higher</td>
</tr>
<tr>
<td>OAI Server MOG 600</td>
<td>54.032 or higher</td>
</tr>
<tr>
<td>OAI Server MOG 700</td>
<td>82.017 or higher</td>
</tr>
</tbody>
</table>

- Finally, ensure that the Battery Pack on the Wireless IP Telephone is fully charged.

### 5.2 Configuration Process

Follow these steps to configure the Wireless IP Telephone.

1. Contact your service representative for information about downloading the latest Avaya 3641/3645 Wireless IP Telephone – IP software.

2. Load the latest version of the Avaya 3641/3645 Wireless IP Telephone code and place it on the TFTP Server and ensure the TFTP Server is started. The following five files are needed:
   - **usb downloader**: `pd14udcc.bin`
   - **functional filename**: `pd14ccc.bin`
   - **phntl filename**: `pi1400cc.bin`
   - **ota downloader**: `pd14odcc.bin`
   - **config file**: `slink_cfg.cfg`

3. If statically assigning IP addresses, ensure that the static addresses are accurate in the Admin menu. If using a DHCP Server, ensure that the DHCP option is set. See the *Avaya 3641/3645 Wireless IP Telephone Configuration* section for detailed configuration instructions.

4. Ensure the Wireless IP Telephone has properly configured SSID and Reg Domain within the Admin menu.

5. Using the Admin menu on the Wireless IP Telephone, ensure the Telephony Protocol menu option is set to 33. This ensures the handset will check for the proper software.
files each time it powers on. See the *Avaya 3641/3645 Wireless IP Telephone Configuration* section for detailed configuration instructions.


7. The code will now download to the handset. The status bar will increment fully across the display for each function that is being performed in the download process and the filename will display. Upon completion of the update process, the handset will re-boot with the new firmware.

8. After code has been downloaded for the first time, the Wireless IP Telephone will ask for an extension and password. Once these have been entered, the phone will register with the Avaya Communication Manager.

For future software upgrades, simply update the files that are stored on the TFTP Server. Each time the Wireless IP Telephone is powered up, it will check with the TFTP Server to ensure it has the proper software version. If a new version of code is downloaded, the currently-entered extension and password will be preserved.
6. **Avaya Communication Manager Integration Factors**

This section describes the mapping between the emulated Avaya 4612 IP Telephone and the Avaya 3641/3645 Wireless IP Telephone.

**Voice Messaging Access**
Voicemail is accessed on the Wireless IP Telephone as **FCN** + a character that corresponds to the administered button.

**CODECs**
The Avaya 3641/3645 Wireless IP Telephone is compatible with the G.711 and G.729a/ab codecs. There is no setting required on the Wireless IP Telephone. If an incompatible codec is specified, there will be no voice path.

**DHCP**
Dynamic Host Configuration Protocol (DHCP) is a standardized protocol that enables clients to be dynamically assigned with various configuration parameters, such as an IP address, subnet mask, default gateway, and other critical network configuration information. DHCP servers centrally manage such configuration data, and are configured by network administrators with settings that are appropriate for a given network environment. The Wireless IP Telephone will use the following DHCP options if DHCP use is enabled:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Subnet mask</td>
</tr>
<tr>
<td>3</td>
<td>Default gateway</td>
</tr>
<tr>
<td>6</td>
<td>DNS server</td>
</tr>
<tr>
<td>15</td>
<td>Domain name</td>
</tr>
<tr>
<td>43</td>
<td>Avaya-specific options</td>
</tr>
<tr>
<td>60</td>
<td>Vendor class ID</td>
</tr>
<tr>
<td>66</td>
<td>TFTP server</td>
</tr>
<tr>
<td>151</td>
<td>Avaya Voice Priority Processor</td>
</tr>
<tr>
<td>152</td>
<td>NL OAI Gateway</td>
</tr>
<tr>
<td>176</td>
<td>Avaya-specific options</td>
</tr>
<tr>
<td>siaddr</td>
<td>Boot server or next server</td>
</tr>
</tbody>
</table>

**TFTP**
The Wireless IP Telephone uses TFTP to update its software over the 802.11 wireless LAN.

**DNS**
Domain Name System (DNS), an industry-standard protocol, locates computers on an IP-based network. IP networks rely on number-based addresses to move information on the network. However, users are better at remembering friendly names than number-based addresses, so, it is necessary to translate user-friendly names into addresses that the network can recognize. The Wireless IP Telephone will use DNS to automatically translate names into IP addresses for these components – TFTP Server, Avaya Voice Priority Processor, and Avaya Communication Manager.
**Entering an Extension and Password**
Several conditions (new phone, Restore Defaults, Extension Error, Password Error, and Extension in use) can result in the Wireless IP Telephone asking the user for a new extension and password. The entry process is described below. When a new extension or password is being entered, the asterisk (*) key can be used to back up and correct an error.

The Wireless IP Telephone will display:

**Ext.–XXX**
**#–OK New –**

At this point, a new extension can be entered, or if the # key is pressed, the Wireless IP Telephone will retain the current extension.

After a new extension is entered, press # to continue.

The Wireless IP Telephone will then display:

**Password – **********
**# – OK**

A new password can be entered at this time, or if the # key is pressed, the Wireless IP Telephone will continue with its current password.

After a new password is entered, press # to continue.

**Extension Error**
If the Communication Manager (or all Communication Managers if there are more than one) does not recognize the extension the phone is trying to register with, the Wireless IP Telephone will display:

**Extension Error**
This will last 5 seconds, and then the Wireless IP Telephone will ask the user to enter a new extension and password.

**Password Error**
If the Wireless IP Telephone has an incorrect password, the display will show:

**Password Error**
**# to continue**

Press # to continue on to enter a new extension and password.

**Extension Override**
The Avaya Communication Manager will detect when a Wireless IP Telephone tries to register with the same extension as any telephone that is already registered to that extension. If this happens, the Wireless IP Phone will display:

**Extension in use**
**# to continue**

Press # to continue.

If the user chooses to continue on with the override information, the Wireless IP Telephone will register with the override bit set. Any telephone currently registered with the given extension will be unregistered, and any activity on the currently-registered telephone will be stopped. If that telephone is in a call, the call will be dropped.

If the user does not want to override the existing extension, either enter a different extension and password, or simply END the Wireless IP Telephone.
If two Wireless IP Telephones are assigned to the same extension, the Avaya Communication Manager will not properly resolve the registration conflict due to the presence of the Avaya Voice Priority Processor. Both Wireless IP Telephones may fail to operate properly.

**Retry / Restart**
Some errors will result in the following display, once # is pressed to continue:

* to retry
# to restart

Press * to immediately retry registering with the Communication Manager. Press # to restart the Wireless IP Telephone, which will take about 20 seconds.
7. **Feature Programming**

The Avaya 3641/3645 Wireless IP Telephone emulates the Avaya 4612 IP Telephone.

The 12 programmable keys for line appearances and features are emulated in the Wireless IP Telephone **LINE** and **FCN** menus. The dedicated Transfer, Conference, Hold, Mute, Speakerphone and Redial buttons are emulated by the Wireless IP Telephone softkeys.

All telephone functions and messaging features are supported if possible. Functions that require the use of the volume keys are not supported.

The **Menu**,◄, ►, **Exit** and softkeys on the 4612 IP Telephone are not supported.

Detailed explanation of the Avaya 3615/3645 Wireless IP Telephone functionality is explained in the User Guide (21-601633).
7.1 **Softkey Assignment**

The dedicated buttons on the Avaya 4612 IP Telephone appear while in a call or during active mode and are assigned to the softkeys in two sets:

<table>
<thead>
<tr>
<th>Spkr</th>
<th>Tran</th>
<th>Conf</th>
<th>More</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold</td>
<td>Mute</td>
<td>Redl</td>
<td>More</td>
</tr>
</tbody>
</table>

The **More** softkey toggles the screen to the other set. Pressing the softkey activates the feature.

7.2 **Function Assignment**

The keypad mapping for each Avaya 3641/3645 Wireless IP Telephone is administered through the Avaya Communication Manager administration software (for example, Avaya Site Administration). Programmable keys are accessed by pressing the **LINE** or **FCN** key on the Wireless IP Telephone, followed by the appropriate digit key. The line appearances assigned to any of the twelve programmable feature keys on the Avaya 4612 IP Telephone are emulated by the **LINE** menu on the Wireless IP Telephone. The features are emulated by the **FCN** menu. Lines and features may be assigned in any combination.

Lines and features are automatically assigned to shortcut keys which may be used to expedite access. The Wireless IP Telephone receives line and feature information from the Communication Manager and places it on the appropriate menu for access by the end user.

**Line Appearances**

Any of the 12 programmable keys on the Avaya 4612 IP Telephone may be assigned to lines. Typically, three line appearances are assigned. These line appearances may be displayed on the **LINE** menu. While off-hook, press the **LINE** key to view the shortcut keys and assigned extensions for line appearances. There are nine possible line appearances which correspond to the nine indicators at the top of the Wireless IP Telephone display. When a line is in use, the indicator converts to the line number. Press the **LINE** key again to display the second page of the list if more than four line keys have been programmed. To use an extension, press the corresponding shortcut key. Use the **Nav** buttons to navigate and activate the line appearances on this list. Up and down arrows on the display indicate additional items may be viewed.

**Feature List**

Any of the 12 programmable keys on the Avaya 4612 IP Telephone may be assigned to features. Typically, three line appearances are assigned and the remaining nine keys are programmed to features. These features may be accessed through the **FCN** menu on the Wireless IP Telephone. When **FCN** is pressed, the display lists the first four features and the assigned shortcut keys. A plus sign (+) may appear to indicate that the corresponding feature is turned on. Pressing **FCN** repeatedly will display the remaining items on the list. Shortcuts programmed to OAI features will preempt programming assigned to other keys.

Activate the fixed features on the off-hook Wireless IP Telephone by pressing **FCN** + the shortcut key. You may also use the **Nav** buttons to navigate and activate the features on this list. Up and down arrows on the display indicate that additional items may be viewed.

Changes to feature programming in the Communication Manager will take effect after the Wireless IP Telephone is powered off and back on again.
If an Open Application Interface (OAI) is operational, one or more function key sequences will be assigned in the OAI configuration and they will override any function sequence established here.

The Wireless IP Telephone relies on the PBX’s response to a Button Request message to allocate **LINE** and **FCN** keys to the appropriate list, as well as to supply correct labels for the keys. If the PBX fails to respond, or if the response cannot be properly parsed, the following default behavior is applied:

If the IP Office mode is enabled, six default keys are assigned under the **LINE** key, and are labeled L/F 01 through L/F 06. These keys send the same codes as P1 through P6 on the 4606/4612 terminal.

If the IP Office mode is disabled, an additional six keys labeled L/F 07 through L/F 12 are assigned under the **FCN** key, and send the same key codes as P7 through P12 of the 4612 terminal.
8. Testing a Wireless IP Telephone

Verify proper registration and operation of each Wireless IP Telephone by performing the following tests on each Wireless IP Telephone in an active wireless area.

1. Power on the Wireless IP Telephone by pressing the END key. You will see a series of messages displayed as the Wireless IP Telephone acquires the system. The Wireless IP Telephone should display the user extension. Any error messages should clear.

2. Press the START key. The extension number should be replaced by information from the Avaya Communication Manager and you should hear a dial tone. Place a call and listen to the audio quality. End the call by pressing the END key.

3. Place a call to the Wireless IP Telephone and verify ring, answer, clear transmit and clear receive audio.

4. Press the START key.

5. Use the softkeys and the FCN key to verify all programmed features on the Wireless IP Telephone, and press END when finished.

6. Use the LINE key to verify the programmed line appearances, and press END when finished.

7. Press the END key. Any line indicators should turn off and the extension number display will return.
9. Diagnostic Tools

Run Site Survey, Diagnostics Enabled and Syslog Mode are three diagnostic tools provided to assist the WLAN administrator in evaluating the functioning of the Wireless IP Telephone and the system surrounding it. Diagnostic Tools are enabled in the Admin menu.

9.1 Run Site Survey

Site survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area to look for all APs regardless of SSID. The information available through site survey includes:

- SSID
- Beacon Interval
- Information regarding support of 802.11d, 802.11g, 802.11h, and other 802.11 amendment standards as required.
- Current security configuration

START the site survey by selecting Run Site Survey from the Admin menu. The mode starts immediately.

When the test is started, it is by default in “single SSID” mode. When the Any soft key is pressed (softkey A) all APs, regardless of SSID, are displayed and the softkey changes to say MyID. Pressing the MyID soft key will revert the display to the “single SSID” mode and change the softkey back to Any.

The display would look like the following for the multiple AP mode.

```
1 1 1 1 1 1 - 2 2 3 3 4 4 4
1 1 1 1 1 1 - 2 2 3 3 4 4 4
1 1 1 1 1 1 - 2 2 3 3 4 4 4
1 1 1 1 1 1 - 2 2 3 3 4 4 4
A n y         D e t l
```

Where:

- 111111 – The last three octets of the on-air MAC address for a discovered AP.
- 22 – The signal strength for the specified AP.
- 33 – The channel number of the specified AP.
- 444 – The beacon interval configured on the specified AP.
- Any/MyID – Softkey to toggle between “single SSID” and “any SSID” mode.
- Detl/Smry – Softkey to toggle between the multiple AP (summary) display, and the single (detail) displays for each AP.

The following screen shows how the display would look when there are three APs configured with an SSID that matches that of the Wireless IP Telephone. The first has a signal strength of –28 dBm, is configured on channel 2, with a beacon interval of 100ms. The second has a signal strength of –48 dBm, is configured on channel 6, with a beacon interval of 200ms. The third has a signal strength of –56 dBm, is configured on channel 11 with a beacon interval of 100ms.
When the **Any** SSID mode is selected, the summary display contains the first six characters of the APs SSID instead of the beacon interval as in the example below.

```
a b 7 b c 8  - 2 8  0 2  1 0 0
2 a e 5 7 8  - 4 8  0 6  2 0 0
2 a e 5 9 6  - 5 6  1 1  1 0 0
Any       Detl
```

In the **Detl** (detail) mode the display would appear as follows. The Left/Right arrow keys will move between AP indices.

```
i : b b b b b b b s n c h b c n
e e e e e e e e e e e e e e e D G H I
r r r r r r r r r r r r r r r r r r + x x x x x
m m m G : g g g g g P : p p p p p
Any    Smry
```

Where:

- **i** – Index of selected AP (value will be from 0 to 3 inclusive)
- **bbbbbbbb** – The last three octets of the BSSID for a discovered AP.
- **sn** – Signal strength in –dBm
- **ch** – Channel
- **bcn** – Beacon interval
- **eeeeeeeeee** – SSID (Up to first 11 characters)
- **DGHI** – Standards supported
- **rrrrrrrr** – Rates supported. Basic rates will have a “b” following the rate.
- **+** – more rates are supported than those displayed
- **xxxx** – WMM or UPSD if those QoS methods are supported
- **mmm** – Security mode
- **G:gggg** – Group key security
- **P:pppp** – Pairwise key security
- **Any/MyID** – Softkey to toggle between “single SSID” and “any SSID” modes.
- **Detl/Smry** – Softkey to toggle between the multiple AP display (summary), and the single AP display (detail).

Numbers racing across the Wireless IP Telephone display indicate AP information is being obtained. A **Waiting** message indicates the system is not configured properly and the Wireless IP Telephone cannot find any APs.

**Solving Coverage Issues**
Coverage issues are best resolved by adding and/or relocating access points.
Overlap issues may be resolved by reassigning channels to the access points or by relocating the access points. See the *Troubleshooting* section *Access Point Problems* for more information.

### 9.2 Diagnostics Enabled

The **Diagnostics** option is used to evaluate the overall quality of the link between the Wireless IP Telephone, AP, and infrastructure side equipment, such as PBX, AVPP, and gateways. Unlike Site Survey, the Diagnostics mode is used while the functional code is running, and during a call.

When **Diagnostics** is enabled in the Admin menu, the Wireless IP Telephone can display diagnostic screens any time it is active (in a call).

The display of information is instigated by pressing the **Nav** or **Nav** key. Only four of the diagnostic counters listed below can be shown at a time. Pressing the **Nav** keys multiple times will cycle through the various counters and the normal off-hook (IP PBX) display. The numeric icon at the top of the display indicates what screen number is being displayed. For example: the first time the **Nav** key is pressed, the **1** icon is shown, and the first four counters are displayed. The next time it is pressed, the **2** icon is shown, and the next four counters are displayed. The counters will be cycled through in this fashion until there are no more counters to be displayed. After all the counters have been displayed, the screen returns to the normal off-hook IP PBX screen.

The information provided when **Diagnostics** is enabled includes:

**Screen 1**
- Missed receive packet count since power up (MissedRcvCnt)
- Missed transmit packet count since power up (MissedXmtCnt)
- Receive retry count since power up (RxRetryCount)
- Transmit retry count since power up (TxRetryCount)

<table>
<thead>
<tr>
<th>MissedRcvCnt</th>
<th>nnnnnn</th>
</tr>
</thead>
<tbody>
<tr>
<td>MissedXmtCnt</td>
<td>nnnnnn</td>
</tr>
<tr>
<td>RxRetryCount</td>
<td>nnnnnn</td>
</tr>
<tr>
<td>TxRetryCount</td>
<td>nnnnnn</td>
</tr>
</tbody>
</table>
Screen 2
- Jitter – average error or “wobble” in received packet timing, in microseconds
- Last successful transmit data rate (LastRate)
- Gateway type (GatewayType)

\[
\begin{array}{c}
\text{Jitter} \\
\text{Last Rate} \\
\text{Gateway Type}
\end{array}
\]

Where:
- mnemo – A mnemonic that indicates what type of gateway is being used
- 11Mb – AVPP in use and no legacy Wireless IP Telephones. This system can run at the full speed.

Screen 3
- Screen 3 contains a list of the APs that are heard and the following parameters from each AP:
  - Indicator as to whether this is the current AP or an index into the list of other APs heard
  - Last two octets of the MAC address of the AP
  - Channel number
  - Signal strength
  - Either the 802.11 Association ID from the current AP or a mnemonic for the reason code indicating why the Wireless IP Telephone didn’t hand off to this other AP.

\[
\begin{array}{c}
C : m m m m c h - s s a i d \\
1 : m m m m c h - s s m n e m \\
2 : m m m m c h - s s m n e m \\
3 : m m m m c h - s s m n e m
\end{array}
\]

Where:
- C – Indicates the AP that the Wireless IP Telephone is currently using
- n – Indicates an index into the list of other APs, where n is equal to 1, 2, or 3
- mmmmm – This hexadecimal number is the last 2 octets of this AP’s MAC address
- ch – Channel number the AP is configured on
- -ss – Signal strength for the AP in dBm
- aid – The Association ID for the currently associated AP
- mnem – A mnemonic indicating the reason code:
  - Unkn – Reason unknown
  - Weak – Signal strength too weak
  - Rate – One or more basic rates not supported
- Full – AP can not handle bandwidth requirements
- AthT – Authentication timeout
- AscT – Association timeout
- AthF – Authentication failure
- AscF – Association failure
- SecT – Security handshake timeout
- SecF – Security handshake failure
- Cnfg – AP not configured correctly for security, QoS mode or infrastructure network.

**Screen 4**
- Association count since power-up (AssocCount)
- Re-association count since power-up (ReAssocCount)
- Association failures since power-up (AssocFailure)
- Re-association failures since power-up (ReAssocFail)

```
AssocCount nnnnn
ReAssocCount nnnnn
AssocFailure nnnnn
ReAssocFail nnnnn
```

**Screen 5**
- Security error count since power up (Sec-ErrCount)
- MAC sequence number of frame with last security error (LstSecErrSeq)

```
Sec-ErrCount nnnnn
LstSecErrSeq nnnnn
```
9.3 Syslog Mode

A syslog server must be present on the network in order for the Wireless IP Telephone to send the log messages and have them saved. The syslog server will be found with DHCP option 7 if the Wireless IP Telephone is using DHCP. If static addresses are configured, the syslog server’s IP address can be configured statically in the Admin menu.

If the syslog server address is blank (000.000.000.000 or 255.255.255.255) or the Wireless IP Telephone is using DHCP and no option 7 is received from the DHCP server, the Wireless IP Telephone will not send any syslog messages.

Admin menu options:

*Disabled* turns syslog off.

**Errors** causes the Wireless IP Telephone to log only events that we consider to be an error (see below).

**Events** logs all errors plus some other interesting events (see below).

**Full** logs all the above plus a running stream of other quality information (see below).

The table below lists the syslog messages and which level of logging will produce them:

<table>
<thead>
<tr>
<th>Message type</th>
<th>Errors</th>
<th>Events</th>
<th>Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Handoff</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Successful Handoff</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Error</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call START/End</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Audio stats</td>
<td>No</td>
<td>No</td>
<td>Yes (every 5 secs)</td>
</tr>
<tr>
<td>Audio error threshold exceeded</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Radio stats</td>
<td>No</td>
<td>No</td>
<td>Yes (every 5 secs)</td>
</tr>
<tr>
<td>Radio error threshold exceeded</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Error Handling Mode</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

All syslog messages will include:

- Date and time (to 1/100th of second) since handset START (currently set to Jan-1 00:00:00)
- Wireless IP Telephone’s MAC address
- Wireless IP Telephone’s IP address
- Sequence number

The table below lists the additional items in each message type:
### Failed Handoff
(Sent whenever the Wireless IP Telephone attempted handoff, but failed trying.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed AP MAC</td>
<td>Failed AP signal strength</td>
</tr>
<tr>
<td>Failed AP signal strength</td>
<td></td>
</tr>
<tr>
<td>Current AP MAC</td>
<td>Current AP signal strength</td>
</tr>
<tr>
<td>Current AP signal strength</td>
<td></td>
</tr>
<tr>
<td>Failure reason</td>
<td></td>
</tr>
</tbody>
</table>

### Successful Handoff

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New AP MAC</td>
<td>New AP signal strength</td>
</tr>
<tr>
<td>New AP signal strength</td>
<td></td>
</tr>
<tr>
<td>Old AP MAC</td>
<td>Old AP signal strength</td>
</tr>
<tr>
<td>Old AP signal strength</td>
<td></td>
</tr>
<tr>
<td>Reason for handoff</td>
<td>Reason for handoff</td>
</tr>
<tr>
<td>Other candidate APs: MAC</td>
<td>Other candidate APs MAC</td>
</tr>
<tr>
<td>Signal strength</td>
<td>Signal strength</td>
</tr>
<tr>
<td>Reason not used</td>
<td>Reason not used</td>
</tr>
</tbody>
</table>

### Security Error

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP MAC</td>
<td>AP signal strength</td>
</tr>
<tr>
<td>AP signal strength</td>
<td></td>
</tr>
<tr>
<td>Security mode</td>
<td>Security mode</td>
</tr>
<tr>
<td>Error details (mode-dependent)</td>
<td>Error details (mode-dependent)</td>
</tr>
</tbody>
</table>

### Call START

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call type (telephony, OAI, PTT)</td>
<td>Call type (telephony, OAI, PTT)</td>
</tr>
<tr>
<td>AP MAC</td>
<td>AP MAC</td>
</tr>
<tr>
<td>AP signal strength</td>
<td>AP signal strength</td>
</tr>
</tbody>
</table>

### Call End

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP MAC</td>
<td>AP MAC</td>
</tr>
<tr>
<td>AP signal strength</td>
<td>AP signal strength</td>
</tr>
</tbody>
</table>

### Audio stats

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP MAC</td>
<td>AP MAC</td>
</tr>
<tr>
<td>AP signal strength</td>
<td>AP signal strength</td>
</tr>
<tr>
<td>Payload size (in msec)</td>
<td>Payload size (in msec)</td>
</tr>
<tr>
<td>Payloads sent</td>
<td>Payloads sent</td>
</tr>
<tr>
<td>Payloads received</td>
<td>Payloads received</td>
</tr>
<tr>
<td>Payloads missed (not received)</td>
<td>Payloads missed (not received)</td>
</tr>
<tr>
<td>Payloads missed rate (over last 5 seconds)</td>
<td>Payloads missed rate (over last 5 seconds)</td>
</tr>
<tr>
<td>Payloads late</td>
<td>Payloads late</td>
</tr>
<tr>
<td>Payloads late rate (over last 5 seconds)</td>
<td>Payloads late rate (over last 5 seconds)</td>
</tr>
<tr>
<td>Average jitter</td>
<td>Average jitter</td>
</tr>
</tbody>
</table>

### Audio error threshold exceeded
(Sent if payloads missed rate or payloads late rate exceeds 2%, or if the average jitter is over 2 msec)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same as audio stats</td>
<td>Same as audio stats</td>
</tr>
</tbody>
</table>

### Radio stats

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP MAC</td>
<td>AP MAC</td>
</tr>
<tr>
<td>AP signal strength</td>
<td>AP signal strength</td>
</tr>
<tr>
<td>Directed packets sent</td>
<td>Directed packets sent</td>
</tr>
<tr>
<td>Directed packets received</td>
<td>Directed packets received</td>
</tr>
<tr>
<td>Multicast packets sent</td>
<td>Multicast packets sent</td>
</tr>
<tr>
<td>Multicast packets received</td>
<td>Multicast packets received</td>
</tr>
<tr>
<td>Broadcast packets sent</td>
<td>Broadcast packets sent</td>
</tr>
<tr>
<td>Broadcast packets received</td>
<td>Broadcast packets received</td>
</tr>
<tr>
<td>TX dropped count</td>
<td>TX dropped count</td>
</tr>
<tr>
<td>TX drop rate (over last 5 seconds)</td>
<td>TX drop rate (over last 5 seconds)</td>
</tr>
<tr>
<td>TX retry count</td>
<td>TX retry count</td>
</tr>
<tr>
<td>TX retry rate (over last 5 seconds)</td>
<td>TX retry rate (over last 5 seconds)</td>
</tr>
<tr>
<td>RX retry count</td>
<td>RX retry count</td>
</tr>
<tr>
<td>RX retry rate (over last 5 seconds)</td>
<td>RX retry rate (over last 5 seconds)</td>
</tr>
</tbody>
</table>

### Radio error threshold exceeded
(Sent if TX drop rate exceeds 2% or TX or RX retry rate exceeds 5%)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same as radio stats</td>
<td>Same as radio stats</td>
</tr>
</tbody>
</table>

Messages are formatted like the following example:

```
Jan 1 00:01:26.72 0090.7a02.2a1b (172.16.0.46) [001a] RStat: AP 00:40:96:48:1D:0C (-56 dBm), Sent 783523, Recvd 791342, MSnt 245, MRcd 5674, BSnt 43, BRcd 10783, TX drop 43 (0.0%), TX retry 578 (1.2%), RX retry 1217 (1.6%)
```
10. **Certifying the Wireless IP Telephones**

Prior to determining that an installation is complete, test the Wireless IP Telephones following the sequence given in the previous *Testing a Wireless IP Telephone* section and conduct a site survey mode test according to the directions given in the previous *Diagnostic Tools* section.

The installation may need some adjustments. Note any areas where coverage is conflicting or inadequate. Note any system difficulties and work with your wireless LAN and/or LAN system administrator to determine the cause and possible remedy. See the section *Wireless IP Telephone Problems* for clues to possible sources of difficulties. If any adjustments are made to the system, re-test the device in the same vicinity to determine if the difficulty is resolved.

These tests must be performed in typical operating conditions, especially if heavy loads occur. The testing sequence and procedure is different for every installation. Generally, you should organize the test according to area and volume, placing numerous calls to others who can listen while you perform coverage tests. Note any areas with excessive static or clarity problems and report it to an Avaya service engineer.

The coverage test will also require you to put the Wireless IP Telephone in Site Survey mode and walk the entire coverage area to verify all access points.

10.1 **Conducting a Site Survey**

Conduct a Site Survey of the installation by walking the site looking for interfering 802.11 systems, adequate coverage and channel assignment, and correct AP configuration.

1. Referring to section *Run Site Survey*, put a Wireless IP Telephone into Site Survey in the Any/Smry SSID mode. Walk throughout the site checking for any expected APs or other SSIDs.

2. Then, walk the site again, in MyID/Smry SSID mode, this time checking that every location has adequate coverage (there should be at least one AP stronger than -70dBm in all areas) and has good channel allocation (at any point, the strongest AP shown should be on a different channel than the next-best choice).

3. Finally, use the single AP (MyID/Detl) display to check each AP, to ensure it is configured for the proper data rates, beacon interval, 802.11 options enabled, QoS method, and security method.

Make any necessary adjustments to AP locations and configurations and repeat steps 1-3 until the Site Survey shows adequate coverage and correct configuration at every location.

The installation is not complete until these certification steps have been performed. Do not hand out Wireless IP Telephones at a site that has not been certified.
11. Software Maintenance

The Avaya 3641/3645 Wireless IP Telephones use proprietary software programs maintained by Avaya. The software versions that are running on the Wireless IP Telephones may be displayed by selecting the Firmware Version option on the admin menu. Firmware Version is also an option on the Config menu.

Avaya or its authorized dealer will provide information about software updates and how to obtain the software (for example, downloading from a web site).

11.1 Upgrading Wireless IP Telephones

After software updates are obtained from Avaya, they must be transferred to the appropriate location in the LAN to update the code used by the Wireless IP Telephones.

Avaya 3641/3645 Wireless IP Telephones allow over-the-air transfer of software updates from the designated TFTP server to the Wireless IP Telephones. The download function in the Wireless IP Telephone checks its software version every time the Wireless IP Telephone is turned on. If there is any discrepancy the Wireless IP Telephone immediately begins to download the update.

Normal Download Messages

When the Wireless IP Telephone is powered on, it displays a series of messages indicating that it is searching for new software, checking the versions, and downloading. The normal message progression is:

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking Code</td>
<td>Wireless IP Telephone is contacting the TFTP Server to determine if it has a newer version of software that should be downloaded.</td>
</tr>
<tr>
<td>Erasing Memory</td>
<td>Wireless IP Telephone has determined that a download should occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line the erase operation is complete.</td>
</tr>
<tr>
<td>Updating Code</td>
<td>Wireless IP Telephone is downloading new software into memory. When the progress bar fills the display line the update operation is complete on that file.</td>
</tr>
</tbody>
</table>

When the update is complete, the Wireless IP Telephone displays the extension number and is ready for use.
## Download Failure or Recovery Messages

The following display messages indicate a failure or recovery situation during the download process.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Busy</td>
<td>Wireless IP Telephone is attempting to download from a TFTP Server that is busy downloading other phones and refusing additional downloads. The Wireless IP Telephone will automatically retry the download every few seconds.</td>
</tr>
</tbody>
</table>
| TFTP ERROR(x):yy | A failure has occurred during the TFTP download of one of the files. (x) – The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are:  
01 – TFTP server did not find the requested file.  
02 – Access violation (reported from TFTP server).  
07 – TFTP server reported "No such user" error. Check the TFTP server configuration.  
81 – File put into memory did not CRC. The Wireless IP Telephone will attempt to download the file again.  
FF – Timeout error. TFTP server did not respond within a specified period of time. |
| Erase Failed     | Download process failed to erase the memory in the Wireless IP Telephone. This operation will retry.                                           |
| Waiting          | Wireless IP Telephone has attempted some operation several times and failed, and is now waiting for a period of time before attempting that operation again. |
C. Handset Administration Tool

Installation and Use
1. **Handset Administration Tool Installation**

The Handset Administration Tool is a software utility installed on a PC with a USB port that can be cabled to the USB port of the Dual Charger. It is designed as a time-saving device for rapid administration and configuration of a number of handsets. Configuration options include:

- Setting all options on the Admin menu,
- Setting all options on the Config menu,
- Assist troubleshooting by recording error information,
- Upgrade handset software.

1.1 **Installing the USB Driver**

Necessary components:

- PC running Windows 2000 or Windows XP with a USB port,
- Dual Charger for the Avaya 3641/3645 Wireless IP Telephone,
- Power supply for the appropriate country or region,
- Avaya USB cable or comparable cable (with 5-pin “mini-B” connector).

USB cables vary in their ability to make a proper connection to the Dual Charger’s USB port. Use of the USB cable available through Avaya is recommended to ensure compatibility.

If retrieving files from the Avaya Installation Manuals CD, the files are available as two separate links on the Administration Software page.

1. Set up a folder for Avaya 3641/3645 Wireless IP Telephone configuration on the PC. Load the Handset Administration Tool software into this folder. If the exe file is delivered in a zip file, extract the individual file(s).

2. The USB driver files may be delivered in a separate zip file. If so, set up a folder for the USB files and extract the two files from the zip file into this folder. These are named slnkusb.sys and slnkusb.inf.

   The USB driver may be left on the Installation Manuals CD and installed from there if preferred.

3. Place the Dual Charger on a flat, horizontal surface and plug the power supply into the Dual Charger and into an appropriate wall outlet. Plug the USB cable into the Dual Charger and into an available USB port on the PC.

4. Power off an Avaya 3641/3645 Wireless IP Telephone, remove the Battery Pack, and place the handset in the Charger. The handset will automatically power up in USB mode.

5. Microsoft Windows will start the Found New Hardware Wizard and ask if it can connect to Windows Update to search for software. Click “No, not this time.” Click Next.
6. The next screen prompts you for information about installing the USB device. Click “Install from a list or specific location” and click Next.
7. The next screen prompts you for the location. Click “Search for the best driver in these locations”. Clear the “Search removable media” checkbox. Select the “Include this location in the search” checkbox and browse to the location of the USB driver files. Click Next.

8. The Microsoft Wizard will display the following warning message. The USB software has been fully tested in our laboratories and will not harm your system. Click Continue Anyway:

9. Microsoft Wizard will now install the software:
10. The final screen indicates that the USB driver has been successfully installed. Click Finish to close the wizard and proceed with handset configuration.

1.2 Install the Handset Administration Tool

Note that there is no installer or uninstaller for the Handset Administration Tool since the program does not modify your system or registry. It runs from its current location and stores its settings locally.

1. If not already done, create a folder for the Handset Administration Tool files and then copy the exe file into it.

2. Navigate to the folder established in step 1 above and click the HandsetAdminAvxx_xx_xx_xx.exe file to run the utility.

3. Accept the Software License Agreement.
Part C: Handset Administration Tool

4. The **HandsetAdmin Setup** window allows you to run the program from its current location or set up Start Menu shortcuts and/or move the program to a different folder, if desired.

If you select **Run From Current Location**, the Handset Administration Tool will start. Note that the tool will not be fully functional if it is run from a non-writeable location such as a CD.

If you select **Setup Instructions...**, another window will help you set up shortcuts and if desired, move the .exe file to another location. Once the shortcut is created, click the new shortcut to open the program.

**Update Application**

The **Update Application** button allows you to retrieve a more recent version of the Handset Administration Tool from a local folder or from the SpectraLink FTP site.

SpectraLink recommends downloading the updated versions from the FTP site when first installing the program.

The FTP option allows you to go to an FTP site and download the most recent version while updating the software on the connecting computer. Once the file is downloaded, you can copy it to a local location and update other computers using the local option.

If the FTP option is selected, a dialog box will open to direct you to the FTP site. If selecting the **Update from FTP server** option, be sure your computer has Internet access.
Once you connect to the server, you can select and download the file. The file will have version number with a .pkg extension in this format HandsetAdminAvyy_yy_yy_yy.pkg

Package (pkg) files are bundled versions of the Handset Admin Tool exe. Package files are made available by SpectraLink for download via an anonymous FTP site. Users must have a valid HandsetAdmin.exe installed on the connecting PC in order to unpack and install the upgrade.

Package files are located beneath the /pub folder on the FTP server. From there, navigate to the appropriate folder for your PBX and vendor type.

Setup Instructions

Setup instructions are a series of tips and tricks for installing the Handset Administration Tool on your system. A dialog box with instructions on installing it on the Start Menu displays.

The buttons on this dialog will open instances of Windows Explorer that are preset to paths that may be convenient for manually copying HandsetAdmin.exe to an appropriate path and creating start menu shortcuts. There is no automatic installer or un-installer but these procedures are simple to perform manually since this application consists of a single program file that stores all of its settings in a single initialization file. The initialization file is a text file named HandsetAdmin.ini which is automatically created in the path that contains HandsetAdmin.exe (if the path is writable). All settings are kept in this file rather than in your registry or system folders so that they are easy to find (to backup, restore, transfer, etc.) and so that it is easy to manually "upgrade", "move", and "uninstall" the application without losing settings or leaving junk behind.

The full instructions shown in the box above are reproduced in full below.
Installing HandsetAdmin

The buttons on this dialog will open instances of Windows Explorer that are preset to paths that may be convenient for manually copying HandsetAdmin.exe to an appropriate path and creating start menu shortcuts. There is no automatic installer or uninstaller but these procedures are simple to perform manually since this application consists of a single program file that stores all of its settings in a single initialization file. The initialization file is a text file named HandsetAdmin.ini which is automatically created in the path that contains HandsetAdmin.exe (if the path is writable). All settings are kept in this file rather than in your registry or system folders so that they are easy to find (to backup, restore, transfer, etc.) and so that it is easy to manually "upgrade", "move", and "uninstall" the application without losing settings or leaving junk behind.

To install the application:
- Copy HandsetAdmin.exe to a write-enabled folder. If you create a new folder specifically for this application, the folder can double as a convenient place to save handset firmware updates or other files associated with this application.
- Create Start menu or desktop shortcuts if desired.
- The first time you run it from its new location, you will need to accept the License Agreement then choose "Run From Current Location" when the "Setup" dialog appears. These dialogs will not appear again unless you delete HandsetAdmin.ini.

To upgrade the application:
- Overwrite HandsetAdmin.exe with a newer version. New versions of the application are compatible with (will recognize) the old settings contained in your existing HandsetAdmin.ini file.

To move the application:
- Move HandsetAdmin.exe and HandsetAdmin.ini to a new path or move or rename the folder containing these two files. Windows XP will automatically modify shortcuts for you when their targets are moved or renamed via Windows Explorer, so, even if you created start menu shortcuts to these files, you can move them using Explorer without having to re-do the shortcuts.
- If moving the application to a new machine, you will have to create new shortcuts, if desired, on the new machine. By copying HandsetAdmin.ini to the new machine, your old settings will be retained.

To uninstall the application:
- Delete HandsetAdmin.exe, HandsetAdmin.ini, and any shortcuts or folders you created for it.

How to use Windows Explorer and create Start menu shortcuts

Consult the documentation that came with your operating system for details. The instructions below describe one set of tips and techniques. Other techniques exist and are just as valid. These instructions were written for Windows XP and may or may not work under different operating systems.

To move or copy a file, drag it from one Explorer window and drop it into another Explorer window.

To create a shortcut, use the right mouse button to drag a file or folder (for instance, HandsetAdmin.exe) to an Explorer window, then choose "Create Shortcuts Here" from the menu that appears when you release the right mouse button.

A file, folder, or shortcut in one of the Start menu paths (either "current user" or "all users") will show up in the Start menu under the "All Programs" submenu. Folders show up as submenus and the contents of folders show up as items under the folder's submenu.

To make a shortcut show up in your Start menu up above the most-recent list (rather than under the "All Programs" submenu), right-click on the target or existing shortcut (either in
the Start menu or in Windows Explorer), then choose “Pin to Start menu”. To reverse this effect, right-click on the Start menu shortcut and choose “Unpin from Start menu”.

Ini tricks and tips:
- The program reads HandsetAdmin.ini when it starts, keeps settings in memory while it runs, and writes HandsetAdmin.ini when it exits. Thus if you modify HandsetAdmin.ini while the program is running, your changes will have no effect.
- Delete, move, or rename HandsetAdmin.ini to make the program forget its history and revert to default settings (for example, to make it re-show this dialog which is normally shown only once).
- Copy HandsetAdmin.ini to another machine to share or transfer settings.
- Edit HandsetAdmin.ini with a text editor to erase or modify specific settings.
- Backup and restore HandsetAdmin.ini to preserve settings.
- If you rename HandsetAdmin.exe then the name of the .ini will likewise change (just replace “.exe” with “.ini” to determine the new name). The old .ini will be orphaned unless you also rename it.

To print or copy this text
Copy-and-paste this text into WordPad. All formatting will be preserved. Use WordPad to save or print the text.
2. **Using the Handset Administration Tool Console**

The Handset Administration Tool uses indicators to alert you to the status of the action being performed.

- **Green** – the adjacent label is “true” and this state is desirable or required.
- **Yellow** – the adjacent label is “true” and this state requires caution or attention. For example, a yellow *New folder* indicator cautions that the file path will be created. A yellow *File exists* indicator cautions that the file will be overwritten.
- **Red** – the adjacent label is “true” and this state is undesirable or is accompanied by an error (in which case a message on the prompt line or a dialog box will describe the nature of the error).
- **Gray** – the adjacent label is not “true”. For example, the handset is not connected.
- **Blinking** – file status indicators blink yellow when the file status is being queried but is not yet known (for example: when attempting to access slow drives or unresponsive network devices). File status indicators blink red when the path is invalid (mistyped). The *Handset* indicator blinks when the handset's password needs to be entered.

A prompt line at the bottom of the window provides information about what action should be taken or the status of the utility.

2.1 **Connecting the Handset**

The first window prompts you to insert a handset into the Dual Charger. The tab labels describe each of the available functions.

Insert the handset into the Dual Charger and enter the password.
When the handset is inserted for the first time, the password must be entered. If you check the **Remember password** box, the password is retained as the default password for all handsets. Unique passwords for each handset are not remembered. Enter the password and click **Submit**. The default password is **123456**.

When connection is established between the program and the handset the **Handset connected** indicator turns green and **Connected** displays on the prompt line. The handset is now ready for configuration.
2.2 Password Configuration

In order to change a password, the existing password must be entered. Then the new password may be entered and confirmed. If the Enable password checkbox is unchecked, no password will be required to access Admin Settings in the handset’s standby menu.

A password may be up to 18 characters.

The following table illustrates how numbers and letters are entered on the handset’s keypad. The CAPS/caps softkey toggles to allow both upper and lowercase letters.
2.3 **Error Information**

The **Error info** tab provides a utility to assist the Avaya customer service team to troubleshoot handset errors. When directed by customer service, this utility enables you to save any errors as a file which can then be sent to Avaya for handling.

Use the **Browse** button to establish the path and then enter the filename. Future saves will point to this same location as the default so that the same file may be overwritten if desired. A dropdown list box displays the most recently used filenames. The **File time** window displays the modification timestamp of the file in the **Save...as** window.

Save the file by clicking the **Get file** button. The file will be copied from the handset to the location. The **Read/Write** indicators will reflect the action as it occurs. File transfer progress is shown by a progress indicator above the prompt line.

This sample screen shows a new file being created in an existing folder.
2.4 **Software Updates**

The **Firmware** tab allows you to update the software in the handset by copying it from a location on your computer to the handset memory.

Download the software update following directions provided by your service representative.

Extract the pt28c.bin file from the zip to a folder set up for this purpose.

Use the **Browse** button to locate the software file. A dropdown list box displays the most recently used filenames. The **File time** window displays the modification timestamp of the file in the **Firmware file** window. The file version and handset version will also display for comparison. Verify that the information indicates that the correct file will be downloaded and then click the **Update** button. The file will be copied from the location to the handset. The **Read/Write** indicators will reflect the action as it occurs.

Should an **Error** indication occur, retry the update after ensuring that the handset is properly seated and that the USB cable is in good condition and connected securely. Contact Customer Service if an error persists.

Note that the firmware file path, file time, file version and handset version shown in the above example screen are for illustration only.

While a firmware update is in progress, you may open other tabs and the handset indicators shown on those tables will inform you of the status of the update.
2.5 Version

The **Version** tab displays the serial number of the handset and the software version being run.

![Handset Administration Tool](image)

HandsetAdmin Version 1.01.05
Built 27 SEP 2006 17:17
Copyright (C) 2006 SpectraLink Corp.

Handset status:
- Handset Serial Number: 4294967295
- Handset Firmware Version: 117.001

Ready.
3. **Configuring Admin Menu Settings**

The **Settings** tab allows you to configure required and optional settings in the Admin menu. End user Config menu options such as user name may also be assigned. Which options are available depends on the software used by the handsets. Specific configuration requirements are detailed in the *Configuration and Administration* document that pertains to the protocol used by your facility’s system.

The **Settings** tab displays the serial number of the handset and the software version being run. The **Tool Version** button will display the version of the config charger software you are running.

To enter and modify menu settings, click the **Show Settings Editor** button.

When you have opened the **Handset Settings Editor**, you may click **Close this window** to close the **Settings** tab window. Display it again from the **Handset Settings Editor** by clicking **View** and **Admin functions**.

**The Handset Settings Editor Toolbar**

The Handset Settings Editor toolbar allows you to name, open, and save configuration files and download and upload configuration settings to and from the handset in the charger.

The three filename windows allow you to open and save settings by **System**, **Group** or **User** type as separate files. Any filename can be assigned by entering it into the field and clicking the **Save** button. By default, the files will be saved in a new folder named **ConfigData** under the folder where the program is stored. The new folder will be created automatically the first time a file is saved. To open an existing file, click the **Open** button and browse to the file. Use the File menu to customize the file structure, if desired.
The file indicators beside the **Save** buttons have four colors to indicate the status of the file displayed in the window:

- **Red** – file does not exist. The filename in the window has not been created.
- **Yellow** – file not loaded. The filename in the window exists in the **ConfigData** folder but has not been loaded into the **Editable settings**.
- **Green** – unsaved edits. When changes are made in the **Editable settings** field(s) the green indicator indicates these have not been saved.
- **Gray** – file up-to-date. The settings have been saved.

There are two columns of configuration options. The **Editable settings** column shows settings that may be saved as files. The **Handset settings** column shows settings that have been copied from or may be copied to the handset in the cradle. The **Copy settings** arrows and boxes allow you to copy settings to the handset column where they may then be written to the handset in the charger. Or the configuration in a handset may be copied to the **Editable settings** area and edited or saved. The **Sys Grp Usr** checkboxes allow you to copy just the settings you require.

When clicked, the **Read Handset** and **Write Handset** buttons initiate the transfer of configuration data from or to the handset in the charger.

The four labeled indicators on the right indicate the status of the configuration transfer.

**Creating Your Configuration Plan**

When first setting up a configuration plan you will enter information into the **Editable settings** fields, indicate which of the three categories each option belongs to, and save as **System**, **Group** or **User** files.

Do not create a plan that saves an option in two different categories. Option categories should be established and should not overlap. Example: Speakerphone and Push-to-talk settings are typically tagged as **Grp** options and saved in **Group** files.

Once you have established which options will be categorized as System, Group or User, enter the configuration information into the **Editable settings** fields. Start with the System options and enter all system-level field values. Click the **Sys** category button on the left side of the window for each option. Save these settings as a System file by entering the filename in the **System** filename field and clicking **Save**.

Note that when a setting is changed, it is highlighted in yellow until it is saved.

In the same way, create each Group plan by entering the values in the fields designated as Group types. Click the **Grp** category button on the left side of the window for each option. Save each plan under a different name in the **Group** filename field.

Create one basic **User** file for default (or desired) values for each **User** field. Click the **Usr** category button on the left side of the window for each option.

User settings don’t necessarily need to be saved for each handset, but they can be saved if desired. It may be useful, for example, to save a user’s ring preferences from a handset being replaced so that the new handset can be configured the same way. If you determine that each handset configuration should be saved, it is easiest to do this during the configuration process. See **Downloading a configuration plan to a handset**, below.

**Sample configuration window**

Shown below is an abbreviated example of some configuration options that have not yet been set. The list of options that appears in your editor will differ.
Part C: Handset Administration Tool
Configuration planning worksheet
Use this or a similar worksheet to design your configuration plan.

Plan category________________ Filename__________________________

<table>
<thead>
<tr>
<th>Sys</th>
<th>Grp</th>
<th>Usr</th>
<th>Label</th>
<th>Editable Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Downloading and Uploading Configuration Plans**
Once your configuration plans are-established, the settings are easily downloaded into the handsets.

**Downloading a configuration plan to a handset**
1. Use the toolbar to open the System, Group and User plans for this handset.
2. Enter information unique to the handset, e.g. Extension and User name. Note that the Extension field has a **Next** button that is useful when configuring a quantity of handsets.
3. Copy the settings to the Handset settings fields.
4. Click **Write Handset** to begin the download.
5. You may save the settings unique to this handset by ensuring the correct extension number or other filename is entered in the User filename field and then clicking **Save**. You may also load files or edit settings for the next handset (steps 1 and 2) during the download.
6. When the Handset indicator turns off, the download has finished and the handset may be removed from the charger.

**Uploading a configuration plan from a handset**
1. Click the **Read Handset** button to begin the upload.
2. When the Handset indicator turns off, the handset’s settings will appear in the Handset settings fields.
3. You may copy these settings over to the Editable settings fields to use them to create configuration plans as described above or to save them by user or extension.
Notes:
D. Appendix

On occasion, you may run into transmission problems due to any number of factors originating from the wireless LAN. Wireless IP Telephones can exhibit transmission problems in several ways. They can cease functioning properly, display error messages or display incorrect data. When using and troubleshooting Wireless IP Telephones, consider the following problem sources to determine the best method of approaching any specific situation.

Troubleshooting Wireless IP Telephone Problems

Wireless IP Telephones can exhibit transmission problems in several ways. They can cease functioning properly, display error messages, or display incorrect data. When using and troubleshooting Wireless IP Telephones, consider the following problem sources to determine the best method of approaching any specific situation:

Access Point Problems

Most, but not all, Wireless IP Telephone audio problems have to do with access point range, positioning and capacity. Performing a Site Survey as described in the Diagnostics section can isolate the AP causing these types of problems. If the Wireless IP Telephone itself is suspected, conduct a parallel Site Survey with a Wireless IP Telephone that is known to be properly functioning.

- In-range/Out-of-range – service will be disrupted if a user moves outside the area covered by the wireless LAN access points. Service is restored if the user moves back within range. If a call drops because a user moves out of range, the Wireless IP Telephone will recover the call if the user moves back into range within a few seconds.

- Capacity – in areas of heavy use, the call capacity of a particular AP may be filled. If this happens, the user will hear three chirps from the Wireless IP Telephone. The user can wait until another user terminates a call, or move within range of another AP and try the call again. If a user is on a call and moves into an area where capacity is full, the system attempts to find another AP. Due to range limitations, this may be the same as moving out of range.

- Transmission Obstructions – prior to system installation, the best location for APs for optimum transmission coverage was determined. However, small pockets of obstruction may still be present, or obstructions may be introduced into the facility after system installation. This loss of service can be restored by moving out of the obstructed area, or by adding APs.

Configuration Problems

Certain problems are associated with improper configuration of the Avaya Communication Manager or the Wireless IP Telephone. Configuration problems are generally corrected by changing the configuration at the Avaya Communication Manager or on the Wireless IP Telephone. See the sections “Avaya Call Server Configuration” and “Avaya 3641/3645 Wireless IP Telephone Configuration” for specific configuration steps. There may also be incorrect programming of the AP. See the Configuration Note for the AP in use at the site.

If the Avaya Communication Manager registration fails, note any error messages on the display including which line icons are active. This information will help with problem resolution.
### Wireless IP Telephone Status Messages

Wireless IP Telephone status messages provide information about the Avaya 3641/3645 Wireless IP Telephone's communication with the AP and host telephone system. The following table summarizes the status messages, in alphabetical order.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 chirps</td>
<td>Wireless IP Telephone is not able to communicate with the best AP, probably because that AP has no bandwidth available.</td>
<td>None. This is only a warning, the call will hand-off to the best AP once it becomes available.</td>
</tr>
<tr>
<td>Address Mismatch</td>
<td>Wireless IP Telephone software download files are incorrect or corrupted.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Assoc Failed xxxxxxxxxx</td>
<td>Wireless IP Telephone association was refused by AP; displays MAC of failing AP.</td>
<td>Check Wireless IP Telephone and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.</td>
</tr>
<tr>
<td>Assoc Timeout xxxxxxxxxx</td>
<td>Wireless IP Telephone did not receive association response from AP; displays MAC of failing AP.</td>
<td>Check Wireless IP Telephone and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.</td>
</tr>
<tr>
<td>Auth Failed xxxxxxxxxx</td>
<td>Wireless IP Telephone authentication was refused by AP; displays MAC of failing AP.</td>
<td>Check Wireless IP Telephone and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.</td>
</tr>
<tr>
<td>Auth Timeout xxxxxxxxxx</td>
<td>Wireless IP Telephone did not receive authentication response from AP; displays MAC of failing AP.</td>
<td>Check Wireless IP Telephone and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.</td>
</tr>
<tr>
<td>Bad Code Type xx</td>
<td>xx, yy – software license types Wireless IP Telephone software does not match current handset license selection.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Bad Config</td>
<td>Some needed configuration parameter has not been set.</td>
<td>Check all required Wireless IP Telephone configuration parameters for valid settings.</td>
</tr>
<tr>
<td>Bad SSID</td>
<td>The Wireless IP Telephone is configured for “static SSID” (as opposed to “Learn once” or “Learn always” and no ESS ID has been entered.</td>
<td>Enter an SSID in the configuration settings or change to one of the “Learn” modes.</td>
</tr>
<tr>
<td>Bad Phintl File</td>
<td>Wireless IP Telephone software download files are incorrect or corrupted.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Bad Program File</td>
<td>Wireless IP Telephone software download files are incorrect or corrupted.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Bad Term, Type</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Verify the gatekeeper or PBX’s configuration</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| (battery icon), Battery Low, beep (audio) | Low battery.                                                               | In call: the battery icon displays and a soft beep will be heard when the user is on the Wireless IP Telephone and the battery charge is low. User has 15–30 minutes of battery life left.  
The Battery Pack can be changed while the call is still in progress. Do not press END.  
Place call on Hold or Park. Quickly remove the discharged battery and replace with a charged battery, START the Wireless IP Telephone, and press START to resume the call in progress.  
Not in call: The battery icon displays whenever the battery charge is low. The message Battery Low and a beep indicate a critically low battery charge when user is not on the Wireless IP Telephone. The Wireless IP Telephone will not work until the Battery Pack is charged. |
| Battery Failure             | The Battery Pack is not functioning.                                        | Replace the Battery Pack with a new or confirmed Avaya Battery Pack. Any non-Spectra-Link Battery Packs will not work.                                                                                   |
| Battery Failed              | Battery Pack is damaged or incompatible with Wireless IP Telephone.         | Replace the Battery Pack with a new or confirmed Avaya Battery pack. Any non-Avaya Battery Packs will not work.                                                                                           |
| CalSig Addr Bad             | Gatekeeper rejected registration request from the Wireless IP Telephone.    | Check the H.323 gatekeeper configuration in the Wireless IP Telephone.  
Verify the gatekeeper or PBX’s configuration.  
Verify the handset has been assigned the correct extension and that no other H.323 devices share that extension.                                 |
<p>| Can’t Renew DHCP yyy.yyy.yyy.yyy | DHCP server IP address DHCP server is not responding to initial renewal attempt. | Configuration problem. Check the IP address configuration in the DHCP server.                                                                                                                               |
| Charging ...                | The Wireless IP Telephone is charging in the Desktop Charger.              | No action needed.                                                                                                                                          |
| Charge Complete             | The Wireless IP Telephone is now fully charged.                             | No action needed.                                                                                                                                                                                             |
| Checking Code               | Wireless IP Telephone is contacting the TFTP Server to determine if it has a newer version of software that should be downloaded. | None, this message should only last for approximately one second. If message remains displayed, END and contact customer support for a replacement handset.                                                   |
| Checking DHCP IP            | The Wireless IP Telephone is retrieving DHCP information from the DHCP server. | None. This is informational only.                                                                                                                                                                           |
| CRC Code Error              | The software which has been TFTP downloaded has a bad redundancy code check. | Try the download again; it is possible the software was corrupted during download. If the error repeats, check that the download image on the TFTP server is not corrupted. |</p>
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Mismatch!</td>
<td>The software loaded into the Wireless IP Telephone is incorrect for this model handset.</td>
<td>Verify that the License Management value is correct. Replace the software image on the TFTP server with software that is correct for the handset model.</td>
</tr>
<tr>
<td>DCA Timeout</td>
<td>The Wireless IP Telephone has detected a fault for which it cannot recover, possibly due to a failure to acquire any network.</td>
<td>Turn the Wireless IP Telephone off then on again. If error persists, contact Avaya Technical Support and report the error.</td>
</tr>
<tr>
<td>Dest Unreachable</td>
<td>Unable to establish network connectivity with the gatekeeper</td>
<td>Verify gatekeeper is running and has network connectivity to WLAN infrastructure.</td>
</tr>
<tr>
<td>DHCP Error (1-5)</td>
<td>DHCP Error 1.</td>
<td>The Wireless IP Telephone cannot locate a DHCP server. It will try every 4 seconds until a server is located.</td>
</tr>
<tr>
<td></td>
<td>DHCP Error 2.</td>
<td>The Wireless IP Telephone has not received a response from the server for a request to an IP address. It will retry until a server is found.</td>
</tr>
<tr>
<td></td>
<td>DHCP Error 3.</td>
<td>The server refuses to lease the Wireless IP Telephone an IP address. It will keep trying.</td>
</tr>
<tr>
<td></td>
<td>DHCP Error 4.</td>
<td>The server offered the Wireless IP Telephone a lease that is too short. The minimum lease time is 10 minutes but Avaya engineers recommend at least one hour minimum lease time. The Wireless IP Telephone will stop trying. Reconfigure the server and power-cycle the Wireless IP Telephone.</td>
</tr>
<tr>
<td></td>
<td>DHCP Error 5.</td>
<td>Failure during WEP Key rotation process (proprietary feature).</td>
</tr>
<tr>
<td>DHCP Lease Exp</td>
<td>y...y – DHCP Server IP address. DHCP is not responding to renewal attempts (at least one renewal succeeded).</td>
<td>The Wireless IP Telephone failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator. The Wireless IP Telephone will attempt to negotiate a new lease, which will either work or change to one of the above DHCP errors (1-4).</td>
</tr>
<tr>
<td>DHCP NACK error</td>
<td>y...y – DHCP server IP address. DHCP server explicitly refused renewal.</td>
<td>The DHCP lease currently in use by the Wireless IP Telephone is no longer valid, which forces the Wireless IP Telephone to restart. This problem should resolve itself on the restart. If it does not, the problem is in the DHCP server.</td>
</tr>
<tr>
<td>Discov. Required</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Check the H.323 gatekeeper configuration in the Wireless IP Telephone.</td>
</tr>
<tr>
<td>DL Not On Sector</td>
<td>Wireless IP Telephone software download files are incorrect or corrupted.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DO NOT END</td>
<td>The Wireless IP Telephone is in a critical section of the software update.</td>
<td>None. Do not remove the Battery Pack or attempt to END the handset while this is displayed. Doing so may require the handset to be returned to Avaya to be recovered.</td>
</tr>
<tr>
<td>Duplicate Addr/#</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Check the H.323 gatekeeper configuration in the Wireless IP Telephone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the gatekeeper or PBX's configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the handset has been assigned the correct extension and that no other H.323 devices share that extension.</td>
</tr>
<tr>
<td>Duplicate IP</td>
<td>The Wireless IP Telephone has detected another device with its same IP address.</td>
<td>If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If using Static IP, check that the Wireless IP Telephone was assigned a unique address.</td>
</tr>
<tr>
<td>Erase Failed</td>
<td>Download process failed to erase the memory in the Wireless IP Telephone.</td>
<td>Operation will retry but may eventually report the error &quot;int. error: 0F&quot; Power cycle the handset.</td>
</tr>
<tr>
<td>Erasing Memory</td>
<td>Wireless IP Telephone has determined that a download should occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line the erase operation is complete.</td>
<td>None. When the progress bar fills the display line the erase operation is complete. Do not turn the Wireless IP Telephone off during this operation.</td>
</tr>
<tr>
<td>Error!...</td>
<td>A fatal software error is detected. All handset operation is halted and any call is lost.</td>
<td>This message appears during Halt on Error mode. An error message displays. Note the message details and power cycle the handset.</td>
</tr>
<tr>
<td>Extension Error</td>
<td>Displayed for 5 seconds when all of the Communication Managers contacted indicate that they do not recognize the current extension as valid.</td>
<td>The user will be asked to enter a valid extension and password.</td>
</tr>
<tr>
<td>Extension in Use</td>
<td>The phone is trying to register with an extension that is already registered on the Communication Manager.</td>
<td>See Avaya Communication Manager Integration Factors section.</td>
</tr>
<tr>
<td>Files Too Big</td>
<td>Wireless IP Telephone software download files are incorrect or corrupted.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Flash Config Error</td>
<td>Wireless IP Telephone internal configuration is corrupt.</td>
<td>Perform &quot;Restore Defaults&quot; operation via administrator menus (or reprogram with Configuration Cradle).</td>
</tr>
<tr>
<td>Gatekeeper REJ</td>
<td>Gatekeeper rejected Discovery Request from the Wireless IP Telephone.</td>
<td>Check the H.323 gatekeeper configuration in the Wireless IP Telephone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the gatekeeper or PBX’s configuration.</td>
</tr>
<tr>
<td>H225 Listen Fail</td>
<td>Wireless IP Telephone cannot communicate with the AP or the AVPP.</td>
<td>This message may display with another diagnostic message. Follow diagnostic actions for the second message (such as No Net Found).</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>H245 Listen fail</td>
<td>Wireless IP Telephone cannot communicate with the AP or the AVPP.</td>
<td>This message may display with another diagnostic message. Follow diagnostic actions for the second message (such as No Net Found).</td>
</tr>
<tr>
<td>Incompatible</td>
<td>The switch is rejecting the software version presented by the phone.</td>
<td>If this condition persists, contact the Avaya system administrator.</td>
</tr>
<tr>
<td>Initializing ...</td>
<td>The Wireless IP Telephone is performing START initialization.</td>
<td>None. This is informational only.</td>
</tr>
<tr>
<td>Internal Err. # #</td>
<td>The Wireless IP Telephone has detected a fault from which it cannot recover. OE – Error while writing the Flash (return Wireless IP Telephone to factory). OF – No functional code (contact Avaya Technical Support).</td>
<td>Record the error code so it can be reported. Turn the Wireless IP Telephone off then on again. If error persists, try registering a different Wireless IP Telephone to this telephone port. If error still persists, contact Avaya Technical Support and report the error.</td>
</tr>
<tr>
<td>Invalid Revision</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Verify the gatekeeper or PBX’s configuration. Ensure the gatekeeper and PBX will support version 2 of the H.323 protocol.</td>
</tr>
<tr>
<td>Multiple GW Reg yyy.yyy.yyy.yyy</td>
<td>y...y – Gateway IP address. Wireless IP Telephone received responses from multiple gateways; displays IP address of one responding gateway.</td>
<td>Check each NetLink Telephony Gateway for the Wireless IP Telephone’s MAC address on the Telephone Line Configuration screen. Delete any duplicate entries, leaving only one entry on the correct Telephone Gateway and port for this Wireless IP Telephone.</td>
</tr>
<tr>
<td>Multiple SVP Reg yyy.yyy.yyy.yyy</td>
<td>y...y – AVPP IP address. Wireless IP Telephone received responses from multiple AVPPs; displays IP address of one responding AVPP.</td>
<td>This can happen if the Wireless IP Telephone has been re-configured to use a different AVPP and then powered-up before the previous server has had time to determine that the Wireless IP Telephone is no longer connected to it. The problem should go away after about 30 seconds.</td>
</tr>
<tr>
<td>Must Upgrade SW!</td>
<td>Wireless IP Telephone software is incompatible with hardware.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Net Busy xxxxxxxxxxxxxx</td>
<td>x...x – AP MAC address. Wireless IP Telephone cannot obtain sufficient bandwidth to support a call; displays MAC of failing AP.</td>
<td>Try the call again later.</td>
</tr>
<tr>
<td>No Answer</td>
<td>Called party did not answer the Wireless IP Telephone.</td>
<td>No action. Not an error.</td>
</tr>
<tr>
<td>No Call Server (The No Call Server message may include an error indication)</td>
<td>This indicates that while a Communication Manager has responded to the Gatekeeper Request message, it is not responding to the Registration Request message.</td>
<td>Check that the Wireless IP Telephone is contacting the correct Communication Manager, and that the Communication Manager is correctly configured for the extension in question.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>No Call Server IP</td>
<td>The Wireless IP Telephone cannot obtain an IP address for an Avaya Communication Manager.</td>
<td>Assure that the Wireless IP Telephone is administered properly for its environment. Refer to the section on Wireless IP Telephone Configuration and Communication Manager Integration Factors for details on configuring the Wireless IP Telephone.</td>
</tr>
<tr>
<td>No DHCP Server</td>
<td>Wireless IP Telephone is unable to contact the DHCP server.</td>
<td>Check that DNS is operational and connected to WLAN or use Static IP configuration in the Wireless IP Telephone.</td>
</tr>
<tr>
<td>No SSID</td>
<td>Attempted to run site survey application without an SSID set.</td>
<td>Let Wireless IP Telephone come completely up. Statically configure an SSID in the Admin menu.</td>
</tr>
<tr>
<td>No Extension</td>
<td>All Wireless IP Telephones require an Extension for H.323.</td>
<td>Enter a valid Extension in the configuration settings.</td>
</tr>
<tr>
<td>No Func Code</td>
<td>Wireless IP Telephone software download files are incorrect or corrupted.</td>
<td>Reconfigure the handset to gain access to the WLAN and download new code.</td>
</tr>
<tr>
<td>No Gatekeeper</td>
<td>The Wireless IP Telephone has not received a response from the gatekeeper.</td>
<td>Verify that the gatekeeper is running and has network connectivity to WLAN infrastructure.</td>
</tr>
<tr>
<td>No Gatekeeper IP</td>
<td>The Wireless IP Telephone is configured for static IP addresses and no valid unicast IP address is assigned for gatekeeper configuration.</td>
<td>Configure a valid IP address in Admin menus.</td>
</tr>
<tr>
<td>No Gateway IP</td>
<td>The Wireless IP Telephone is configured for static IP addresses and no valid unicast IP address is assigned for gateway configuration.</td>
<td>Configure a valid IP address in Admin menus.</td>
</tr>
<tr>
<td>No Host IP (Addr)</td>
<td>The Wireless IP Telephone is configured for “static IP” (as opposed to “use DHCP”) and no valid host IP address (the Wireless IP Telephone’s IP address) has been entered.</td>
<td>Enter a valid IP address in the configuration settings or change to “use DHCP”.</td>
</tr>
<tr>
<td>No IP Address</td>
<td>Invalid IP.</td>
<td>Check the IP address of the Wireless IP Telephone and re-configure if required.</td>
</tr>
<tr>
<td>No Net Access</td>
<td>Cannot authenticate / associate with AP.</td>
<td>Verify the AP configuration. Verify that all the WEP settings in the Wireless IP Telephone match those in the APs.</td>
</tr>
<tr>
<td>No Net Found No APs</td>
<td>Wireless IP Telephone cannot find any APs. This indicates any of the following: No radio link. No SSID — Incorrect SSID. AP does not support appropriate data rates.</td>
<td>Verify that the AP is turned on. Verify the SSID of the wireless LAN and enter. Check the AP configuration against configuration document for AP.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>Out of range.</td>
<td></td>
<td>Try getting closer to an AP. Check to see if other Wireless IP Telephones are working within the same range of an AP. If so, check the SSID of this Wireless IP Telephone. Verify that all the Security settings in the Wireless IP Telephone match those in the APs.</td>
</tr>
<tr>
<td>Incorrect security settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Net Found</td>
<td>x…x – AP MAC address. yy – AP signal strength. Wireless IP Telephone cannot find a suitable access point; displays MAC and signal strength of “best” non-suitable AP found.</td>
<td>Check AP and handset network settings such as SSID, Security, Reg domain and Tx power. Ensure APs are configured per Configuration Note. Try Site Survey mode to determine more specific cause.</td>
</tr>
<tr>
<td>No Reg Domain</td>
<td>Regulatory Domain not set.</td>
<td>Configure the Regulatory Domain of the Wireless IP Telephone.</td>
</tr>
<tr>
<td>No SVP IP</td>
<td>The Wireless IP Telephone is configured for “static IP” (as opposed to “use DHCP”) and no valid AVPP address has been entered.</td>
<td>Enter a valid AVPP IP address in the configuration setting or change to “use DHCP.”</td>
</tr>
<tr>
<td>No SVP Response</td>
<td>y…y – AVPP IP address. Wireless IP Telephone has lost contact with the AVPP.</td>
<td>This may be caused by bad radio reception or a problem with the AVPP. The Wireless IP Telephone will keep trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the Wireless IP Telephone will restart. Report this problem to the system administrator if it keeps happening.</td>
</tr>
<tr>
<td>No SVP Server</td>
<td>Wireless IP Telephone can’t locate AVPP. AVPP is not working. No LAN connection at the AVPP.</td>
<td>IP address configuration of AVPP is wrong or missing. Check error status screen on AVPP. Verify AVPP connection to LAN.</td>
</tr>
<tr>
<td>No SVP Server No DNS Entry</td>
<td>Wireless IP Telephone unable to perform DNS lookup for AVPP, server had no entry for AVPP.</td>
<td>The network administrator must verify that a proper IP address has been entered for the AVPP DHCP option.</td>
</tr>
<tr>
<td>No SVP Server No DNS IP</td>
<td>Wireless IP Telephone is unable to perform DNS lookup for AVPP, no IP address for DNS server.</td>
<td>The network administrator must verify proper DHCP server operation.</td>
</tr>
<tr>
<td>No SW Found</td>
<td>A required software component has not been identified.</td>
<td>Check that the Wireless IP Telephone license type has a corresponding entry in the slnk_cfg.cfg file. Check that the pd14ccc.bin and pi1400.bin entries exist in under this license type in the slnk.cfg.cfg file.</td>
</tr>
<tr>
<td>Not Installed!</td>
<td>A required software component is missing.</td>
<td>Check that all required software files are on the TFTP server, if over-the-air downloading is being used. If the error repeats, contact Avaya Technical Support.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Error</td>
<td>The phone is not encrypting the challenge string correctly. This indicates</td>
<td>Enter the correct password in the phone. See Avaya Communication Manager Configuration section.</td>
</tr>
<tr>
<td></td>
<td>that the password set in the phone disagrees with the password administered</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in the Communication Manager.</td>
<td></td>
</tr>
<tr>
<td>Press END</td>
<td>The far end of a call has hung up.</td>
<td>Hang up the near end.</td>
</tr>
<tr>
<td>RAS Addr Bad</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Check the H.323 gatekeeper configuration in the Wireless IP Telephone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the gatekeeper or PBX’s configuration.</td>
</tr>
<tr>
<td>Registration REJ</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Check the H.323 gatekeeper configuration in the Wireless IP Telephone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the gatekeeper or PBX’s configuration.</td>
</tr>
<tr>
<td>Resource Unavailable</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Check the H.323 gatekeeper configuration in the Wireless IP Telephone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the gatekeeper or PBX’s configuration.</td>
</tr>
<tr>
<td>Retarting…</td>
<td>The Wireless IP Telephone is in the process of rebooting. There will be a</td>
<td>None.</td>
</tr>
<tr>
<td></td>
<td>20-second delay in an attempt to let potential network/system errors clear.</td>
<td></td>
</tr>
<tr>
<td>Retry / Restart</td>
<td>The Wireless IP Telephone is waiting for user input prior to retrying the</td>
<td>See Avaya Communication Manager Integration Factors section.</td>
</tr>
<tr>
<td></td>
<td>registration process, or restarting after a delay.</td>
<td></td>
</tr>
<tr>
<td>Select License</td>
<td>The correct protocol has not been selected from the license set.</td>
<td>Using the administrative menus, select one license from the set to allow the Wireless IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Telephone to download the appropriate software.</td>
</tr>
<tr>
<td>Server Busy</td>
<td>Wireless IP Telephone is attempting to download from a TFTP Server that is</td>
<td>None, the Wireless IP Telephone will automatically retry the download every few seconds.</td>
</tr>
<tr>
<td></td>
<td>busy downloading other devices and refusing additional downloads.</td>
<td></td>
</tr>
<tr>
<td>Service Unavailable. Restarting …</td>
<td>An error has caused the handset to lose the call. It is now making its</td>
<td>Occurs during Restart on Error mode. The handset is attempting to register with the PBX</td>
</tr>
<tr>
<td></td>
<td>best effort to restart and return to standby mode.</td>
<td>and resume normal operation. Error details may be available through the syslog server and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>by download with the Handset Administration Tool.</td>
</tr>
<tr>
<td>SKT Open Failed</td>
<td>Socket open fail. Occurs when the Wireless IP Telephone tries to connect to</td>
<td>If the PBX is inoperative and resiliency is not active or the Wireless IP Telephone cannot</td>
</tr>
<tr>
<td></td>
<td>the PBX but there is no response. If resiliency is active, the Wireless IP</td>
<td>locate a backup PBX, turn off the Wireless IP Telephone and repair the primary PBX. Note</td>
</tr>
<tr>
<td></td>
<td>Telephone will keep trying.</td>
<td>that it may be advisable to reconfigure the backup PBX to be the primary PBX if the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>repair is more time-consuming than the reconfiguration.</td>
</tr>
<tr>
<td>Socket Failure</td>
<td>Wireless IP Telephone cannot communicate with the AP or the AVPP.</td>
<td>This message may display with another diagnostic message. Follow diagnostic actions for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the second message (such as No Net Found).</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Storing Config</td>
<td>Wireless IP Telephone is storing changes to handset configuration.</td>
<td>None. Informational only. The handset may display this briefly following a configuration change or software download.</td>
</tr>
<tr>
<td>SVP Service Rej.</td>
<td>The AVPP has rejected a request from the Wireless IP Telephone.</td>
<td>The Wireless IP Telephone will restart and attempt to re-register with the AVPP, which should fix the problem. Report to your administrator if it keeps happening.</td>
</tr>
<tr>
<td>System Busy yw.yw.yw.yw</td>
<td>y…y – AVPP IP Address. AVPP has reached call capacity.</td>
<td>All call paths are in use, try the call again in a few minutes.</td>
</tr>
<tr>
<td>System Busy</td>
<td>Avaya Voice Priority Processor is busy or out of resources.</td>
<td>All call paths are in use, try call again in a few minutes.</td>
</tr>
<tr>
<td>System Error</td>
<td>An internal failure has occurred in the Avaya Communication Manager.</td>
<td>If this condition persists, contact the Avaya system administrator.</td>
</tr>
<tr>
<td>System Locked (with Busy Tone)</td>
<td>Avaya Voice Priority Processor is locked.</td>
<td>Try call again later, system has been locked for maintenance</td>
</tr>
<tr>
<td>Terminal Exclude</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Verify the handset has been assigned the correct extension and that no other H.323 devices share that extension.</td>
</tr>
<tr>
<td>TFTP ERROR(x):yy</td>
<td>A failure has occurred during a TFTP software download. (x) = The file number which was being downloaded, yy = an error code describing the particular failure. Possible error codes are: 01 – TFTP server did not find the requested file. 02 – Access violation (reported from TFTP server). 07 – TFTP server reported &quot;No such user&quot; error. 81 – File put into memory did not CRC. FF – Timeout error. TFTP server did not respond within a specified period of time.</td>
<td>Error code 01, 02 or 07 – check the TFTP server configuration. Error code 81 – the Wireless IP Telephone will attempt to download the file again. For other messages, END the Wireless IP Telephone, then turn it on again to retry the download. If the error repeats, note it and contact Avaya Technical Support.</td>
</tr>
<tr>
<td>Too Many Errors</td>
<td>The Wireless IP Telephone continues to reset and cannot be recovered.</td>
<td>Fatal error. Return handset to Avaya.</td>
</tr>
<tr>
<td>Trying xxx.xxx.xxx.xxx</td>
<td>The phone is attempting to register with the Avaya Communication Manager at IP xxx.xxx.xxx.xxx.</td>
<td>This display is a progress indicator, and may not appear long enough to recognize during a normal check-in. If the Wireless IP Telephone appears to hang at this message, showing one or more IP addresses, it indicates that the Communication Manager(s) being contacted is not responding. Check that the Communication Manager is active, that the Wireless IP Telephone is getting the correct IP address for the Communication Manager(s), that the Wireless IP Telephone is correctly configured on the Communication Manager, and that there is a LAN connection between the AVPP and the Communication Manager.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Undefined Error</td>
<td>The system is rejecting the registration of the Wireless IP Telephone with an unrecognized error code.</td>
<td>If this condition persists, contact the Avaya system administrator.</td>
</tr>
<tr>
<td>Unknown xx:yy:zz</td>
<td>A phrase is missing from your pintl file.</td>
<td>Download new software from the Avaya site per Software Maintenance.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Dialed number does not exist.</td>
<td>Check number and try again.</td>
</tr>
<tr>
<td>Unsupp Transport</td>
<td>Gatekeeper rejected registration request from the Wireless IP Telephone.</td>
<td>Verify the gatekeeper or PBX’s configuration. Ensure the gatekeeper and PBX will support version 2 of the H.323 protocol.</td>
</tr>
<tr>
<td>Updating ...</td>
<td>The Wireless IP Telephone is internally updating its software images.</td>
<td>None. The Wireless IP Telephone may do this briefly after a download. This is informational only.</td>
</tr>
<tr>
<td>Updating Code...</td>
<td>Wireless IP Telephone is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.</td>
<td>None. When the progress bar fills the display line the update operation is complete on that file. Do not turn the Wireless IP Telephone off during this operation.</td>
</tr>
<tr>
<td>Updating Options</td>
<td>Appears the first time the handset is powered on and upon restoring default settings.</td>
<td>No action needed. Allow handset to restart automatically.</td>
</tr>
<tr>
<td>Waiting...</td>
<td>Wireless IP Telephone has attempted some operation several times and failed, and is now waiting for a period of time before attempting that operation again.</td>
<td>None. The Wireless IP Telephone is waiting for a specified period of time before attempting that operation again.</td>
</tr>
<tr>
<td>Wrong Code Type</td>
<td>The software loaded into the Wireless IP Telephone is incorrect for this model Wireless IP Telephone.</td>
<td>Verify the license type is set correctly. If the license type is correct, replace the software image on the TFTP server with the software that is correct for the Wireless IP Telephone model.</td>
</tr>
<tr>
<td>Wrong Set Type</td>
<td>The set type administered on the Communication Manager disagrees with the set type for the Wireless IP Telephone.</td>
<td>Make sure that set type 4612 is used for the Wireless IP Telephone.</td>
</tr>
<tr>
<td>(No message shown)</td>
<td>There is no voice path.</td>
<td>Verify that the CODEC is G.711 or G.729a/ab.</td>
</tr>
<tr>
<td>(No message shown)</td>
<td>Messages are left at the principal station, but the MSG icon is not lit on the Wireless IP Telephone.</td>
<td>Verify that “Message Lamp Ext” on the station form for the Wireless IP Telephone is set to the extension of the principal station.</td>
</tr>
</tbody>
</table>
# E. Index

## A
- Access point
  - 802.11 rate, 24
- Cisco Aironet, 51
- Coverage, 67
- Coverage test, 72
- Defined, 13
- Diagram, 12
- Each subnet has own, 11
- Overlap issues, 67
- Phones per, 24
- Problems, 97
- Active, 41
- Admin menu
  - Defined, 44
- Administrative computer
  - Defined, 14
- Avaya 3641 Wireless IP Telephone
  - Defined, 13
- Avaya 3641/3645 Wireless IP Telephone
  - Feature programming, 61
- Avaya 3641/3645 Wireless IP Telephones
  - Diagram, 38
  - Feature list, 62
  - Firmware Version option, 73
  - Line appearances, 62
  - Security, 50
  - Software updates, 73
- Avaya 4612 IP Telephone, 37
- Avaya Communication Manager
  - Configuration, 42
  - Defined, 13
  - Routing to and from, 13
- Avaya IP Phone
  - Defined, 14
- Avaya MultiVantage™, 36
- Avaya Voice Priority Processor
  - Administration, 18
  - Alarms, 31
  - Configuration of, 23
  - Connection to, 18
  - Defined, 8
  - Front panel, 15
  - Installing, 16
  - Location, 16
  - Mounting, 16, 17
  - Network configuration, 20
  - Software maintenance, 29
  - Swapping/Add/Deleting, 28
  - System diagram, 12
  - Troubleshooting, 30
- Avaya™ S8100 Media Server, 36

## B
- Beacon Interval, 65

## C
- Capacity, 97
- Cisco Fast Secure Roaming, 51
- CMC1 Media Gateway, 36
- Codecs, 58
- Configuration
  - Avaya Communication Manager, 42
  - AVPP, 11
  - AVPP network, 20
  - Handset Administration Tool, 79, 86, 91
  - Problems, 97
- Coverage issues, 67

## D
- Data packets, 8
- DEFINITY® Server SI, 36
- Desk station, 42
- DHCP, 44
- Direct sequence spread spectrum radio technology, 13
- Domain Name System (DNS)
  - Defined, 58
- Download messages
  - Failure or Recover, 74
  - Normal, 73
- Dynamic Host Configuration Protocol, 58

## E
- Enable H.323 Gatekeeper, 24
- Encryption protocol, 50
- Ethernet link, 24
- Ethernet switch
  - Defined, 13
  - Diagram, 12
- Extension, 59

## F
- Filters, 11, 37
- First Alias IP address/Last Alias IP Address, 24

## G
- Gateway function, 9
Part E: Index

H
Handset Administration Tool
  Configuration, 79
  Defined, 76
  Installation, 76
  Using, 84
  Version, 89

I
IEEE 802.11b standards, 8
IEEE 802.11b standards, 13
Inactivity Timeout, 25
IP addressing, 16
IP multicast, 11
IP multicast addresses, 37
IP telephony gateway, 12

L
Layer-2 tunnel, 11

M
Maintenance Lock, 25
Multicast traffic, 37

N
Navigation keys, 44, 45
Network Status, 32

O
Obstructions, 97
Open Application Interface (OAI)
  Defined, 63
  Out of range, 97

P
Password
  Avaya 3641/3645, 44, 52, 57
  AVPP, 19, 20, 26
  Communications Manager, 59
  Handset Administration Tool, 84, 86
  PBX, 39
  Power, 16
  Power cycle, 11
  Predial, 41
  Priority Channel, 48

Q
QoS Configuration, 25

R
Regulatory Domain, 52
Reset All SVP Servers, 25
Reset System, 25
Restore Defaults, 53
Router
  Configuration, 11, 37
  Defined, 14

S
Serial Connection, 18
Site Preparation, 16
Site survey, 52, 72
  802.11 support, 65
Softkeys, 39, 45, 61, 62
Software updates, 20, 21, 29, 57, 73, 88
SpectraLink Voice Priority (SVP), 8
SSID, 50, 56, 65, 66, 72
Stand-alone station, 42
Standby menu, 44
Standby mode, 41
Status messages, 99
Subnets, 11
SVP-II Master, 24
Switched Hub, description, 14
System Locked, 24

T
Telephony areas, 11
Telnet, 18
TFTP
  Download Master, 21
  Server, 37
  Server IP, 50
  Server, defined, 14
  Timing function, 9
Troubleshooting, 30, 34, 76, 97

V
Voice over IP (VoIP), 36
Voice packets, 8

W
Wi-Fi Multimedia, 8
Wired Equivalent Privacy, 50
Wireless IP Telephone
  Access point problems, 97
  Configuration problems, 97
  Problems with, 97
  Status messages, 99, 104
WPA2-PSK, 51
WPA-PSK, 51