SpectraLink 8020/8030 Wireless Telephone

Administration Guide

Session Initiation Protocol (SIP)

December 2011 Edition
1725-36038-001
Version N

POLYCOM®

Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

Copyright Notice

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY POLYCOM FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF POLYCOM WHATSOEVER.

Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.
4750 Willow Road,
Pleasanton, CA 94588
http://www.polycom.com

About this Guide

This document explains how to configure and maintain the SpectraLink 8020/8030 Wireless Telephones using Session Initiation Protocol (SIP).

> This document pertains to Polycom SIP software version 131.031 and above only.

Polycom Model Numbers

This document covers the following registered model numbers:

802X, 803X

Related Documents

SpectraLink 8020/8030 Wireless Telephone and Accessories User Guide for SIP (1725-36165-001)

SpectraLink 8000 SVP Server: Administration Guide for SIP (1725-36033-001)

SpectraLink 8020/8030 Wireless Telephone: SIP User Agent: Features and Standards (1725-36037-001)

SpectraLink 8020/8030 Wireless Telephones Handset Administration Tool (7125-36039-001)

The Handset Administration Tool software

Available at http://www.polycom.com/usa/en/support/voice/wi-fi/wi-fi.html

Polycom VIEW Certified Products Guide (1725-36040-001)

VIEW Configuration Guide 1725-36xxx-001 where xxx indicates a number corresponding to the type of access point)

Available at http://www.polycom.com/support/voice/wi-fi/view_certified.html

Deploying Enterprise-Grade Wi-Fi Telephony
Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones
Available at
http://www.polycom.com/products/resources/white_papers/index.html

Open Application Interface (OAI) Specification (1725-36196-001)
Available at
www.polycom.com/forms/spectralink_oai_sw_dl.html

Asterisk cmd VoiceMailMain (Shows how to enter the Asterisk voicemail system, its menu structure, and related information.)
Available at
http://www.voip-info.org/wiki/index.php?page=Asterisk+cmd+VoiceMailMain

Customer Support

Polycom wants you to have a successful installation. If you have questions, please contact our Customer Support Hotline at 1-888-POLYCOM (1-888-765-9266).

The hotline is open Monday through Friday, 6 a.m. to 6 p.m. Mountain time.

For Technical Support: technicalsupport@polycom.com

For Knowledge Base:
http://www.polycom.com/usa/en/support/voice/voice.html

For Return Material Authorization: rmacoordinator@polycom.com

Icons and Conventions

This manual uses the following icons and conventions.

⚠	Caution! Follow these instructions carefully to avoid danger.
📌	Note these instructions carefully.
Label	This typeface indicates a key, label, or button on SpectraLink hardware.

Contents

1

SpectraLink 8020/8030 Wireless Telephone Overview

The SpectraLink 8020/8030 Wireless Telephones is a Wi-Fi handset for workplace telephone systems. The handsets operate over a VIEW Certified 802.11a/b/g/n wireless LAN (WLAN) providing users a wireless extension of the SIP call server. By seamlessly integrating into a SIP environment, wireless telephone users are provided with high-quality mobile voice communications throughout the workplace, giving users the freedom to roam throughout the workplace while providing all the features and functionality of a wired SIP desk phone.

In a SIP environment, each handset may have up to six sets of credentials to identify itself as belonging to a particular user. In the SIP environment, the handsets support up to three SIP call servers. Each handset may have five line appearances and two calls per line. Each handset may have up to 10 sets of credentials to identify itself by current user.

> The latest wireless telephone and Handset Administration Tool software versions are required to support the features described in this document. See Chapter 4: Download and Install Handset Software.

WLAN Quality of Service

WLAN Quality of Service (QoS) is provided by using one of three available mechanisms: SpectraLink Voice Priority (SVP), Wi-Fi Standard QoS, or Cisco Compatible Extensions (CCX) version 4. These QoS modes can not be mixed within the same WLAN; therefore, all Wireless Telephones on the network must have the same QoS setting.

SVP

SpectraLink Voice Priority (SVP) is a proprietary method of WLAN QoS, developed by Polycom, to ensure enterprise-grade voice quality, battery life and call capacity for SpectraLink Wireless Telephones. SVP requires the use of the SVP Server, which is an Ethernet LAN device that works with in conjunction with Wi-Fi APs to ensure QoS over the WLAN. Voice packets to and from the Wireless Telephones are tunneled through the SVP Server to ensure voice prioritization as they are routed between the handset and SIP call server. See the *SpectraLink 8000 SVP Server: Administration Guide for SIP* document for detailed information about this device.

Wi-Fi Standard QoS

SpectraLink Wireless Telephones support WMM, WMM Power Save and WMM Admission Control - all QoS standards from the Wi-Fi Alliance based on IEEE 802.11e. The combination of these three standards provides enterprise-class QoS in terms of voice quality, battery life and call capacity. The WLAN must also support and enable each of these QoS mechanisms in order to ensure they are utilized. This option does not require the SVP Server.

CCXv4

The CCX program requires WLAN client devices operating on Cisco APs to use a defined set of industry standards and Cisco-specific features. The SpectraLink 8020/8030 Wireless Telephone has been certified by Cisco as CCXv4 compliant. When the CCXv4 operating mode is selected on the handset, it automatically initiates the required set of Cisco-specific and industry standard QoS mechanisms. This option does not require the SVP Server.

WLAN Security

The following security methods are supported by the handset.

WPA2 Enterprise

The handset supports WPA2 Enterprise, as defined by the Wi-Fi Alliance. WPA2, which is based on the 802.11i standard, provides government-grade security by implementing the Advanced Encryption Standard (AES) encryption algorithm. The Enterprise version of WPA2 uses 802.1X authentication, which is a port-based network access control mechanism using dynamic encryption keys to protect data privacy. Two 802.1X authentication methods are supported on the Wireless Telephone, EAP-FAST and

PEAPv0/MSCHAPv2. Both of these methods require a RADIUS authentication server to be available on the network and accessible to the phone. See the System Components section for tested models. Additional details are provided in Chapter 3

Normal 802.1X authentication requires the client to renegotiate its key with the authentication server on every AP handoff, which is a time-consuming process that negatively affects time-sensitive applications such as voice. Fast AP handoff methods allow for the part of the key derived from the server to be cached in the wireless network, thereby shortening the time to renegotiate a secure handoff. The Wireless Telephone supports two fast AP handoff techniques, Cisco Client Key Management (CCKM) (only available on Cisco APs) or Opportunistic Key Caching (OKC). One of these methods must be configured for support on the WLAN to ensure proper performance of the handset.

WPA and WPA2 Personal

The handset supports WPA and WPA2 Personal, as defined by the Wi-Fi Alliance. WPA2, which is based on the 802.11i standard, provides government-grade security by implementing the Advanced Encryption Standard (AES) encryption algorithm. WPA, which is based on a draft version of the 802.11i standard before it was ratified, uses Temporal Key Integrity Protocol (TKIP) encryption. The Personal version uses an authentication technique called WPA2 is based on the 802.11i standard. Pre-Shared Key (PSK) allows the use of manually entered keys or passwords to initiate WPA security.

Cisco Fast Secure Roaming

Cisco’s Fast Secure Roaming (FSR) mechanism uses a combination of standards-based and proprietary security components including Cisco Client Key Management (CCKM), LEAP authentication, Michael message integrity check (MIC) and Temporal Key Integrity Protocol (TKIP). FSR provides strong security measures for authentication, privacy and data integrity along with fast AP handoff on Cisco APs.

WEP

The handset supports Wired Equivalent Privacy (WEP) with both 40-bit and 128-bit encryption.

Minimum System Requirements

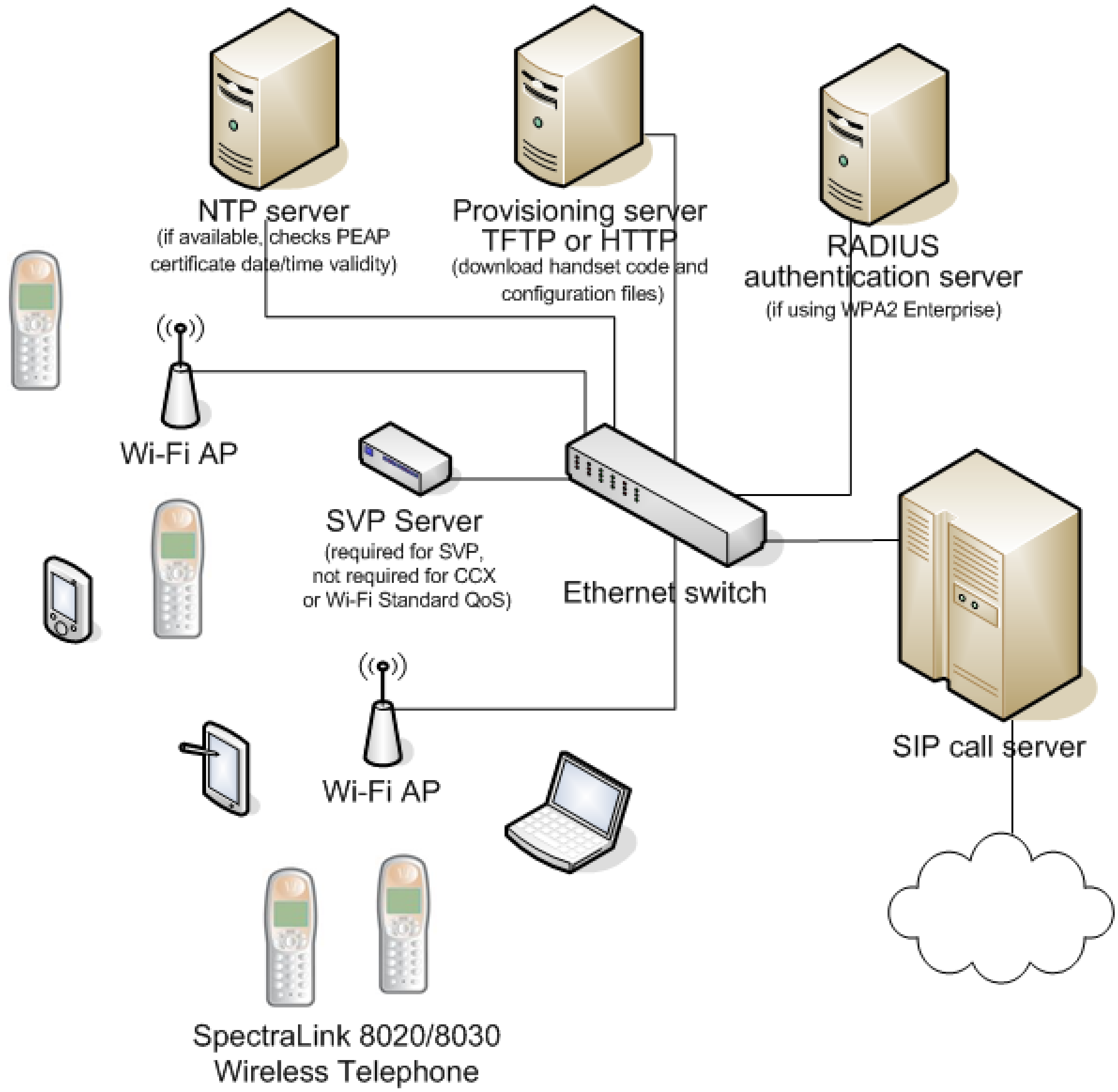
- A wireless LAN must be properly configured and operational through the use of 802.11a/b/g/n wireless APs. Consult the *VIEW Configuration Guide* for the appropriate make/model of WLAN.
- To load software and configuration files to the handset over the air, a provisioning Server (either HTTP or TFTP) must be available on the network. The current handset software must be installed in the proper download directory on the provisioning server. If this server is not found, the handset will boot with the last known configuration.
- If SVP is used for QoS, the SVP Server must be installed and properly configured.
- Software versions required, if SVP and/or OAI are used:

Component	Version
SpectraLink 8000 SVP Server	17x.034 or higher
OAI Server MOG 600	54.032 or higher
OAI Server MOG 700	82.019 or higher

- If Wi-Fi Standard QoS is used, then each AP must be configured for such features as WMM-Power Save; WMM-Admission Control; proper EDCA parameters; DSCP mapping for voice and control traffic; call admission control and Proxy ARP. Consult the appropriate *VIEW Configuration Guide* for these settings.
- If WPA2-Enterprise is used, then all portions of the Public Key Infrastructure (PKI) need to be installed and configured properly in order acquire the network.
- An approved SIP call server must be installed and operational on the LAN. A complete list of approved product can be found on the Polycom website at http://support.polycom.com/global/documents/support/user/products/voice/spectralink_8020_8030_sip_feature_matrix.pdf

System Diagram

The following diagram shows the Polycom components residing on a network with APs and wireless LAN Ethernet Switch.


NTP server
(if available, checks PEAP certificate date/time validity)
Provisioning server
TFTP or HTTP
(download handset code and configuration files)
RADIUS authentication server
(if using WPA2 Enterprise)
Wi-Fi AP
SVP Server
(required for SVP, not required for CCX or Wi-Fi Standard QoS)
Ethernet switch
SIP call server
Wi-Fi AP
SpectraLink 8020/8030 Wireless Telephone

System Components

SpectraLink 8020/8030 Wireless Telephone

The SpectraLink 8020 Wireless Telephone is a lightweight, durable handset specifically designed for mobile workplace use. The SpectraLink 8030 Wireless Telephone has the same features and function, but in a more durable design with and includes push-to-talk capability.

Like a wired desk phone, the handset can receive calls directly, receive transferred calls, transfer calls to other extensions, and make outside and long distance calls. The Wireless Telephones can only be used on-premises within the WLAN coverage area with the local SIP call server.

SpectraLink 8000 SVP Server (required when using SVP)

As described earlier, the SVP Server is a Polycom wired LAN device that is required when using SpectraLink Voice Priority for QoS.

Access points

Enterprise-grade Wi-Fi access points provide the connection between the wired LAN and the wireless LAN. VIEW Certified 802.11a/b/g/n APs must be positioned in all areas where Wireless Telephones will be used to ensure seamless radio coverage. The number, type and placement of access points will affect the coverage area and capacity of the wireless system. Careful planning of the WLAN is necessary to ensure good voice quality. See the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for additional guidance.

APs must be properly configured to support the corresponding QoS and security methods selected for the handset.

Ethernet switch

One or more Ethernet switches interconnect multiple network devices, including the SpectraLink 8000 SVP Server (if used for QoS), the proxy server(s), wired IP phones, TFTP Server, RADIUS authentication server (if using WPA2 Enterprise) and WLAN access points. Enterprise Ethernet switches provide the highest performance networks, which can handle combined voice and data traffic, and are required when using the SpectraLink 8020/8030 Wireless Telephones.

Although a single Ethernet switch network is recommended, the handsets and the SpectraLink 8000 SVP Server can operate in larger, more complex networks, including networks with multiple Ethernet switches, routers, VLANs and/or multiple subnets, as long as the SVP Server and access points and handsets are on the same subnet. However, in such networks, it is possible for the quality of service (QoS) features of the SVP Server to be compromised, and consequently voice quality may suffer. Any network that consists of more than a single Ethernet switch should be thoroughly tested to ensure any quality issues are addressed. See *the Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for additional guidance.

SpectraLink 8020/8030 Wireless 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 enable 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.

Ensure that all your APs are attached to the same subnet for proper operation. The handset can change subnets if DHCP is enabled and the handset is powered off then back on when within range of APs on the new subnet. Note that the wireless telephones cannot “roam” across subnets, since they cannot change IP addresses while operational.

SIP server

The SIP server is a component from a third-party vendor that provides access to telephony services. The handsets can recognize up to three distinct SIP servers in a single system.

The handsets can operate with SIP proxy servers such as SER (SIP Extensible Router) or with SIP Back-to-Back User Agents (B2BUA) – the most common form of SIP server for PBX-based systems. In this case the IP address location services provided by the SIP server are not available, so direct IP address dialing must be used.

The SIP proxy server connects to another device such as a PBX or gateway and from there, other wired phones and the PSTN.

Provisioning Server (HTTP or TFTP)

A provisioning server is required to distribute firmware and configuration files to the handsets. The SpectraLink 8020/8030

Wireless Telephones support both HTTP and TFTP download servers for provisioning the phones. The provisioning server may be on a different subnet than the APs and/or handsets.

NTP (Network Time Protocol) Server

If WPA2 Enterprise security is used, the handset will confirm the PEAP certificate has a valid date and time with the NTP Server on the network, if one is available. If an NTP Server is not available, the certificate will be assumed valid and operate accordingly.

Authentication Server (if using WPA2 Enterprise)

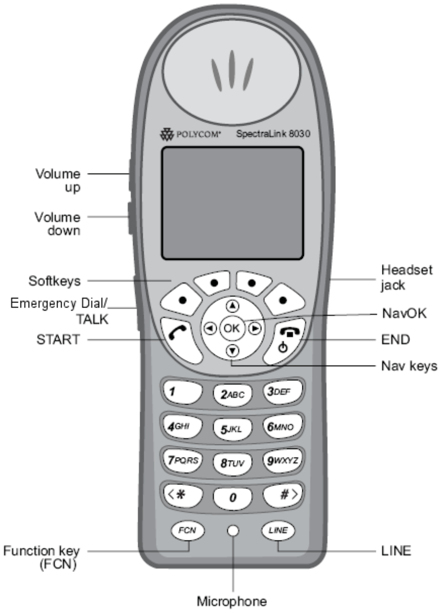
A RADIUS authentication server must be used to provide username/password-based authentication using RSA certificates for PEAPv0/MSCHAPv2 or PAC files for EAP-FAST.

The following authentication servers have been validated for use with R3.0:

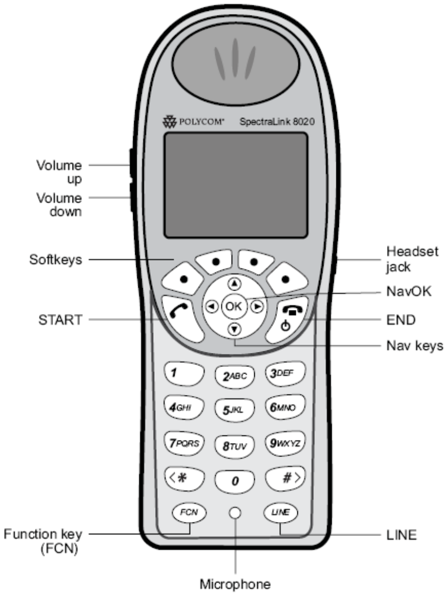
- Juniper Networks Steel-belted Radius Enterprise Edition (formerly Funk), v6.1
- Microsoft Internet Security and Acceleration (ISA) Server 2003, Windows 2008 NPS
- Cisco Secure Access Control Server (ACS), v5.2, 4.1
- FreeRADIUS v2.1.10, 2.0.1 and 1.1.7

Other RADIUS servers may work properly with SpectraLink handsets, but have not been tested. Inquiries on untested servers will receive limited, *"Best Effort"*, support.

SpectraLink 8020/8030 Wireless Telephone Specifications



SpectraLink 8030 Wireless Telephone



SpectraLink 8020 Wireless Telephone

Table of Specifications

Radio mode (selectable)	(802.11b, 802.11g)	2.4–2.4835 GHz
	(802.11a)	5.150–5.250 GHz 5.250–5.350 GHz 5.470–5.650 GHz 5.470–5.725 GHz 5.725–5.825 GHz 5.725–5.850 GHz
Transmission type	Direct-sequence spread spectrum (DSSS)	
Transmit data rate	up to 54 Mb/s	
WLAN QoS	SpectraLink Voice Priority (SVP) Wi-Fi Standard QoS (using WMM, WMM-Power Save and WMM-Admission Control) CCXv4	
WLAN security	WEP (Wired Equivalent Privacy) Cisco FSR (Fast Secure Roaming) WPA Personal WPA2 Personal WPA2 Enterprise: 802.1X Authentication EAP-FAST PEAPv0/MSCHAPv2: PEAP certificate sizes: 512*, 1024*, 2048, 4096 bit (*recommended) Encryption Ciphers: AES, RSA, RC4 Data Integrity: Hashed Message Authentication Code MD5 (HMAC-MD5) (RFC 2403, 2104) and Secure Hash Algorithm-1 SHA (HMAC-SHA-1) (RFC2404) Fast AP Handoff Opportunistic Key Caching (OKC) Cisco Client Key Management (CCKM)	
FCC certification	Part 15.247	
Other certifications	IP 53 certified for resistance to dust and liquid resistance MIL 810F Proc IV 516.5 for shock resistance Cisco Compatible Extensions (CCX) v4	
Voice encoding	ADPCM (Proprietary) G.711µ-law, G.711a-law and G.729	
Transmit power	Up to 100mW Transmit Power Control (formerly 802.11h), see Appendix A for details.	
Display	Up to five lines of text plus two icon status rows and one row for softkey labels.	
8020 Dimensions	5.7" x 2.0" x 0.9" (14.5 x 5.1 x 2.3 cm)	

8030 Dimensions	5.4" x 2.0" x 0.9" (13.7 x 5.1 x 2.3 cm)
8020 Weight*	3.9 oz. (110.6 g) with Standard Battery Pack
8030 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

SIP Integration Factors

See Appendix B: Remote Configuration Parameters Definition for more information on the SIP commands mentioned in this chapter.

CODECs

The SpectraLink 8020/8030 Wireless Telephones are compatible with the G.711μ-law, G.711a-law and G.729 codecs. the codecs can be used in a preferred order which is set in the configuration files.

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 handset will use the DHCP options shown in the following table if DHCP use is enabled. The DHCP setting will always take precedence if it is set and if it is available.

Option	SIP Parameter	Meaning
1	NA	Subnet mask
3	NA	Default gateway
6	DNSSRVR	DNS server
7	LOGSRVR	Syslog server logging
15	DOMAIN	Domain name
42	SNTPSRVR	NTP Server
66	TFTPSRVR	TFTP server
151	SVPSRVR	SpectraLink 8000 SVP Server
152	OAISRVR	SpectraLink 8000 OAI Gateway
siaddr	NA	Boot server or next server

Some of these values can be statically configured on the phone. If values are not received via DHCP, the handset will use the statically-defined values.

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, it is easier to remember user-friendly names than number-based addresses, so it is necessary to translate user-friendly names into addresses that the network can recognize. The handset can use DNS for HTTP server IP addresses, SNMP server IP addresses, and the call server.

Sample DHCP Server Configuration File

A sample DHCP server configuration file is illustrated below. Please note that this is only a sample and will not work on your system as written here. In addition, this file is specific to the ISC DHCP server. Your configuration files must be locally programmed according to your site requirements.

dhcpd.cfg

```
# /etc/dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Type "man dhcp-options" at prompt to get help for these options.
#

# Global parameters start at beginning of file.

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
# This means the DHCP server will send DHCPNAK messages to misconfigured
# clients.
authoritative;

# Use local address if you want the DHCP server to listen for DHCP requests
# on a specified address, rather than requests send to all addresses.
local-address 192.168.0.1;

# define the default gateway / router option 3
option routers 192.168.0.1;

# define the DNS server(s) option 6
option domain-name-servers 192.168.0.1;

# define the SYSLOG server option 7
option log-servers 192.168.0.1;

# define the domain name option 15
option domain-name "polycom.com";

# define the SVP server option code 151 as an IP address.
option svp-server code 151 = ip-address;
```

```
# define the OAI server option code 152 as an IP address.
option oai-server code 152 = ip-address;

# This should  be  the  length  in seconds that will be
# assigned to a lease if the client requesting the lease does not ask
# for a specific expiration time. 86400 seconds is 1 day.
default-lease-time 86400;

# This should be the maximum length in seconds that will  be  assigned
# to a lease.
max-lease-time 86400;

# minimum lease time of 10 minutes
min-lease-time 600;

# You can declare a class of clients and then do address allocation
# based on that.  The example below shows a case where all clients
# in a certain class get addresses in the range 192.168.0.100 to 192.168.0.149,
# and all other clients get addresses in the range 192.168.0.150 to
# 192.168.0.199.

class "SpectraLinkPhones" {
  match if substring (option vendor-class-identifier, 0, 11) = "SpectraLink";
}

# subnet definition also sets netmask option 1
subnet 192.168.0.0 netmask 255.255.255.0 {

  # DHCP lease pool for Polycom SpectraLink phones
  pool {
    allow members of "SpectraLinkPhones";
    range 192.168.0.100 192.168.0.149;

    # define the siaddr / next server field as the alternative TFTP server address
    next-server 192.168.0.1;

    # define the NTP server option 42
    option ntp-servers 192.168.0.1;

    # define the primary TFTP server address option 66
    option tftp-server-name "192.168.0.1";

    # define the SVP server address option 151 if using SVP QoS
    option svp-server 192.168.0.5; # option 151

    # define the OAI server address option 152
    option oai-server 192.168.0.6; # option 152
  }

  # DHCP lease pool for other devices
  pool {
    deny members of "SpectraLinkPhones";
    range 192.168.0.150 192.168.0.199;
    next-server 192.168.0.1;
    option tftp-server-name "192.168.0.1";
```

3

System Configuration

Each handset 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 handset being configured is affected by the **Admin** menu settings.

The wireless telephone user may select several usability options from the Config menu, described below in the User-Defined Preferences section. This information is also provided in the end-user manual.

The SpectraLink Handset Administration Tool is a software utility that enables rapid configuration of handsets by utilizing the USB port on the Dual Charger. See the *Handset Administration Tool (HAT)* document for specific instructions. Please see your service representative or contact Polycom customer service for more information about this time-saving tool.

The SpectraLink 8020/8030 Wireless Telephone may be initially configured with minimum system requirements using the HAT tool. Thereafter, the Remote Configuration File method can be used to set the remaining parameters.

> Version 1 configuration mode can be used for backward compatibility if desired. See Version 1 and Version 2 Configuration Files section below for additional information.

When WPA2 Enterprise security is used, PAC files for EAP-FAST can be provisioned wirelessly or by using the HAT. For PEAP, certificates can be enrolled either using HAT or via the Remote Configuration File.

Other settings that must be configured include, but are not limited to, WLAN QoS, DSCP tagging, DHCP and regulatory domain information. If these are not selected by the administrator the handset will use the default settings. Certain settings do not have default values and must be configured. SSID and related security settings and Regulatory Domain parameters are mandatory, have no default value and need to be specified.

Version 1 and Version 2 Configuration Files

Starting with Polycom SIP software version 131.031, Polycom extended the SIP configuration files to allow all phone settings that are available in HAT and the Admin menus to be set through the configuration files. The formatting of parameters has changed for the new configuration files, but the old method is available for backward compatibility.

The older version of SIP configuration file format is referred to as Version 1 Configuration format. The new version is referred to as Version 2 Configuration format.

Users can convert from one file format to the other. Version 1 Configuration format is limited to the parameters it supported in the past and may be deprecated in future versions of the software as additional parameters are added and older ones retired.

The 8020/ 8030 Wireless Telephone uses Version 1 Configuration files as the default. You can switch to Version 2 Configuration files using HAT, the Admin menus, or by adding the new CONFIG_MODE parameter to the Version 1 Configuration file.

Here are the basic behavioral changes introduced for Version 2 Configuration mode. These features are not available in Version 1 Configuration mode:

- The 8020/ 8030 Wireless Telephone still uses a generic configuration file and a phone specific file. The default name for the generic Version 2 Configuration file is changed to **settings.txt** . The phone specific file is called **sip_xxxx.txt**, where xxxx is the username assigned to each individual user by the system administrator. This name can be from 1 to 16 characters but must use only characters supported by Windows for a file name and must match the username of the phone. These files have a different format than the Version 1 Configuration files. Note that the extension of the file has changed from ‘cfg’ to ‘txt’.
- There is now an option to use a GET statement in the slnk_cfg.cfg file. This can be used to specify a filename different than the default of settings.txt. This statement is ignored in Version 1 Configuration mode.
- Parameter values specified in the Version 2 Configuration files are saved permanently to flash memory in the phone. Values are saved to the same memory location as values set by HAT or the Admin menus. This is called persistence. Once in the phone, they will continue to be used by the phone even if they are removed

from the configuration file, or if the configuration file cannot be loaded (for example, if the provisioning server is down). To clear a value from the phone's persistent memory, the parameter may be set to 'Null' in the configuration file or written again with another value by the configuration file, HAT or the Admin menus.

- SIP specific parameters written to the phone via HAT take effect if the phone is in Version 2 Configuration mode, if the parameter is not overridden by a value specified in a configuration file.
- If either of the configuration files (generic or phone specific) cannot be found, the phone continues to initialize using stored parameter values (if possible).

The following are behavioral changes that apply to both Version 1 and Version 2 Configuration modes:

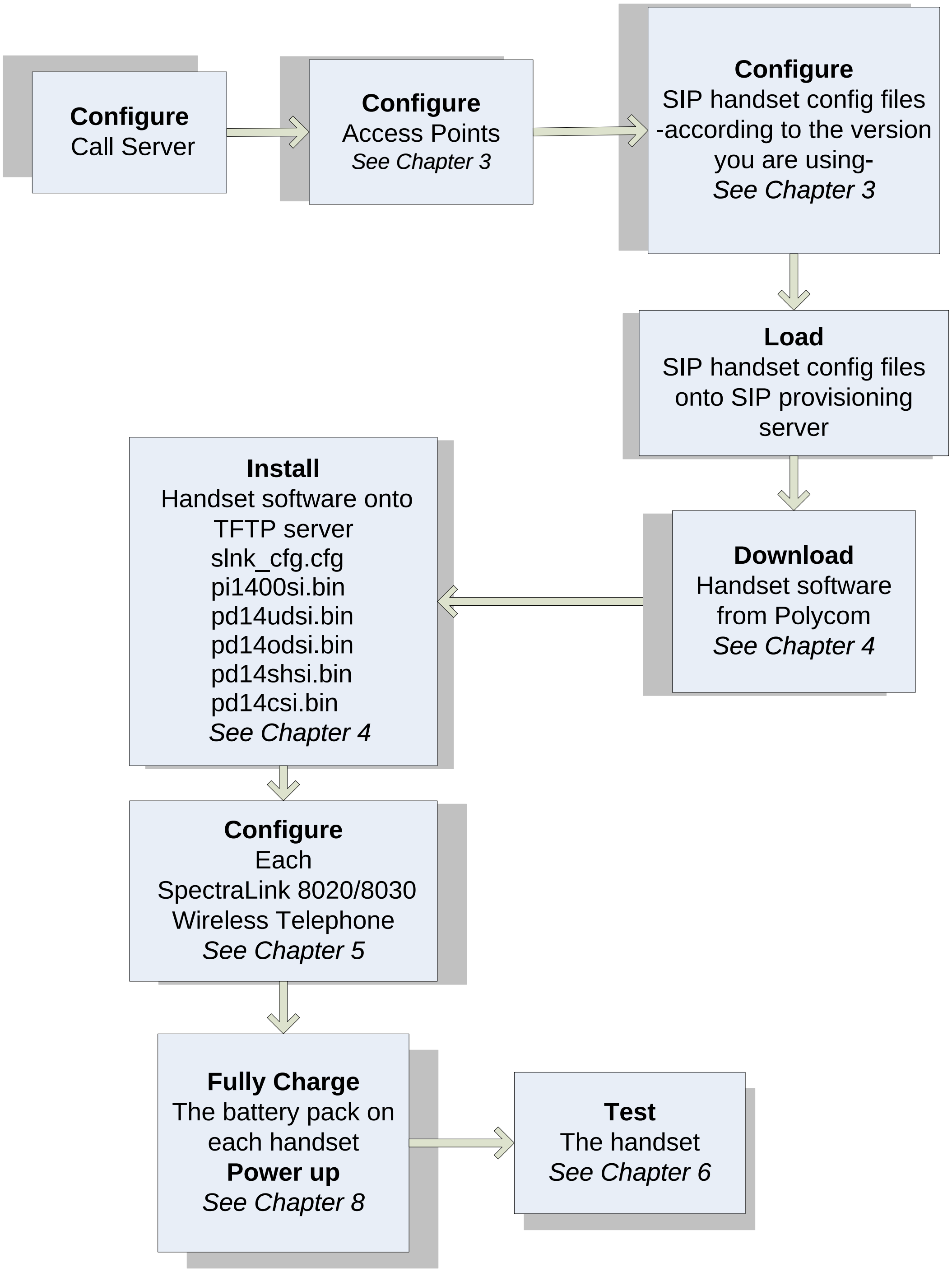
- If using DHCP, and the values for TFTP IP, LOG IP, SNTP IP, SVP IP, OAI IP, DNS IP, or DNS Domain are not received via DHCP, the phone will use the value saved in the phone (if any) from previous configurations via HAT, menus, or configuration files.
- If all specified lines that have proxies fail to register and there are no lines defined without proxies, the phone will reboot (with "N of M lines unregistered" message).

SIP code no longer uses the SIP TFTP IP address to get configuration files, it now uses the same address for downloading files via either HTTP or TFTP.

The HTTP Server Address takes precedence over the TFTP Server address. The TFTP Server address will only be used if an HTTP Server address is not provided or the configuration files cannot be found at the HTTP Server address.

Configuration Flow Chart

(Each step is explained in the following pages)



Configure Call Server

See the documentation which accompanies your call server. Review the proxy information in this document for configuration requirements. You will also need to configure an extension and related information for each handset to be deployed.

Configure Access Points

See the documentation which accompanies your access point. Polycom VIEW certified access points are listed in the *Polycom VIEW Certified Products Guide*. Configuration Guides for each certified product can be found on the Polycom website. See the Related Documents section at the beginning of this document for link information.

Configure SIP Handset Files

During normal handset setup in the SIP environment, two files are downloaded from the provisioning server during startup. These files are obtained from either the default HTTP directory (specified in the HTTPDIR parameter) or the root directory of the TFTP server.

Version 1 Configuration Mode

The first file, the sip_allusers.cfg file, contains generic system information and is downloaded by every handset during the power-up sequence. A second file, the sip_xxxx.cfg file, which is unique for each handset, is then downloaded. It contains specific information for each handset such as username, password, and line appearances. Both of these files must be written specifically for the facility where the handsets will operate.

If the handset cannot find at least one of these files, then it will not boot to the application, but will display a warning message.

Version 2 Configuration Mode

The first file, the settings.txt file, contains generic system information and is downloaded by every handset during the power-up sequence. A second file, the sipxxxx.txt file, which is unique for each handset, is then downloaded. It contains specific information for each handset such as username, password, and line appearances. Both of these files must be written specifically for the facility where the handsets will operate.

If the handset cannot find one or both of these files, it will initialize using previously stored parameters. These parameters may have been obtained from configuration files during a previous startup or from handset configuration procedures or some combination of these two methods.

Sample files are provided with the software downloaded from the website. We recommend using these sample files as a starting point and editing them according to your system requirements.

Provisioning Server Configuration Files

The two file types, generic and specific, are identical in format within the same Configuration Mode. Any or all of the configuration information can be contained in either file. Any information in the specific file that conflicts with the information in the generic file will take precedence over that in the generic file. Authentication information will be accepted from both files. For ease of administration, it is recommended both file types be utilized within each type of Configuration Mode.

Version 1 Configuration Guidelines

- The files are in plain text, US-ASCII. The general form of the configuration file data is “parameter = value.”
- The generic filename must be SIP_allusers.cfg.
- Each specific filename must have the form of SIP_xxxx.cfg where xxxx is as assigned to each individual user by the system administrator. See Chapter 5 Configure Each SpectraLink 8020/8030 Wireless Telephone, section The Admin Menu, subsection SIP Registration.
- Username parameters are: alphanumeric, no spaces, no punctuation, case is ignored, 1-16 characters.
- Generic file information should contain proxy server information and other SIP system data.
- Information in the specific file should contain data specific to each user such as authentication credentials and line appearance data.
- Some parameter lines accept more than one value, separated by a colon or semicolon character as defined below.

- Any line that begins with a pound sign (#) is ignored.
- In general, space characters are ignored. Space characters may be included in string values by replacing the space with "%20" or by enclosing the string in quotes (").
- If necessary, other special characters may be included by using a hexadecimal representation: (%hh) where hh is the representation of the character.
- Lines may appear in any order although maintenance may be simplified by preserving the order in the supplied example file.

Version 2 Configuration Guidelines

- The files are in plain text, US-ASCII. The general form of the configuration file data is "SET parameter value."
- The generic filename is settings.txt and this is the default filename expected by the software. A different filename may be assigned as long as the GET statement in the slnk_cfg.cfg command is programmed to find it. If there is no GET statement, the software looks for a settings.txt file.
- Each specific filename must have the form of SIP_xxxx.txt where the xxxx is the username assigned to each individual user by the system administrator that is entered into the handset at the login prompt or the one specified by the parameter SIP_USERNAME1 in a remote configuration file. See Chapter 5 Configure Each SpectraLink 8020/8030 Wireless Telephone, section The Admin Menu, subsection SIP Registration.
- Username parameters are: numbers only, no spaces, no punctuation, case is ignored, 1-16 characters.
- Generic file information should contain proxy server information and other SIP system data.
- Information in the specific file should contain data specific to each user such as authentication credentials and line appearance data.
- Lines may appear in any order although maintenance may be simplified by preserving the order in the supplied example file. Lines in the WLAN section of the 8020/8030 section should remain in the same order as they appear in the sample file as some later parameters depend on earlier parameters.

Version 1: The Generic File (SIP_allusers.cfg)

Gather information and open the sample file

> The generic file name must be SIP_allusers.cfg. It should contain proxy server information and other SIP system data as outlined below.

The maximum number of characters allowed per line (excluding comments) in this configuration file is 121.

The sample cfg files are populated with commonly-used values. Consult the SIP Proxy Server Command Table in Appendix B for detailed information on configuration options.

1. Gather the following information:

– proxy server name

– SIP server address and domain name

– voicemail system pilot number

2. Open the SIP_allusers.cfg file.

Configure proxy settings

3. Identify your proxy in the list and remove the # at the left to uncomment it and mark it for use.
   PROXYn_TYPE: use the list of proxy types in the sample file and uncomment the one in use in your facility. E.g.

```
PROXY1_TYPE     = MITEL
```

> If you are using the NEC iS3000 as your proxy server, configure it using the Asterisk settings as shown in Appendix C.

> If you have more than one proxy server, each server must be given a number and each parameter must be defined for each server. See examples below. All proxy settings must be in the same generic file. Up to three proxy servers may be defined.

4. Set parameters for each proxy server. In the sample file, scroll down to the section for your server brand. Refer to Appendix B and the section below for information about each of the PROXYn parameters.

a PROXYn_ADDR: Enter the Proxy Server's IP address. One PROXYn_ADDR (PBX/Call Server) entry is required; additional ones are optional as you can register secondary line appearances with other PROXY servers. E.g.

```
PROXY1_ADDR      = 172.29.102.131:5060
PROXY2_ADDR      = 172.29.0.140:5060
```

> For each proxy of type NECSIP, one PROXYn_CONF_IP_ADDRESS is required. This value is the address of NEC PBX's IP PAD card. E.g.
>
> ```
> #PROXY1_CONF_IP_ADDRESS       = 172.29.102.131
> ```

b PROXYn_KEYPRESS_2833: controls generation of in-stream RFC2833 formatted keypress events. Normally you want this to be disabled for Asterisk but it depends on your configuration and what you want to be able to do. The default is disable. E.g.

```
PROXY1_KEYPRESS_2833 = disable
```

c PROXYn_KEYPRESS_INFO: controls generation of SIP INFO requests to the SIP server for keypress events. Normally you want this to be enabled. The default is enable. E.g.

```
PROXY1_KEYPRESS_INFO = enable
```

d PROXYn_HOLD_IP0: controls setting of media stream IP destination to 0.0.0.0 when a call is put on hold. PROXYn_HOLD_IP0 is not required for current versions of Asterisk. For older PBXs that require this, set this to enable. E.g.

```
PROXYn_HOLD_IP0 = enable
```

e PROXYn_PRACK: enables ACK'd provisional responses to INVITE requests. The PRACK mechanism will be used if this switch is enabled and the Proxy server specifies support for the PRACK mechanism. PRACK is not supported in current versions of Asterisk, but is to be supported on subsequent versions. PRACK should not be required on local area networks. E.g.

```
PROXY1_PRACK = disable
```

f PROXY1_REREG_SECS specifies the re-registration interval for a PROXY. This is the requested expiration interval sent in the REGISTER request message. It can be set to anything between 35 and 3600 seconds. The default value (which is applied if no parameter is supplied in this file) is 3600 which means the phone will attempt to register every 3580 seconds, if the server's response interval doesn't take precedence.

If the server has a lower maximum setting or a higher minimum setting that this value then the server's response will take precedence and this parameter will be ignored.

The phone will always attempt to re-register with the PROXY 20 seconds prior to the expiration interval. Thus, if this parameter is set to 35 seconds, and the server's response interval doesn't take precedence, then the phone will attempt to re-register every 15 seconds. E.g.

```
PROXY1_REREG_SECS=3600
```

g PROXYn_KEEPALIVE_SECS: specifies that the handset should send keepalives to the PROXYn server. It can be set to 0 or anywhere from 10 to 3600 seconds. The default value (which is applied if no parameter is supplied in this file) is 0 which means the handset will not send keepalives to PROXYn.

If the handset fails to get a keepalive response within the SIP 32 second timeout, the keepalives are terminated for that PROXY until the next successful registration to the PROXY.

This parameter is REQUIRED when the handsets are operating in WI-FI standard QoS mode. This is because Linux, the OS running Asterisk, has a ARP Cache flushing mechanism. For 8020 and 8030 handsets operating in SVP mode, ARP Cache is refreshed by the SVP server. If the handsets are operating in standard based QoS method ARP cache refresh has to be done by handset.

The value of this parameter for handsets should be just less than the minimum ARP Cache flushing time on the Linux box running Asterisk. For Redhat this minimum flushing time is 15 seconds, so the parameter needs to be set for 14 seconds or less. For other Linux Distributions, you may have to determine what this minimum value is, however 14 seconds should work fine. E.g.:

```
PROXY1_KEEPALIVE_SECS=14
```

The lower this setting, the more the impact on the handset's standby battery life.

8020/8030 handsets running version 131.017 and earlier code ignore this parameter if present).

h PROXYn_DOMAIN = axlx.engr.local
Replace this with your SIP Domain's name. E.g.

```
PROXY1_DOMAIN = plcmengr.com
```

```
PROXY1_DOMAIN = 10.0.0.138
PROXY1_DOMAIN = axlx.engr.local
```

ProxyDomain can be omitted if a specific proxy domain name is not defined at the proxy server. If omitted, the ProxyDomain defaults to the IP address of the proxy server.

i PROXYn_CALLID_PER_LINE controls sending of the same Call-ID header field for registrations sent to a particular registrar. If this is enabled we will send Call-ID headers differently. This may be needed for Mitel 3300 Controller software prior to Release 9. E.g.

```
PROXY1_CALLID_PER_LINE = enable
```

j PROXYn_MAIL_ACCESS: Enter your Voice Mail System's Pilot Number. This is the main voicemail dial number. E.g.

```
PROXY1_MAIL_ACCESS = 7999
PROXY1_MAIL_ACCESS = sip:7999@10.0.0.138
PROXY1_MAIL_ACCESS = 7999@10.0.0.138
PROXY1_MAIL_ACCESS = 7999
```

PROXYn Mail Subscr is the proxy for mail center notifications. It is almost never required in current versions of Asterisk. If you are using Asterisk (non-business edition) before v1.2, this is necessary only if the user is not subscribed automatically at registration. E.g. (specific for a line number:3001)

```
PROXY1_MAIL_SUBSCR = sip:3001@vmail.asterisk.com
```

k PROXYn_FAILOVERIP is required for ININ Redundancy. This value is the secondary IP address of the ININ server. If the primary server fails this address is needed to make the calls. E.g.

```
PROXY1_FAILOVERIP = 172.24.144.136
```

Proxy settings can differ depending on your server. See the sample .cfg file and Appendix B for additional explanations about configuring multiple proxies and other proxy settings not found in the above list.

Configure Call Logs

Call logs provide the user with logs of the most-recently incoming, answered and missed calls. When enabled, the handset will locally story the 20 most recent numbers. If disabled, the handset will not log any calls. If this setting is enabled, it may be overridden on the handset but such a disable will not persist after a power cycle.

5. CALL_LOGGING: enable or disable this feature. E.g.

```
CALL_LOGGING = disable
```

As of this writing, Call Logs are only qualified on the Asterisk Business Edition (ABE), version 1.6 and above. **Call Logs can be enabled on other call servers, but the functionality has not been validated to work properly.**

Configure Favorites

The **Favorites** menu provides access to a predefined list of dial numbers. The list is programmed by the system administrator and may include common or handset-specific entries. Favorites in the allusers file will be present in the Favorites on all handsets.

The username can be blank and can include escaped characters. The Favorites list can include either complete dial numbers for named parties or partial numbers that need additional data entry.

If a PBX feature access code for call forwarding is defined in the Favorites list but you need to add the forwarding destination information before sending the call to the PBX to activate the feature, you can create a Favorite with the access code only.

6. To add phone numbers to the Favorites:

a After **FAVORITE** =, enter the number for the contact in quotes. If you wish to attach a name (or escape characters), place a semi-colon and a space after the end quotes and enter the name in quotes. E.g.

```
FAVORITE = "1234"; "Site Security"
FAVORITE = "*98"; "Call Forwarding"
```

b To add a Favorite that prompts additional digits use brackets (<>) for the prompt phrase.
E.g. if the Feature Access code for call forwarding is #21:

```
FAVORITE =  #21<Enter Destination:>; "Call
Forward"
```

This shows on the screen as
Call Forward Enter Destination:_
The user then enters the forward destination number and presses **Start** to compete the action.

E.g. to enter a call pickup number for a Feature Access Code starting with *5

```
FAVORITE =  *5<Pickup Number:>; "Call Pickup"
```

This shows on the screen as
Call Pickup Pickup Number:_
The user then enters the pickup number and presses **Start** to compete the action.

c Commenting a Favorites entry: Place any comments pertaining to a Favorites entry on the next line. Do not place them on the same line as the command.

Numbers added to favorites in the allusers file will appear on all handsets in the system. You can also add favorites to the specific file, and they will only be available to that line. You can add up to 8 entries to a specific file. See below.

Completed generic file example

```
PROXY1_TYPE         = ASTERISK
PROXY1_ADDR         = 172.29.102.131:5060
PROXY1_KEYPRESS_2833    = disable
PROXY1_KEYPRESS_INFO    = enable
PROXYn_HOLD_IPO     = enable
PROXY1_PRACK        = disable
PROXY1_REREG_SECS   = 3600
PROXY1_KEEPALIVE_SECS   = 14
PROXY1_DOMAIN       = plcmengr.com
PROXY1_CALLID_PER_LINE  = enable
PROXY1_MAIL_ACCESS  = 7999
CALL_LOGGING        = enable
FAVORITE            = "1234"; "Site Security"
```

Version 1: The Handset-Specific Files (e.g. sip_3001.cfg)

The handset-specific configuration file provides specific information for the handset to identify itself and communicate with other handsets. Each handset must have its own file with a unique filename. You may use the same parameters as the generic file when programming the handset files if you wish to override a common setting.

You must configure a unique handset file for each handset being deployed. Typically each of these files is named with the extension number or name of the person assigned the handset. For example John Doe’s handset could have a handset filename of sip_3001.cfg or sip_JohnDoe.cfg.

The maximum number of characters allowed per line (excluding comments) in this configuration file is 121.

Items in the PROXY section should be in the allusers .cfg file. If a specific user requires an override, that PROXY setting should be uncommented in the handset specific file.

Gather information and open the sample file

Each handset must have a specific filename with the form of SIP_xxxx.cfg where xxxx is as assigned to each individual user by the system administrator (e.g. sip_3001.cfg or sip_JohnDoe.cfg). Username requirements are: alphanumeric, no spaces, no punctuation, case is ignored, 1-16 characters.

The sample cfg files are populated with commonly-used values. Consult the SIP Proxy Server Command Table in Appendix B for detailed information on configuration options.

The specific file should contain data specific to each user such as authentication credentials and line appearance data. See Chapter 5 Configure Each SpectraLink 8020/8030 Wireless Telephone, section The Admin Menu, subsection SIP Registration.

1. Gather the following information:
   - username and password for this handset;
   - dial number for this line;
   - number of proxy server for this phone;
   - data that should appear on the caller ID at the far end of a call;
   - Favorites required for each handset/user, if any.
2. Retrieve the SIP_xxxx.cfg file from the .zip.
3. PROXYn settings: These should match the allusers settings except if a specific handset needs an override.
4. Enter the username and password at # AUTH =.

Authentication credentials are normally not stored in the file for security reasons, but the option is available if desired.

For lines on proxies of type NECSIP and SHORETEL the LINEn AUTH setting should be used instead as each NEC or SHORETEL line must respond to any authentication challenge using a single UN/PW pair.

Enter specific line definitions

Each handset may have several lines. These would be labeled as LINE1, LINE2, LINE3 and so forth as shown in the sample .cfg file in Appendix C.

1. LINEn: Enter the dial number of the handset. You can enter up to four additional lines (e.g. LINE2 etc.). E.g.
   ```
   LINE1 = 3001
   ```
2. LINEn_PROXY is the number of the proxy server this line should register with, as defined in the sip_allusers.cfg file. E. g.
   ```
   LINE1_PROXY = 1
   ```
3. LINEn_SECONDARY_PROXY is the proxy server to be used in case the primary proxy server fails. This command will only be implemented when the line has a proxy type of MITEL. E.g.
   ```
   LINE1_SECONDARY_PROXY = 2
   ```

A line can only use a secondary proxy if it and the primary proxy (defined with LINEn_PROXY) are both of PROXYn_TYPE = MITEL. If both the primary and secondary proxies are not type MITEL, the secondary definition will be ignored.

The Mitel Communications Director (MCD) 4.0 or greater is the only server that supports this redundancy feature.

4. LINEn_CALLID is the data you wish to appear on the caller ID of the far end of a call. E.g.
   ```
   LINE1_CALLID = John Doe
   ```

For CCME, the value for LINEn_CALLID cannot have commas or special characters. If a comma or a special character is in this command, the phone will display an error message "Bad Request 'Mal".

Program specific Favorites

You can define up to 15 total entries including any defined in sip.allusers.cfg. Enclose a string in quotes if spaces are required. Each Favorite can be a complete SIP URI. A user name can be blank and can include escaped characters.

1. Format for Favorites entry
   ```
   FAVORITE = dial_string: username
   ```

   Examples of Favorites entries:
   ```
   FAVORITE = 3001; User Name 1
   FAVORITE = 93035551212; User Name 5 Cell
   ```
2. See the *Favorites* section for the allusers file above for configuration options that prompt users to enter more digits.
3. Save the file with its specific name.
4. Repeat for each handset.

Sample user specific file

```
LINE1    = 3001
LINE1_PROXY    = 1
LINE1_SECONDARY_PROXY      = 2 # MITEL only
LINE1_CALLID   = User Name 1
LINE1_AUTH     = 3001; 3001

LINE2    = 3002
LINE2_PROXY    = 1
LINE2_SECONDARY_PROXY      = 2 # MITEL only
LINE2_CALLID   = User Name 2
LINE2_AUTH     = 3002; 3002

LINE3    = 3003
LINE3_PROXY    = 1
LINE3_SECONDARY_PROXY      = 2 # MITEL only
LINE3_CALLID   = User Name 3
LINE3_AUTH     = 3003; 3003

LINE4    = 3004
LINE4_PROXY    = 3
LINE4_SECONDARY_PROXY      = 1 # MITEL only
LINE4_CALLID   = User Name 4
LINE4_AUTH     = 3004; 3004

LINE5    = 3005
LINE5_PROXY    = 2
LINE5_SECONDARY_PROXY      = 3 # MITEL only
LINE5_CALLID   = User Name 5
LINE5_AUTH     = 3005; 3005

FAVORITE = 3001; User Name 1
FAVORITE = 3002; User Name 2
FAVORITE = 3003; User Name 3
FAVORITE = 3004; User Name 4
FAVORITE = 93035551212; User Name 5 Cell
FAVORITE = 3006; User Name 6
FAVORITE = 3007; User Name 7
FAVORITE = 3008; User Name 8
FAVORITE = 3009; User Name 9
FAVORITE = 3010; User Name 10
FAVORITE = 3011; User Name 11
FAVORITE = 3013; User Name 12
FAVORITE = 3013; User Name 13
FAVORITE = 3014; User Name 14
FAVORITE = 3015; User Name 15
```

Version 2: The Generic File (settings.txt)

The settings file contains the parameters that you can use to customize the SpectraLink 8020/8030 Wireless Telephones for your enterprise. Contact your service representative for a sample of this file or if you need additional assistance.

> Polycom recommends that the settings file have the extension ***.txt**. While the file can have any extension the user wants, using the **txt** extension allows easy identification that Version 2 Configuration file are in use.

The settings that pertain to the 8020/ 8030 Wireless SIP Telephones can include the following types of statements, one per line. Any invalid statement is ignored. The statement types are:

- SET statements of the form **SET** ***parameter_name value***. If the desired value contains a blank or a comma, the entire value must by placed within double quotes.
- GOTO statements, of the form **GOTO** ***tag***. GOTO statements cause the telephone to continue interpreting the configuration file after a line that begins with a "**# tag**" statement. If no such line exists in the upgrade or settings file after the GOTO, the phone ignores anything in the file after the GOTO.
- Tags are lines that begin with a **#** tag; tag is an unquoted string and cannot contain a space or comma.
- IF statements, of the form **IF $*name SEQ string*** **GOTO** ***tag***, where name is one of the system parameters shown in the table below. Conditionals cause the GOTO command to be processed if the (string equivalent) value of name is equal to string. Note that the string comparison ignores case, so "Abc" matches "ABC" or "abc". If no such name exists, the entire conditional is ignored.
- Format of SET statements: the string must be included in double quotes if it includes spaces or commas. Any string may be in double quotes, so 1 and "1" are equivalent as are "abc" and abc.
- Any line which does not match one of the previous statement types is ignored and, therefore, can be treated as a comment. By convention, in the settings files distributed by Polycom, any line intended to be ignored by the phone or read as a comment starts with "##".

Values for $name that can be tested in an IF statement

MACADDR	
MODEL4	Will always be 80x0
MODEL	Will always be 80x0
GROUP	The value is whatever the user sets in the Admin menus/HAT for Phone Group– number from 0-999 (default is 0)

See the self-documenting sample settings.txt file for complete information about the settings. Use the information in Chapter 5: Configure Each SpectraLink 8020/8030 Wireless Telephone for Admin menu settings and the table in Appendix B: Remote Configuration Parameters Definition for further information about configuration parameters.

Version 2: The Handset-Specific Files (e.g. sip_xxxx.txt)

The handset-specific configuration file provides specific information for the handset to identify itself and communicate with other handsets. Each handset must have its own file with a unique filename. You may use the same parameters as the generic file when programming the handset files if you wish to override a common setting. The **** SIP SETTINGS **** section of the settings.txt file contains sample parameter information. Use this section to start your custom user files.

> Each handset must have a specific filename with the form of SIP_xxxx.txt where xxxx is as assigned to each individual user by the system administrator (e.g. sip_3001.txt or sip_JohnDoe.txt). Username requirements are: numbers only, no spaces, no punctuation, case is ignored, 1-16 characters.

> The specific file should contain data specific to each user such as authentication credentials and line appearance data. See Chapter 5 Configure Each SpectraLink 8020/8030 Wireless Telephone, section The Admin Menu, subsection SIP Registration.

Gather information

Gather the following information:

- Username(s) and password(s) for this username;
- Extension numbers for up to 5 lines per user;
- Caller ID for each of the 5 lines (optional);
- Other parameters as shown in the sample file;
- Favorites to be programmed in the generic file. A total of 15 Favorites are allowed.

Create username file

Program a file for each username. The following parameters are good options to include in the username file:

SIP_USERNAME (1-6): the first set is required (SIP_USERNAME1 and SIP_PASSWORD1) unless they are to be entered at handset startup in the login screen or are already added by HAT or the Admin menus. Usernames 2-6 are optional and are used to provide more credentials for authentication when more than one line is defined.

SIP_PASSWORD (1-6): as above.

SIP_LINE (1-5): up to five lines may be identified.

SIP_LINE_CALLID (1-5): a different caller ID may be set for each line.

SIP_FAVORITES: up to 15 Favorites are allowed. These should be specified in the generic configuration file or the phone specific file but not both, as the parameter in the phone specific file will override the same parameter in the generic file.

Sample user specific file

This sample file has all six usernames and passwords defined. It has all five lines defined and each line has a defined caller ID. Two Favorites are defined. See the settings.txt file for information on allowed characters and other parameter possibilities.

The name of the file is SIP_USERNAME1.txt.

```
SET SIP_USERNAME1 "1234"
SET SIP_PASSWORD1 "1234"
SET SIP_USERNAME2 "1245"
SET SIP_PASSWORD2 "1245"
SET SIP_USERNAME3 "1256"
SET SIP_PASSWORD3 "1256"
SET SIP_USERNAME4 "1267"
SET SIP_PASSWORD4 "1267"
SET SIP_USERNAME5 "1278"
SET SIP_PASSWORD5 "1278"
SET SIP_USERNAME6 "1289"
SET SIP_PASSWORD6 "1289"
##
SET SIP_LINE1 "1234"
SET SIP_LINE2 "1234"
SET SIP_LINE3 "1234"
SET SIP_LINE4 "1234"
SET SIP_LINE5 "1234"
##
SET SIP_LINE_CALLID1 "1234 Andy"
SET SIP_LINE_CALLID2 "1234 Andy"
SET SIP_LINE_CALLID3 "1234 Andy"
SET SIP_LINE_CALLID4 "1245 Pamela"
SET SIP_LINE_CALLID5 "1256 Paul"
##
SET SIP_FAVORITES 1231;"Favorite1",123;"Favorite2"
```

Load SIP Configuration Files onto Provisioning Server

Move the settings.txt file and each SIP_xxxx.txt file to the server designated for handset support. If using a TFTP server, the files must be in the root directory. If using an HTTP server, the exact location of the files must be specified in the HTTP Server Directory Path setting. See the Admin menu options for more information.

Ensure the provisioning server is started.

4

Download and Install Handset Software

SpectraLink 8020/8030 Wireless Telephones support a number of different IP protocol integrations. All SpectraLink 8020/8030 Wireless Telephones are shipped from Polycom with a generic software load that allows them to associate to a wireless LAN and download functional software from the provisioning server. **The handsets will not function properly without downloading appropriate software.**

The following details the process to properly configure SpectraLink 8020/8030 Wireless Telephones and download software via over-the-air file transfer.

You may need to charge the handset first. See Chapter 8: Using the 8020/8030 Handset.

Minimum Configuration Process

Recent hardware changes affect the Polycom SpectraLink 8020/8030 Wireless Telephones. The affected products can be identified by a “Rev C” on the label.
The minimum version if you have a Rev C handset is **131.029**.
Any attempt to load earlier versions will result in a download failure.
See Appendix D for full information.

The handset requires minimum configuration in order to associate with an AP. Once the network is accessed, the remaining configuration parameters can be automatically obtained through the configuration files if using Version 2 Configuration mode . If Version 2 Configuration files are not used, non-SIP parameters may be configured by using the HAT tool or manually using the Admin menu on each handset and entering the configuration information. The options are listed below in decreasing order of efficiency:

- HAT plus Remote Configuration (Version 2): Use the HAT tool to set minimum parameters in each handset and then turn on the handset and allow it to download remaining parameters from the settings.txt file.

- Manual plus Remote Configuration (Version 2): Manually configure the minimum settings in each handset and then turn on the handset and allow it to download remaining parameters from the settings.txt file.
- All HAT (Version 2): use the HAT tool to set all parameters in each handset.
- All HAT (Version 1): use the HAT tool to set all non-SIP parameters in each handset. In Version 1 Configuration mode, the configuration files must be used to set the SIP parameters.

Which option you choose depends upon a number of factors including the number of handsets you need to configure, the availability of the settings file, and the installation of the HAT utility.

Configuration sequence

1. Download the latest SpectraLink 8020/8030 Wireless Telephone IP software from http://support.polycom.com/PolycomService/support/us/support/voice/wi-fi/spectralink_8030_wireless.html.
2. Load the latest version of the SIP code and place it on the designated provisioning server and ensure the server is started. The slnk_cfg.cfg is downloaded first by the phone, and defines the SIP code files that will be subsequently downloaded. Be sure to use the slnk_cfg.cfg file that comes with the latest version of the SIP code and do not change the order of the files within slnk_cfg.cfg.

The following six files are included in the typical SIP software package.

Description	Filename
Configuration file	slnk_cfg.cfg
PHINTL (language translation)	pi1400si.bin
USB downloader	pd14udsi.bin
Over-The-Air Downloader (OTADL)	pd14odsi.bin
OTADL Shim[1]	pd14shsi.bin
Functional (telephony protocol)	pd14csi.bin

[1] New filename: pd14shsi.bin was formerly named pd14shim.bin in release packages prior to Polycom SIP software version 131.031.

> See the next chapter for complete information on configuring the handsets as described in steps 3 through 5 below.

3. If using the settings.txt file for remote configuration, set the parameters in the file. See previous chapter, Chapter 4: System Configuration, and Appendix B for detailed information. Ensure the slnk_cfg.cfg GET statement points to the correct filename if it is different than settings.txt.

4. Depending on which configuration method you have chosen, set parameters on each handset.

a Version 2: HAT plus Remote: set minimum parameters for associating to the WLAN:

– QoS method: Configure the QoS handset mode to match the AP and site QoS plan. Follow the VIEW Configuration Guide for the appropriate make/model of WLAN.

– SSID

– Security method: Configure handset security settings to match AP configuration and RADIUS server settings. If WPA2-Enterprise security is used, credentials will need to be installed onto the handset. For EAP-FAST, the PAC file needs to be provisioned and for PEAP the handset will need to be enrolled with a certificate (initial configuration requires use of the HAT). See the WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning section in this guide for details.

– Any security sub-options required for initial access to network

– Regulatory domain

– Radio band

– DHCP or static IP addresses

b Version 2: Manual plus Remote: set minimum parameters for associating to the WLAN as above using the Admin menus

c HAT: set all parameters for associating to the WLAN as above.

See the next chapter, for detailed configuration instructions.

5. Power cycle the handset.

6. The SIP 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. Upon completion of the update process, the handset will re-boot with the new firmware.

During the second download evolution, the handset receives configuration files from the provisioning server for system configuration and for its own settings. Once this second evolution is complete, the handset is ready to use.

For future software upgrades, simply update the files that are stored on the provisioning server. Each time the handset is powered on, it will check with the provisioning server to ensure it has the proper software version.

5

Configure Each SpectraLink 8020/8030 Wireless Telephone

Power up the handset and download the software.

If the handset code needs to be updated, the SIP 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. Upon completion of the update process, the handset will re-boot with the new firmware.

During the second download evolution, the handset receives code from the provisioning server for system configuration and for its own settings. Once this second evolution is complete, the handset is ready to use.

Handset Administration Tool

The Handset Administration Tool is a software utility developed by Polycom Corporation to automate the configuration of multiple SpectraLink 8020/8030 Wireless Telephones and perform various administration tasks. For complete data, please see *SpectraLink 8020/8030 Wireless Telephones Handset Administration Tool*. The tool may be downloaded from the Polycom website.

Remote Configuration

After initial settings are configured either manually or via HAT, the handset can obtain the remaining parameters from the configuration files.

In Version 1 Configuration mode, only SIP settings can be configured remotely. In Version 2 Configuration mode, all settings can be remotely configured.

The Admin (Administration) Menu

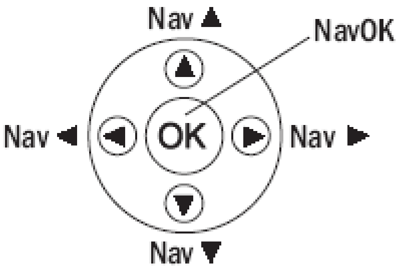
The **Admin** menu contains configuration options that are stored locally (on each handset). Each handset is independent, and if the default settings are not desired, the **Admin** options must be set in each handset requiring different settings. Default settings can be found later in this document. The handset **Admin** menu can be accessed in one of two ways:

1. With the handset powered off, press and hold the **START** key. While holding the **START** key, press and release the **END** key. When the **Admin** menu appears, release the **START** key.
2. Press and release the **END** key. Press and hold the **START** key. When the **Admin** menu appears, release the **START** key.

If an admin password has been set, the display will require its entry 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**.



Toggle options

Some menu items have only two options, which operate on a toggle basis. The current setting is shown below the menu heading on the info line. The other available setting is highlighted in the menu list. Press **NavOK** to activate the highlighted setting.

For example, when predial is disabled, the info line displays **Predial Disabled** and the highlighted menu item is the **Enable Predial** option. Press **NavOK** to enable predial. The info line will change to display **Predial Enabled**.

In another example, when the info line displays **Currently Speaker**, the highlighted menu option is **Ring in Headset**. Press **NavOK** to select **Ring in Headset**, The ring will now sound in the headset and the info line will change to **Currently Headset**.

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:

Key	caps	CAPS
1	1	1
2	2 a b c	2 A B C
3	3 d e f	3 D E F
4	4 g h I	4 G H I
5	5 j k l	5 J K L
6	6 m n o	6 M N O
7	7 p q r s	7 P Q R S

Key	caps	CAPS
8	8 t u v	8 T U V
9	9 w x y z	9 W X Y Z
0	0	0
*****	* . ! $ % & ' ( ) + , : ; / \ = @ ~ - _	
#	<space>	

Admin Menu Table

The following table lists the **Admin** menu items. The default settings have an * prior to the option. Detailed descriptions of each option appear below the table.

1st level	2nd level	3rd level	4th level	5th level
Phone Config	Language	*English Français Deutsch Español Italiano		
	Telephony Protocol	*Type 036		
	PTT/Emerg. Button	Emergency Dial	Emergency # [Enable/Disable]	
			Emergency Number	[Enter Number] [Enter Name]
		Push-to-talk	PTT [Enable/*Disable]	
			Allowed Channels	*Channel 1 *Channel 2 *.... *Channel 24
			Name Channels	[list]
			Priority Channel	Priority Channel On/*Off
				Name Channel
	Time Zone	[list] *GMT		

1st level	2nd level	3rd level	4th level	5th level
	Daylight Savings	*DST No Adjust DST Auto (USA) DST Auto (AUS) DST Auto (EURO)		
	Protected Spd-dial	Enter Number	Enter Name	Assign Speed-Dial
	Password *Enable/Disable			
	[If Password is enabled] Change Password			
	Phone Group			
	Config Mode	*Version1 Version2		
	SIP Registration	Login Reg 2 Reg 3 Reg 4 Reg 5 Reg 6	[for each option] Username Password	
	Clear SIP Regist.			
	*Enable OAI Disable3 OAI			
	Location Service	Enable RTLS *Disable RTLS		
		Transmit Interval	15 seconds 30 seconds 1 minute 5 minutes *10 minutes	
		Location Server IP		
		ELP Port	Enter Port *8552	
	SNMP Settings	Enable SNMP *Disable SNMP		
			SNMP IP Address Public Community Private Community	

1st level	2nd level	3rd level	4th level	5th level
Network Config	IP Addresses	*Use DHCP		
		Static IP	Phone IP Default Gateway Subnet Mask	
			File Servers	TFTP Server IP HTTP Server IP HTTP Port HTTPDir Path
			Syslog Server IP DNS Server IP DNS Domain Time Server IP SVP Server IP OAI Server IP	
	SS ID	[enter]		
	WLAN Settings			

3rd level	4th level	5th level	6th level	7th level
*Custom	Security	*None		
		WEP	Authentication	*Open System Shared Key
			WEP [Enable/*Disable]	
			Key Information	Default Key Key Length Key 1-4
		WPA2-PSK	*Passphrase Pre-Shared Key	
		WPA-PSK	*Passphrase Pre-Shared Key	
		Cisco FSR	Username Password	
		WPA2-Enterprise	Authentication	*EAP-FAST PEAP
			Fast Handoff	*CCKM OKC
			Username	
			Password	
			Delete [Cert./PAC]	

3rd level	4th level	5th level	6th level	7th level
	QoS	*SVP	DSCP tags	WT in call (*46) WT standby (*26) Other (*0)
		Wi-Fi Standard	DSCP tags	Voice (*46) Control (*26) Other (*0)
			Admission Cntrl	*Mandatory Optional
CCX	WPA2-Enterprise	Authentication	*EAP-FAST PEAP	
		Fast Handoff	*CCKM	
		Username		
		Password		
		Delete [Cert./PAC]	[Yes/No]	
	QoS	DSCP tags	Voice (*46)	
			Control (*26)	
			Other (*0)	

1st level	2nd level	3rd level	4th level	5th level
Network Config	Reg. Domain	01 02 03 04 05 06 07 08		
		→	[802.11 Config]	
			a →	[802.11a]† 5.150–5.250 5.250–5.350 DFS 5.470–5.725 DFS 5.470-5.650 DFS 5.725–5.825 5.725-5.850
			‡b & b/g mixed g only	

1st level	2nd level	3rd level	4th level	5th level
			→	[Transmit Power] 5mW (7dBm) 10mW (10dBm) 20mW (13dBm) *30mW (15dBm) 40mW (16dBm) 50mW (17dBm) 100mW (20dBm)
Diagnostics	Run Site Survey			
	Enable Diagnostics *Disable Diagnostics			
	Syslog Mode	*Disabled Errors Events Full		
	Halt on Error *Restart on Error			
Restore Defaults				
Demos	Graphics Demo			

* default setting

† Only those 802.11a bands that are available in the selected domain will be listed. See Appendix A for complete information.

‡ Subbands have not been established for the b and b/g mixed or the g-only mode at this writing. Provision is made in the software to accommodate these ranges once established. Until added, selecting either of these two modes will immediately bring up Transmit Power options.

Modifications of settings under **WLAN Settings** = "**CCX**" may get reflected in the corresponding settings under **WLAN Settings** = "**Custom**" or vice versa. If the configuration is changed from "**CCX**" to "**Custom**" or vice versa, it is recommended to double-check all settings.

Phone Config

Language

The **Language** option is available on both the **Admin** and **Config** menus. Select the desired language from the list. The default is **English**.

Telephony Protocol

Telephony Protocol lets you select the VoIP protocol that your site is licensed to download and run. The SIP protocol used for the SpectraLink 8020/8030 Wireless Telephones requires license option selection **36**. Any other protocol will cause the handset to malfunction.

PTT/Emerg. Button

This option appears only on the SpectraLink 8030. The Push-to-talk button on the left side of the handset may be configured to either standard PTT functionality or to dial the specified emergency call number when pressed twice within two seconds. These are mutually exclusive options. Both are disabled by default.

When using the Handset Administration Tool to configure this option, ensure the PTT option in the **PTT Admin tab** under **Handset type** is disabled before enabling the **Emergency Dial** option in the **Phone Config** tab. When **PTT** is enabled, the **Emergency Dial** option will be grayed out.

Push-to-talk [Disable/Enable] – If enabled, the PTT options will appear on the **Config** menu for the end user to subscribe to allowed channels, etc. If disabled, the PTT options will not appear on the **Config** menu and the Emergency Dial option may be enabled.

PTT is disabled by default. When enabled, all 24 PTT channels are allowed by default. To toggle the allowed status of any channel, select **Allowed Channels**, 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. 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.

Emergency Dial – the **Emergency Dial** option allows you to enable or disable the feature. When enabled, the handset will dial the number programmed into the **Emergency Number** option when the panic button is pressed twice within two seconds.

⚠ **Caution**! Emergency dial just sets up a telephone call and will be inoperable if the wireless system or the call server fails for any reason. Do not rely on it as your sole method of emergency notification.

Follow your dial plan rules when entering the emergency number to be dialed. E.g. if an outside number is to be dialed and a prefix is required to obtain an outside line, enter the prefix as part of the emergency number.

Once an Emergency Number has been entered, it can be modified, but can only be cleared by restoring the handset to defaults.

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.

Protected Speed Dial

The protected speed-dial number is designed to be programmed to a number that should be called in emergency situations. It 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. Only one such number can be programmed Enter the number to be dialed, the name (e.g. Security), and scroll to assign to one key press. The choices for this key press are 1-9, 0, *, or #. The caret represents the volume up and down buttons. This number must be programmed in every handset. This setting cannot be modified by the user. This feature is not available in a handset where the user has disabled **Pre-dial** in the **Config** menu.

Password Enable/Disable/Change

The password option controls access to the **Admin** menu. It is enabled by default with the password 123456. 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. To modify the password requirement, the default or previously set password must be entered to verify the change. **Change Password** will appear only if the password is enabled. The password is disabled by default. The password must be set in each handset for which controlled access is desired. The password may be up to 18 characters in length. Only numbers and letters are allowed.

> The admin password can be defined in the HAT, in the Admin menu or by using the PROCPSWD configuration setting in the Version 2 Configuration settings.txt file. HAT and Admin menus allow a wider range of passwords than remote configuration. If you decide to set the PROCPSWD parameter, it is limited to a maximum of seven (7) digits. Only numbers may be used. See the PROCPSWD parameter in Appendix B: Remote Configuration Parameters Definition for more information.

Phone Group

An integer from 0 to 999. The default is 0. This value can be used by the Version 2 Configuration files for specifying some parameters only for some groups. See the settings.txt file.

Config Mode

Config Mode determines whether the handset will use Version 1 configuration files or Version 2 configuration files.

SIP Registration

Individual handsets may be configured to correspond with the SIP configuration information in the provisioning server. If both HTTP and TFTP IP addresses are present, the handset attempts to download files from the HTTP server(s) first and only tries TFTP if the file(s) are not found on the HTTP server. The handset is then automatically identified at startup. If username and password information is not configured in the **Admin** menu, then this information will be requested at startup.

In either case, the username must agree with a corresponding configuration file. See Version 1 and Version 2 Configuration Files.

Login allows you to specify a username and password for automatically acquiring SIP configuration information. If no username is specified, the SIP handset will request username and password at startup and any additional registrations specified here are ignored.

The username should correspond to the primary (line 1) dial number assigned to the user. The username and password should also correspond to the authentication credentials as created by your system administrator for your primary line registration. Usernames or passwords can be erased by selecting the item, then pressing the **Bksp** softkey and then the **Save** softkey.

Reg 2 through **Reg 6** allow you to specify additional authentication usernames and passwords that may be required by your handset for any additional line appearances (registrations) that may appear in the specific user's configuration file. This information will be ignored if a **Login** username is not provided.

OAI Enable/Disable

Polycom's Open Application Interface (OAI) enables third-party computer applications to display alphanumeric messages on the handset display and take input from the handset keypad. Refer to the *OAI Specification (Version 2.0)* 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 handset. You may select whether the handset should attempt to connect to the SpectraLink 8000 OAI Gateway by choosing either the **Enable** or **Disable** options in this menu.

If OAI is enabled, and an IP address (called the **OAI Server IP**) is available to the handset (either via DHCP or Static IP configuration), the handset will communicate with the OAI Gateway at power-on, and periodically while it is powered-on. If you don't have a SpectraLink 8000 OAI Gateway installed at your site, you should disable the OAI feature to preserve network bandwidth and battery life.

Location Service

Location service may be used to enable or disable the Ekahau Real-Time Location System (RTLS), select a transmit interval, or enter a static IP address for the Ekahau Positioning Engine (EPE). Location services capability is provided by the EPE 4.0 using Ekahau Location Protocol (ELP). See Ekahau's user documentation for more information.

RTLS [Enable/Disable] The RTLS is disabled by default. Press **NavOK** to toggle to the alternate setting. When RTLS is enabled, the handset will display the RTLS icon ▣ in the top center of the screen.

The ring indicator icon will take precedence over the RTLS icon, i.e. the new icon will not be visible while the handset is ringing. When ringing has ceased and the ring indicator becomes inactive, the RTLS icon will again appear (regardless of hook state).

Transmit interval Allows selection of **15 seconds**, **30 seconds**, **1 minute**, **5 minutes**, or **10 minutes** for maximum time between transmit intervals. Default transmit interval is 10 minutes. Press **NavOK** to select the desired transmit interval.

To optimize battery life, the interval between sending out ELP updates will vary based on handset state. It is expected that ELP updates will occur at most every two to six seconds and at least every few minutes. If improved tracking capability is desired, set the transmit interval for a shorter time between ELP updates. Increasing the frequency of transmissions will decrease battery life.

Location Server IP Allows the user to statically enter the IP address of the EPE. Enter the IP address and press **NavOK** to save.

Ekahau clients are not expected to find the EPE automatically. Regardless of the handset's selection of DHCP or static IP, the EPE IP address must be statically entered in the Ekahau Admin menus or HAT.

ELP Port Allows the user to select the port number which ELP updates get sent to at the Location Server IP address. It must match the value configured in the Ekahau Positioning Engine for proper functionality. The ELP port number must be greater than zero and less than 65536. Default is 8552. Enter the port number and press **NavOK** to save.

SNMP Settings

The SNMP option is designed for system administrator use when troubleshooting.

If the SNMP IP address is set, only SNMP queries from this address will be accepted. SNMP Community string. For complete information about these SNMP values, see Chapter 9, the *SNMP* section.

Network Config

IP Addresses

There are two modes in which the handset 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 handset is turned on. If DHCP is enabled, the handset also receives all other IP Address configurations from the DHCP server. If a needed parameter is not supplied by DHCP and there is a static value, the static value will be used.

Static IP Allows you to manually set a fixed IP Address. If selected, the handset will prompt for the IP addresses for 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 handset is operating, the following components are required and must be configured as part of the SIP system:

Phone IP The IP address of the handset. This is automatically assigned if DHCP is used. If using Static IP configuration, you must obtain a unique IP address for each handset 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 handset 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 the network administrator for the proper settings for the network.

SpectraLink 8020/8030 Wireless 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 enable 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.

Ensure that all your APs are attached to the same subnet for proper operation. The handset can change subnets if DHCP is enabled and the handset is powered off then back on when within range of APs on the new subnet. Note that the wireless telephones cannot “roam” across subnets, since they cannot change IP addresses while operational.

Please see *Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony* for detailed configuration information.

Provisioning Servers The provisioning server holds software images for updating the handsets and contains the handset configuration files. If the HTTP server IP or TFTP server IP is configured (not set to 0.0.0.0 or 255.255.255.255) with either Static IP configuration or using DHCP option 66 for TFTP, or the boot server/next server (siaddr) field, the handset will check for newer software each time it is powered on or comes back into range of your network. This check takes only seconds and ensures that all handsets in your network are kept up-to-date with the same version of software.

TFTP Server IP The IP address of a TFTP server on your network, A TFTP server is not required if the files are on an HTTP server.

HTTP Server IP address A single IP address for the HTTP server on your network. An HTTP server is not required if the files are on a TFTP server.

HTTP Port An integer from 0-65535 and will default to 80

HTTP Server Directory Path A string from 1-127 characters that identifies the location of the configuration files.

Syslog Server IP The IP address of the syslog server. See the *Diagnostic Tools* section for more information.

DNS Server IP / DNS Domain The IP address of the DNS server. The DNS domain is a string from 1-127 characters.

Time Server IP The IP address of the time server.

SVP Server IP The IP address of the SpectraLink 8000 SVP Server. If using Static IP configuration, this is simply the IP address of the SpectraLink 8000 SVP Server. Note that the SpectraLink 8000 SVP Server must be statically configured to have a permanent IP address. If DHCP is being used, the handset 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.

The SIP TFTP Server IP address no longer exists. Older versions of Polycom SIP allowed the user to specify different TFTP servers for downloading code and downloading configuration files. Version 131.031 and above allow specification of only one TFTP server address. Both functional code and configuration files are downloaded from the same location.

OAI Server IP The IP address of the SpectraLink 8000 OAI Gateway. If using Static IP configuration, this is simply the IP address of the SpectraLink 8000 OAI Gateway. If DHCP is being used, the handset will try the DHCP option 152.

SSID

Enter the SSID.

WLAN Settings

Select between Custom and CCX modes. The Custom mode allows explicit control of all of the security and QoS settings. Using CCX mode automatically enables the CCXv4 features and functions, with only the 802.1X mechanism needing to be selected.

Custom – Security

Handset security setting should match exactly the settings in your APs. Consult the *VIEW Configuration Guide* for the APs installed in your facility for information on which of the security methods are certified.

Encryption keys, Username and Password display as they are entered. For security reasons, these items will not display when a user returns to the Administration menu.

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

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 handset to correspond with the encryption protocol set up in the APs. Select the entries from the options below to enable the handset 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 handsets. 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 through F.

WPA2-PSK The security features of WPA2 (Wi-Fi Protected Access) using PSK are available and may be used if supported by the APs 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 APs 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) FSR is designed to minimize call interruptions for SpectraLink 8020/8030 Wireless Telephone users as they roam throughout a facility. Cisco FSR requires specific configuration of the Cisco APs in your site. See your Cisco representative for detailed documentation on configuring the APs and other required security services on the wired network. To configure Cisco FSR on a handset, you must enter a Radius Server username and password into each handset.

Username

Enter a username that matches an entry on the 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.

WPA2-Enterprise

The **Authentication** setting can select either ***EAP-FAST** or **PEAP** as the authentication method for RADIUS server. See the *System Components* section for tested models.

Fast Handoff allows the use of either ***CCKM** or **OKC**. These mechanisms allow a phone to quickly and securely roam between APs with a minimum disruption of audio.

Username: Enter a username that matches an entry on your RADIUS server. Alphanumeric strings can be entered using the alphanumeric string entry technique.

Password: Enter the password that corresponds to this username.

The **Delete [PAC/Cert.]:** option removes expired credentials from the phone. When the authentication method is EAP-FAST the PAC on the phone is deleted. If the RADIUS server has enabled "anonymous in-band PAC provisioning ", then the phone will automatically re-acquire these credentials from the RADIUS server over the air. When the authentication method is PEAP or EAP-FAST manual provisioning , the credential on the phone is deleted and a new one needs to be downloaded through the HAT. See additional details in WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning section later in this chapter.

Custom – QoS

SVP mode uses the SVP Server to provide enterprise-grade QoS.

DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the Wireless Telephone. Default values are given but may be overwritten: **WT in call = 46, WT standby = 26, Other = 0**.

Wi-Fi Standard QoS mode uses standards-based traffic controls for QoS, instead of the SVP Server.

DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the Wireless Telephone. Default values are given but may be overwritten: **Voice = 46, Control = 26, Other = 0**.

Admission Cntrl is used to enable and disable the use of WMM Admission Control by the handset for the AC_VO and AC_VI access categories. If the WLAN is using WMM Admission Control, the handset should be set to ***Mandatory**. If the WLAN is not using WMM Admission Control, the handset should be set to ***Optional**. See *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for a detailed explanation of the use of WMM Admission Control.

CCX

CCX settings configure the handset for operation as a CCX V4 certified client.

WPA2-Enterprise

The **Authentication** setting can select either ***EAP-FAST** or **PEAP** as the authentication method for RADIUS server. See the *System Components* section for tested models.

Note that for **Fast Handoff**, the only selection available is ***CCKM.**

Username: Enter a username that matches an entry on your RADIUS server. Alphanumeric strings can be entered using the alphanumeric string entry technique.

Password: Enter the password that corresponds to this username.

The **Delete [PAC/Cert.]**: Option removes expired credentials from the phone. When the authentication method is EAP-FAST the PAC on the phone is deleted. If the RADIUS server has enabled "anonymous in-band PAC provisioning ", then the phone will automatically re-acquire these credentials from the RADIUS server over the air. When the authentication method is PEAP or EAP-FAST manual provisioning , the credential on the phone is deleted and a new one needs to be downloaded through the HAT. See additional details in WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning section later in this chapter.

QoS – DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the Wireless Telephone. Default values are given but may be overwritten: **Voice = 46, Control = 26, Other = 0**.

Regulatory Domain/802.11 Config/Transmit Power

Regulatory domain, 802.11 configuration and transmit power are interdependent. See Appendix A: Regulatory Domains for regulatory domain setting specifications. Polycom recommends that you check with local authorities for the latest status of national regulations for both 2.4 and 5 GHz wireless LANs. A regulatory domain must be selected in order for the handset to operate. There is no default setting.

FCC requirements dictate that the menu for changing the regulatory domain be available by password, which in our case is the **LINE** key. Press **LINE** and then navigate to the desired domain. Press **NavOK** to set the domain.

01 - North America

02 – Europe

03 – Japan

04 – Singapore

05 – Korea

06 – Taiwan

07 – Hong Kong

08 – Mexico, India

802.11 config

Once the regulatory domain is set, the **802.11 Config** modes are displayed. Only one may be chosen. **802.11(b & b/g mixed)** is the default. Press **NavOK** to set the mode. If the mode has subbands, the **Subband** list will open. If the mode does not have subbands, the **Transmit Powe**r list will open.

Use **g only** mode if all of your infrastructure and client devices will use only 802.11g. The handsets will operate up to 54 Mb/s in this mode. If any 802.11b capable clients or infrastructure are used in your wireless LAN then do not use **g only** mode, instead use **802.11b and b/g mixed** mode for optimum performance.

Use **b & b/g mixed** if some of your infrastructure components only understand 802.11b. The handsets will operate up to 11 Mb/s.

Subbands have not been established for the **b and b/g mixed** or the **g only** mode at this writing. Provisions are made in the software to accommodate these ranges once established. Newly added subbands may not appear in the **Admin** menu table above.

Subband

Once a mode is set the subband list will display, if applicable. Only those ranges which are allowed in the set regulatory domain and that pertain to the set mode are displayed. Note that for 802.11a the bands labeled **DFS** will vary depending on the set regulatory domain. Multiple subbands may be set. Navigate to the desired subband and set with **NavOK.** The **Transmit Power** menu will open. Once the **Transmit Power** setting is done, you will be returned to the subband list.

To deselect a subband, navigate to it and press **NavOK**.

Once the subband settings are as desired, press the **Done** softkey to exit to the **Network Setup** menu.

Transmit power

For subbands: The **Transmit Power** list opens when **NavOK** is pressed from the **Subband** menu. A transmit power setting is required for each subband. Only one level may be set per subband. Only those power levels which apply to the regulatory domain and 802.11 mode are listed. Navigate to the desired level and press **NavOK** to set and return to the subband list. Another subband may be selected which repeats the process.

If the highlighted power transmit level is legal on all of the subbands for the set mode, an **All** softkey will appear. Press the **All** softkey to apply that level to all subbands and return to the subband menu where all subbands will now be selected. **All** overrides any previously set power transmit levels.

Without subbands: When the 802.11 mode has no subbands, the **Transmit Power** list opens when **NavOK** is pressed to set the mode. Only those power levels which apply to the domain and 802.11 mode are listed. Navigate to the desired level and press **NavOK**. This sets the transmit power level and exits the **Regulatory Domain** menus. The **Network Setup** menu will again display.

Note that the power setting selected specifies the maximum for that band/subband. When Transmit Power Control (TPC) is enabled in the infrastructure, the AP may instruct the handset to use a lower value to match its own transmit power.

Diagnostics

Run Site Survey

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

Diagnostics Mode

Diagnostics can be enabled or disabled. See Chapter *8* Diagnostic Tools, section Diagnostics Enabled for a detailed explanation of the **Diagnostics** mode options.

Syslog Mode

See Chapter 8 *Diagnostic Tools*, section *Syslog Mode* 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. **Restart On Error** should be used unless specific error conditions are being investigated.

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. An error memory dump can be taken and sent to Customer Service for escalation and analysis.

Restore Defaults

The Restore Defaults option will set all user and administrative parameters except Telephony Protocol to their factory defaults.

Demos

The **Graphics Demo** option starts a demonstration of the handset's OAI graphical capabilities immediately upon selection.

WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning

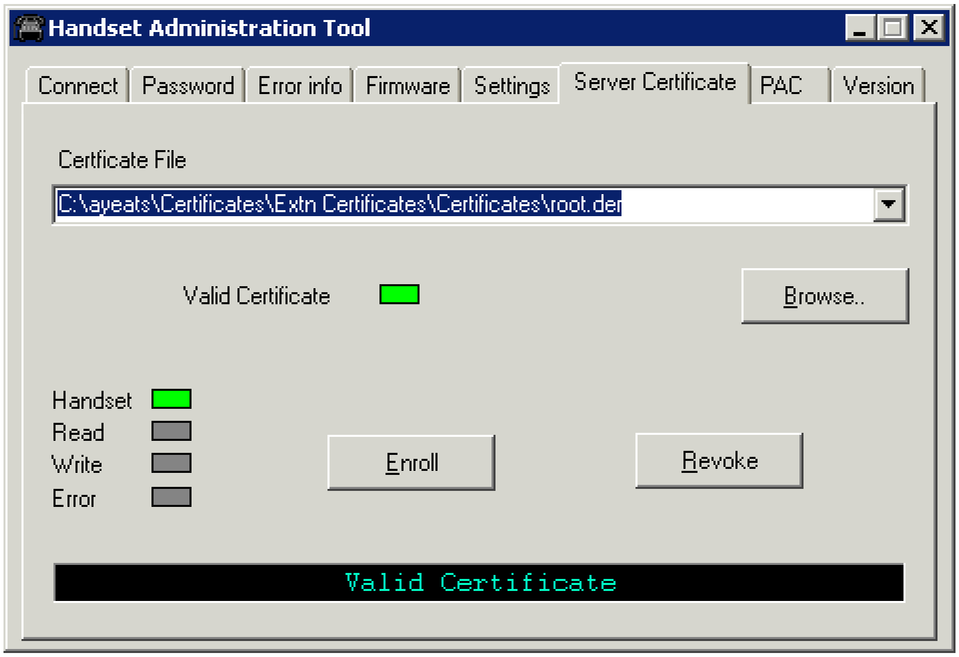
A PEAP certificate or PAC file may be initially provisioned manually through the Admin menu or through the Handset Administration Tool (HAT) since they must be present before the handset can acquire the wireless LAN.

The remote configuration parameters can be set so that the cert can be upgraded or replaced when it expires. Put the cert on the provisioning server and specify either the PAC_FILENAME or SERVER_CERT_FILENAME, where [FILENAME] is the filename of the certificate or file.

PEAP

The Handset Administration Tool (HAT) is used for enrolling a handset with a PEAP certificate in DER format. Only the DER certification format is supported. All other certificate formats need to be converted into the DER format prior to enrolling the handset. Choose the **Certificate** tab and use the file browser to identify the certificate to be loaded. Once chosen, HAT will perform a rudimentary check on the file to make sure the format is DER and that the certificate date is valid. If these tests pass, HAT will indicate that it is valid and enable the **Enroll** button. Click **Enroll** to install the certificate onto the handset.

The screen below shows a valid certificate that has been identified with the file browser.

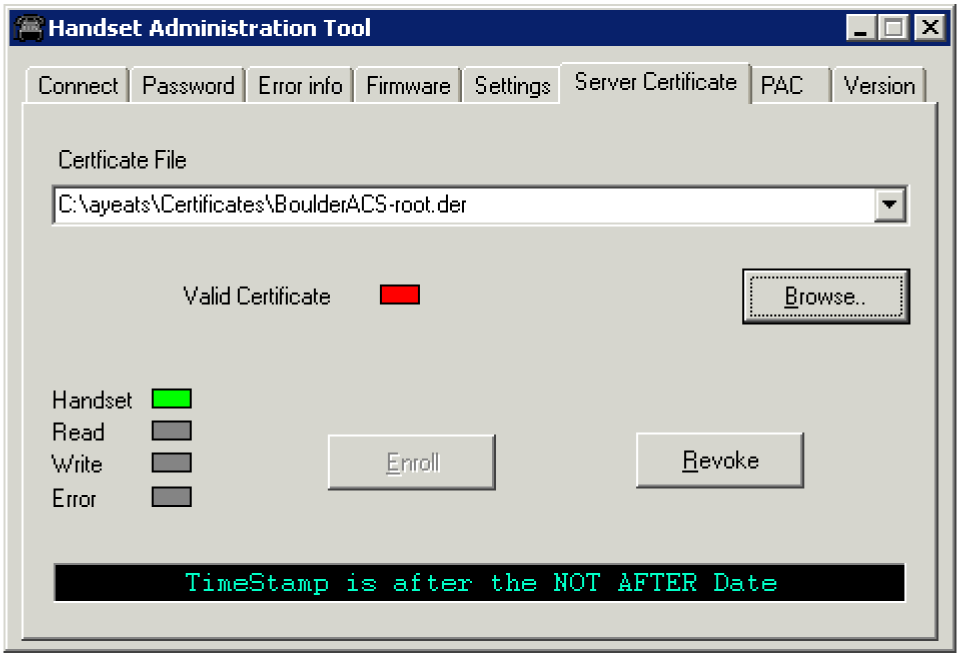


Certficate File

C:\ayeats\Certificates\Extn Certificates\Certificates\root.der

Valid Certificate

The screen below shows a certificate chosen with the file browser, but found to be invalid because it has expired.



Certficate File

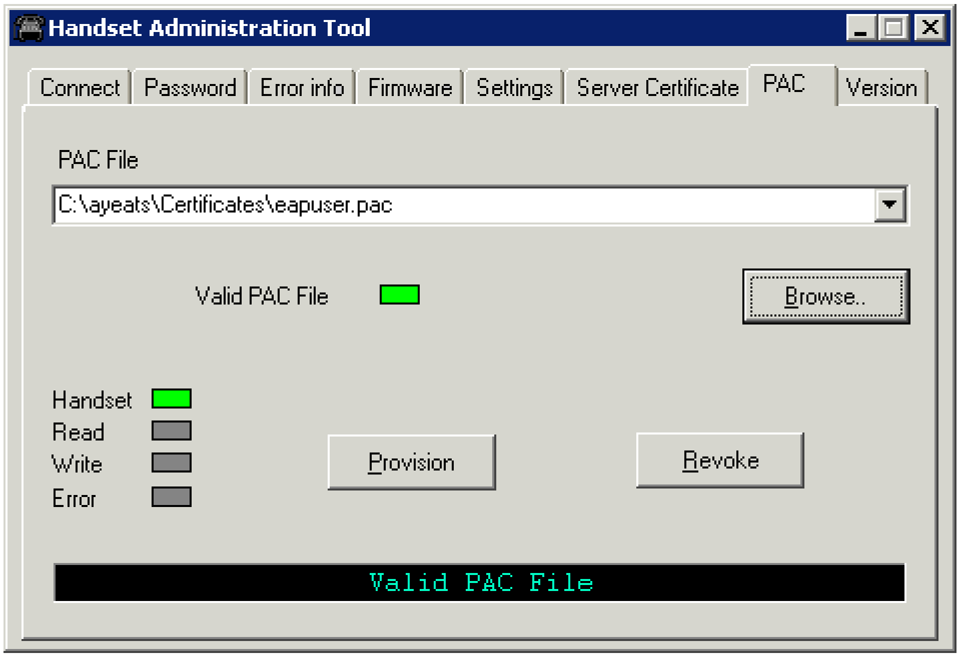
C:\ayeats\Certificates\BoulderACS-root.der

TimeStamp is after the NOT AFTER Date

EAP-FAST

For EAP-FAST, HAT is also used for manually provisioning a handset with a Protected Access Credential (PAC). Choose the PAC file with the file browser. The user will be prompted to enter the password used to generate the PAC as part of its validation process. Once the PAC is considered to be valid, the **Provision** button will be available for installing the PAC onto the handset.

The screen below shows a valid PAC identified with the file browser after a valid password has been entered.



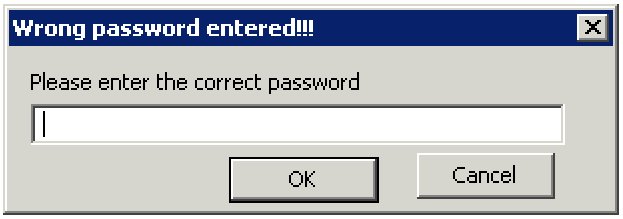
PAC File: C:\ayeats\Certificates\eapuser.pac

Valid PAC File 🟩

Handset 🟩

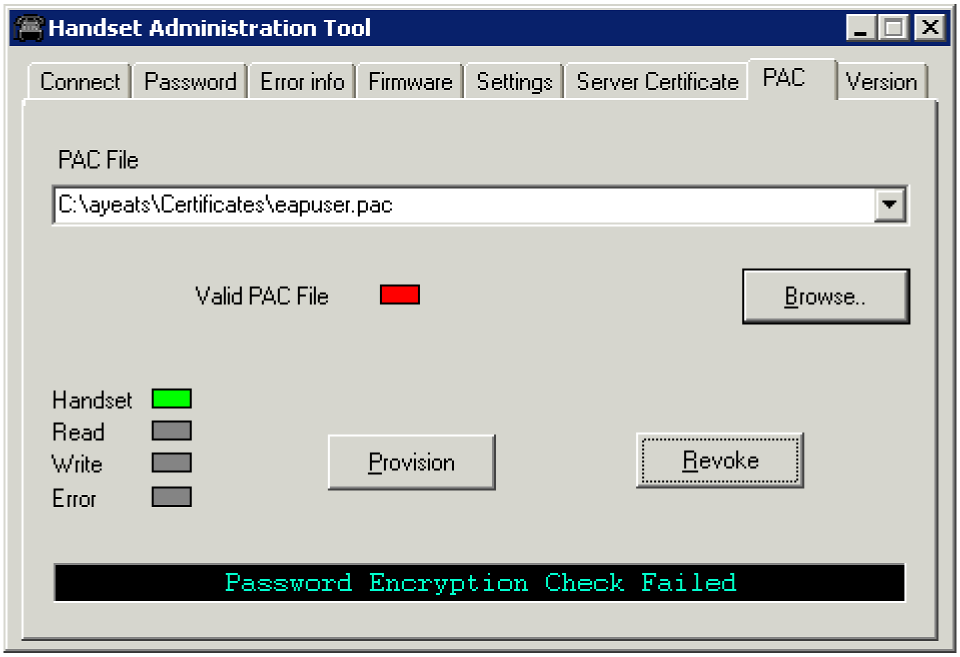
Valid PAC File

The two screens below show the result of entering the wrong password.



Wrong password entered!!!

Please enter the correct password



PAC File: C:\ayeats\Certificates\eapuser.pac

Valid PAC File 🟥

Handset 🟩

Password Encryption Check Failed

If anonymous in-band PAC provisioning is enabled on the RADIUS server, then it is not necessary to download PAC files through HAT. The phone will automatically re-acquire credentials from the RADIUS server over the air.

Admin Menu Default Table

When the **Restore Defaults** option is selected, administrative parameters will be reset to their factory defaults as shown in the table below. The **Telephony Protocol** setting will not change. User parameters will be reset per the user-defined preferences default settings table in the next section.

Menu option	Setting	Sub-option	Sub-sub-option	Default
Phone Config	Language			English
	PTT/Emerg. Button	Emergency Dial		Disabled
		PTT		Disabled
		[if enabled]	Allowed Channels	[all]
			Name Channels	[None set]
			Priority Channel	Disabled
	Time Zone			GMT
	Daylight Saving			DST No Adjust
	Password			Enabled
	Change Password			[n/a]
	Phone Group			0
	Config Mode			Version1
	SIP Registration			[None set]
	Clear Regist.			[n/a]
	OAI			Enabled
	Location Service			
		RTLS		Disabled
		Transmit Interval		10 minutes
		Location Server IP		[None set]
		ELP Port		8552
Network Config	IP Addresses			Use DHCP
	SSID*			[None set]
	WLAN Settings	Custom/Security		None
		Custom/QoS	WEP Key Length	40 bit
			QoS (Mode)	SVP

Menu option	Setting	Sub-option	Sub-sub-option	Default
		Custom/QoS	QoS (DSCP tabs)	WT in call = 46 WT standby = 26 Other = 0
		Cisco FSR	Username Password	[none set]
	Reg. Domain*			[none set]
		802.11 mode		b & b/g mixed
		Transmit Power		30 mW (15 dBm)
Diagnostics	Run Site Survey			[n/a]
	Diagnostics			Disabled
	Syslog Mode			Disabled
	[Error Handling Mode]			Restart on Error

*Minimum requirements for functionality after Restore Defaults:
Set SSID to an available AP and set Regulatory Domain to 01.

6

Testing a Handset

It may be necessary to charge the handset before performing this test. If so, place the handset into the charger for a minimum of two hours before using it.

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

1. Power on the handset by pressing the **END** key. A series of messages will be displayed as the handset acquires the system. The handset should display the user extension.
2. Place a call and listen to the audio quality. End the call by pressing the **END** key.
3. Place a call to the handset and verify ring, answer, clear transmit, and clear receive audio.
4. Use the softkeys to verify all softkey programmed features on the handset.
5. Press the **END** key. Any line indicators should turn off and the extension number display will return.

If any of these steps fails to operate as described, refer to Chapter 11: Troubleshooting for corrective action.

7

Certifying the Handsets

Prior to determining that an installation is complete, test the handsets following the sequence given in the previous Testing a Handset section and conduct a **Site Survey** mode test according to the directions given in Chapter 9: Diagnostic Tools.

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 Chapter 11 *Troubleshooting* 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.

The installer should not leave the site before performing installation verification.

These tests must be performed in typical operating conditions, especially if heavy loads occur. 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 a Polycom service engineer.

The coverage test will also require you to put the handset in **Site Survey** mode and walk the entire coverage area to verify all APs.

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. The site survey discussed here does not replace an RF site survey conducted by professionals who specialize in WLAN design and voice optimization implementations. Polycom offers professional services including RF site surveys.

> The handset's site survey mode is not a replacement for a professional site analysis and should be used only for testing, limited site validation, and troubleshooting.

The handset's site survey mode does not include functionality to allow for analysis or troubleshooting of 802.11n specific WLAN features.

1. Referring to Chapter 11 Diagnostic Tools, section Run Site Survey, put a handset into **Site Survey** in the **Any/Smry** ESSID mode. Walk throughout the site checking for any expected APs or other ESSIDs.
2. Then, walk the site again, in **MyID/Smry** ESSID mode, this time checking that every location has adequate coverage and has good channel allocation.

There should be at least one AP stronger than -the minimum specified in the following tables.

At any point, the strongest AP shown should be on a different channel than the next best choice.

The handset configured for 802.11b requires:

- -70dBm when all 802.11b data rates are available (with only 1Mbps set Required)
- -65dBm when only 2Mbps is set Required and other higher rates enabled
- -64dBm when only 5.5Mbps is set Required with 11Mbps set enabled
- -60dBm when 11Mbps is set required and other 802.11b rates disable or enabled

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s

- The critical factor is the highest data rate set Required or Mandatory. Other 802.11b data rates can be set enabled or disabled. The highest data rate set Required or Mandatory determines the RF power available to the wireless telephone for proper operation.

The handset configured for 802.11g requires:

- -60dBm when all 802.11g data are available (with only 6Mbps set Required)

- -45dBm when 54Mbps is set Required and other 802.11g rates Required, Enabled or Disable

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum “Mandatory” Data Rate
802.11g	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

- The critical factor is the highest data rate set Required or Mandatory. Other 802.11g data rates can be set Required, Enabled or Disabled. The highest data rate set Required or Mandatory determines the RF power available to the wireless telephone for proper operation.

-45dBm when 54Mbps is set Required and other 802.11g rates Required, Enabled or Disable

The handset configured for 802.11g requires:

- -60dBm when all 802.11a data are available (with only 6Mbps set Required)
- -45dBm when 54bps is set Required and other data rates Required, Enabled or Disabled

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum “Mandatory” Data Rate
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

- The critical factor is the highest data rate set Required or Mandatory. Other 802.11a data rates can be set enabled or disabled. The highest data rate set Required or Mandatory determines the RF power available to the wireless telephone for proper operation.

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 through 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 handsets at a site that has not been certified.

8

Using the 8020/8030 Handset

The handset's Battery Pack must be fully charged before its first use. Place the handset into the charger for a minimum of two hours before using it.

For complete operational instructions see *SpectraLink 8020/8030 Wireless Telephone and Accessories User Guide for SIP*.

Startup Sequence

The SpectraLink 8020/8030 Wireless Telephone goes through an initialization sequence at startup. The line icons 1-9 display and count down as the handset steps through this sequence. This is usually very rapid. 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.

Icon	The icon(s) shown in bold turns off when:
12345678**9**	The handset has located and authenticated and associated with at least one AP, and is proceeding to bring up higher-layer networking functions.
1234567**8**	The handset is either configured for Static IP, or if configured for DHCP, the DHCP discovery process has started.
123456**7**	If DHCP is configured, a DHCP response was received which contains a good DNS server configuration.
12345**6**	Note: Used for SVP QoS only and not present when using Wi-Fi Standard QoS or CCXv4. Indicates one of the following possibilities: 1. Static IP configuration 2. SVP Server address found in DHCP option 151 response 3. SVP Server address found via DNS lookup
1234**5**	All networking functions are complete (notably, DHCP), and the handset is proceeding with establishing the SRP link to the SpectraLink 8000 SVP Server.
123**4**	Note: Used for SVP QoS only and not present when using Wi-Fi Standard QoS or CCXv4. The SRP link is established; all network stack initialization is complete, proceeding with

Icon	The icon(s) shown in bold turns off when:
	application-specific initialization.
12**3**	SIP application startup. Icon 3 is extinguished if a generic SIP configuration file is found.
1**2**	Icon 2 is extinguished if a handset specific SIP configuration file is found.
(no icons) **Registering**	Handset is attempting to register each of the specified line contacts.
(no icons) **EXT. XXXXX**	Handset has registered with at least one contact on one proxy server. Initialization is complete. The handset is in standby mode ready to receive and place calls. The line one contact is displayed.

During the last three steps of this process, the handset contacts the provisioning server and downloads general SIP information about the proxy server(s), downloads specific information pertaining to the handset, registers with the SIP server, and verifies handset credentials. Once this process is complete, the handset is ready to use.

If the username and password have not been defined in the **Admin** menu or previously via the Remote Configuration file, you will be prompted to enter both of these items before the extension number can display. The user name must correspond to the configuration file that contains user-specific information. If the file is not found, an error message will appear and the handset will restart.

Handset Modes

Standby mode (on-hook)

In standby mode, the handset 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 handset is conserving battery power and wireless LAN bandwidth.

When an incoming call arrives, the handset rings; the handset enters the active mode and remains in this mode until the call is ended. The call is answered by pressing the **START** key or the **Answ** or **Spkr** softkey. The handset will ring according to user preference as specified in the standby menus. The ringing can be silenced by pressing the **END** key. If you do not wish to accept the call, some SIP call servers support the ability to press the **Rej** softkey. If supported, the SIP call server will redirect the call as configured by the system administrator.

Active mode (off-hook)

The handset is in the active mode when an incoming call is answered.

When an incoming call occurs during an active call, the handset will play the second call ringing sound until the call is answered, the caller hangs up, or the call transfers to voicemail. If the **END** key is pressed, the first call is terminated and the handset reverts to a full ring.

The active mode utilizes the most bandwidth and battery power. To conserve battery resources, return the handset to the standby mode when a call is completed by pressing the **END** key.

Push-to-talk (PTT) mode

The SpectraLink 8030 Wireless Telephones utilize 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.

Configuration menu mode

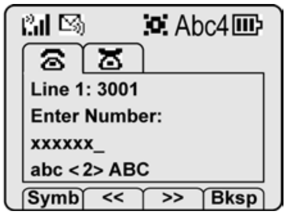
When user preferences are being configured in the Config menu, the handset is on but is not active. If the handset is idle 20 seconds while in the Config menu, it will return to the standby state. Calls can be received but cannot be answered unless you exit the Config menu. If a call was trying to be established while in the Config menu, it will ring as soon as it returns to the standby state.

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.

The Handset Display

When active, the handset screen will display either a call status screen or one of several menu screens. The call status screen has the following format:



Line 1: 3001
Enter Number:
xxxxxx_
abc < 2> ABC

This example shows two call tabs indicating that two calls are in progress. The un-selected call tab indicates that we have put another call on hold. The call-status icon for the selected call indicates that this call is being dialed. The text indicates the selected call is on line 1, extension 3001. Enter Number indicates that the handset is ready to be dialed. Once this call is connected, the connected party's information will appear on the third line, and the fourth line contains help or error messages, as appropriate. The softkeys during this action offer text editing functions.

System icons

Indicator	Function
📶 📶 📶 📶 📶	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.
🔋 🔋 🔋 🔋	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.
✉	The voicemail icon is activated when a new voicemail message is received if the feature is supported by the phone emulation.
✆✕	The missed call icon is displayed when a call is not answered. Such calls can be viewed in the Missed Log. It is active only when Call Logging has been enabled by the system administrator.
🔊	The speakerphone icon displays when the speakerphone is active.
← ↑ ↓ →	Up and down arrows are displayed when the menu has additional options above or below. Left or right arrows are displayed during editing when the cursor may be moved left or right.
📳	The Push-to-talk (PTT) ring icon. A PTT call is coming in.
‼	The priority PTT ring icon. A call is coming in on the priority PTT channel. This call will override any other.
⌖	Location Service icon: indicates the Ekahau Real-Time Location System (RTLS) is enabled.
Locked	Locked indicates that the keypad is locked to prevent accidental activation.

Indicator	Function
	Use the **Unlk** softkey plus the **#** key to unlock it.
[No Service message]	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 service is reestablished.
📥	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.
☒	The download failure icon indicates that the handset has failed to download code because the code is incompatible with the handset hardware. Contact your system administrator should this icon appear.
MUTED	The muted icon indicates the current call is locally muted.
XXXX	During character entry, Indicates current data entry symbol mode.

Call status icons

Indicator	Function
☎	On-hook icon, Solid when in standby mode to indicate that at least one call is on hold. Flashing when incoming call is ringing.
☏	Off-hook icon. Solid when a call is being dialed.
⧗	Hold icon. Call is on hold
✕	Transfer icon. Call is in the process of being transferred
⇆	Audio flowing icon. Audio is flowing both ways on a call.
=	No audio icon. No audio is flowing. Call is terminating or far end hold with audio disable.

NavOK functions

The **NavOK** key acts as a fifth softkey with implicit functionality as follows:

State	NavOK key function
Dialing	Place phone call.
Answering	Answer a second phone call (same or different line)
Holding	Resume audio.
Displaying menu	Select the highlighted menu option.
Displaying call status	Resume audio on the currently selected call and place previous call on hold. If the selected call is ringing, the call will be answered.
Entering login name or login password	Save name or password and proceed with startup.

Softkeys

Softkey	Name	Displayed during…	Press to…
<<	Cursor backward	Entering a dial number.	Move the cursor back one position.
>>	Cursor forward	Entering a dial number.	Move the cursor forward in alphanumeric mode, if the cursor is at the end of the line, adds a space character.
Answ	Answer	Incoming call on the selected line.	Answer the call (equivalent to **START** key).
Bksp	Backspace character	Entering a dial number.	Delete the character prior to the cursor position.
Back	Back one screen	Displaying a menu.	Exit the menu.
End	End Call	An active call on the selected line.	Terminate the call without going back to standby mode.
Favr	Favorites	Prior to entering the first character of a dial number	Activate the Favorites menu.
Logs	Call Logs	Standby mode	Open the Call Log menu.
Hold	Hold	In an active call.	Place the call on hold. The line status shows ☎ when the call is on hold or ⇆ when audio is flowing.
Msg	Message	Initial dial screen when new line is selected and a dial tone is active prior to entering first character of the number to be dialed.	Initiate a call to the specified message center contact address for retrieval or administration of voicemail.
Mute	Toggle muting	In an active call.	Toggle audio transmission to the far end. The line status shows ⇆ when not muted or ⇇ when muted.
OK	OK	Power up registration if username is not configured in **Admin** menu.	Send the username and password to the SIP server for authorization to register the handset.
Redl	Redial	Prior to entering the first character of a dial number.	Redial the last number that was dialed.
Rej	Reject	Incoming call on the selected line.	Reject the incoming call. The SIP server will then redirect the call elsewhere.
Resm	Resume	In an active call and you have placed the call on hold or in standby mode if any call is on hold.	Resume a call that was previously placed on hold or that went on hold when another line was activated.
Save	Save	Entering a dial number as a forward destination.	Save the dial number as the forwarding destination for the selected line.

Softkey	Name	Displayed during…	Press to…
Symb	Symbols	Entering a username or password. Entering the digits of a number.	Select the set of symbols available on the keypad while entering data.
Tran	Transfer	In an active call, to transfer using one key press. Also displayed in the dial screen during a transfer to allow a blind transfer.	Transfer a call. This is the same functionality as FCN-1.

Menus

Line menu

The Line menu allows you to activate a call on a selected line or to view the status of lines.

Pressing the **LINE** key from the active mode displays a menu of line appearances as programmed in the provisioning server configuration file. The **LINE** key can be pressed while the handset is in the standby mode to activate the handset and to activate a new call on the selected line.

The currently selected line is indicated by an asterisk (*****). Lines for which the corresponding proxy server has outstanding new mail are flagged with plus (**+**) characters. The proxy server IP address is displayed on the info line. Lines that should be registered to a proxy but have failed registration for any reason are displayed in faded text and are not selectable from the menu.

Exit the **LINE** display by pressing a line number key to start a new call on the selected line and put any other call on hold, or by pressing the **END** key to exit without starting a new call. Press the **More** softkey to page through additional items on the Line menu.

Symbol menu

The symbol menu allows you to change the set of characters available for data entry through multiple key presses of the dial pad keys.

While dialing a number or entering login information, press the **Symb** softkey to view a menu of possible sets of characters that can be entered using multiple key presses of the dial pad keys. Normally, a simple numeric mode is selected; selecting other symbol modes allows convenient access to the complete printable US ASCII character set. The following table shows what characters are available through repeated key presses in various symbol modes.

Key	Numeric	Alpha-Numeric	Numeric-Alpha	Punctuation
1	1	1 ; : / \ ! ‘	1	@ : 1
2	2	a b c 2 A B C	2 A B C a b c	; , 2
3	3	d e f 3 D E F	3 D E F d e f	& | ` ~ 3
4	4	g h I 4 G H I	4 G H I g h i	( ) 4
5	5	j k l 5 J K L	5 J K L j k l	< > 5

Key	Numeric	Alpha-Numeric	Numeric-Alpha	Punctuation
6	6	m n o 6 M N O	6 M N O m n o	{ } 6
7	7	p q r s 7 P Q R S	7 P Q R S p q r s	[ ] 7
8	8	t u v 8 T U V	8 T U V t u v	‘ “ \ 8
9	9	w x y z 9 W X Y Z	9 W X Y Z w x y z	^ _ 9
0	0	@ - _ 0 = , < >	0 - _	[space] 0
*	. *	. $ * & % + ( )	* .	* . = + / -
#	# @	[space] , ( ) |	# [space]	# ! ? $ %

Favorites menu

The Favorites menu assists you in dialing by providing access to a predefined list of dial numbers. The predefined list can include either complete dial numbers for named parties or partial numbers that need additional data entry. This might be the case, for example, if a PBX feature access code for call forwarding is defined in the favorites list but you need to add the forwarding destination information before sending the call to the PBX to activate the feature.

While in a dialing state, press the **Favr** softkey to display a menu of pre-defined numbers or names that can be dialed (as programmed in the Remote configuration file.) When an item is selected from the list, the dial number is displayed. You may edit or add digits to the displayed number if necessary before pressing the **NavOK** key or **START** to place the call.

FCN menu

The FCN menu is accessible while in the active mode and provides these features:

Transfer

Do Not Disturb

Set/Clear Forward

<OAI>

<OAI>

<OAI>

Items on this menu are accessible through navigation and selection keys or through short-cut keys as displayed with the menu items. OAI functions are automatically added as items at the end of this menu when defined on an OAI server.

Notes on Battery Packs

- Polycom offers the following battery types with increasing capacity: Standard, Extended and Ultra-Extended.
- Battery Pack life will vary depending on handset model and features and system infrastructure.
- Batteries are shipped with a partial charge. Polycom recommends fully charging them before using them in phone operation.
- Maximum Battery Pack performance is achieved after a few charge/discharge cycles.
- If multiple Battery Packs are supplied with your handset, Polycom recommends that each be fully charged upon receipt to prolong battery life. Battery Packs will slowly lose charge if unused. To maintain battery potential, charge unused Battery Packs occasionally or alternate Battery Pack use.
- After a length of time Battery Packs will lose the ability to maintain a charge and to perform at maximum capacity and will need to be replaced. This is normal for all batteries.
- Overnight charging is best done while the handset is turned off.
- If the handset does not charge, clean Battery Pack, charger and handset contacts with an alcohol swab.
- When the handset is properly seated, the backlight comes on briefly to indicate charging has begun.
- Any battery which exhibits swelling, cracking or other abnormality should be disposed of promptly and properly.

User-Defined Preferences

The SpectraLink 8020/8030 Wireless Telephone features a configuration menu ("Config menu") that is available to the user to configure user preferences and display handset information. The Config menu is opened by pressing the **Cfg** softkey from standby mode. See *the* *SpectraLink 8020/8030 Wireless Telephone and Accessories User Guide*.

Config Menu

Config menu	2nd level	3rd level	4th level	5th level	6th level
Lock Keys					
Language	*English Français Deutsch Español Italiano				
User Profiles	Silent Vibrate Loud Soft Custom				
		Set as Active			
		Ring Settings	Telephone Ring Message Alert 1 Message Alert 2		
				Ring Cadence	Off PBX Continuous Short Pulse Long Pulse
				Ring Tone	Tones 1-10
				Ring Volume	Volume ■■■■■■■
				Vibrate Cadence	Off PBX Continuous Short Pulse Long Pulse

Config menu	2nd level	3rd level	4th level	5th level	6th level
		Noise Mode[2]	Normal High Severe		
		Ring in Headset Ring in Speaker			
		Warnings Disable/Enable			
		Key Tones Disable/Enable			
		PTT Disable/Enable			
Phone Settings	Keypad Autolock	Disable 5 Seconds 10 Seconds 20 Seconds			
	Display Contrast	Set Contrast			
	Use Hearing Aid Use No Hearing Aid				
	Play Startup Song Inhibit Song				
	Predial Disable/Enable				
Push-to-talk *	Default Channel	Channel 1 …. Channel 24			
	Subscribed Channels	Channel 1 Channel 2 Channel 3 …. Channel 24			
	PTT Audio Volume	Audio Volume ■■■■■■■■			
	PTT Tone Volume	Tone Volume ■■■■■■■■			

[2] High and Severe noise modes increase microphone, speaker, and ring volume settings above Normal mode baseline. All measures are approximate.

Config menu	2nd level	3rd level	4th level	5th level	6th level
	PTT Vibrate Disable/Enable				
System Info	Phone IP Address				
	Alias IP Address				
	SVP IP Address				
	OAI IP Address				
	Firmware Version				
	Emergency Dial *	Emergency Number Emergency Name			

* **Push-to-talk** and **Emergency Dial** only appear if enabled.

Default settings

Default global settings

Options on the Config menu may be reset to their default values by the **Restore Defaults** option in the **Admin** menu. These are the default global settings that affect every Profile:

Menu option	Default
Language	English
Lock Keys	Unlocked
Display Contrast	Medium
Use Hearing Aid	Disabled
Play Startup Song	Enabled
Predial	Enabled

Default Profile 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:

Setting/profile	Silent	Vibrate	Soft	Loud	Custom
Language	English	English	English	English	English
Ring Cadence	Off	Off	PBX	PBX	PBX
Ring Tone	Tone 1	Tone 1	Tone 1	Tone 1	Tone 1
Ring Volume	1	1	3	7	5
Vibrate Cadence	Off	PBX	Off	Off	PBX
Ring Delay	0	0	0	0	5
Noise Mode	Normal	Normal	Normal	Normal	Normal
Headset/Speaker	Speaker	Speaker	Speaker	Speaker	Speaker
Key Tones	Off	Off	On	On	On
Warning Tones	Off	Off	Off	Off	Off
Push-to-talk	Off	Off	On	On	On
PTT Vibrate	Disabled	Disabled	Disabled	Disabled	Disabled
Emergency Dial	On	On	On	On	On

Push-to-talk must be enabled by the system administrator before it can be activated by the user. If it is not enabled, then it will not appear on the Config menu and will not be "On" for any profile.

PTT Vibrate is available only when Push-to-talk has been enabled by the system administrator.

Emergency Dial must be enabled by the system administrator. If enabled, it will be “On” (or available for use) in every profile.

Diagnostic Tools

Run Site Survey, **Diagnostics Enabled** and **Syslog Mode** are three diagnostic tools provided to assist the LAN administrator in evaluating the functioning of the SpectraLink 8020/8030 Wireless Telephone and the system surrounding it. Diagnostic Tools are enabled in the **Admin** menu.

The **Halt on Error** option in the Admin menu is a diagnostic tool that will cause the handset to stop operating when an unrecoverable error occurs. Error details will be shown on the display and available for download with the Handset Administration Tool and may be captured by the syslog server. Unless the error is a fatal one, normal operation may be resumed by power-cycling the handset.

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 the site survey includes:

- SSID
- Beacon Interval
- AP information regarding support of 802.11d, 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 to the “single SSID” mode and change the softkey back to **Any**.

The display would look like the following for the single SSID mode.

```

111111 -22333 444
111111 -22333 444
111111 -22333 444
111111 -22333 444
Any           Detl
```

Where:

- 111111 – the last two octets of the on-air MAC address for a discovered AP.
- 22 – the signal strength for the specified AP.
- 333 – the channel number of the specified AP.
- 444 – the beacon interval in milliseconds 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 handset. The first has a signal strength of –28 dBm, is configured on channel 2, with a beacon interval of 100 ms. The second has a signal strength of –48 dBm, is configured on channel 6, with a beacon interval of 200 ms. The third has a signal strength of –56 dBm, is configured on channel 11 with a beacon interval of 100 ms.

```

ab7bc8 -28002 100
2ae578 -48006 200
2ae596 -56011 100

Any           Detl
```

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.

```

ab7b  -28002  ALPHA
2ae5  -48006  WSMTES
2ae5  -56011  voice

MyID              Detl
```

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

```

i:bbbbbb  sn  ch  bcn
eeeeeeeeeee  DGHI
rrrrrrrrrrrrr+xx xx
Q:XP  C:vC  sssssss
Any              Smry
```

Where:

- i – index of selected AP (value will be from 0 to 3 inclusive)
- bbbbbb – the last three octets of the BSSID for a discovered AP
- sn – signal strength in –dBm
- ch – channel
- bcn – beacon interval
- eeeeeeeeeee – SSID (up to first 11 characters)
- DGHI – standards supported i.e. 802.11d, 802.11g, etc. in addition to 802.11a and 802.11b.
- 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
- Q:XP
  - X is a hexadecimal representation of the access categories configured with admission control mandatory (ACM). Bit3 = voice, Bit2 = video, Bit1 = background, Bit0 = best effort. For example, if an AP advertises voice and video as ACM then X=c. If all the ACs are set as ACM then X=f. If AP

    - does not have WMM support, this character space will be blank.
    - P is displayed when the AP advertises WMM-PS. If the AP does not advertise WMM-PS then this character space will be blank.
- C:vC
    - v is a decimal number indicating the CCX version advertised by the AP.
    - C is displayed when AP advertises CCKM. If the AP does not advertise CCKM then this character space will be blank.
- ssssssss – Security modes: “None”, “WEP”, “WPA-PSK”, “WPA2-PSK”, “WPA2-Ent”
- 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 handset display indicate AP information is being obtained. A **Waiting** message indicates the system is not configured properly and the handset cannot find any APs.

Solving coverage issues

Coverage issues are best resolved by adding and/or relocating APs. Overlap issues may be resolved by reassigning channels to the APs or by relocating them. See Chapter 11 Troubleshooting, section Access Point Problems for more information.

Diagnostics Enabled

Diagnostics is used to evaluate the overall quality of the link between the handset, AP, and infrastructure side equipment, such as IP PBX, SpectraLink 8000 SVP Server, and gateways. Unlike **Site Survey**, **Diagnostics** is used while the functional code is running, and during a call.

When **Diagnostics** is enabled in the **Admin** menu, the handset can display diagnostic screens any time it is in active mode. However, navigation among calls cannot be done as the **Nav** keys are used to display diagnostic screens.

The display of information is instigated, when in call, by pressing the **Nav◄** or **Nav►** key. Only one of the six diagnostic screens listed below can be shown at a time. Pressing the **Nav** keys multiple times will cycle through the various diagnostics screens and the normal off-hook (IP-PBX) display.

The text portion of each debug display is read from the language translation file, and therefore may be translated to the language the phone would otherwise use. The examples in this document reflect the debug displays as shown in English.

The debug displays refresh once per second, although the information displayed may take longer to update.

Unless otherwise noted, all numbers are displayed as 16-bit unsigned integers, which will wrap from 65535 to 0.

The information provided by **Diagnostics** includes:

Diagnostic display #1:

```
   ........
MissedRcvCnt 00075
MissedXmtCnt 00024
RxRetryCount 00041
TxRetryCount 00142
```

- MissedRcvCnt: The number of 10 ms audio frames for which audio was not present when the phone tried to play it. The phone therefore used its ClearTalk algorithm to fill in the missing audio. Note this is NOT the same as the missed audio payloads reported in the Syslog audio statistics messages.

- MissedXmtCnt: The number of transmit packets dropped for not receiving an ACK from the AP after all retries are exhausted.
- RxRetryCount: The number of packets received with the retry bit set.
- TxRetryCount: The number of packets transmitted as retries.

Diagnostic display #2

```
   ........
Jitter      07500
LastRate     00054
GatewyType   NoA2
TxPower(dBm) 00015
```

- Jitter: Audio jitter in microseconds (us.) This is calculated in the same way as the jitter reported in the audio statistics Syslog message.
- LastRate: The highest transmit date rate in megabits per second (Mbps) at which the phone has successfully transmitted a packet and received an ACK in the last second.
- GatewyType: The gateway type (if any) that the phone is checked in to. This will be one of the following:
  - 2Mb: SVP server operating at 2 Mbps max speed.
  - 11Mb: SVP server operating at 11 Mbps max speed.
  - NoA2: No gateway in use (used with Wifi Qos.)
- TxPower(dBm): Current transmit power in dBm. A table of dBm values and the associated power in milliwatts is shown below:

dbM	mW
7	5
10	10
13	20
15	30
16	40
17	50
20	100

Diagnostic display #3:

```
   ........
9970 060 -67 c011
7020 064 -71 Weak
a340 116 -72 Weak
b2e0 153 -72 Rate
```

The third debug display shows the status and signal strength of the current AP and up to three other candidate APs. The first line shows the current AP, and the next three lines show up to three candidates, if there are that many. If there are fewer than three candidates, extra lines will be blank.

Each line has four fields:

1. Last 4 (hexadecimal) digits of the AP's MAC address.
2. The channel being used by that AP.
3. The signal strength of that AP.
4. For the current AP, the Association Identifier (AID) with the highest two bits set. To extract the actual AID, subtract 0xc000.

For the candidates, a reason code telling why the current AP was a better candidate.

The reason codes are as follows: The numbers in brackets are the associated handoff codes)

- Unkn: Unknown
- Weak: The AP's signal strength was weaker than the current AP, or not enough stronger to justify roaming. {0, 1, 2, 6, 12, 13}
- Rate: The data rates required by the AP were not supported by the phone. {5}
- Full: The AP was already handling as much voice traffic as it could support, and had no additional bandwidth for this call. {7}
- AthT: Authorization timeout. {8}
- AscT: Association timeout. {9}
- AthF: Authorization failed. {10}
- AscF: Association failed. {11}
- SecT: Security timeout. {29, 30, 31, 32, 33, 34, 35}
- SecF: Security failed. {37, 39}
- Cnfg: Configuration failure. (19, 38, 41, 45}

- CCX: AP does not support CCX (52}
- CCKM: AP does not support CCKM {53}
- WMM: APp does not support WMM {54}

Diagnostic display #4:

```
   ........
AssocCount   00002
ReAssocCount 00000
Assocfailure 00000
ReassocFail 00000
```

- AssocCount: The number of times the phone has associated since starting the functional code. This number will always be at least one (the initial association) and higher numbers reflect hard handoffs (where the phone completely lost the AP. Note that hard handoffs in standby are normal, only hard handoffs while in call reflect problems.
- ReAssocCount: The number of times the phone has reassociated since starting the functional code. This is equivalent to the number of soft handoffs.
- AssocFailure: The number of times the phone has failed to associate, defined as the number of times the phone attempts to associate minus the number of times it has successfully associated.
- ReassocFail: The count of reassociation failures, again this is tries minus successes.

Diagnostic display #5:

```
   ........
Sec-ErrCount 00000
LstSeqErrSeq 00000
QosFailCnt   00000
```

- Sec-ErrCount: The number of radio packets that have failed to decrypt properly.
- LstSeqErrSeq: The 802.11 sequence number of the last radio packet (if any) that failed to decrypt properly.
- QosFailCnt: The number of times the QOS admission control negotiation (TSPECS) has failed.

Diagnostic display #6:

```
   ........
EapErrCnt    00000
LstEapErCode 00000
```

- EapErrCnt: The number of EAP (Extensible Authentication Protocol) errors which have happened since the phone was powered up.
- If the EapErrCnt is non-zero, the second line will show a reason code for the last EAP error. These error codes are:
  - 0: No EAP error.
  - 1: Unknown EAP error.
  - 2: EAP type mismatch.
  - 3000: Invalid certificate presented by EAP-AS.
  - 4000: General TLS alert.
  - 5000: Credentials produced by client are invalid.

Syslog Mode

A syslog server must be present on the network in order for the handset to send the log messages and have them saved. The syslog server will be found with DHCP option 7 (log server) if the handset 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 handset is using DHCP and no option 7 is received from the DHCP server, the handset will not send any syslog messages.

Admin menu options:

- ***Disabled** – turns syslog off.
- **Errors** – causes the handset 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).

Messages are formatted like the following example:

```
JAN 21 12:51:26 172.29.76.67:11133>Jan 21 19:50:46.00
0090.7a05.18f6 (172.029.076.067) [0000] Successful
Handoff to 0013.5f59.9970 (-68 dBm) from 0000.0000.0000
(-0 dBm), Reason 24, other APs:0013.5f59.9970 (-68 dBm)
0, TxPO:15 dBm, TxPN:15 dBm
```

The message may be divided into three parts, a header added by the logger program, a header added by the handset, and the message itself.

The header added by the logger program is the first part of the message.
<JAN 21 12:51:26 172.29.76.67:11133>

The information in this header includes the date and time from the logging computer's internal clock, as well as the IP address of the device sending the message. The additional information from p-Logger (11133) is the UDP source port number from the handset.

The handset header in above example is:

Jan 21 19:50:46.00 0090.7a05.18f6 (172.029.076.067) [0000]

The handset header contains the date and time, but this time from the handset's clock, followed by the Phone's MAC (Media Access Control) address, the phone's IP address in parentheses, and a message number in brackets.

If the handset is not configured to use the SNTP (Simple Network Time Protocol) to determine the correct date and time, it will set its clock to midnight, January 1, 2001 on power up.

The message number starts at 0 on power up, and increments for every Syslog message sent. Note that the message number is in hexadecimal.

The remainder of the Syslog message is the message itself, and can be any text, and often includes data as well as the text.

Syslog Messages

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

Message type	Errors	Events	Full
SW ERROR	Yes	Yes	Yes
CHARGER-Placed in charger	No	Yes	Yes
CHARGER-Removed from charger	No	Yes	Yes
CHARGER-Vbat: 4187mV	No	Yes	Yes
CHARGER-Charge complete	No	Yes	Yes
Handoff report	No	Yes	Yes
Failed Handoff	Yes	Yes	Yes
In-Call Syslog Messages			
Call Start	No	Yes	Yes
Call End	No	Yes	Yes
AStat	No	Yes	Yes
AThresh	Yes	Yes	Yes
NStat	No	Yes	Yes
NThresh	Yes	Yes	Yes
Rare Syslog Messages			
CHARGER Battery temp out of range	No	Yes	Yes
CHARGER Battery temp out of range in unit	No	Yes	Yes
Download aborted, code incompatible	Yes	Yes	Yes
DCA initiated radio reset	No	Yes	Yes
LockUpRecovery	Yes	Yes	Yes

Message type	Errors	Events	Full
Probe Recovery	No	Yes	Yes
DCA unknown MgmtAction	Yes	Yes	Yes
txMissedIrptPatchCnt	No	Yes	Yes
SIP Specific Syslog Messages			
Number of methods in header exceed maximum size	Yes	Yes	Yes
SIP <method> request received from <ipaddr>	No	Yes	Yes
SIP <method> request sent to <ipaddr>	No	Yes	Yes
SIP <code> response received from <ipaddr>	No	Yes	Yes
SIP <code> response sent to <ipaddr>	No	Yes	Yes
Call established to <ipaddr>	No	Yes	Yes
Call terminated to <ipaddr>	No	Yes	Yes
Invalid SIP <method> request received from <ipaddr>, rc <code>	Yes	Yes	Yes
Invalid SIP <code> response received from <ipaddr>, rc <code>	Yes	Yes	Yes
Invalid value for <parameter> in generic configuration file	Yes	Yes	Yes
Invalid value for <parameter> in specific configuration file	Yes	Yes	Yes
Value too long for <parameter> in generic configuration file	Yes	Yes	Yes
Value too long for <parameter> in specific configuration file	Yes	Yes	Yes
Download aborted code incompatible. Error=####	Yes	Yes	Yes
DCA unknown MgmtAction category code=###	Yes	Yes	Yes
CHARGER-Battery temp out of range	Yes	Yes	Yes

SNMP

SNMP Get commands may be issued to the handset from an SNMP remote application if SNMP is enabled on the handset. SNMP Set and Trap commands are not supported except for a Set command for a single parameter to allow remotely enabling or disabling SNMP. An SNMP address and public or private community strings must be configured and SNMP enabled on the handset for SNMP Get commands to be processed. An SNMP address and private community string must be configured on the handset for SNMP Set commands to be processed.

- SNMP Enable – SNMP must be enabled for the handset to process SNMP Get commands. SNMP may be enabled or disabled from the Administration Menus or Version 2 configurations files. SNMP may also be enabled or disabled interactively from a remote SNMP application through an SNMP Set command. The only SNMP parameter on the handset supporting a Set command is diagSNMPEnabled. Setting this parameter to TRUE(1) enables SNMP. Setting this parameter to FALSE(2) disables SNMP. The Set command is accepted whether or not SNMP is enabled but is only accepted from devices with an IP address matching one configured in the SNMP IP address(es) and using the SNMP Private Community String.
- SNMP IP address – The handset only responds to SNMP commands originating from devices with one of these IP addresses. In Version 2 configuration files, multiple comma separated IP addresses and/or DNS names may be entered in the settings.txt or phone specific configuration files. A single IP address may be entered from the Administration Menus. If an IP address is entered from the Administration Menus, any previously configured IP address(es) are erased.
- SNMP Public Community String – This value is set to enable viewing of the phone's MIB. The handset responds to SNMP Get commands if the public community string set on the handset matches the community string in the Get command. Ensure the public community string is set to the same value on the handset and the remote SNMP application. The public community string may be set from the Administration Menus or Version 2 configuration files. The string can be 1-32 characters.
- SNMP Private Community String - This value must be set to enable processing of a Set command for the diagSNMPEnabled parameter on the handset. The handset responds to SNMP Set and Get commands if the private community string set on the handset matches the community string in the SNMP command. Ensure the private community string is set to the same value on the handset and the remote SNMP application. The private community string may be set from the Administration Menus or Version 2 configuration files. The string can be 1-32 characters.

If the source IP address of the SNMP command does not match one of the SNMP addresses configured in the handset or the SNMP community string in the SNMP command does not match the community string in the handset, the handset will not respond to the SNMP command.

The handset supports portions of the standard RFC1213 and IEEE802.11 MIBs and the proprietary Polycom-80x0 MIB. The supported MIBs are included with the handset software package. For information on specific MIB parameters refer to the descriptions in the MIBs.

10

Software Maintenance

The SpectraLink 8020/8030 Wireless Telephones use proprietary software programs written and maintained by Polycom Corporation. The software versions that are running on the handsets can be displayed during power on by holding down the **END** button. **Firmware Version** is also an option on the Config menu.

Polycom Customer Service or an authorized dealer will provide information about software updates and how to obtain the software (for example, downloading from a website).

After software updates are obtained, they must be transferred to the appropriate provisioning server located on the LAN to update the code used by the Wireless Telephone.

The handset allows over-the-air transfer of software updates from the provisioning server to the handsets. The download function in the Wireless Telephone checks its software version every time the handset is powered on, when the TFTP server is active. If there is a different version available, the handset immediately begins to download the update.

Upgrading Handsets

After software updates are obtained from Polycom, they must be transferred to the appropriate location in the LAN to update the code used by the handsets.

SpectraLink 8020/8030 Wireless Telephones allow over-the-air transfer of software updates from the designated provisioning server to the handsets. The downloader function in the handset checks its software version every time the handset is turned on. If there is any discrepancy the handset immediately begins to download the update.

Normal Download Messages

When the handset 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:

Message	Description
Checking Code	Handset is contacting the TFTP server to determine if it has a newer version of software that should be downloaded.
Erasing Memory	Handset 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.
Updating Code	Handset 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.

When the update is complete, the handset 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.

Message	Description
Server Busy	Handset is attempting to download from a provisioning server that is busy downloading other phones and refusing additional downloads. The handset will automatically retry the download every few seconds.
TFTP ERROR(x):yy	A failure has occurred during the provisioning 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 = provisioning server did not find the requested file. 02 = Access violation (reported from provisioning server). 07 = provisioning server reported "No such user" error. Check the provisioning server configuration. 16 = No provisioning server address. Check the provisioning server configuration. 81 = File put into memory did not CRC. The handset will attempt to download the file again. FF = Timeout error. provisioning server did not respond within a specified period of time.
Erase Failed	Download process failed to erase the memory in the handset. This operation will retry.
Waiting	Handset has attempted some operation several times and failed, and is now waiting for a period of time before attempting that operation again.

11

Troubleshooting

On occasion, you may run into transmission problems due to any number of factors originating from the wireless LAN. SpectraLink 8020/8030 Wireless Telephones can exhibit transmission problems in several ways. They can cease functioning properly, display error messages, or display incorrect data. When using and troubleshooting handsets, consider the following problem sources to determine the best method of approaching any specific situation.

Access Point Problems

Most, but not all, handset audio problems have to do with AP range, positioning, and capacity. Performing a site survey as described in this document can isolate the AP causing these types of problems. If the handset itself is suspected, conduct a parallel site survey with a handset 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 APs. Service is restored if the user moves back within range. If a call drops because a user moves out-of-range, the handset 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 handset. 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 should have been 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/rearranging APs.

Handset Status Messages

SpectraLink 8020/8030 Wireless Telephone status messages provide information about the SpectraLink 8020/8030 Wireless Telephone's communication with the AP and host telephone system. The following table summarizes, in alphabetical order, the status messages.

Message	Description	Action
☒	Download failure icon	Update handset code in the provisioning server and power cycle the handset.
3 chirps (audio)	Handset is not able to communicate with the best AP, probably because that AP has no bandwidth available.	None. This is only a warning, the call will hand off to the best AP once it becomes available.
802.1X Failure Xxxxxxxxxxxx XXX	When WPA2-Enterprise or Cisco FSR is selected, the handset failed to connect because the user credentials are restricted based on the user account properties. In the case of EAP-FAST, the PAC ID may not match the username. The second line of the error message contains the twelve digits of the AP MAC address and three digits that indicate the error code as defined in RFC2759.	Verify and resolve if the user account has any restrictions such password expired, account restricted/ disabled, or in case of EAP-FAST, the handset PAC and username matching the authentication server.
Address Mismatch	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per Chapter 10: Software Maintenance.
Assoc Failed xxxxxxxxxxxx	x…x = AP MAC address. Handset association was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Assoc Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive association response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Auth Failed xxxxxxxxxxxx	x…x = AP MAC address. Handset authentication was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.

Message	Description	Action
Auth Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive authentication response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Bad Code Type xx Expected Code Type yy	xx, yy = software license types. Handset software does not match current handset license selection.	Download new software from the Polycom website per Chapter 10: Software Maintenance.
Bad Config	Some needed configuration parameter has not been set.	Check all required handset configuration parameters for valid settings.
Bad SSID	The handset has not had an SSID entered.	Statically configure an SSID in the **Admin** menu.
Bad Phintl File	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per Chapter 10: Software Maintenance.
Bad Program File	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per Chapter 10: Software Maintenance.
(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 handset and the battery charge is low. User has 15–30 minutes of battery life left. 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 handset. The handset 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 SpectraLink Battery Pack. Only SpectraLink Battery Packs will work.
Battery Failed	Battery Pack is damaged or incompatible with handset.	Replace the Battery Pack with a new or confirmed SpectraLink Battery Pack. Only SpectraLink Battery Packs will work.
Can't Renew DHCP yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP server is not responding to initial renewal attempt.	Configuration problem. Check the IP address configuration in the DHCP server.

Message	Description	Action
Cert Expired	When WPA2-Enterprise with PEAP authentication is selected, the handset failed to connect due to an expired certificate on the handset or authentication server.	Verify that the NTP server is properly configured with the correct time. Verify that the certificates loaded on the handset and authentication server have valid start/end dates by looking at “valid to” field from “validity” data in certificates. If any of the certificates have expired replace them with new certificates.
Cert Invalid	When WPA2-Enterprise with PEAP authentication is selected, the Wireless Telephone failed to connect to the network because the certificate start date is in the future.	Verify that the NTP server is properly configured with the correct time. Verify that the certificates loaded on the handset and authentication server have valid start/end dates by looking at “valid from” field from “validity” data in certificates. If any of the certificates have expired replace them with new certificates.
Charging …	The handset is charging in the desktop charger.	No action needed.
Charge Complete	The handset is now fully charged.	No action needed.
Charger Error	The handset has detected a problem with the charging circuitry.	Allow the charger and battery to cool. If the problem persists, try a new or confirmed battery. If the problem still persists, contact technical support and report the error.
Checking Code	Handset is contacting the provisioning 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, power off and contact customer support for a replacement phone.
Checking DHCP IP	The handset is retrieving DHCP information from the DHCP server.	None. This is informational only.
CRC Code Error	The software which has been provisioning 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.
Code Mismatch!	The software loaded into the handset is incorrect for this model handset.	Verify the License Management value is correct. Replace the software image on the TFTP server with software that is correct for the handset model.

Message	Description	Action
Config reboot	Appears when the handset reboots after the remote configuration if a parameter changed that requires the handset to reboot (for instance, it the ESSID or the Security method is changed, the handset has to reboot to start using the new values). This message appears for a few seconds while the handset is rebooting	Informative only. No action required.
DCA Timeout	The handset has detected a fault for which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off, then on again. If error persists, contact Polycom Technical Support and report the error.
DHCP Error (1-5)	DHCP Error 1.	The handset cannot locate a DHCP server. It will try every four seconds until a server is located.
	DHCP Error 2.	The handset has not received a response from the server for a request for an IP address. It will retry until a server is found.
	DHCP Error 3.	The server refuses to lease the handset an IP address. It will keep trying.
	DHCP Error 4.	The server offered the handset a lease that is too short. The minimum lease time is 10 minutes but Polycom Engineers recommend at least one-hour minimum lease time. The handset will stop trying. Reconfigure the server and power cycle the handset.
	DHCP Error 5.	Failure during WEP Key rotation process (proprietary feature).
DHCP Lease Exp yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP is not responding to renewal attempts (at least one renewal succeeded).	The handset 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 handset will attempt to negotiate a new lease, which will either work, or it will change to one of the above DHCP errors (1 through 4).
DHCP NACK error yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP server explicitly refused renewal.	The DHCP lease currently in use by the handset is no longer valid, which forces the handset to restart. This problem should resolve itself after the restart. If it does not, the problem is in the DHCP server.
DL Not On Sector	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per Chapter 10: Software Maintenance.

Message	Description	Action
DO NOT POWER OFF	The handset is in a critical section of the software update.	None. Do not remove the Battery Pack or attempt to power off the phone while this is displayed. Doing so may render the handset inoperable.
Duplicate IP	The handset has detected another device with its same IP address.	If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using Static IP, check that the handset was assigned a unique address.
Erase Failed	Download process failed to erase the memory in the handset.	Operation will retry but may eventually report the error "int. error: 0F" Power cycle the handset.
Erasing Memory	Handset has determined that a download should occur and is erasing the current software from memory.	None. When the progress bar fills the display line the erase operation is complete. Do not turn the handset off during this operation.
Files Too Big	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per *Software Maintenance*.
Flash Config Error	Handset internal configuration is corrupt.	Perform "Restore Defaults" operation via Admin menu (or re-program with Configuration Cradle).
Initializing …	The handset is performing power-on initialization.	None. This is informational only.
Initializing SIP	The handset is performing a power-on initialization of the SIP application. The phone is initializing its data structures and attempting to access the SIP provisioning server and download the SIP configuration files.	None. This is informational only.
Internal Err. # #	The handset has detected a fault from which it cannot recover.	Record the error code so it can be reported. Turn the handset off then on again. If error persists, try registering a different handset to this telephone port. If error still persists, contact Polycom Technical Support and report the error.

Message	Description	Action
Invalid Usr/Pwd	When WPA2-Enterprise or Cisco FSR is selected, the handset failed to connect due to incorrect device credentials or unavailability of authentication server. If the error is because of the incorrect device credentials then the username or password doesn't match with those configured on the authentication server.	Verify that the required credentials {username, password} are created on the authentication server and should match the handset. This may also happen when the authentication server is not reachable while doing the EAP authentication. Make sure the authentication server is active and reachable from the WLAN access points/controller at all times.
Multiple GW Res	More than one SpectraLink 8000 SVP Server has responded.	Caused by two or more handsets sharing the same IP address. Assign unique IP addresses to each handset.
Multiple SVP Reg yyy.yyy.yyy.yyy	y…y = SVP IP address Handset received responses from multiple SVP Servers; displays IP address of one responding SVP Server.	This can happen if the handset has been reconfigured to use a different SVP server and then powered on before the previous server has had time to determine that the handset is no longer connected to it. The problem should go away after about 30 seconds.
Must Upgrade SW!	Handset software is incompatible with hardware.	Download new software from the Polycom website per Chapter 10: Software Maintenance.
Net Busy xxxxxxxxxxxx	x…x = AP MAC address. Handset cannot obtain sufficient bandwidth to support a call; displays MAC of failing AP.	Try the call again later.
No 802.11a Sub-bands Enabled	'a' radio selected but no sub-bands are enabled	Configure 'a' radio sub-bands from **Admin** menus
No 802.11 Sub-bands Enabled	'b/g radio selected but no sub-bands are enabled	Configure 'b/g' radio sub-bands from **Admin** menus
No APs Heard	The handset is unable to hear beacons/probes from any AP in the network in site survey mode.	Verify that network is properly configured and the handset is able to hear beacons from the AP.
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DHCP is operational and connected to WLAN or use Static IP configuration in the handset.
No ESSID	Attempted to run Site Survey application without an ESSID set.	Let handset come completely up. Statically configure an ESSID in the **Admin** menu.
No Func Code	Handset software download files are incorrect or corrupted.	Reconfigure the handset to gain access to the WLAN and download new code.
No Host IP	The handset is configured for "static IP" (as opposed to "use DHCP") and no valid host IP address (the handset's IP address) has been entered.	Enter a valid IP address in the configuration settings or change to "use DHCP."

Message	Description	Action
No IP Address	Invalid IP.	Check the IP address of the handset and reconfigure if required.
No Net Access	Cannot authenticate / associate with AP.	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.
No Net Found No APs	This indicates that the handset cannot find any access points and has no additional information to display as to why. Possible problems are enumerated below.	
	No radio link.	Verify that the AP is turned on.
	No ESSID: Auto-learn not supported (or) incorrect ESSID.	Verify the ESSID of the wireless LAN and enter or Autolearn it again if required.
	AP does not support appropriate data rates.	Check the AP configuration against Configuration Guide for AP.
	Out of range.	Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the ESSID of this handset.
	Incorrect Security settings.	Verify that all the Security settings in the handset match those in the APs.
No Net Found xxxxxxxxxxxx yy	x…x = AP MAC address. yy = AP signal strength. Handset cannot find a suitable AP; displays MAC and signal strength of "best" non-suitable AP found.	Check AP and handset network settings such as ESSID, Security, Reg domain and Tx power. Ensure APs are configured per *VIEW Configuration Guide* for AP Try Site Survey mode to determine a more specific cause.
No Net Found No CCX APs	The Wireless Telephone is configured for CCX compatible operation, but cannot find an access point that is advertising CCX capability.	Check the AP configuration against *VIEW Configuration Guide* for AP.
No Net Found No CCKM APs	The Wireless Telephone is configured to use CCKM for fast and secure handoffs, but cannot find an access point that is configured appropriately.	Check the AP configuration against *VIEW Configuration Guide* for AP.
No Net Found No WMM APs	The Wireless Telephone is configured to use Wi-Fi Standard QoS, but cannot find an AP configured appropriately.	Check the AP configuration against *VIEW Configuration Guide*.
No PBX Response	The handset has exceeded its retransmission limit with no ACK response from proxy server.	Verify that proxy server IP address and port are properly configured.
No Reg Domain	Regulatory Domain Not Set.	Configure the Regulatory Domain of the handset.

Message	Description	Action
No Server IP	In the case of static IP configuration, the handset failed to find the call server IP.	Verify that call server info is properly configured on the handset.
No SIP user file	The phone is attempting to download a SIP configuration file from the provisioning server. A file must be available for the username that was entered either in the **Admin** menus or as requested at power-on.	Ensure a SIP configuration file is available on the provisioning server and is named as specified (sip_username.cfg).
No SVP IP	The handset is configured for "Static IP" (as opposed to "use DHCP"), and no valid SpectraLink 8000 SVP Server address has been entered.	Enter a valid SpectraLink 8000 SVP Server IP address in the configuration setting or change to "use DHCP."
No SVP Response yyy.yyy.yyy.yyy	y…y = SVP Server IP address. Handset has lost contact with the SVP Server.	This may be caused by bad radio reception or a problem with the SpectraLink 8000 SVP Server. The handset will keep trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the handset will restart. Report this problem to the system administrator if it keeps happening.
No SVP Server	Handset can't locate SpectraLink 8000 SVP Server. SpectraLink 8000 SVP Server is not working. No LAN connection at the SpectraLink 8000 SVP Server.	IP address configuration of SpectraLink 8000 SVP Server is wrong or missing. Check error status screen on SpectraLink 8000 SVP Server. Verify SpectraLink 8000 SVP Server connection to LAN.
No SVP Server No DNS Entry	Handset unable to perform DNS lookup for SVP Server, server had no entry for SVP Server.	The network administrator must verify that a proper IP address has been entered for the SVP Server DHCP option 151.
No SVP Server No DNS IP	Handset unable to perform DNS lookup for SVP Server, no IP address for DNS server.	The network administrator must verify proper DHCP server operation.
No SW Found	A required software component has not been identified.	Check that the handset license type has a corresponding entry in the slnk_cfg.cfg file. Check that the pd11sid.bin and pi110000.bin entries exist in under this license type in the slnk_cfg.cfg file.
No TFTP Response	The handset could not get the provisioning server to respond.	The handset will continue to boot without checking if its current code is the latest available. Check that the provisioning server is operational. If the Wireless Telephone is using DHCP, check that the DHCP options are set correctly.

Message	Description	Action
No WPA PassPhrase	This error only appears when the Admin Menus are exited. The handset is configured for WPA-PSK or WPA2-PSK and no pass phrase or shared key has been entered.	Enter the pass phrase or pre-shared key and restart the handset
Not Installed!	A required software component is missing.	Check that all required software files are on the provisioning server, if over-the-air downloading is being used. If the error repeats, contact Polycom Technical Support.
Press END	The far end of a call has hung up.	Hang up the near end.
Press END to quit	The handset is waiting to acquire bandwidth required for voice communication.	Press **END** or wait until bandwidth is available.
Prom Bad Length	The handset software downloaded files that are incorrect or corrupted.	Download new software from the OEM site per Chapter 10: Software Maintenance.
Registering	The handset has completed initialization of the SIP application and is attempting to register lines to the SIP proxy servers.	If registrations are failing, the phone can stay in this state for a considerable length of time. After the phone leaves this state, press the **LINE** key to view what lines have failed to register. Ensure usernames and passwords have been entered in administrative menus for registrations that have failed and that proxy information is correct in the SIP configuration files.
RTP Open Failed	The handset attempted to open an RTP port for audio but was unsuccessful.	Verify that SpectraLink 8000 SVP Server capacity has not been exceeded.
Select License	The correct protocol has not been selected from the license set.	Using the **Admin** menu, select one license from the set to allow the phone to download the appropriate software.
Server Busy	Handset is attempting to download from a provisioning server that is busy downloading to other devices and refusing additional downloads.	None, the handset will automatically retry the download every few seconds.
SIP Login	Prompt for login information – username and password.	At power-on initialization, no username was detected in the **Admin** menu items for SIP registrations. Enter a valid username and password for an existing SIP configuration file.
Skt Open Fail	Socket open fail. Occurs when the handset attempts to open a connection to the proxy server but fails.	Verify that SpectraLink 8000 SVP Server capacity has not been exceeded.

Message	Description	Action
Service Rej.	The SpectraLink 8000 SVP Server has rejected a request from the handset.	The handset will restart and attempt to re-register with the SpectraLink 8000 SVP Server, which should fix the problem. Report to your administrator if it keeps happening.
Storing Config	Handset is storing changes to handset configuration.	None. Informational only. The handset may display this briefly following a configuration change or software download.
SVP Service Rej.	The SpectraLink 8000 SVP Server has rejected a request from the handset.	The handset will restart and attempt to re-register with the SVP Server, which should fix the problem. Report to your administrator if it keeps happening.
System Busy yyy.yyy.yyy.yyy	y…y = SVP Server IP Address. SVP Server has reached call capacity.	All call paths are in use, try the call again in a few minutes.
System Locked (with Busy Tone)	SpectraLink 8000 SVP Server is locked.	Try call again later, system has been locked for maintenance.
TFTP ERROR(x):yy	A failure has occurred during a provisioning software download. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are: 01 = provisioning server did not find the requested file. 02 = Access violation (reported from provisioning server). 07 = provisioning server reported "No such user" error. 16 = No provisioning server address. 81 = File put into memory did not CRC. FF = Timeout error. provisioning server did not respond within a specified period of time.	Error code 01, 02, 07, or 16 - check the provisioning server configuration. Error code 81, the handset will attempt to download the file again. For other messages, power off the handset, then turn it on again to retry the download. If the error repeats, note it and contact Polycom Customer Support.
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to Polycom.
Unknown xx:yy:zz	A phrase is missing from the phintl file.	Download new software from the Polycom website per Chapter10: Software Maintenance.
Updating …	The handset is internally updating its software images.	None. The handset may do this briefly after a download. This is informational only.

Message	Description	Action
Updating Code…	Handset 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.	None. When the progress bar fills the display line the update operation is complete on that file. Do not turn the handset off during this operation.
Wait for bandwidth	The phone is waiting for bandwidth sufficient for voice communication.	No action required. You will have the option of pressing **END** to abort the phone call.
Waiting…	Handset has attempted some operation several times and failed.	None. The handset is waiting for a specified period of time before attempting that operation again.
Wrong Code Type	The software loaded into the handset is incorrect for this model phone.	Replace the software image on the provisioning server with software that is correct for the handset model.

12

Appendix A: Regulatory Domains

This table details the specifications for regulatory domain settings. Polycom recommends that you check with local authorities for the latest status of their national regulations for both 2.4 and 5 GHz wireless LANs.

Domain Identifier	802.11 Mode	Band	Channels	DFS Required?	Max. Power Limit (peak power)	Countries
01	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	US Canada Brazil
	a	5.1500 – 5.2500 GHz	36 – 48	No	50mW (+17dBm)	
		5.2500 – 5.3500 GHz	52 – 64	Yes	100mW (+20dBm)	
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		
02	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Europe Australia New Zealand UAE
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.7250 GHz	100 – 140	Yes		
03	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Japan
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
04	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Singapore
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
05	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Korea
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.6500 GHz	100 – 124	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		

Domain Identifier	802.11 Mode	Band	Channels	DFS Required?	Max. Power Limit (peak power)	Countries
06	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	Taiwan
	a	5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8500 GHz	149 – 165†	No		
07	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Hong Kong
	a	5.1500 – 5.2500 GHz	36 – 48	No	50mW (+17dBm)	
		5.2500 – 5.3500 GHz	52 – 64	Yes	100mW (+20dBm)	
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		
08	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	Mexico India
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.7250 – 5.8500 GHz	149 – 161	No		

† Channel 165 is not currently supported on the handset when the UNI-3 (5.7250 – 5.8250) band is enabled for 802.11a.

Appendix B: Remote Configuration Parameters Definition

Version 1 Configuration Parameter Definition

Use the following parameters when programming the Version 1 Configuration files. See the sample configuration files in the next section for more detailed information.

See the table footnotes at the end of the table.

Parameter	Allowable Values	Description	Notes
CONFIG_MODE	version1 version2	If this statement is encountered and is set to Version 2, the phone will stop processing the configuration files and immediately reboot and begin using version 2 configuration mode.	

PROXYn_ADDR	xxx.xxx.xxx.xxx:pppp
	or
		Proxy address. One proxy address is required but additional proxy addresses may be used to register secondary line appearances.	n = 1, 2, 3
			xxx.xxx.xxx.xxx = IP4 address
			pppp = port (optional, 5060 is the default)

	proxyname:pppp		proxyname = computer name (DHCP only)

PROXYn _DOMAIN	Domain name	Domain served by this proxy server.	n = 1, 2, 3
			DOMAIN = [example: spectralink.com]
			Can be omitted if a specific proxy domain name is not defined at the proxy server. If omitted, defaults to the IP address of the proxy server (see above).

Parameter	Allowable Values	Description	Notes
PROXYn_TYPE	Asterisk[1] Asterisk_Compatible NECSIP NECThirdParty Toshiba Mitel InIn Pingtel Shortel CCME DeltaPath	Specify the manufacturer of each defined proxy server. See sample files for vendor notation.	n = 1, 2, 3 Used by the handset to perform proxy-specific actions based on known behavior for specific proxy types. Only the three shown values may be used.
PROXYn_ KEEPALIVE_SECS	0 or 10 to 3600 seconds	Specifies that the handset should send keepalives to the PROXYn server.	n = 1, 2, 3 The keepalive interval defaults to ZERO which disables the feature. When specified, the interval can be set to zero or to 10 to 3600 seconds. If a keepalive fails to get a response within the SIP 32 second timeout, then keepalives are terminated until the next successful registration to the proxy.
PROXYn_ KEYPRESS_2833	enable disable	Controls generation of in-stream RFC2833 formatted key press events. Match what is required by your PBX. See RFC2833. See sample .cfg file for more information.	n = 1, 2, 3
PROXYn_ KEYPRESS_INFO	enable disable	Controls generation of SIP INFO requests to the SIP server for keypress events..	n = 1, 2, 3
PROXYn_HOLD_IP0	enable disable	Controls setting of the media stream IP destination address to 0 (zero) when a call is put on hold.	n = 1, 2, 3 Use for compatibility with older SIP servers that may not recognize newer stream attribute parameters for HOLD status.
PROXYn_PRACK	enable disable	Enables reliable provisional responses to INVITE requests	n = 1, 2, 3

Parameter	Allowable Values	Description	Notes
PROXYn _ MAIL_SUBSCR	name@xxx.xxx.xxx.xxx or sip:name@domain	Contact to whom the handset should subscribe for mail notification. See sample .cfg file for more information.	n = 1, 2, 3 name = mail server contact name. xxx.xxx.xxx.xxx = IP4 address. Domain where the mail resides. This command is only necessary if the proxy server does not automatically create and renew subscriptions when the handset registers.

PROXYn_ MAIL_ACCESS	name@xxx.xxx.xxx.xxx
	or
	sip:name@domain
		Contact to whom the handset should invite to access the mail center. This is the main voicemail dial number.	n = 1, 2, 3
			name = mail server contact name.
			xxx.xxx.xxx.xxx = IP address
			Domain where the mail resides.

PROXYn_ REREG_SECS	35 seconds to 3600 seconds	The requested expiration interval in REGISTER request messages.	n = 1, 2, 3 If the server has a lower maximum setting or a higher minimum setting than that requested, the server response takes precedence. See example file

PROXYn_FAILOVER IP_ADDRESS	xxx.xxx.xxx.xxx:pppp
	or
	proxyname:pppp
		The IP address of the Interactive Intelligence failover call server.	n = 1, 2, 3
			xxx.xxx.xxx.xxx = IP4 address
			pppp = port (optional, 5060 is the default)
			proxyname = computer name (DHCP only)

AUTH [see warning note below]	username;password	Credentials. In general credentials are needed for each registered line.	username = The dial number or string that identifies the line appearance. Generally an extension or phone number. password = a secure password created by the system administer which enables a handset to register and/or function.

Parameter	Allowable Values	Description	Notes
CODECS	codec1, codec2 e.g. g711u, g711a, g729	Comma-separated list of supported codecs in order of preference.	Defaults to “g711u, g711a”. If either is omitted it will be added to the end of the list.
LINEn	username	The dial # or name. All LINEn user names should be unique for a given LINEn_ PROXY. This may be enforced in future software revisions.	n = 1, 2, 3, 4, 5 The registered contact becomes: sip:username@domain
LINEn _PROXY	i	SIP proxy server for this line.[2]	n = 1, 2, 3, 4, 5 i = the number of the proxy server 1, 2, 3. LINEn_PROXY can be omitted if the line is not to be registered and you wish to do direct phone to phone calls.
LINEn _SECONDARY_ PROXY	i	SIP secondary proxy server for this line.	n = 1, 2, 3, 4, 5 i = the number of the proxy server 1, 2, 3. LINEn_SECONDARY_ PROXY is only valid if the proxy types for both this definition and LINEn_ PROXY are MITEL, otherwise it will be ignored.
LINEn _CALLID	callerid	String that displays at the far end.	n = 1, 2, 3, 4, 5 callerid = the text that will display as the caller ID on the called handset.
FAVORITE	Dialstring;identifier	Phonebook list of numbers accessible from the Favorites menu. Favorites in the allusers file will be present in the Favorites on all handsets. See sample .cfg file for more information.	Up to 15 entries permitted which may be divided between generic and phone specific files. Dialstring = complete SIP URI or local extension # Identifier = name. If omitted, the dial string appears on Favorites menu.
CALL_LOGGING	enable disable	When enabled, permits the handset to capture the 20 most-recent incoming, answered and missed calls in local logs.	

Version 1 Configuration Table Notes

1. For up-to-date Asterisk voicemail commands, go to: http://www.voip-info.org/wiki/index.php?page=Asterisk+cmd+VoiceMailMain
2. WARNING: providing credentials by using the AUTH parameters in the configuration files is a security risk and should be avoided by entering usernames and passwords in **Admin** menu or by allowing the user to login at startup time. Credentials entered here are in plain text and accessible by anyone who can access the provisioning server. Credentials stored in the SIP server or in the handsets are protected.

Version 2 Configuration Parameter Definition

The following table describes the parameters that can be used in the Version 2 configuration files. The generic file is typically named settings.txt. Note that double quotes can be used around the entire value that a parameter is set to, with the exception of the SIP_FAVORITES parameter. They can also be used to denote the NULL string (“”). They cannot be used any other way except on the SIP_FAVORITES parameter. See the sample file for more information.

Persistency

The handset saves configuration information in its memory and uses it if the value is not available otherwise. This persistence is true for all the parameters.

In order to remove a parameter that was previously set and no longer needed, one must clear it or set it back to the default in the configuration file. The null string (“”) can be used to clear out any parameter that is a string or an IP address. Other parameters, such as a port address, have to be deliberately set back to the default to get rid of a particular definition. For parameters that are enabled or disabled, just removing them from the configuration file does not disable them if they were previously enabled, you must deliberately set them to 0 to disable them (for instance, the OAI_ENABLE parameter).

In some installations, it is advisable to set all user specific values, such as lines, to the null string rather than leaving them unconfigured.

Precedence and how the handset initializes and uses the supplied parameters

If the handset is configured to use DHCP, it initializes using the values supplied by DHCP. Note that these values supplied by DHCP are used by the handset, but they are not stored in persistent storage on the handset. If any of the requested parameters are not supplied by DHCP, values for those same parameters in persistent storage (if any) will be used.

If the handset is not configured to use DHCP, it initializes using values from persistent storage on the handset.

Next, the handset reads in the generic configuration file if possible. Any values specified in this generic configuration file are saved in persistent storage on the handset (overwriting any previously saved data). The handset will start using the new values immediately as long as these are values that do not require a configuration reboot.

Then the handset reads in the handset specific configuration file if possible. Any values specified in this handset specific configuration file are saved in persistent storage on the handset (overwriting any previously saved data). The handset will start using the new values immediately as long as these are values that do not require a configuration reboot.

If any of the parameters that can cause a configuration reboot (see table) were modified by either of the configuration files, the handset will now reboot and initialize using the values supplied by DHCP (if configured to use DHCP) and the latest values of all other parameters.

Configuration reboot

If a parameter is changed by one of the configuration files and the handset cannot begin to use that parameter without rebooting (see table below for these parameters), the handset will reboot when it finishes reading in and processing the configuration files. The handset will not prompt the user for login info and it will not re-read the configuration files, it just reboots and starts using all the new configuration values.

The handset does not reboot if none of these indicated parameters have changed. It does not reboot for changes in other parameters (those that are not indicated in the table as parameters that cause a reboot).

Certain phone parameters allow values that the installed PBX may not support. The PBX restrictions should be taken into account when configuring the handsets using these SIP parameters. For instance, a PBX may support up to 13 digits for a username value where the phone itself has broader options. In this case, you must limit your options to those supported by the PBX. Other such situations may exist in your facility. Be sure to configure values that all components used by the phones can recognize.

Parameter	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot
CONFIG_MODE	version1, version2	version1		yes
SYSLANG[4]	English, Francais, Deutsch, Espanol, Italiano	English		no
GMTOFFSET	"0:00"[5]	00:00		yes
DSTADJUST	none, usa, aus, euro	none		yes
PROCPSWD	1-16 digits or NULL (no password)	123456		no
PROTECTED_SPEEDDIAL _NUMBER	1-32 chars or NULL[6]. Valid chars: 0123456789()x-+# and space.	Null		no
PROTECTED_SPEEDDIAL_NAME	1-18 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	Null		no
PROTECTED_SPEEDDIAL _KEY	1 character or NULL. Valid chars: 0123456789*#^ where ^ stands for the volume buttons and the rest for dial pad keys.	Null		no
TFTPSRVR[4]	ip addr or NULL[6]	not set	static	no
LOGSRVR	ip addr or NULL[6]	not set	static	yes
SNTPSRVR	ip addr or NULL[6]	not set	static	yes
SVPSRVR	ip addr or NULL[6]	not set	static	yes
OAISRVR	ip addr or NULL[6]	not set	static	yes
DNSSRVR	ip addr or NULL[6]	not set	static	no
DOMAIN (for dns)	1-63 chars, no spaces or NULL[6]	Null	static	no
HTTPSRVR	ip addr/DNS name list or NULL[6] - up to 255 chars	not set		no

Parameter	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot
HTTPPORT	number from 0-65535	80		no
HTTPDIR	0-127 chars, no spaces or NULL[6]	none		no
WLAN_ESSID	1-32 chars[7]	not set		yes
WLAN_USE_CCX	0,1 (0=custom, 1=use CCX))	0		yes
WLAN_SECURITY	none, wep, wpa2psk, wpapsk, fsr, wpa2e	none		yes
WEP_AUTHENTICATION	openSystem, sharedKey	open system	wep	yes
WEP_DEFAULT_KEY	1-4	1	wep	yes
WEP_KEY_LEN	40bit, 128bit	40bit	wep	yes
WEP_KEY1	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes
WEP_KEY2	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes
WEP_KEY3	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes
WEP_KEY4	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes
WPA_TYPE	passphrase, psk	passphrase	wpa2psk, wpapsk	yes
WPA_PASSPHRASE	1-63 chars or NULL[6]. Illegal Characters : ascii 34("),ascii 63 (?),ascii 96 (`).	not set	wpa2psk, wpapsk	yes
WPA_PSK	64 hex chars or NULL[6]	not set	wpa2psk, wpapsk	yes
WPA2E_AUTH	eapfast,peap	eapfast	wpa2e	yes

Parameter	**Allowable values**[1]	**Default**[2]	**Assoc info**[3]	**Causes reboot**
WPA2E_FAST_HANDOFF	cckm, okc	cckm	wpa2e	yes
WLAN_SEC_USERNAME	1-32 chars or NULL[6]. Valid chars:A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set	fsr, wpa2e	yes
WLAN_SEC_PASSWORD	1-32 chars or NULL[6]. Valid chars:A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set	fsr, wpa2e	yes
WLAN_QOS_TYPE	svp, wifiStandard	svp		yes
WMM_ACCESS_CONTROL	mandatory, optional	mandatory	qos= wifi standard	yes
DSCPAUD	0-63	46		yes
DSCPSIG	0-63	26[10]		yes
DSCP_OTHER	0-63	0		yes
WLAN_RADIO_MODE	a, b&b/g, g	b&b/g		yes
WLAN_A_SUBBANDS	Comma separated list of 1-6[6]	none	radio mode a	yes
WLAN_TX_POWER_A1	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes
WLAN_TX_POWER_A2	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes
WLAN_TX_POWER_A3	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes
WLAN_TX_POWER_A4	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes

Parameter	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot
WLAN_TX_POWER_A5	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes
WLAN_TX_POWER_A6	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes
WLAN_TX_POWER_BG	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio modes b&b/g, g	yes
DIAG_DISPLAY_ENABLE	0,1 (0=disable, 1=enable)	0		yes
SYSLOG_MODE	disabled, errors, event, full	disabled		yes
ERROR_HANDLING	halt, restart	restart		yes
OAI_ENABLE	0,1 (0=disable, 1=enable)	0		yes
RTLS_ENABLE	0,1(0=disable, 1=enable)	0		yes
RTLSSRVR	ip addr or NULL[6]	not set		yes
RTLS_PORT	1-65535	8552		yes
RTLS_INTERVAL	15sec, 30sec, 1min, 5min, 10min	10min		yes
PTT_OR_EMERGENCY_DIAL	ptt, emergency_dial, none	none		yes
PHNEMERGNAME	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	null		yes
PHNEMERGNUM	1-16 numeric digits or NULL[6]	null		yes
PTT_CHANNELS	1,2,3,….24 (any or none)	all 24		yes

Parameter	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot
PTT_CH_NAME_01-24	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes
PTT_PRIORITY_CH_ENABLE	0,1 (0=disable, 1=enable)	0		yes
PTT_PRIORITY_CH_NAME	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes
SIP_USERNAME1	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes
SIP_USERNAME2-6	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		no
SIP_PASSWORD1	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes
SIP_PASSWORD2-6	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set	Ignored if corresponding username is not set	no
SIP_CODEC_LIST	one or more (in preferred order) of: g711u, g711a, g729	g711a, g711u		no

Parameter	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot
SIP_PROXYn_TYPE (n=1-3)	Asterisk, Asterisk_Compatible, NECSIP, NECThirdParty, Toshiba, Mitel, Inin, Pingtel, Shortel, Ccme, Deltapath	Asterisk		no
SIP_PROXYn_PORT (n=1-3)	0-65535	5060		no
SIP_PROXYn _SRVR(n=1-3)	ip addr/ DNS name	none		no
SIP_PROXYn_KEYPRESS_2833 (n=1-3)	0,1 (0=use inband, 1=use rfc2833)	0		no
SIP_PROXYn_KEYPRESS_INFO (n=1-3)	0,1 (0=do not send INFO requests, 1=send INFO requests)	0		no
SIP_PROXYn_HOLD_IP0 (n=1-3)	0,1 (0=disable, 1=enable)	0		no
SIP_PROXYn_PRACK (n=1-3)	0,1 (0=disable, 1=enable)	0		no
SIP_PROXYn_REREG_SECS (n=1-3)	seconds; 35-3600	3600		no
SIP_PROXYn_KEEPALIVE_SECS (n=1-3)	seconds; 10-3600 or 0 (no keep alives)	0 (no keep alives)		no
SIP_PROXYn_DOMAIN (n=1-3)	ip addr/FQDN no spaces; 1-60 chars or NULL[6]	null		no
SIP_PROXYn_CALLID_PER_LINE (n=1-3)	0,1 (0=can use same Call-ID header value for different lines, 1=must use unique call id per line)	0		no
SIP_PROXYn_MAIL_ACCESS (n=1-3)	dial string; 1-50 chars, no spaces or NULL[6]	none		no
SIP_PROXYn_MAIL_SUBSCR (n=1-3)	dial string; 1-50 chars, no spaces or NULL[6]	none		no
SIP_PROXY1_FAILOVER_IP (note: only for proxy 1)	ip addr or NULL[6]	none	ININ only	no
SIP_PROXY1_FAILOVER_PORT (note: only for proxy 1)	0-65535	5060	ININ only	no

Parameter	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot
SIP_PROXYn_CONF_IP (n=1-3)	ip addr or NULL[6]	none	NECSIP only	no
SIP_PROXYn_CONF_PORT (n=1-3)	0-65535	5060	NECSIP only	no
SIP_FAVORITES	comma separated list of up to 15 "number";"name" (number can appear without quotes) or NULL[6]	none		no
SIP_LINEn(n=1-5)	1-16 chars or NULL[6]	not set		no
SIP_LINEn_CALLID (n=1-5)	1-18 chars or NULL[6]	not set		no
SIP_LINEn_PROXY (n=1-5)	1,2, 3 (proxy) or 0 for no proxy	0 (no proxy)		
SIP_LINEn_SECONDARY_PROXY (n=1-5)	1,2, 3 (proxy) or 0 for no proxy	0 (no proxy)	Mitel only	
SIP_LINEn_USERNAME (n=1-5)	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		
SIP_LINEn_PASSWORD (n=1-5)	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set	Ignored if corresponding username is not set	
SNMPADD	ip addr/DNS name list or NULL[6] - up to 255 chars	not set		no
SNMP_PUBLIC_STRING	1-32 chars (no spaces) or NULL[6]	not set		no
SNMP_PRIVATE_STRING	1-32 chars (no spaces) or NULL[6]	not set		no
SNMP_ENABLE	0,1 (0=disable, 1=enable)	0		no
PAC_FILENAME	1-32 chars or NULL[6]	none		yes
SERVER_CERT_FILENAME	1-32 chars or NULL[6]	none		yes

Parameter	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot
CALL_LOG_ENABLE	0,1 (0=disable, 1=enable)	0		no

Version 2 Configuration Table Notes

Footnotes

1. The allowable values column specifies the allowable values that can be set using the version 2 configuration parameter. The allowable values for the same configuration item in HAT and menus may not adhere to these listed allowable values.
2. Default means the value used if no value is specified in the saved parameters on the phone (from HAT, Admin menus or previous initialization of phone), or from DHCP or a configuration file. Or the value has been cleared using NULL.
3. The Assoc info column indicates when the parameter is used or ignored. Specifically it is to indicate:
   - Which IP addresses belong to the group called static IP addresses. These appear on the IP Address menu in the Admin menus and HAT.
   - The security type that a label goes with (e.g., WPA_PSK is used only with security types WPAPSKand WPA2PSK).
   - Which power variables go with which radio modes.
   - WMM_ACCESS_CONTROL is only used for WIFI Standard QOS.
4. The SYSLANG parameter value will always be overridden by any user entered language. That is, this parameter will take effect only if the user has not modified the language via the standby menus since the last restore defaults.
5. GMTOFFSET: Valid values are a positive or negative number of hours and minutes less than 13 hours. 1 to 6 ASCII characters, optionally beginning with "+" or "-", followed by one or two ASCII numeric digits whose combined value is from 0 to 12, optionally followed by a ":" and 2 ASCII numeric digits that can be any of 00, 15, 30, or 45. Other minute values in the range 01 to 59 will not generate an error but will be interpreted as if they were 00. Minute values not 2 digits long will be rejected.

6. NULL means the null string (“”) and will cause the phone to act as if the item was never set. This gives the user a way to “clear” a parameter that was set once, since, in general, we do not allow the user to set an IP address to 0.0.0.0. Used for strings and IP addresses.

Other notes

The SIP TFTP server IP address parameter has been removed. TFTPSRVR is now used for the SIP TFTP server.

WLAN_A_SUBBANDS: Comma separated list of the following numbers. Only the sub-bands that are available in the selected Regulatory Domain will be used. Others, if listed, will be ignored.

1 = 5.150-5.250

2 = 5.250-5.350 DFS

3 = 5.470-5.725 DFS

4 = 5.725-5.825

5 = 5.725-5.850

6 = 5.470-5.650 DFS

Version 1 vs. Version 2 Parameter Names

Many new parameters that exist in Version 2 Configuration mode do not exist in Version 1 Configuration mode. Some of the SIP parameters were carried over to Version 2 from Version 1. However, the SIP parameter names in version 2 mode are not the same as in version 1 mode. The following table describes the differences in parameter names between the two modes. If a parameter is not listed in the table, then it did not exist in Version 1 Configuration mode.

Parameter name in version 1 mode	Parameter name in version 2 mode
None	SIP_USERNAME1-6
None	SIP_PASSWORD1-6
CODECS	SIP_CODEC_LIST
PROXYn_TYPE (n=1-3)	SIP_PROXYn_TYPE (n=1-3)
PROXYn_ADDR[1] (n=1-3)	SIP_PROXYn_SRVR (n=1-3)
PROXYn_ADDR[1] (n=1-3)	SIP_PROXYn_PORT (n=1-3)
PROXYn_KEYPRESS_2833 (n=1-3)	SIP_PROXYn_KEYPRESS_2833 (n=1-3)
PROXYn_ KEYPRESS_INFO (n=1-3)	SIP_PROXYn_KEYPRESS_INFO (n=1-3)
PROXYn_HOLD_IP0 (n=1-3)	SIP_PROXYn_HOLD_IP0 (n=1-3)
PROXYn_PRACK (n=1-3)	SIP_PROXYn_PRACK (n=1-3)
PROXYn_REREG_SECS (n=1-3)	SIP_PROXYn_REREG_SECS (n=1-3)
PROXYn_KEEPALIVE_SECS (n=1-3)	SIP_PROXYn_KEEPALIVE_SECS (n=1-3)
PROXYn_DOMAIN (n=1-3)	SIP_PROXYn_DOMAIN (n=1-3)
PROXYn_ CALLID_PER_LINE (n=1-3)	SIP_PROXYn_CALLID_PER_LINE (n=1-3)
PROXYn_ MAIL_ACCESS (n=1-3)	SIP_PROXYn_MAIL_ACCESS (n=1-3)
PROXYn_ MAIL_SUBSCR (n=1-3)	SIP_PROXYn_MAIL_SUBSCR (n=1-3)
PROXY1_ FAILOVERIP[2]	SIP_PROXY1_FAILOVER_IP
PROXY1_ FAILOVERIP[2]	SIP_PROXY1_ FAILOVER_PORT
PROXYn_ CONF_IP_ADDRESS[3] (n=1-3)	SIP_PROXYn_CONF_IP (n=1-3)
PROXYn_ CONF_IP_ADDRESS[3] (n=1-3)	SIP_PROXYn_CONF_PORT (n=1-3)
FAVORITE[4]	SIP_FAVORITES
SIP_LINEn (n=1-5)	SIP_LINEn (n=1-5) ---- same
SIP_LINE_CALLIDn (n=1-5)	SIP_LINEn_CALLID (n=1-5)

Parameter name in version 1 mode	Parameter name in version 2 mode
None	SIP_LINEn_PROXY (n=1-5)
None	SIP_LINEn_SECONDARY_PROXY (n=1-5)
LINEn_AUTH (n=1-5)[5]	SIP_LINEn_USERNAME (n=1-5)
LINEn_AUTH (n=1-5)[5]	SIP_LINEn_PASSWORD (n=1-5)
CALL_LOGGING	CALL_LOG_ENABLE

Version 1 vs. Version 2 Parameter Names Notes

1. The proxy server and port (optional) are specified together on the version 1 parameter PROXYn_ADDR. For version 2 config, these are specified on the two different parameters shown.
2. The failover proxy server and port (optional) are specified together on the version 1 parameter PROXY1_FAILOVERIP. For version 2 config, these are specified on the two different parameters shown.
3. The conference proxy server and port (optional) are specified together on the version 1 parameter PROXYn_CONF_IP_ADDRESS. For version 2 config, these are specified on the two different parameters shown.
4. In version 1 mode, up to 15 FAVORITE parameters can be specified (on different lines). In version 2 mode, the information for 15 favorites can be specified on one line with the SIP_FAVORITES parameter.
5. In version 1, the line username and password were specified together on the LINEn_AUTH parameter. In version 2 configuration mode these are specified separately.