

MH150/MH160 Mobile Handset

Administration Guide

NEC NEC Unified Solutions, Inc.

August 2009
NDA-30920, Revision 2

Liability Disclaimer

NEC Unified Solutions, Inc. reserves the right to change the specifications, functions, or features, at any time, without notice.

NEC Unified Solutions, Inc. has prepared this document for the exclusive use of its employees and customers. The information contained herein is the property of NEC Unified Solutions, Inc. and shall not be reproduced without prior written approval from NEC Unified Solutions, Inc.

© 2009 NEC Unified Solutions, Inc.

*Microsoft® and Windows® are
registered trademarks of Microsoft Corporation.*

*All other brand or product names are or may be trademarks or
registered trademarks of, and are used to identify products or services
of, their respective owners.*

Contents

About This Guide	1-1
Icons and conventions	1-1

NEC MH150/MH160 Mobile Handset Overview	2-1
System Diagram	2-1
Quick Network List	2-2
System Components	2-3
NEC MH150/160 Wireless Handset	2-3
NEC MH150/MH160 Wireless Handset Security	2-3
WPA2-Enterprise with 802.1X	2-3
WPA and WPA2 Personnel	2-4
Cisco Fast Secure Roaming	2-4
UNIVERGE NEAX 2000 IPS, UNIVERGE NEAX 2400 IPX, SV7000	2-4
Quality of Service (QoS)	2-4
Wi-Fi Standard QoS	2-5
CCXv4	2-5
Access points	2-5
Ethernet switch	2-6
TFTP server	2-6
NTP (Network Time Protocol) Server	2-6
Authentication Server (if using WPA2 Enterprise)	2-6
NEC MH150/MH160 Mobile Handsets Specifications	2-7
Startup Sequence	2-9
Handset Modes	2-10
Standby mode (on-hook)	2-10
Active mode (off-hook)	2-10
Push-to-talk (PTT) mode	2-10
Configuration menu mode	2-10
Messaging mode	2-11

NEC MH150/MH160 Wireless Handset Configuration 3-1

The Admin Menu	3-2
Opening the Admin menu	3-2
Navigation	3-2
Toggle options	3-2
Data entry and editing	3-3
Admin menu	3-4
Phone Config.	3-7
Telephony Protocol	3-7
Push-to-talk (PTT)	3-7
Time Zone	3-7
Daylight Savings	3-7
Password Enable/Disable/Change	3-8
SIP Registration	3-8
OAI Enable/Disable	3-8
Network Config	3-9
IP Addresses	3-9
SSID	3-10
WLAN Settings	3-11
Custom-Security	3-11
Custom – WPA2-Enterprise	3-12
Custom – QoS	3-12
CCX	3-13
Regulatory Domain/802.11 Config/Transmit Power	3-13
Diagnostics	3-15
Run Site Survey	3-15
Diagnostics Mode	3-15
Syslog Mode	3-15
Error Handling Mode	3-15
Restore Defaults	3-15
Graphics Demo	3-16
WPA2 Enterprise PEAP Certificate Enrollment and PAC Provisioning	3-16
Admin Menu Default Table	3-19
User-Defined Preferences	3-20
Default settings	3-22

Software License and Protocol Management 4-1

Requirements	4-1
Configuration Process	4-2

SIP Integration Factors 5-1

CODECs	5-1
DHCP	5-1
DNS	5-2

Programming the Mobile Handset Features 6-1

SIP TFTP Server Configuration Files	6-1
Proxy server commands	6-3
Sample Configuration Files	6-5

Using the MH150/MH160 Mobile Handset 7-1

The Handset Display	7-1
Calling/Called Party Display	7-1
System icons	7-2
Call status icons	7-3
NavOK functions	7-3
Softkeys	7-3
Menus	7-5
Line menu	7-5
Symbol menu	7-5
Favorites menu	7-6
FCN menu	7-6
Dialing Modes	7-7
predial mode	7-7
Overlapped dial mode	7-7
Combined mode	7-7

Call-Waiting Modes	7-7
Wait request while hearing busy signal.....	7-7
Using the Call-Waiting access code	7-8
PBX-activated Call-Waiting.....	7-8
Handset Operation	7-9

Testing a Handset 8-1

Diagnostic Tools 9-1

Run Site Survey	9-1
Solving coverage issues	9-4
Diagnostics Enabled	9-4
Screen 2	9-5
Screen 3	9-5
Screen 4	9-6
Screen 5	9-7
Screen 6 - EAP Information	9-7
Syslog Mode	9-8

Certifying the Handsets 10-1

Conducting a Site Survey	10-1
--------------------------------	------

Software Maintenance 11-1

Upgrading Handsets	11-1
Normal Download Messages	11-1
Download Failure or Recovery Messages.....	11-2

Troubleshooting 12-1

Access Point Problems	12-1
In range/out-of-range	12-1
Capacity	12-1
Transmission obstructions	12-2
Configuration Problems	12-2
Handset Status Messages	12-2

Regulatory Domains

Appendix-1

Figures

Figure	Title	Page
2-1	Network with SIP components	2-1
2-2	NEC MH 150/MH160 Mobile Handsets	2-7
3-1	Navigation keys	3-2
7-1	Handset call status screen.	7-1
9-1	Multiple AP mode display	9-1
9-2	Three APs with SSID matching handset	9-2
9-3	Any SSID mode selected.	9-2
9-4	Detail mode display	9-3
9-5	Diagnostics screen 1	9-4
9-6	Diagnostics screen 2	9-5
9-7	Diagnostics screen 3	9-5
9-8	Diagnostics screen 4	9-6
9-9	Diagnostics screen 5	9-7



Tables

Table	Title	Page
2-1	NEC MH150/MH160 Wireless Handsets Table of Specifications	2-8
2-2	Startup sequence display	2-9
3-1	Alphanumeric entries	3-3
3-2	Admin Menu.	3-4
3-3	Admin Menu default table	3-19
3-4	Config Menu	3-20
3-5	High and Severe noise mode volume adjustments	3-22
3-6	Profile options Default settings	3-22
4-1	Software version requirements	4-2
5-1	DHCP options	5-1
6-1	Proxy server parameters	6-3
7-1	System icons	7-2
7-2	Call status icons.	7-3
7-3	NavOK functions	7-3
7-4	Softkeys.	7-3
7-5	Characters available in symbol modes	7-6
9-1	Syslog messages.	9-9
9-2	Additional Syslog items	9-9
11-1	Normal software download messages.	11-1
11-2	Download failure or recovery messages during download	11-2
12-1	Mobile Handset status messages	12-2
Appendix-1	Regulatory domain settings	Appendix-1

1

About This Guide

This document explains how to configure and maintain the NEC MH150/MH160 Mobile Handsets with NEC SIP Extensions. The NEC PBX systems supported are the 2400 platform and NEC IPS. Each line on a MH150 or MH160 mobile handset requires an NEC SIP license. For multiple lines, additional SIP licenses are required.

Please refer to the configuration and administration document that pertains to the system in your facility for exact configuration options of the handset. Specific configuration options are explained in detail in the configuration and administration document for your system.



REFERENCE

- NEC MH150/MH160 Mobile Handset Administration Tool
- NEC MH150/MH160 Deployment Best Practices Guide
- NEC WLAN Voice Gateway Administration Guide

For additional information or support on this NEC Unified Solutions, Inc. product, contact your NEC Unified Solutions, Inc. representative.

Icons and conventions

This manual uses the following icons and conventions.



Caution! Follow these instructions carefully to avoid danger.



Note these instructions carefully.

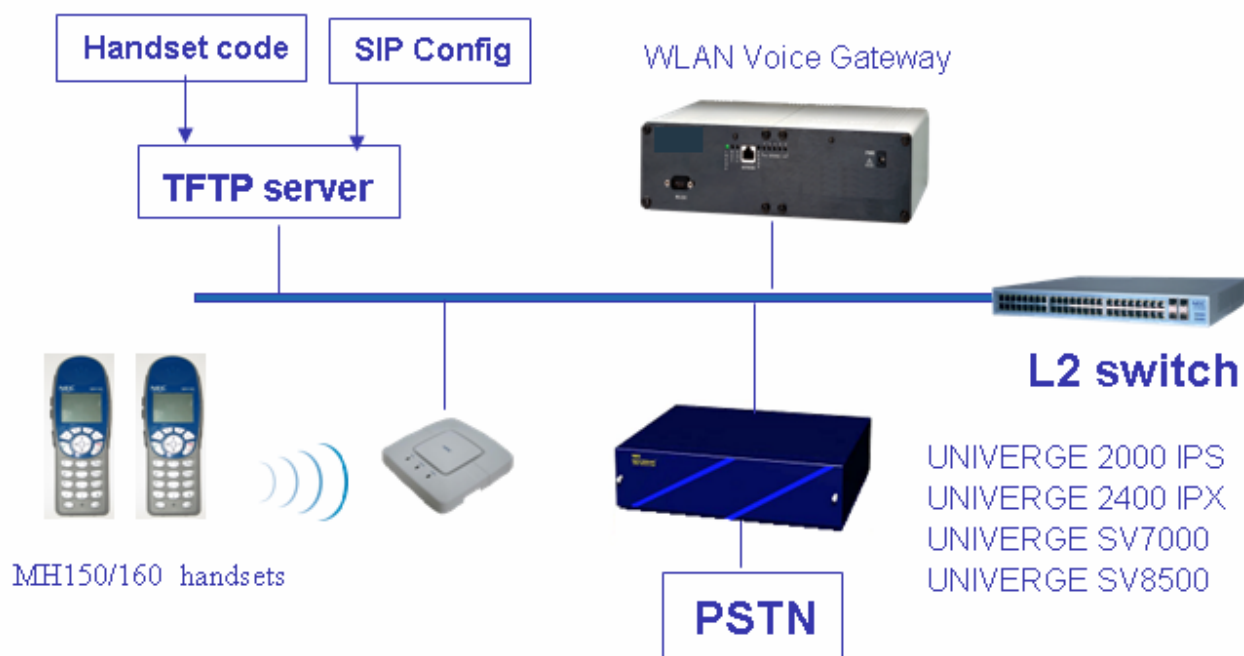
2

NEC MH150/MH160 Mobile Handset Overview

System Diagram

Figure 2-1 is an example of the SIP system components residing on a network with APs and wireless LAN Ethernet Switch.

Figure 2-1 Network with SIP components



Quick Network List

- Step 1** A wireless LAN must be properly configured and operational through the use of 802.11 wireless APs.
- Step 2** TFTP server must be available on the network in order to load the appropriate software onto the handset. See [“Software License and Protocol Management” on page 4-1](#) for detailed instructions for loading software on handsets.
- Step 3** The supported NEC UNIVEGE PBX system components must be connected to your network and completely operational.
- Step 4** The WLAN Voice Gateway, which facilitates the QoS on the wireless LAN for the handsets, must be on the same subnet as the handsets and have the proper versions of software.

—Ensure you have the following versions for the WLAN Voice Gateway:

173	svp100.toc
174	zvmlinux
175	flashfs

- Step 5** Install the correct handset software per [“Configuration Process” on page 4-2](#).
- Step 6** Install any updates to the WLAN Voice Gateway software per *WLAN Voice Gateway Administration Guide for SIP, Chapter 5 Software Maintenance*. Ensure the software is properly loaded on the TFTP server.
- Step 7** Configure your handset to ensure that it is associated with the wireless LAN, has the appropriate software, and has the correct IP address for the supported PBX. See [“Software License and Protocol Management” on page 4-1](#) and [“NEC MH150/MH160 Wireless Handset Configuration” on page 3-1](#) for detailed instructions for loading software onto and configuring handsets.
- Step 8** Create configuration files on the SIP TFTP server to define parameters for the SIP application. See [“SIP TFTP Server Configuration Files” on page 6-1](#).

System Components

NEC MH150/160 Wireless Handset

The NEC MH150/160 Wireless Handset is a lightweight, durable handset specifically designed for mobile workplace use within a facility using SIP and an 802.11 wireless LAN (802.11a/b/g/n). The NEC MH160 Wireless Handset has the same features and function, but in a more durable design with push-to-talk functionality. The handsets are to be used on-premises; they are not cellular or satellite phones.



The latest handset and Handset Administration Tool (HAT) software versions are required to support the features described in this document.

NEC MH150/MH160 Wireless Handset Security

The following security methods are supported by the mobile handsets.

WPA2-Enterprise with 802.1X

The handset supports WPA2-Enterprise, as defined by the Wi-Fi Alliance, which is based on the 802.11i standard. WPA2 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 mobile handset, 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. Additional details are provided in ["Requirements" on page 4-1](#).

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 mobile handset 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 Personnel

NEC MH150/160 Wireless Handsets support the 802.11i standard including Wi-Fi Protected Access (WPA and WPA2) in the pre-shared key (PSK) mode. The NEC MH150/160 Wireless Handset also supports Wired Equivalent Privacy (WEP) as defined by the 802.11 standard. NEC offers the product with both 40-bit and 128-bit encryption.

NEC highly recommends the use of WPA/WPAII for wireless security for the MH160 and MH160 Mobile Handsets.

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 (CKM), LEAP authentication, Michael message integrity check (MIC) and Temporal Key Integrity Protocol (TKIP). FSR provides strong security measures for authentication, privacy and data integrity on Cisco APs.

UNIVERGE NEAX 2000 IPS, UNIVERGE NEAX 2400 IPX, SV7000

UNIVERGE NEAX 2000 IPS, the UNIVERGE NEAX 2400 IPX, and the SV7000 are the three NEC PBX models with SIP functionality. These NEC SIP servers are referred to generically as proxy servers. The terms PROXY and PROXY SERVER are used for configuration file commands as detailed in ["Programming the Mobile Handset Features" on page 6-1](#). For the sake of clarity, we will refer to these models individually and collectively as "the NEC PBX".

Each MH150 or MH160 Mobile Handset requires one SIP license per line. If multiple lines are required on a MH150 or MH160, then additional SIP licenses are required. When the MH150/MH160 registers with the PBX, it uses a license. When the MH150/MH160 is powered off, the license is not released. It has been determined that this is normal operation.

Quality of Service (QoS)

Quality of Service is provided by using NEC WLAN Voice Gateway Voice Priority (WVG), Wi-Fi Standard QoS, or Cisco Client Extensions (CCX) version 4. QoS modes cannot be mixed within the same WLAN; all mobile handsets on the network must have the same QoS setting.

The WLAN Voice Gateway (WVG) is a network device running the SVP code. The SVP code is a quality of service (QoS) mechanism that is implemented in the handset and an access point (AP) to enhance voice quality over the wireless networks. The SVP code provides a quality of service (QoS) mechanism that is implemented in the AP to enhance voice quality over the wireless network. SVP code gives preference to voice packets over data packets on the wireless medium, increasing the

probability that all voice packets are transmitted efficiently and with minimum or no delay. SVP code is fully compatible with the IEEE 802.11 standard.

The WLAN Voice Gateway is an Ethernet LAN device that works with the AP to provide quality of service (QoS) on the wireless LAN. Voice packets to and from the NEC MH150/160 Wireless Handsets are intercepted by the WVG and encapsulated for prioritization as they are routed to and from either the NEC UNIVERGE 2400 or 2000 PBX. See the *WLAN Voice Gateway Administration Guide* for SIP document for detailed information about this device.

Wi-Fi Standard QoS

NEC MH150 and MH160 Mobile Handsets support WMM, WMM Power Save and WMM Admission Control - all QoS standards from the Wi-Fi Alliance based on IEEE 802.11e. The AP must support and enable all three of these QoS mechanisms in order for the handset to work properly. If the handset is configured for this option and the AP does not advertise all of these features, it will fail to operate. The combination of these three standards provides enterprise-class QoS in terms of voice quality, battery life and call capacity. This option does not require the WLAN Voice Gateway.

CCXv4

The CCX program allows WLAN client devices operating on Cisco APs to take advantage of Cisco-specific features. The NEC MH150 and MH160 Mobile Handsets mobile handset has been certified by Cisco as CCXv4 compliant. When the CCXv4 operating mode is selected on the handset, it operates using the required set of Cisco-specific and industry standard QoS mechanisms. This option does not require the WLAN Voice Gateway.

Access points

Access Points (APs) provide the connection between the wired Ethernet LAN and the wireless (802.11) LAN. Access points must be positioned in all areas where handsets will be used. The number and placement of APs will affect the coverage area and capacity of the wireless system. Typically, the requirements for use of NEC MH150/160 Wireless Handsets are similar to that of wireless data devices.

Access points may use SVP code in conjunction with an WLAN Voice Gateway; Wi-Fi Standard QoS (including WMM, WMM-Power Save and WMM-Admission Control) or in the case of Cisco APs, CCXv4. **APs must be properly configured to support the corresponding QoS and security methods selected for the handset.**

Ethernet switch

Ethernet switches interconnect multiple network devices, including the WLAN Voice Gateway, the NEC PBX, wired IP phones and the APs. Ethernet switches provide the highest performance networks, which can handle combined voice and data traffic, and are required when using the NEC MH150/160 Wireless Handsets.

Although a single Ethernet switch network is recommended, the handsets and the WLAN Voice Gateway can operate in larger, more complex networks, including networks with multiple Ethernet switches, routers, VLANs and/or multiple subnets. However, in such networks, it is possible for the quality of service (QoS) features of the WLAN Voice Gateway to be compromised and voice quality may suffer. Any network that consists of more than a single Ethernet switch should be thoroughly tested to ensure any quality issues are detected.

TFTP server

TFTP server software is required in the system to distribute software to the handsets.

There are two types of files that are delivered to the MH150/MH160 SIP handset whenever a handset is powered-up: 1) configuration software and 2) SIP configuration parameters.

The TFTP software may be on a different subnet than the gateway, APs and/or handsets.

Required in the system to deliver SIP configuration parameters to the SIP handset whenever a SIP handset is powered-up. The location of the SIP TFTP server is separately specified in SIP handset administration parameters. Refer to [“NEC MH150/MH160 Wireless Handset Configuration” on page 3-1](#) (*The Admin Menu* section). Normally, the SIP TFTP server is the same as the network TFTP server, see reference above.

NTP (Network Time Protocol) Server

If WPA Enterprise security is used, the handset will verify 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 deemed 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.

NEC MH150/MH160 Mobile Handsets Specifications

Figure 2-2 illustrates the NEC MH150/MH160 Mobile Handsets.

Figure 2-2 NEC MH 150/MH160 Mobile Handsets

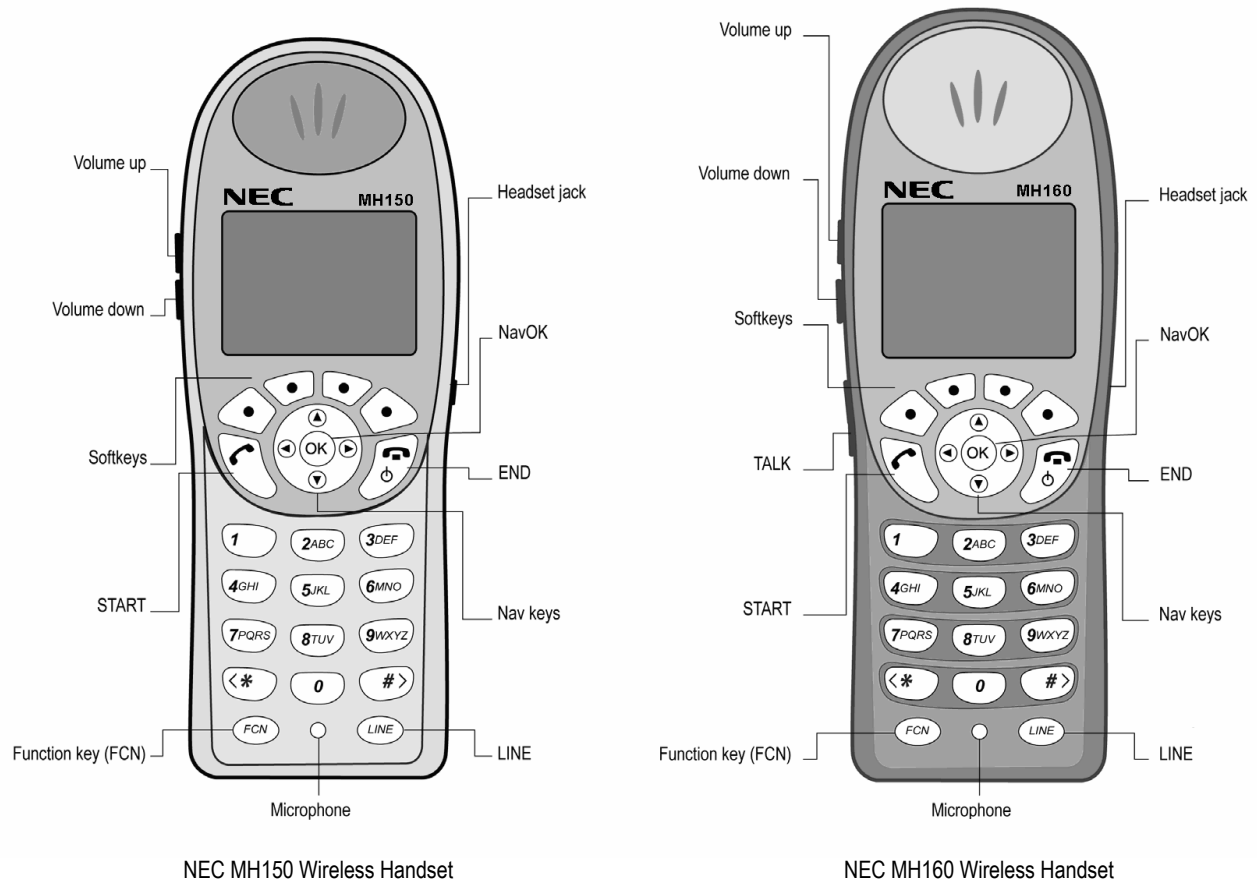


Table 2-1 NEC MH150/MH160 Wireless Handsets Table of Specifications

Radio mode (selectable)	(802.11b, 802.11g)	2.4-2.4835 GHz
	(802.11a)	5.150-5.250 GHz 5.250-5.350 GHz 5.470-5.725 GHz 5.725-5.825 GHz
Transmission type	Direct-sequence spread spectrum (DSSS)	
Transmit data rate	up to 54 Mb/s	
WLAN QoS	SVP Code, 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 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 certificates	Cisco Client Extensions (CCX)v4	
Voice encoding	ADPCM (Proprietary)	
Transmit power	Up to 100mW Transit Power Control (formerly 802.11h), see the Appendix for details.	
Display	Up to five lines of text plus two icon status rows and one row for softkey labels.	
MH150 Wireless Handset Dimensions	5.7" x 2.0" x 0.9" (14.5 x 5.1 x 2.3 cm)	
MH160 Wireless Handset Dimensions	5.7" x 2.0" x 0.9" (13.7 x 5.1 x 2.3 cm)	
MH150 Wireless Handset Weight*	3.9 oz. (110.6 g) with Standard Battery Pack	
MH160 Wireless Handset 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	

Startup Sequence

The NEC MH150/MH160 Mobile Handset 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 (refer to [Table 2-2 on page 2-9](#)). 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 ["Handset Status Messages" on page 12-2](#) for instructions on how to handle error messages that occur during initialization.

Table 2-2 Startup sequence display

Icon	The icon(s) shown in bold turns off when:
123456789	The handset has located and authenticated and associated with at least one AP, and is proceeding to bring up higher-layer networking functions.
12345678	The handset is either configured for Static IP, or if configured for DHCP, the DHCP discovery process has started.
1234567	If DHCP is configured, a DHCP response was received which contains a good DNS server configuration.
123456	Note: Only valid on non-SRP protocol. Indicates one of the following: <ul style="list-style-type: none"> • Static IP configuration, or • WLAN Voice Gateway address found in DHCP response, or • WLAN Voice Gateway address found via DNS lookup.
12345	All networking functions are complete (notably, DHCP), and the handset is proceeding with establishing the SRP link to the WLAN Voice Gateway.
1234	The SRP link is established; all network stack initialization is complete, proceeding with application-specific initialization.
123	SIP application startup. Icon 3 is extinguished if a generic SIP config file is found.
12	Icon 2 is extinguished if a handset specific SIP config 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 PBX. 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 SIP TFTP server and downloads general information about the PBX, downloads specific information pertaining to the handset, registers with the PBX, 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, 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. See ["SIP TFTP Server Configuration Files" on page 6-1](#).

A specific ".cfg" file will be required for the primary line of each handset registering against an NEC PBX - regardless of whether the primary

line's username and password is read from memory or entered by the user at power-on.

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 so until the call is ended. The call is answered by pressing the **START** key, the **Answ** softkey, or the **NavOK** key. The handset will ring according to user preference as specified in the standby menus. The ringing can be silenced by pressing the **END** key.

Active mode (off-hook)

To place or receive a call, press the **START** key. This transitions the mobile handset to active off-hook mode. When there is a dial tone, the handset is in communication with the PBX, and the display shows information as it is received from the PBX. The user may place a call or press a softkey or the **FCN** or **LINE** key to access additional operations. To conserve these resources, return the handset to the standby mode when a call is completed by pressing the **END** key.

Push-to-talk (PTT) mode

The NEC MH160 Wireless Handsets 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. It cannot receive calls while in the Config menu.

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.

3

NEC MH150/MH160 Wireless Handset 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 mobile handset user may select several usability options from the Standby menu, described in ["User-Defined Preferences" on page 3-20](#). This information is also provided in the end-user manual.

When WPA2 Enterprise security is used, PAC files for EAP-FAST can be provisioned wirelessly or by using the HAT. For PEAP, the HAT must be used to enroll certificates. See WPA2 Enterprise PEAP Certificate Enrollment and PAC Provisioning at the end of this chapter.

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.

The NEC Mobile Handset Administration Tool is a software utility that enables rapid configuration of handsets by utilizing the USB port on the Dual Charger. See the *NEC MH150/MH160 Mobile Handset Administration Tool* document for specific instructions. Please see your service representative or contact NEC customer service for more information about this time-saving tool.

The Admin 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.

Opening the Admin menu

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



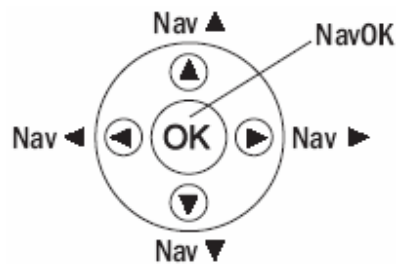
NOTE

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**.

Figure 3-1 Navigation keys



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 **Ring in 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 **Ring in 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. Refer to [Table 3-1](#).

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.

Table 3-1 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
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 3-2 lists the Admin menu items. The default settings have an asterisk (*) prior to the option. Detailed descriptions of each item appear below the table.

Table 3-2 Admin Menu

1st level	2nd level	3rd level	4th level	5th level
Phone Config	Telephony Protocol	* Type 036		
	Push-to-talk	PTT Enable/*Disable		
		Allowed Channels	* Channel 1 * Channel 2 * ... * Channel 24	
		Name Channels	[list]	Enter Name
		Priority Channel	Priority Channel On/*Off	
			Name Channel	[Enter Name]
	Time Zone	[list] * GMT		
	Daylight Savings	* DST No Adjust DSO Auto (USA) DST Auto (AUS) DST Auto (EURO)		
	Password * Enable/Disable			
	[If Password is enabled] Change Password			
	SIP Registration	Login Reg 2 Reg 3 Reg 4 Reg 5 Reg 6	[for each option] Username Password	
	Clear SIP Regist			
	OAI	* Enable OAI Disable OAI		
	Location Service	Enable RTLS * Disable RTLS		
		Transmit Interval	1 minute 5 minutes *10 minutes	
		Location Server IP	Enter IP	
		ELP Port	Enter Port *8552	
Network Config	IP Address	* Use DHCP		

1st level	2nd level	3rd level	4th level	5th level
		Static IP	Phone IP Default Gateway Subnet Mask TFTP Server IP Syslog Server IP Time Server IP 5 IP SIP TFTP Svr IP OAI Server IP	
	SS ID	[enter]		
	WLAN Settings	* Custom		
4th Level	5th Level	6th Level	7th Level	8th Level
Security	* None			
	WEP	Authentication	* Open System Shared Key	
		WEP [Enable/*Disable]		
		Key Information	Default Key Key Length Key 1-4	
		Rotation Secret		
	WPA2-PSK	* Passphrase Pre-Shared Key		
	WPA-PSK	* Passphrase Pre-Shared Key		
	Cisco FSR	Username Password		
	WPA2-Enterprise	Authentication	*EAP-FAST PEAP PEAP	
		Fast Handoff	*CKKM OKC	
		Username		
		Password		
		Delete [Cert/PAC]		
QoS	Mode	*SVP	DSCP tags	WT in Call (*46) WT standby (*40) Other (*0)
		Wi-Fi Standard	DSCP tags	Voice (*46) Control (*40) Other (*0)
	[WLAN Settings]	CCX		

1st level	2nd level	3rd level	4th level	5th level
	4th Level	5th Level	6th Level	7th Level
	WPA2-Enterprise	Authentication	*EAP-FAST	
			PEAP	
		Fast Handoff	*CKM	
		Username		
		Password		
		Delete [Cert/PAC]	[Yes/No]	
	QoS	DSCP tags	Voice	*46
			Control	*40
			Other	*0
Network Config (cont'd)	Reg Domain	01 02 03 04 05 06 07 08		
		→	[802.11 Config]	
			a →	[802.11a]T 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	
			→	[Transmit Power] 5mW (7dBm) 10mW (10dBm) 20mW (13dBm) * 30mW (15dBm) 40mW (16dBm) 50mW (17dBm) 100mW (20dBm)
Diagnostics	Run Site Survey			
	Diagnostics Mode	* Disable Enable		
	Syslog Mode	*Disabled Errors Events Full		
	Error Handling Mode Halt on Error/ * Restart on Error			

1st level	2nd level	3rd level	4th level	5th level
Restore Defaults				
Graphics Demo				

** 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.*

Phone Config

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 NEC MH150/MH160 Mobile Handsets requires license option selection **36**. Any other protocol will cause the handset to malfunction.

Push-to-talk (PTT)

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.

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.

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.

SIP Registration

Individual handsets may be configured to correspond with the SIP configuration information in the TFTP 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 ["SIP Integration Factors" on page 5-1](#).

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, Reg 3, Reg 4, Reg 5 and **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

The MH100 series 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 NEC 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 NEC OAI Gateway installed at your site, you should disable the OAI feature to preserve network bandwidth and battery life.

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.

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.



NEC MH150/MH160 Mobile Handsets 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 mobile handsets cannot “roam” across subnets, since they cannot change IP addresses while operational.

*Please see **NEC MH150/MH160 Deployment Best Practices** for detailed configuration information.*

- **TFTP Server IP** The IP address of a TFTP server on your network, which holds software images for updating the handsets and contains the handset files. If this feature is configured (not set to 0.0.0.0 or 255.255.255.255) with either Static IP configuration or using DHCP option 66 (TFTP server), or the boot server/next server (siaddr) field, the handset will check for newer software each time it is powered on or comes back into range of your network. This check takes only a second and ensures that all handsets in your network are kept up-to-date with the same version of software.
- **Syslog Server IP** The IP address of the syslog server. See [“Diagnostic Tools” on page 9-1](#) for more information.
- **Time Server IP** The IP address of the time server.
- **SVP Server IP** The IP address of the WLAN Voice Gateway. If using Static IP configuration, this is simply the IP address of the WLAN Voice Gateway. Note that the WLAN Voice Gateway 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.
- **SIP TFTP Server IP** The IP address of a TFTP server on your network, which holds SIP configuration files. In static mode, this parameter must be configured with an IP address. In DHCP mode, the SIP TFTP server may be specified by defining the address on the DNS server for the name “siftftp” If this is not defined, the address specified in option 66 will be used. See [SIP Integration Factors](#) for more information.
- **OAI Server IP** The IP address of ethnic OAI Gateway. If using Static IP configuration, this is simply the IP address of the NEC 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 security setting modes. The Custom mode allows explicit control of all of the Security and QoS settings. The CCX setting defaults the phone's operating mode to be compatible with Cisco's CCX V4 (Cisco Compatible Extensions) requirements, with only the 802.1X mechanism needing to be selected.

Custom-Security

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



For WEP, WPA-PSK, and WPA2-PSK set each of the following options to match exactly the settings in the APs.



Encryption codes display as they are entered. For security reasons codes will not display when a user returns to the Admin menu, Encryption options.

WEP (Wired Equivalent Privacy) is a wireless encryption protocol that encrypts data frames on the wireless medium allowing for greater security in the wireless network. If WEP is required at this site, you must configure each 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.
- **Rotation Secret**—This is used for proprietary WEP key rotation. Refer to your custom document if this feature is supported in your system.

WPA2-PSK The security features of WPA2 (Wi-Fi Protected Access) using PSK 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) In order to provide the highest level of security without compromising voice quality on Cisco Aironet wireless LAN APs, Polycom and Cisco Systems have cooperated to implement the Fast Secure Roaming mechanism. FSR is designed to minimize call interruptions for NEC MH150/160 Wireless Handset users as they roam throughout a facility. Existing Aironet 350, 1100, and 1200 APs may require a firmware upgrade to support FSR. Cisco FSR requires advanced configuration of the Cisco 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.

Custom – WPA2-Enterprise

The **Authentication** setting can select either ***EAP-FAST** or **PEAP** as the authentication method for RADIUS server such as those from Cisco, Microsoft, or Juniper.

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.

Fast Handoff allows the use of either ***CCKM** (Cisco Centralized Key Management) or **OKC** (Opportunistic Key Caching) to select a fast handoff mechanism. These mechanisms allow a phone to quickly and securely roam between APs with a minimum disruption of audio.

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 re-acquire these credentials from the RADIUS server over the air. When the authentication method is PEAP the certificate on the phone is deleted and a new certificate needs to be downloaded through the HAT. See WPA2 Enterprise PEAP Certificate Enrollment and PAC Provisioning at the end of this chapter.

Custom – QoS

The **Mode** may be set to either ***SVP** or **Wi-Fi Standard**. **SVP** mode uses the SVP Server to provide high density voice with exceptional quality. **DSCP tags** are used to change the priority settings for various

classes of packets as they are transmitted to the network from the mobile handset. Default values are given but may be overwritten: **WT in call = 46, WT standby = 40, Other = 0.**

Wi-Fi Standard mode uses WMM, WMM Power Save and WMM Admission Control for QoS, in place 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 mobile handset. Default values are given but may be overwritten: **Voice = 46, Control = 40, Other = 0.**

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 such as those from Cisco, Microsoft, or Juniper.

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

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 re-acquire these credentials from the RADIUS server over the air. When the authentication method is PEAP the certificate on the phone is deleted and a new certificate needs to be downloaded through the HAT.

QoS – DSCP tags are used to change the priority settings for various classes of packets (Voice, Control, and Other) as they are transmitted to the network from the mobile handset. Default values are given but may be overwritten. Voice = 46, Control = 40, Other = 0.

Regulatory Domain/802.11 Config/Transmit Power

Regulatory domain, 802.11 configuration and transmit power are interdependent. Refer to the Appendix: [Regulatory Domains](#) for regulatory domain setting specifications. NEC recommends that you check with local authorities for the latest status of national regulations for both 2.4 and 5 GHz wireless LANs.

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

- **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 sub-bands, the **Subband** list will open. If the mode does not have sub-bands, the **Transmit Power** list will open.



NOTE

Use g only if all of your infrastructure devices use only 802.11g. The handsets will operate up to 54 mb/s in this mode.

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. Provision is made in the software to accommodate these ranges once established. Newly added subbands may not appear in the above table.

— 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.

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 ["Diagnostic Tools" on page 9-1](#) for more information about site survey.

Diagnostics Mode

Diagnostics can be enabled or disabled. See ["Diagnostics Enabled" on page 9-4](#) for a detailed explanation of the Diagnostics mode options.

Syslog Mode

See ["Syslog Mode" on page 9-8](#) for a detailed explanation of the Syslog mode options.

Error Handling Mode

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

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

Restore Defaults

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

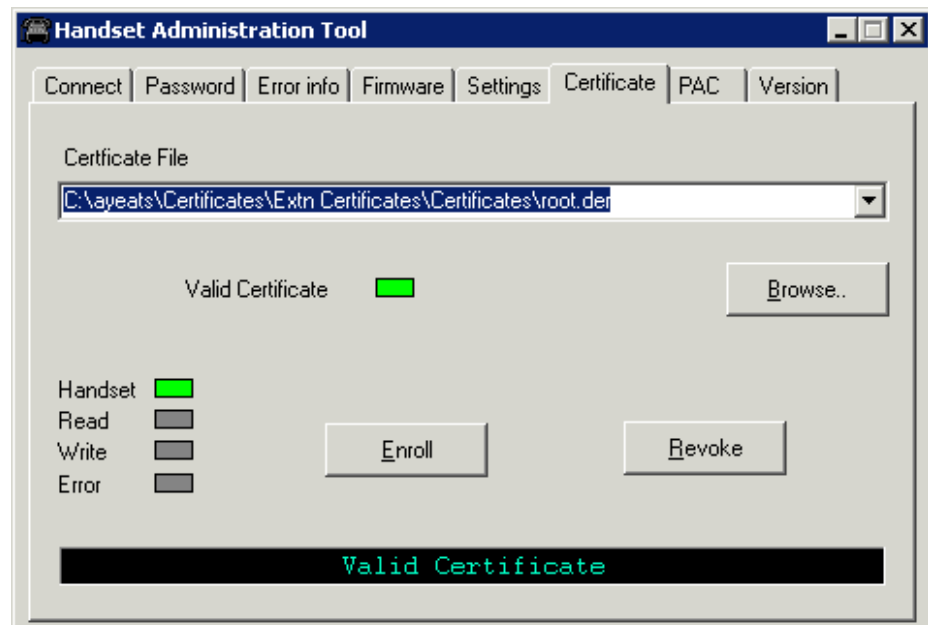
Graphics Demo

The **Graphics Demo** option starts the demo immediately upon selection. First it displays a picture of the earth and then it switches to a moving graph.

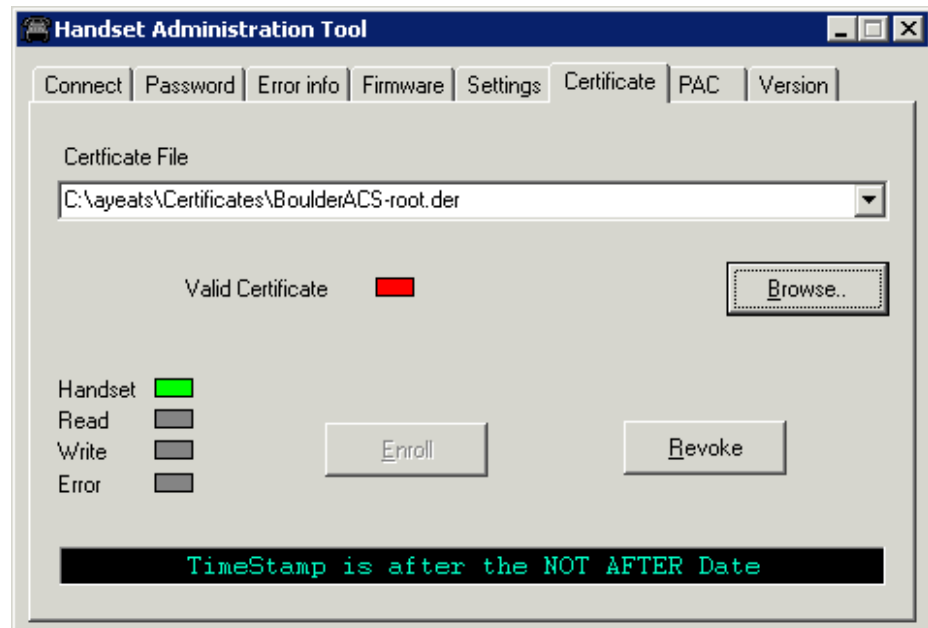
WPA2 Enterprise PEAP Certificate Enrollment and PAC Provisioning

The Handset Administration Tool (HAT) is used for enrolling a handset with a PEAP certificate. 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.

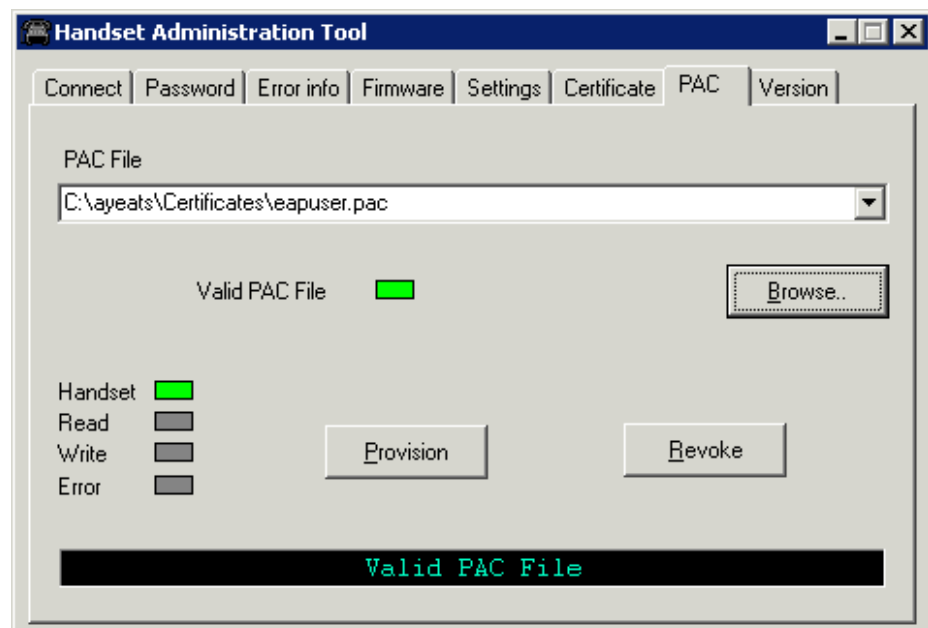


The screen below shows a certificate chosen with the file browser, but found to be invalid because it has expired.

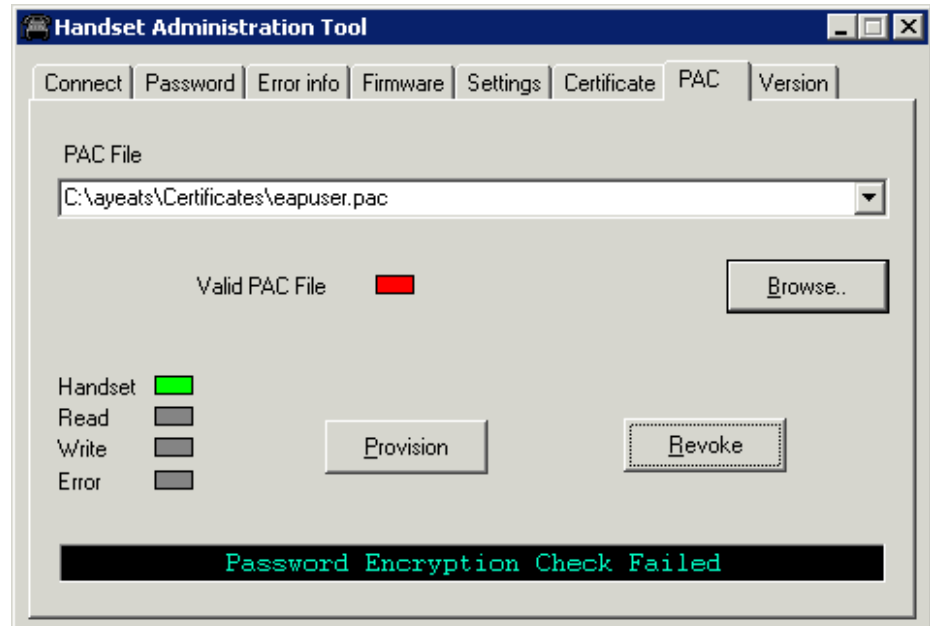


For EAP-FAST, HAT is also used for provisioning a handset with a Protected Access Credential (PAC). Choose the PAC file with the file browser. The user will be prompted to enter the password used to generate the PAC as part of its validation process. Once the PAC is considered to be valid, the Provision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



The screen below shows the result of entering the wrong password.



Admin Menu Default Table

When the **Restore Defaults** option is selected, administrative parameters will be reset to their factory defaults as shown in [Table 3-3](#). The **Telephony Protocol** setting will not change. User parameters will be reset per [Table 3-4 on page 3-20](#).

Table 3-3 Admin Menu default table

Menu Option	Setting	Sub-option	Sub-sub-option	Default
Phone Config	Push-to-Talk			Disabled
		Allowed Channels		[all]
		Name Channels		[None set]
		Priority Channel		Disabled
	Time Zone			GMT
	Daylight Saving			DST No Adjust
	Password			Enabled
	Change Password			[n/a]
	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	WEP Key Length	40-bit
			Mode	SVP
			DSCP tags	WT in call =46 WT standby =40 Other =0
	Reg. Domain*			[None set]
		802.11 mode		b & b/g mixed
		Transmit Power		30 mW (15 dBm)

Menu Option	Setting	Sub-option	Sub-sub-option	Default
Diagnostics	Run Site Survey			[n/a]
	Diagnostics			Disabled
	Syslog Mode			Disabled
	[Error Handling Mode]			Restart on Error

User-Defined Preferences

The NEC MH150/160 Wireless Handset 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 [Table 3-4](#) and the *NEC MH150/160 Wireless Handset and Accessories User Guide*.

Table 3-4 Config Menu

Config Menu	2nd level	3rd level	4th level	5th level	6th level
Lock Keys					
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
		Noise Mode (See Note below)	Normal High Severe		
		Ring in Headset Ring in Speaker			

Config Menu	2nd level	3rd level	4th level	5th level	6th level
		Warning Tones 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 ■■■■■■■			
	PTT Vibrate (Enable/Disable)				
System Info	Phone IP Address				
	Alias IP Address				
	SVP IP Address				
	OAI IP Address				
	Firmware Version				



NOTE

High and Severe noise modes increase microphone, speaker, and ring volume settings above Normal mode baseline. All measures are approximate. See [Table 3-5](#).

Table 3-5 High and Severe noise mode volume adjustments

	Microphone	In-ear speaker	Ring volume
High	+12dB	+6dB	+3dB
Severe	+18dB	+12dB	+6dB

Default settings

The profile options on the standby menu may be reset to their default values by the **Restore Defaults** option in the Admin menu. The default settings are listed in [Table 3-6](#).

Table 3-6 Profile options Default settings

Setting/Profile	Silent	Vibrate	Soft	Loud	Custom
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

4

Software License and Protocol Management

NEC MH150/MH160 Mobile Handsets support a number of different IP protocol integrations. All NEC MH150/MH160 Mobile Handsets are shipped from NEC with a generic software load that allows them to associate to a wireless LAN and download functional software from a TFTP server.



NOTE

The handsets will not function properly without downloading appropriate software

This chapter details the process to properly configure NEC MH150/MH160 Mobile Handsets and download software via over-the-air file transfer.

Requirements

- A wireless LAN must be properly configured and operational through the use of 802.11a/b/g wireless APs.
- A TFTP must be available on the network in order to load the appropriate software into the handsets.
- Software versions are described in [Table 4-1](#).
- If SVP is used for QoS, the SVP Server must be installed and properly configured.
- 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 WLAN Configuration Guide for settings.
- If WPA2-Enterprise is used, then all portions of the Public Key Infrastructure (PKI) need to be installed and configured properly in order to acquire the network.

Table 4-1 Software version requirements

Component	Version
WLAN Voice Gateway	17x.028 or higher
OAI Server MOG 600	54.032 or higher
OAI Server MOG 700	82.017 or higher

- Finally, ensure that the Battery Pack on the handset is fully charged.

Configuration Process

Step 1 Please contact NEC NTAC to obtain the latest software updates for the MH150 and MH160 Mobile Handsets.

Step 2 Load the latest version of the SIP code and place it on the TFTP server and ensure the TFTP server is started. The five files that are needed must be named:

usb downloader	pd14udsp.bin
functional filename	pd14csp.bin
phintl filename	pi1400sp.bin
ota downloader	pd14odsp.bin
config file	slnk_cfg.cfg

Step 3 Use the Handset Administration Tool to set up the configuration of each handset to meet all essential requirements. If not using the Handset Administration Tool, ensure the following parameters are correctly set in the Admin menu for each handset:

- If statically assigning IP addresses, ensure that the Phone IP, Subnet Mask, and Default Gateway information are accurate. If using a DHCP Server, ensure that the DHCP option is set.
- Ensure the handset has properly configured SSID and Reg Domain information.
- Ensure the Telephony Protocol menu option is set to 36. This ensures the handset will check for the proper SRP files each time it powers on.
- Ensure security settings are properly programmed.
- Configure handset security settings to match AP configuration. 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 (requires use of the HAT).

See [NEC MH150/MH160 Mobile Handset Overview](#) for detailed configuration instructions.

Step 4 Configure QoS mode to match the AP and site QoS plan.

Step 5 Power cycle the handset.

Step 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 code from the TFTP server for system configuration and for its own settings. Once this second evolution is complete, the handset is ready to use.



NOTE

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

5

SIP Integration Factors

CODECs

The NEC MH150/MH160 Mobile Handsets are compatible with the G.711 μ -law and G.711a-law codecs. There is no setting required on the handset.

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 listed in [Table 5-1](#) if DHCP use is enabled.

Table 5-1 DHCP options

Option	Meaning
1	Subnet mask
3	Default gateway
6	DNS server
15	Domain server
66	TFTP server
151	WLAN Voice Gateway
152	NEC OAI Gateway
siaddr	Boot server or next server

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 will use DNS to automatically translate names into IP addresses for the TFTP server and WLAN Voice Gateway.

In DHCP mode, the SIP handset will use DNS to look up an address for the logical name "siftftp" to locate the SIP TFTP file server. If this logical name is undefined, then the address specified by option 66 is used for the SIP TFTP server.

6

Programming the Mobile Handset Features

In order for the handset to function in the SIP environment, it downloads two files from the root directory of the SIP TFTP server during startup. The first file contains generic system information and is downloaded by every handset during the power-up sequence. A second file, 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 customized for the specific system in use at the facility. Example files are provided but must be edited according to local requirements.

SIP TFTP Server Configuration Files

The two file types, generic and specific, are identical in format. 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.

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_username.cfg where [username] is as assigned to each individual user by the system administrator. See ["SIP Registration" on page 3-8](#)
- Config file contents must be in agreement PBX values or entities. For example, the PROXYn IP address must match the actual PBX/call-server address and any lines specified must actually be set up on the PBX.
- 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.

- Specific file information 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 in the following table.
- 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.

Program each of the files according to the following instructions.

The generic file (sip_allusers.cfg)

The generic configuration file provides system information common to all handsets.

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 to other phones. 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.

Proxy server commands

Use the parameters when programming the configuration files. See the [“Sample Configuration Files” on page 6-5](#) for additional information about each parameter.

Table 6-1 Proxy server parameters

Parameter	Value	Description	Notes
PROXYn_ADDR	xxx.xxx.xxx.xxx:pppp or proxyname:pppp	Proxy address	n = 1, 2, 3 xxx.xxx.xxx.xxx = IP4 address pppp = port (optional, 5060 is the default) proxyname = computer name (DHCP only)
PROXYn_DOMAIN	Domain name	Domain served by this proxy server	n = 1, 2, 3 DOMAIN = [example: necsolutions.com] Can be omitted if the proxy does not act as a domain server.
PROXYn_TYPE	NECSIP	Specify the manufacturer of each defined proxy server.	Used by the handset to perform proxy-specific actions based on known behavior for specific proxy types. Only the NECSIP value may be used for the NEC handsets.
PROXYn_KEYPRESS_2833	enable disable	Controls generation of in-stream RFC2833 formatted key press events.	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
PROXYn_MAIL_SUBSCR	name@xxx.xxx.xxx.xxx or sip:name@domain	Contact to whom the handset should subscribe for mail notification.	n = 1, 2, 3 name = mail server contact name. xxx.xxx.xxx.xxx = IP4 address. Domain where the mail resides. See Note 1.
PROXYn_MAIL_ACCESS	name@xxx.xxx.xxx.xxx or sip:name@domain	Contact to whom the handset should invite to access the mail center.	See above.

Parameter	Value	Description	Notes
PROXYn_ MAIL_NOTIFY	name@xxx.xxx.xxx.xxx or sip:name@domain	Contact from whom mail notification originates.	See Note 2. See Note 3.
PROXYn_CONF_ IP_ADDRESS	xxx.xxx.xxx.xxx	IP address of the conference resource on the PBX.	n = 1, 2, 3 xxx.xxx.xxx.xxx = IP4 address.
AUTH See Note 4 warning.	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 administrator which enables a handset to register and/or function.
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.
LINE _n	username	The dial # or name. All LINE _n user names should be unique for a given LINE _n _PROXY. This may be enforced in future software revisions.	n = 1, 2, 3, 4, 5 The registered contact becomes: sip:username@domain
LINE _n _PROXY	i	SIP proxy server for this line.	n = 1, 2, 3, 4, 5 i = the number of the proxy server 1, 2, 3. LINE _n _PROXY can be omitted if the line is not to be registered and you wish to do direct phone to phone calls.
LINE _n _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; LINE _n	Phonebook list of numbers accessible from the Favorites menu.	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. LINE _n = can be omitted if dialing can be done on any registered line. Usually omitted but if present, the number will be dialed on the programmed line.

Note 1 For mail notifications, in general you will need to define only one contact parameter for each proxy. If the proxy server automatically creates and renews subscriptions when the handset registers, then only the PROXY_n_MAIL_NOTIFY contact need be specified. If the handset must subscribe to a particular contact to get mail notification, then only the PROXY_n_MAIL_SUBSCR contact needs to be specified.

Note 2 Values as above.

Note 3 **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 TFTP server files. Credentials stored in the SIP server or in the handsets are protected.

Sample Configuration Files

Configuration files are illustrated below. These files are available as a download from the software updates site and may be customized for your application. Please note that these are merely samples and will not work on your system as written here or as downloaded. Your configuration files must be locally programmed according to your site requirements.

SIP_allusers.cfg

```
# SIP ALL USERS Configuration file example

# Configuration file format example with explanatory text

# Codec preference order only. This does not enable/disable codecs
# (Optional)
# can be G.711-ulaw, g.711u, G.711U, g711u, G.711U, etc.
# if g711u is omitted it will be added to end of list.
# if g711a is omitted it will be added to end of list after u.
CODECS = g711u, g711a

# One PROXYn (PBX/Call Server) is required, additional ones are optional as
# you can register secondary line appearances with other PROXY servers
PROXY1_ADDR      = 10.0.0.138:5060
#PROXY2_ADDR     = 172.29.0.140:5060

#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.
# (below are examples of different ways to specify a domain)
#PROXY1_DOMAIN = plcmengr.com
#PROXY1_DOMAIN = 10.0.0.138
#PROXY1_DOMAIN = axlx.engr.local

# PROXY1_MAIL_SUBSCR is who we should subscribe to for mail center
# notifications
# This is needed only if the user is not subscribed automatically at
# registration.
# It is almost never required in current versions of Asterisk to specify
# this.
# If you are using Asterisk (non-business edition) before v1.2, this is
```

```

# necessary.
# This example is actually specific for a line number:3001
#PROXY1_MAIL_SUBSCR = sip:3001@vmail.asterisk.com

# PROXYn_MAIL_NOTIFY is from whom we might get unsolicited mail center
# notifications
# This option is deprecated and no longer needed in versions beyond
# e/h340/i640 phones v108.011, Polycom MH150 phones v130.001, and Polycom
# MH150/MH160 phones 131.001.
# Examples:
#PROXY1_MAIL_NOTIFY = asterisk@10.0.0.138
#PROXY1_MAIL_NOTIFY = sip:asterisk@10.0.0.138

# PROXY1_MAIL_ACCESS is the main voicemail dial number
# Examples:
# 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

#PROXY1_KEYPRESS_2833 controls generation of in-stream RFC2833 formatted key
# press 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.
# If you are going to do OAI integration, this must be disabled.
# The default is disable
PROXY1_KEYPRESS_2833 = disable

#PROXY1_KEYPRESS_INFO controls generation of SIP INFO requests to the SIP
# server for keypress events. Normally you want this to be enabled.
# If you are going to do OAI integration, this must be enabled.
# The default is enable
PROXY1_KEYPRESS_INFO = enable

# 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
#PROXYn_HOLD_IP0 = enable

# PROXY1_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.
PROXY1_PRACK = disable

# Favorites in the allusers file will be present in the favorites on all
# handsets
# The username can be blank and can include escaped chars

```

```
# Useful features can be included such as call forwarding or dialing
# voicemail
FAVORITE = 1234; Site Security
FAVORITE = *98; Call Forwarding
```

Sample handset-specific file

```
# Configuration file format example

# Codec preference order only. This does not enable/disable codecs.
# (Optional) can be G.711-ulaw, g.711u, G.711U, g711u, G.711U, etc.
# if g711u is omitted it will be added to end of list.
# if g711a is omitted it will be added to end of list after u.
#CODECS = g711u, g711a

# One PROXYn (PBX/Call Server) is required, additional ones are optional as
# you can register secondary line appearances with other PROXY servers
#
#PROXY1_ADDR      = 10.0.0.138:5060
#PROXY2_ADDR      = 172.29.0.140:5060

# 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.
# (below are examples of different ways to specify a domain)
#PROXY1_DOMAIN = plcmengr.com
#PROXY1_DOMAIN = 10.0.0.138
#PROXY1_DOMAIN = axlx.engr.local

# PROXY1_MAIL_SUBSCR is who we should subscribe to for mail center
# notifications
# This is needed only if the user is not subscribed automatically at
# registration.
# It is almost never required in current versions of Asterisk to specify
# this.
# If you are using Asterisk (non-business edition) before v1.2, this is
# necessary.
# This example is actually specific for a line number:3001
#PROXY1_MAIL_SUBSCR = sip:3001@vmail.asterisk.com

# PROXYn_MAIL_NOTIFY is from whom we might get unsolicited mail center
# notifications
# This option is deprecated and no longer needed in versions beyond
# MH150/e340/h340/i640 handsets v108.011, Polycom MH150 phones v130.001, and
# Polycom MH150/MH160 phones 131.001.
# Examples:
#PROXY1_MAIL_NOTIFY = asterisk@10.0.0.138
#PROXY1_MAIL_NOTIFY = sip:asterisk@10.0.0.138
```

```

# PROXY1_MAIL_ACCESS is the main voicemail dial number
# Examples:
# PROXY1_MAIL_ACCESS = 7999
# PROXY1_MAIL_ACCESS = sip:7999@10.0.0.138
# PROXY1_MAIL_ACCESS = 7999@10.0.0.138

#PROXY1_KEYPRESS_2833 controls generation of in-stream RFC2833 formatted key
# press 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
#PROXY1_KEYPRESS_2833 = disable

# PROXY1_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
#PROXY1_KEYPRESS_INFO = enable

# 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
#PROXYn_HOLD_IP0 = enable

# PROXY1_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.
#PROXY1_PRACK = disable

# ///////////////////////////////////
# // ABOVE this line should probably be in the sip_allusers.cfg file
# // with items uncommented in this file only for overriding a setting
# // for a particular user.
# ///////////////////////////////////

# Authentication credentials
# (Normally not stored in this file for security reasons)
# AUTH = username; password
AUTH = 3001; 3001

# Line definitions
# Each definition should have LINEn, LINEn_PROXY and LINEn_CALLID
# LINEn is the dial number
# LINEn_PROXY is the PROXYn server this line should register with, typically
# defined in sip_allusers.cfg.
# LINEn_CALLID is shown on the standby display of MH150/MH160 phones but not
# MH150 or e/h340/i640 phones. The Asterisk Server converts the callID
# information to alternative forms defined in the Asterisk configuration
# files for display at the far end of a phone call.
# Up to 5 line definitions can be made for each user
# Line definitions do not necessarily have to have different extensions

```

```

LINE1          = 3001
LINE1_PROXY    = 1
LINE1_CALLID   = Mouse, Mickey

# Two lines may map to the same extension to allow second incoming calls.
LINE2          = 3001
LINE2_PROXY    = 1
LINE2_CALLID   = Brady, Marsha

LINE3          = 3002
LINE3_PROXY    = 1
LINE3_CALLID   = Drew, Nancy

#LINE4         = 804
#LINE4_PROXY   = 3
#LINE4_CALLID  = Sip User 4

#LINE5         = 1014
#LINE5_PROXY   = 2
#LINE5_CALLID  = Sip User 5

# Favorite Dialed Number list.
# You can define up to 8 total entries including any defined in
# sip_allusers.cfg.
# You can enclose a string in quotes to allow for spaces.
# Each favorite can be complete SIP URI
# Format is:
# FAVORITE = dial_string; username
#
# The username can be blank and can include escaped chars.
FAVORITE = 3001; Bob
FAVORITE = 3032; Jill in Accounting
FAVORITE = 3013; SoundPoint 3013
FAVORITE = 3020; Jane
FAVORITE = 93035551212; Richard's Cell

```

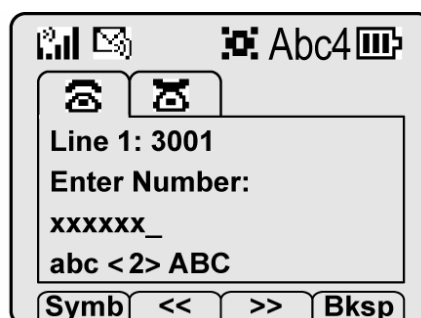

7

Using the MH150/MH160 Mobile Handset

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:

Figure 7-1 Handset call status screen



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.

Use the **Nav** keys to navigate to the other call tab(s).

Calling/Called Party Display



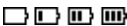






For internally generated received calls, the calling party information that displays on row 3 of the display is either the name as configured in the PBX or the extension number if no name is configured. The first 18 characters are displayed.

The called party name for internal calls is similarly determined. If the name is configured, it will display, if the name is not configured, the extension will display. The first 18 characters are displayed.

Calls originating outside the system display just as they do on wired sets but only the first 18 characters display.







System icons

Table 7-1 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 voicemail icon is activated when a new voicemail message is received if the feature is supported by the phone emulation.
	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 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. 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.
XXXX	During character entry, Indicates current data entry symbol mode.

Call status icons

Table 7-2 Call status icons

Indicator	Function
	On-hook icon, Solid when idle. Flashes while in standby mode to indicate that at least one call is still active or on hold. Flashing when incoming call is ringing.
	Off-hook icon. Solid when a call is being dialed.
	Hold icon. Call is on hold
	Audio flowing icon. Audio is flowing both ways on a call.
	Audio receive-only icon. Locally muted (flash) or far end hold with no music on hold.
	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 described in





Table 7-3 NavOK functions

State	NavOK key function
Dialing	Place phone call
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

Table 7-4 Softkeys

Softkey	Name	Displayed during...	Press to...
<<	Cursor backward	Entering a dial number.	Move the cursor back one position.

Softkey	Name	Displayed during...	Press to...
>>	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.
Dial	Dial Call	A dial number is being entered on the selected line.	Initiate a phone call to the entered dial number.
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.
Hld	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. <i>Note: Appears only if the PROXYn_MAIL_NOTIFY is configured. A message center contact address must be defined for the proxy used by the selected line.</i>	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 predialed. <i>Note: Redial of last overlapped dialed number is not supported.</i>
Rtv	Retrieve	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.
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.

Menus

Line menu

The Line menu allows you to initiate 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 SIP TFTP configuration file. A handset may have up to five line appearances, and can support one call per line. Press the **More** softkey to page through additional items on the **LINE** menu.

Press the **LINE** key from the standby mode to activate the handset and to place a new call on the selected line.

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

Exit the **LINE** display by highlighting a line and pressing **START** or **NavOK** which initiates a call on that line or by highlighting a line and pressing the corresponding line number key to start a new call on the selected line or by pressing **END** to exit the **LINE** display without placing a call.

A new call may be initiated while in an active call. Pressing the **LINE** key places the active call on hold automatically. If there is an existing call, the new call must be placed on a different line. You may press the **END** key to exit the **LINE** display and return to the active call without starting a new call.

If you attempt to make a call on the same line as an already active call, you will get the error message **No selected line**.

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.

Table 7-5 Characters available in symbol modes

Key	Number	English	Number + English	Punctuation
1	1	1; :/\!	'1	@:1
2	2	abc2ABC	2ABCabc	; , 2
3	3	def3DEF	3DEFdef	& `~3
4	4	ghi4GHI	4GHIghi	()4
5	5	jkl5JKL	5JKLjkl	<>5
6	6	mno6MNO	6MNOmno	{ } 6
7	7	pqr7PQRS	7PQRSpqr	[]7
8	8	tuv8TUV	8TUVtuv	' " 8
9	9	wxyz9WXYZ	9WXYZwxyz	^_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.

After pressing **START**, press the **Favr** softkey to display a menu of pre-defined numbers or names that can be dialed (as programmed in the SIP TFTP configuration file.) Highlight the desired number and press **NavOK** or **START** to place the call.

FCN menu

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

Xfer/Conf/Wait (shortcut key **1**)

<OAI> (shortcut key **2**)

<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.

Dialing Modes

predial mode

While in standby mode, dial the number; then press **START** or **NavOK** to place the call.

Overlapped dial mode

While in standby mode, press **START** and dial the number. As each digit is pressed, the handset sends it to the PBX. The PBX places the call automatically when the final digit is pressed.

Combined mode

It is possible to start dialing in predial mode and finish in overlapped-dial mode. The MHS150/MHS160 handset stores the pressed digits until you press **START** or **NavOK**. At that time, the handset switches from predial to overlapped-mode. You may then press the remaining digits to complete dialing the number. This feature is a function of the NEC PBX.

At a user level, the apparent differences between these two modes of operation are slight. The significant differences lie in the SIP messaging.

Call-Waiting Modes

The Call-Waiting feature allows a caller to camp-on to a busy extension in order to wait for the line to become free - either through call termination or through call hold at the busy end.

Wait request while hearing busy signal

This mode may be used when user-A places a call to user-B and hears a busy signal. At that point, while listening to the busy signal, user-A may issue a Wait request by selecting **Xfer/Conf/Wait** from the FCN menu. The MHS150/MHS160 handset acknowledges user-A's request by playing a special dial tone. User-A must then enter the Call-Waiting access code. A call-waiting tone signals user-B that there is a call waiting. User-A hears a call-waiting ring-back tone. User-B may switch

to the waiting call by selecting **Xfer/Conf/Wait** from the FCN menu on his handset. This places user-B's original call on hold and connects him to user-A. This mode is supported on the Univerge NEAX 2400 IPX and Univerge NEAX 2000 IPS.

Using the Call-Waiting access code

When a user knows that the extension he intends to call is busy even before the call is placed, he may issue a Wait request by dialing the Call-Waiting access code directly. When the special dial tone sounds, he dials the busy extension's number. A call-waiting tone signals user-B that there is a call waiting, while user-A hears the call-waiting ring-back tone. User-B may switch to the waiting call as described above. This mode is supported on the Univerge NEAX 2400 IPX.

PBX-activated Call-Waiting



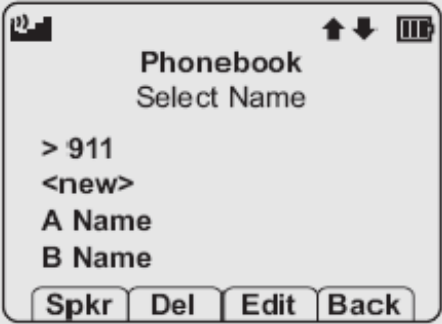
The third mode of Call-Waiting is activated automatically by the PBX without any action required from the user. In this mode, when user-A places a call and the number is busy, the PBX automatically plays the call-waiting-tone to user-B while user-A hears the call-waiting ring-back tone. User-B may switch to the waiting call as described above. This mode is supported on the Univerge NEAX 2400 IPX and Univerge NEAX 2000 IPS.

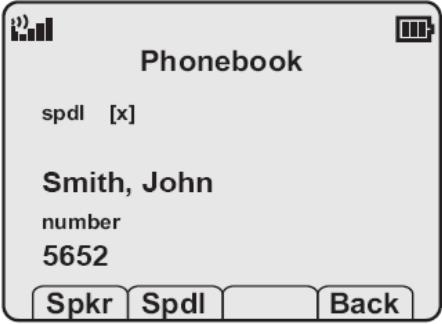

Handset Operation

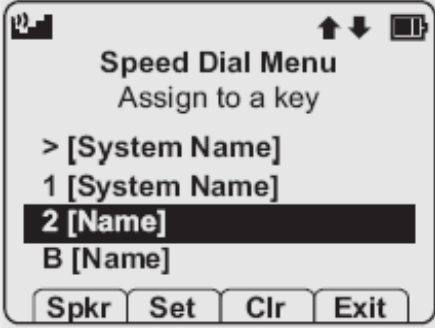
If you want to...	Then...
Turn the handset on	Press and hold the END key until two chirps sound.
Turn the handset off	Press and hold the END key. One chirp will sound. If you are in a call, hang up first, then turn off the handset.
Unlock the keypad	Press the Unlk softkey, then # .
Lock the keypad	While in Standby mode, press the Cfg softkey, then press NavOK .
Place a call	<ol style="list-style-type: none"> To dial a number, follow any one of these sequences <ul style="list-style-type: none"> Press the START key, wait for a dial tone, then dial the number. Dial the number and then press the START key or NavOK. Press the Spkr softkey, then dial the number. Press the START key; press the Favr softkey; use the Nav ▲ ▼ keys to select the number or user from the list; press NavOK to dial the number. Listen for the ring to indicate the alerting of the called party. <p>Note: Line 1 is the default line.</p>
Place a call from Favorites menu	<ol style="list-style-type: none"> Press START or Spkr. Listen for dial tone. Press the FAVR softkey. Use the Nav keys to navigate to the desired entry. Select the entry by pressing NavOK. Press START or NavOK to place the call.
Place a second call	<p>The handset supports one active call per line. To place a second call while the first call is on Hold, the handset must have multiple line appearances.</p> <ol style="list-style-type: none"> To get a dial tone for the second call, press LINE + [different line number]. Press the number key for the line, or press NavOK. The first call is automatically placed on hold and the second call appears in a new active call tab. Dial the number to place the second call. Use the Nav ◀ ▶ keys to toggle between calls. Press NavOK or Rtv to resume the call on the active call tab.
Place a call on a different line	<ol style="list-style-type: none"> Press the LINE key. Navigate to the desired line and press NavOK or press the number key for the line. Dial the number.
Answer a call	<p>Use the Nav keys to display the tab of the inbound call displaying a flashing phone icon. Do one of the following:</p> <ul style="list-style-type: none"> Press START, and hold the handset to your ear. Press the Answ softkey and hold the handset to your ear. Press the Spkr softkey and speak towards the handset.

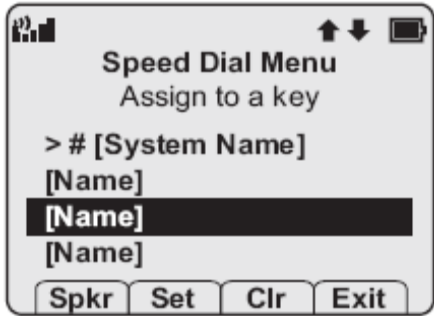

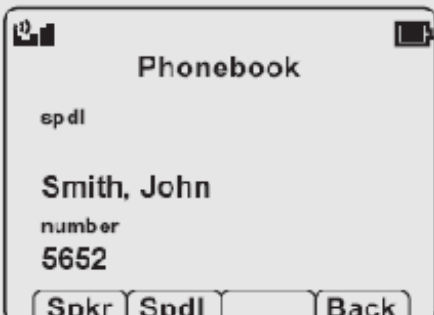
If you want to...	Then...
Answer a call on a second line	<p>If another call comes in on a different line, a new call icon flashes and a tone sounds in the audio stream until the call is answered, the first call is terminated, the caller hangs up, or the call transfers to voicemail.</p> <ol style="list-style-type: none"> To view the caller ID of the incoming call without interrupting the active call, press Nav ►. The original call's audio remains active. The display now shows information about the incoming call. Press NavOK, START or Answ to place the current call on Hold and answer the second call.
Navigate among call tabs	Use Nav ► and Nav ◀ .
Forward all calls	<p>Calls may be forwarded on all lines.</p> <ol style="list-style-type: none"> From the extension you wish to set Call Forward, press START. Listen for Dial Tone. Dial the Call Forward Set Access Code assigned in the PBX. The handset will play a confirmation tone to indicate that Call Forwarding has been activated.
Clear call forwarding	<ol style="list-style-type: none"> From the extension you wish to Clear Call Forward, press START. Listen for Dial Tone. Dial the Call Forward Cancel Access Code assigned in the PBX. The handset will play a confirmation tone to indicate that Call Forwarding has been Canceled.
Listen to voicemail	<ol style="list-style-type: none"> Press START. Press the Msg softkey, or Dial your voice message system number.
Redial the last number you dialed	<ol style="list-style-type: none"> Press START. Press the Redl softkey <p>Note: Redial of last overlapped dialed number is not supported.</p>
Issue a Wait request when you get a busy tone	<p>Note: This is only necessary if the PBX does not automatically activate call waiting.</p> <ol style="list-style-type: none"> While listening to a busy signal, press FCN; select Xfer/Conf/Wait by pressing NavOK. You will hear a special dial tone. Dial the Call-Waiting access code. The Call-Waiting tone will play on the other party's handset, while the Call-Waiting ring-back tone plays on your handset. The other party's selection of Xfer/Conf/Wait places his original call on hold and connects him to you.
Issue a Wait request to an extension you know is busy	<ol style="list-style-type: none"> Press START or Spkr. Dial the Call-Waiting access code. You will hear a special dial tone. Dial the busy extension. The Call-Waiting tone will play on the other party's handset, while the Call-Waiting ring-back tone plays on your handset. The other party's selection of Xfer/Conf/Wait places his original call on hold and connects him to you.
Activate installed custom applications (registered OAI application on an OAI server)	<ol style="list-style-type: none"> Press START or Spkr. Press FCN. Navigate to the desired custom application using Nav ▲ ▼ keys or the More softkey. Select the application using NavOK or shortcut key

If you want to...	Then...
Transfer a call (blind)	<ol style="list-style-type: none"> 1. While in a call, press FCN and select Xfer/Conf/Wait by pressing NavOK. (The current call is placed on hold. You will hear a special dial tone, indicating the start of a new call.) <p>Note: If at this point you press the END key to cancel the transfer, the held call will ring, and should be answered by pressing START or NavOK.</p> <ol style="list-style-type: none"> 2. Dial the number to which you wish to transfer the call or press the Favr softkey and select an entry from the Favorites menu. 3. Press the END key to complete the transfer and return to standby. <p>If the transfer fails, you will see an error message; you can pick up the original call by navigating to the marked call and pressing NavOK.</p>
Transfer a call (consulted)	<ol style="list-style-type: none"> 1. While in a call, press FCN and select Xfer/Conf/Wait by pressing NavOK. (The current call is placed on hold. You will hear a special dial tone, indicating the start of a new call.) 2. Dial the number to which you wish to transfer the call or press the Favr softkey and select an entry from the Favorites menu. 3. When the call is answered, inform the person on the other end that you would like to transfer a call. 4. Press the END key to complete the transfer and return to standby. <p>If you wish to terminate a transfer before the second call is placed press the END key. The call on hold will ring. Resume the call by pressing START.</p>
Transfer an active call to a call on Hold	<ol style="list-style-type: none"> 1. Press FCN and then select Xfer/Conf/Wait by pressing NavOK. The current call is placed on hold. 2. Navigate to the second call (already on hold). 3. Press the Rtv softkey and tell the other party that the call will be transferred. 4. Press the END key to complete the transfer and return to standby.
Start a three-way conference call	<ol style="list-style-type: none"> 1. While in a call, press FCN and select Xfer/Conf/Wait by pressing NavOK. (The current call is placed on hold. You will hear a special dial tone, indicating the start of a new call.) 2. Dial the number of the person you wish to conference with, or press the Favr softkey and select an entry from the Favorites menu. 3. After the call is answered, press FCN and then select Xfer/Conf/Wait by pressing NavOK. You are now in a three-way conference. 4. When any party leaves the conference by pressing the END key, the other two parties will remain in two-way call.
Use Consultation Hold	<p>Consultation Hold becomes available when the three-way conference function is not available.</p> <ol style="list-style-type: none"> 1. While in a call, press FCN and select Xfer/Conf/Wait by pressing NavOK. (The current call is placed on hold. You will hear a special dial tone, indicating the start of a new call.) 2. Dial the number of the person you wish to consult with, or press the Favr softkey and select an entry from the Favorites menu. 3. To place that person on hold and switch back to the first person, press FCN and select Xfer/Conf/Wait by pressing NavOK. 4. Selecting Xfer/Conf/Wait again will switch the parties from on-hold to active and vice-versa. Each time Xfer/Conf/Wait is selected, the call will switch to the party on Hold. 5. Press the END key to return to standby. This will also cause the party on hold to be connected to the other party.

If you want to...	Then...	
Silence the ringing	Press the END key to silence the external speaker ring and convert to in-ear speaker ringing. External speaker ringing will resume when the next incoming call is received while the handset is in standby mode.	
Change the ring volume	Press the up/down volume buttons on the side of the handset during ringing, or while the handset is in standby mode.	
Adjust the speaker volume	While speakerphone is active, press the up/down volume buttons on the side of the handset during the call.	
Adjust the headset volume	While the headset is plugged in, press the up/down volume buttons on the side of the handset during the call.	
Mute/Unmute a call	Press the Mute softkey. When the handset is muted, the audio flowing icon  changes to the audio receive-only icon  . Press the Mute softkey again to restore audio pickup.	
End a call	Press the End softkey to maintain the active mode and view the active calls. Press the END key on the keypad to return to the standby mode.	
Change the profile	Press the Prof softkey and use the Nav keys to select a new profile while in standby mode. The selected profile is marked with an asterisk (*).	
Open the Config menu	Press the Cfg softkey from standby mode.	
Turn on the backlight	The backlight comes on when any key is pressed or when there is an incoming call, and stays on for 10 seconds. It turns off if another key is not pressed within that period.	
Resume a call on hold from standby.	Press the Rtv softkey. If more than one call is on hold, use the Nav ◀▶ keys to select the call you wish to resume and press the Rtv softkey or NavOK .	
Open the Phonebook	Press the Phbk softkey from standby mode. The phonebook may also be opened by pressing the Save softkey when it appears in a call log or during predialing.  The phonebook list is sorted alphabetically. The <new> option appears until the maximum number of entries (20) has been entered.	
View system speed dial number	If the system speed dial key has been programmed, it will be listed as the first entry with a close bracket (>) as the first character. Only the system administrator may change this entry.	
Search for a phonebook entry	Use Nav ▲ and Nav ▼ to scroll through the names or press the keys corresponding to the first letters of the name. Use Nav ◀ and Nav ▶ to edit the search characters as needed.	

If you want to...	Then...	
View a phonebook entry	<p>Select the name and press NavOK.</p>  <p>The entry may be called, assigned a speed dial number or edited from this screen. If a speed dial number has been assigned to this name, it will appear beside spdl.</p> <p>Return to the phonebook list by pressing the Back softkey or NavOK.</p>	
Edit a phonebook entry	<ol style="list-style-type: none"> 1. Select the name to edit from the phonebook list. 2. Press the Edit softkey to open the Edit Number display and edit the existing number. Use the Clr and Del softkeys as needed. 3. Press NavOK to display the Edit Name display and edit the name. 4. Press NavOK to save the changes and exit the editing screens. Press the Back softkey to exit without saving the changes. 	
Dial phonebook number	<p>Select the entry and press START or the Spkr softkey.</p> 	
Enter a new name and number in the phonebook	<ol style="list-style-type: none"> 1. Open the phonebook. 2. Select the <new> option (if available) and press the Edit softkey to open the Enter Number display. 3. Enter the name and number by following the steps for editing a name and number. You must enter alphanumeric characters for the name, not blank spaces. 	
Delete a phonebook entry	<ol style="list-style-type: none"> 1. Open the phonebook and select the entry. 2. Press the Del softkey to delete the entry. 	

If you want to...	Then...	
Open the speed dial list from standby	<p>Press the Spdl softkey from standby mode.</p> 	
View the system speed dial number	<p>If the system speed dial key has been programmed, it will be listed as the first entry with a close bracket (>) as the first character. It is assigned to number 1. Only the system administrator may change this entry.</p>	
Make a speed dial call	<ol style="list-style-type: none"> 1. From standby or while in the speed dial menu, press and hold the corresponding number key on the keypad for one second. The system speed dial key must be pressed for three seconds. 2. The handset will display the name and number for one second before the call is dialed. You may press END during this second to terminate the call. (You may also use the Nav keys to highlight an entry and then press START or the Spkr softkey to dial the number.) <p>If you do not place a call, you may return to standby by pressing the Exit softkey.</p>	

If you want to...	Then...
	<p>A phonebook entry may be assigned to a speed dial key from the speed dial list or from the phonebook edit number display.</p> <p>From the speed dial list:</p> <ol style="list-style-type: none"> 1. Select the speed dial key that you wish to assign. 
Assign a speed dial number	<ol style="list-style-type: none"> 2. Press the Set softkey to open the phonebook list. 3. Use the search routine or the Nav keys to select the desired entry  <ol style="list-style-type: none"> 4. Press NavOK to assign the selected name to that speed dial key. 5. Press NavOK again to exit to standby.
Push to Talk	<p>From the phonebook view number display.</p>  <ol style="list-style-type: none"> 1. Press the Spdl softkey from the view number display in the phonebook. 2. When the speed dial list opens, navigate to an empty slot and press NavOK. This sets the speed dial key to the number in the phonebook. 3. Press END to exit to standby mode and save the speed dial number assignment. <p>Speed dial entries may be edited through the phonebook, as described above.</p> <p>[the PTT Vibrate feature has been added]</p>

If you want to...	Then...
PTT Vibrate	<p>To enhance the alerting of a PTT call, PTT Vibrate may be enabled. When PTT Vibrate is enabled, the handset will vibrate three times whenever a PTT broadcast is received, whether the handset is in standby or in a call. If in a call, the chirp alert will also sound. The vibration does not replace any PTT tone volume already set. To set the handset for PTT vibrate only, enable PTT Vibrate and set the tone volume to zero.</p> <p>PTT Vibrate is disabled by default.</p>

8

Testing a Handset

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

- Step 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.
- Step 2** Place a call and listen to the audio quality. End the call by pressing the **END** key.
- Step 3** Place a call to the handset and verify ring, answer, clear transmit, and clear receive audio.
- Step 4** Use the softkeys to verify all softkey programmed features on the handset.
- Step 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 ["Troubleshooting" on page 12-1](#) for corrective action.

Run Site Survey, Diagnostics Enabled, and Syslog Mode are three diagnostic tools provided to assist the wireless LAN administrator in evaluating the functioning of the NEC MH150/MH160 Mobile Handsets and the system surrounding it. Diagnostic Tools are enabled in the Admin menu.

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

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

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

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

Figure 9-1 Multiple AP mode display

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

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

The following screen shows how the display would look when there are three APs configured with an SSID that matches that of the 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.

Figure 9-2 Three APs with SSID matching handset

a	b	7	b	c	8	-	2	8	0	2	1	0	0		
2	a	e	5	7	8	-	4	8	0	6	2	0	0		
2	a	e	5	9	6	-	5	6	1	1	1	0	0		
A	n	y												D	e
														t	1

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.

Figure 9-3 Any SSID mode selected

a	b	7	b			-	2	8	0	2	A	L	P	H	A
2	a	e	5			-	4	8	0	6	2	0	0		
2	a	e	5			-	5	6	1	1	v	o	i	c	e
M	y	I	D											D	e
														t	1

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

Figure 9-4 *Detail mode display*

i	:	b	b	b	b	b	b	s	n		c	h		b	c	r	
e	e	e	e	e	e	e	e	e	e		D	G	H	I			
r	r	r	r	r	r	r	r	r	r	r	*	x	x	x	x	x	
m	m	m		G	:	g	g	g	g	P	:	p	p	p	p		
A	n	y											S	m	r	y	

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)
- DGHl - standards supported
- rrrrrrrr - rates supported. Basic rates will have a "b" following the rate
- + - more rates are supported than those displayed
- xxxx - WMM or UPSD if those QoS methods are supported
- 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 = decimal number indicating the CCX version advertised by the AP.
 - C = 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"
- mmm - security mode
- G:gggg - group key security
- P:pppp - pairwise key security
- Any/MyID - softkey to toggle between "single SSID" and "any SSID" modes
- Detl/Smry - softkey to toggle between the multiple AP display (summary), and the single AP display (detail)

Numbers racing across the 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.

Screen 2

- Jitter - average error or "wobble" in received packet timing, in microseconds
- Last successful transmit data rate (LastRate)
- Gateway type (GatewayType)

Figure 9-6 Diagnostics screen 2

J	i	t	t	e	r						n	n	n	n	
L	a	s	t	R	a	t	e				n	n	n	n	
G	a	t	e	w	y	T	y	p	e		n	n	n	n	

Where:

mnemo - a mnemonic that indicates what type of gateway is being used

- 11Mb - this system can run at full speed

Screen 3

Screen 3 contains a list of the APs that are heard and the following parameters from each AP:

- Indicator as to whether this is the current AP or an index into the list of other APs heard (C indicates current)
- Last 2 octets of the MAC address of the AP (mmmm)
- Channel number (ch)
- signal strength (ss)
- Either the 802.11 Association ID from the current AP or a mnemonic for the reason code indicating why the handset didn't hand off to this other AP

Figure 9-7 Diagnostics screen 3

C	:	m	m	m	m	c	h	-	s	s	a	i	d		
1	:	m	m	m	m	c	h	-	s	s	m	n	e	m	
2	:	m	m	m	m	c	h	-	s	s	m	n	e	m	
3	:	m	m	m	m	c	h	-	s	s	m	n	e	m	

Where:

- AP mnem - a mnemonic indicating the reason code:
- Unkn - reason unknown
- Weak - signal strength too weak
- Rate - one or more basic rates not supported
- Full - AP can not handle bandwidth requirements
- AthT - authentication timeout

- ## Screen 4

- Figure 9-8** Diagnostics screen 4

[illegible]

Screen 5

- Security error count since power up (Sec-ErrCount)
- MAC sequence number of frame with last security error (LstSecErrSeq)
- (Re)Association failures due to QoS (QoSFailCnt). Usually attributed to insufficient available bandwidth on an AP. add to table?

Figure 9-9 Diagnostics screen 5

S	e	c	-	E	r	r	C	o	u	n	t		n	n	n	n
L	s	t	S	e	c	E	r	r	S	e	q		n	n	n	n
Q	o	S	F	a	i	l	C	n	t				n	n	n	n

Screen 6 - EAP Information

- "xxxxx" in Line 1 is a 5-digit decimal value displaying the EAP authentication failure/error count.
- "xxxxx" in Line 2 is a 5-digit decimal value displaying the error code/sequence for the last EAP authentication reason, listed just below. Line 2 will be blank if the count for Line 1 is zero.
 - 1 = Unknown error
 - 2 = Mismatch in EAP type. The phone is configured with an EAP type (Cisco FSR, PEAP or EAP-FAST) that is not supported by the AP.
 - 3xxx = Certification failure. The certificate presented by the server is found as invalid. "xxx" when having a non-zero value, is the standard TLS alert message code. For example, if a bad/invalid certificate (on the basis of its signature and/or content) is presented by the server "xxx" will be 042. If the exact reason for the certificate being invalid is not known, then the generic certificate error code would be xxx=000. [Refer to <http://www.ietf.org/rfc/rfc2246.txt>, section 7.2 for further TLS alert/error codes].
 - 4xxx = Other TLS failures. This is due to TLS failure other than certification related errors. The reason code (the TLS alert message code) is represented by "xxx". For example, if the protocol version presented by the server is not supported by the phone then xxx will be 70, and the EAP error code would be 4070. [Refer to <http://www.ietf.org/rfc/rfc2246.txt>, section 7.2 for further TLS alert/error codes].
 - 5xxx = Credential Failure. This is due to an invalid username and/or password produced by the phone. xxx when non-zero, presented the 3-digit error code sent by the server in response to phone's credential. For example, if the server has sent the error code as "691", then the EAP error code would be 5691. If the server does not send the error code message, then xxx is defaulted to 000, i.e.,

EAP error code would be 5000. Refer to [1]) <http://www.ietf.org/rfc/rfc2759.txt> section 6, [2] <http://ietfreport.isoc.org/all-ids/draft-zhou-emu-fast-gtc-02.txt> section 2.

E	A	P	E	r	r	C	N	t				x	x	x	x	x	
L	a	s	t	E	A	P	E	R	C	o	d	e	x	x	x	x	

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 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.



NOTE

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).

[Table 9-1](#) lists the syslog messages and which level of logging will produce them.

Table 9-1 Syslog messages

Message type	Errors	Events	Full
Failed Handoff	Yes	Yes	Yes
Successful Handoff	No	Yes	Yes
Security Error	Yes	Yes	Yes
Call Start/End	No	Yes	Yes
Audio stats	No	No	Yes (every 5 secs)
Audio error threshold exceeded	Yes	Yes	Yes
Radio stats	No	No	Yes (every 5 secs)
Radio error threshold exceeded	Yes	Yes	Yes
Error Handling Mode	Yes	Yes	Yes

All syslog messages will include:

- Date and time (to 1/100th of second) since handset power on (The handset time is set when it is powered on to Jan-1 00:00.00 GMT adjusted. If it has obtained a time from the network time server, that time will display instead.)
- Handset's MAC address
- Handset's IP address
- Sequence number

Table 9-2 lists the additional items in each message type.

Table 9-2 Additional Syslog items

Failed Handoff (Sent whenever the handset attempted to handoff, but failed trying.)	Failed AP MAC Failed AP signal strength Current AP MAC Current AP signal strength Failure reason Mobile Handset Transmit Power to Old AP Wireless Telephone Transmit Power to New AP FCCKM - Failed to use CCKM for fast handoff FOKC - Failed to use OKC for fast handoff
Successful Handoff	New AP MAC New AP signal strength Old AP MAC Old AP signal strength Reason for handoff Other candidate APs MAC Signal strength Reason not used Wireless Telephone Transmit Power to Old AP Wireless Telephone Transmit Power to New AP FCCKM* - Failed to use CCKM for fast handoff FOKC* - Failed to use OKC for fast handoff

Security Error	AP MAC AP signal strength Security mode Error details (mode-dependent)
Call Start	Call type (telephony, OAI, PTT) AP MAC AP signal strength
Call End	AP MAC AP signal strength
Audio stats	AP MAC AP signal strength Payload size (in msec) Payloads sent Payloads received Payloads missed (not received) Payloads missed rate (over last 5 seconds) Payloads late Payloads late rate (over last 5 seconds) Average jitter
Average jitter (Sent if payloads missed rate or payloads late rate exceeds 2%, or if the average jitter is over 2 msec)	Same as audio stats
Radio stats	AP MAC AP signal strength Directed packets sent Directed packets received Multicast packets sent Multicast packets received Broadcast packets sent Broadcast packets received TX dropped count TX drop rate (over last 5 seconds) TX retry count TX retry rate (over last 5 seconds) RX retry count RX retry rate (over last 5 seconds)
Radio error threshold exceeded (Sent if TX drop rate exceeds 2% or TX or RX retry rate exceeds 5%)	Same as radio stats
Probe Recovery	Probe Recovery Count
Lockup Recovery	Lockup recovery Count
DCA Initiated radio reset	Reset count when Reset occurred Reset count at the time when the syslog was sent

* Present only when the specific fast handoff method (CCKM, OKC has been enabled.

Messages are formatted like the following example:

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

10

Certifying the Handsets

Prior to determining that an installation is complete, test the handsets following the sequence given in [Testing a Handset](#), and conduct a **Site Survey** mode test according to the directions given in [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 [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 NEC 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.

- Step 1** Referring to [Diagnostic Tools](#), section “[Run Site Survey](#)” on page 9-1, put a handset into **Site Survey** in the **Any/Smry** ESSID mode. Walk throughout the site checking for any expected APs or other ESSIDs.
- Step 2** Then, walk the site again, in **MyID/Smry** ESSID mode, this time checking that every location has adequate coverage (there should be at least one AP stronger than -70 dBm in all areas) and has good channel allocation. (At any point, the strongest AP shown should be on a different channel than the next best choice.)

Step 3 Finally, use the single AP (**MyID/DetI**) 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.

11

Software Maintenance

The NEC MH150/MH160 Mobile Handsets software is maintained by NEC Unified Solutions, Inc. 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.

NEC Unified Solutions, Inc. Customer Service or an authorized associate will provide information about software updates and how to obtain the software.

Upgrading Handsets

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

NEC MH150/MH160 Mobile Handsets allow over-the-air transfer of software updates from the designated TFTP 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 shown in [Table 11-1](#).

Table 11-1 Normal software download messages

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.

Message	Description
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

Table 11-2 lists display messages that indicate a failure or recovery situation during the download process.

Table 11-2 Download failure or recovery messages during download

Message	Description
Server Busy	Handset is attempting to download from a TFTP 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 TFTP download of one of the files. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are: 01 = TFTP server did not find the requested file. 02 = Access violation (reported from TFTP server). 07 = TFTP server reported "No such user" error. Check the TFTP server configuration. 16 = No TFTP server address. Check the TFTP server configuration. 81 = File put into memory did not CRC. The handset will attempt to download the file again. FF = Timeout error. TFTP server did not respond within a specified period of time.
Erase Failed	Download process failed to erase the memory in the 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.

12

Troubleshooting

On occasion, you may run into transmission problems due to any number of factors originating from the wireless LAN. NEC MH150/MH160 Mobile Handsets 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.

Configuration Problems

Certain problems are associated with improper configuration of either the SIP system or the handset.

Configuration problems are generally corrected by changing the configuration on the SIP system or on the handset. There may also be incorrect programming of the AP. See the Configuration Guide for the AP in use at the site.

Handset Status Messages

NEC MH150/MH160 Mobile Handset status messages provide information about the communication between the handsets, AP, and NEC PBX system. [Table 12-1](#) summarizes, in alphabetical order, the status messages.

Table 12-1 Mobile Handset status messages

Message	Description	Action
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.
Address Mismatch	Handset software download files are incorrect or corrupted.	Please contact NEC NTAC for support.
ASSERT xxx c Line yyy	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, please contact NEC NTAC for support.
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 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 Configuration Guide. Try another AP.

Message	Description	Action
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 <i>Configuration Guide</i> . Try another AP.
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 <i>Configuration Guide</i> . 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 NEC Unified Solutions website per <i>Software Maintenance</i> .
Bad Config	Some needed configuration parameter has not been set.	Check all required handset configuration parameters for valid settings.
Bad ESSID	The handset is configured for "static ESSID" (as opposed to "Learn once" or "Learn always"), and no ESS ID has been entered.	Enter an ESSID in the configuration settings or change to one of the "Learn" modes.
Bad Phintl File	Handset software download files are incorrect or corrupted.	Download new software from the NEC Unified Solutions website per <i>Software Maintenance</i> .
Bad Program File	Handset software download files are incorrect or corrupted.	Download new software from the NEC Unified Solutions website per <i>Software Maintenance</i> .
Bad SIP TFTP IP	A bad unicast address has been entered for the SIP TFTP server in static entry mode.	Re-enter the correct IP address in the administrative menus for static IP addresses.
(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 NEC Unified Solutions Battery Pack. Only NEC Unified Solutions Battery Packs will work.
Battery Failed	Battery Pack is damaged or incompatible with handset.	Replace the Battery Pack with a new or confirmed NEC Unified Solutions Battery Pack. Only NEC Unified Solutions 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.
Charging ...	The handset is charging in the desktop charger.	No action needed.
Charge Complete	The handset is now fully charged.	No action needed.
Checking Code	Handset is contacting the TFTP server to determine if it has a newer version of software that should be downloaded.	None, this message should only last for approximately one second. If message remains displayed, 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 TFTP downloaded has a bad redundancy code check.	Try the download again; it is possible the software was corrupted during download. If the error repeats, check that the download image on the TFTP server is not corrupted.

Message	Description	Action
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.
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 NEC Unified Solutions Technical Support and report the error.
DHCP Error (1-5)	DHCP Error 1. DHCP Error 2. DHCP Error 3. DHCP Error 4. DHCP Error 5.	The handset cannot locate a DHCP server. It will try every four seconds until a server is located. The handset has not received a response from the server for a request to an IP address. It will retry until a server is found. The server refuses to lease the handset an IP address. It will keep trying. The server offered the handset a lease that is too short. The minimum lease time is 10 minutes but NEC Unified Solutions Engineers recommend at least one-hour minimum lease time. The handset will stop trying. Reconfigure the server and power cycle the handset. 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 on 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 NEC Unified Solutions website per <i>Software Maintenance</i> .
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 require 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 NEC Unified Solutions website per <i>Software Maintenance</i> .

Message	Description	Action
Flash Config Error	Handset internal configuration is corrupt.	Perform "Restore Defaults" operation via administrator menus (or re-program with Configuration Cradle).
Illegal Proxy Type	Non NEC handset is attempting to run NEC SIP software	Contact Service Representative.
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 TFTP 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 NEC Unified Solutions Technical Support and report the error.
Multiple GW Res	More than one WLAN Voice Gateway 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 NEC Unified Solutions website per 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 DHCP Server	Handset is unable to contact the DHCP server.	Check that DNCP 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."
No IP Address	Invalid IP.	Check the IP address of the handset and reconfigure if required.
No Line Selected	Trying to make a second call on a line that already has an active e call	Press END , press resume, select a different line for your second call.
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

Message	Description	Action
No Net Found No APs	Handset cannot find any APs. This indicates any of the following: No radio link. No ESSID: Auto-learn not supported (or) incorrect ESSID. AP does not support appropriate data rates. Out of range. Incorrect Security settings.	Verify that the AP is turned on. Verify the ESSID of the wireless LAN and enter or Autolearn it again if required. Check the AP configuration against Configuration Guide for AP. 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. Verify that all the Security settings in the handset match those in the APs.
No Net Found No CCX APs	The mobile handset is configured for CCX compatible operation, but cannot find an access point that is advertising CCX capability.	Check the AP configuration against <i>Configuration Guide</i> for AP.
No Net Found No CCKM APs	The mobile handset 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 <i>Configuration Guide</i> for AP.
No Net Found No WMM APs	The mobile handset is configured to use Wi-Fi Standard QoS, but cannot find an AP configured appropriately.	Check the AP configuration against <i>Configuration Guide</i> for AP.
No Net Found xxxxxxxxxx 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 <i>Configuration Guide</i> . Try Site Survey mode to determine a more specific cause.
No PBX Response	The handset has exceeded its retransmission limit with no ACK response from PBX.	Verify that PBX IP address and port are properly configured.
No Reg Domain	Regulatory Domain Not Set.	Configure the Regulatory Domain of the handset.
No SIP DHCP	DHCP is configured but no valid SIP option 43 was found.	Check DHCP configuration for option 43 and reconfigure if required.
No SIP TFTP IP	No IP address has been entered for the SIP TFTP server.	In static IP mode the SIP TFTP server address must be entered in the administrative menus.
No SIP user file	The phone is attempting to download a SIP configuration file from the SIP TFTP 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 SIP TFTP 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 WLAN Voice Gateway address has been entered.	Enter a valid WLAN Voice Gateway 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 WLAN Voice Gateway. 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.

Message	Description	Action
No SVP Server	Handset can't locate WLAN Voice Gateway. WLAN Voice Gateway is not working. No LAN connection at the WLAN Voice Gateway	IP address configuration of WLAN Voice Gateway is wrong or missing. Check error status screen on WLAN Voice Gateway. Verify WLAN Voice Gateway 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.
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.
Not Installed!	A required software component is missing.	Check that all required software files are on the TFTP server, if over-the-air downloading is being used. If the error repeats, contact NEC Unified Solutions 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.
Registering	The handset has completed initialization of the SIP application and is attempting to register lines to the SIP PBX.	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 WLAN Voice Gateway 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 TFTP server that is busy downloading 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 PBX but fails.	Verify that WLAN Voice Gateway capacity has not been exceeded.
Service Rej.	The WLAN Voice Gateway has rejected a request from the handset.	The handset will restart and attempt to re-register with the WLAN Voice Gateway, which should fix the problem. Report to your administrator if it keeps happening.

Message	Description	Action
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 WLAN Voice Gateway 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)	WLAN Voice Gateway is locked.	Try call again later, system has been locked for maintenance.
TFTP ERROR(x):yy	A failure has occurred during a TFTP software download. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are: 01 = TFTP server did not find the requested file 02 = Access violation (reported from TFTP server) 07 = TFTP server reported "No such user" error. 16 = No TFTP server address. 81 = File put into memory did not CRC. FF = Timeout error. TFTP server did not respond within a specified period of time.	Error code 01, 02, 07, or 16 - check the TFTP 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 NEC Unified Solutions Customer Support
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to NEC Unified Solutions.
Unknown xx:yy:zz	A phrase is missing from the phintl file.	Download new software from the NEC Unified Solutions website per Software Maintenance.
Unsupported Codec	The PBX has requested using a codec not supported by the handset.	Check PBX configuration for supported codecs and reconfigure if necessary.
Updating ...	The handset is internally updating its software images.	None. The handset may do this briefly after a download. This is informational only.
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 TFTP server with software that is correct for the handset model.

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.	<p>Verify that the NTP server is properly configured with the correct time.</p> <p>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.</p> <p>If any of the certificates have expired replace them with new certificates</p>
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.	<p>Verify that the NTP server is properly configured with the correct time.</p> <p>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.</p> <p>If any of the certificates have expired replace them with new certificates.</p>
Invalid Usr/Pwd	When WPA2-Enterprise or Cisco FSR is selected, the handset failed to connect due to incorrect device credentials. The username or password doesn't match with the authentication server.	Verify that the required credentials {username, password} are created on the authentication server and match the handset.
802.1X Failure XXXXXXXXXX XXX	<p>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.</p> <p>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.</p>	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.
Unsupported Codec	The handset doesn't have the specified codec to start the RTP stream for a voice call.	Verify that the codecs supported by handset are configured on the call server.
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 Nortel DHCP	In the case of DHCP configuration, the handset is unable to find the call server information from the DHCP message.	<p>Make sure that handset is configured for DHCP mode.</p> <p>Make sure that the DHCP server is configured with all the required IP addresses.</p>
No APs Heard	The handset is unable to hear beacons/probes from any AP in the network in site survey mode.	Verify that the network is properly configured and the handset is able to hear beacons from the AP.



Appendix

Regulatory Domains

Table Appendix-1 details the specifications for regulatory domain settings. NEC recommends that you check with local authorities for the latest status of their national regulations for both 2.4 and 5 GHz wireless LANs.

Table Appendix-1 Regulatory domain settings

Domain Identifier	802.11 Mode	Band	Channels	DFS Required?	Max. Power Limit (peak power)	Countries
01	g only b & b/g mixed	2.4000 - 2.4745 GHz	1 - 11	n/a	100mW (+20dBm)	US Canada Mexico 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	2.4000 - 2.4845 GHz	1 - 13	n/a	100mW (+20dBm)	Europe Australia New Zealand
	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	2412.0 - 2472.0 GHz	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	2.4000 - 2.4835 GHz	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	2.4000 - 2.4845 GHz	1 - 11	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	2.4000 - 2.4745 GHz	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	2.4000 - 2.4845 GHz	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		

For additional information or support on this NEC Unified Solutions, Inc. product, contact your NEC Unified Solutions, Inc. representative.



NEC MH150/MH160 Mobile Handset Administration Guide

NDA-30920, Revision 2