NORTEL

Nortel Communication Server 1000

WLAN Handsets Fundamentals

Release: Release 5.5
Document Revision: 03.02

www.nortel.com

NN43001-505

Contents

New in this release

The following sections detail what is new in *WLAN Handset Fundamentals (NN43001-505)* () for CS 1000 Release 5.5 .

Feature description

Support is provided for the WLAN Handset 6120/6140 through the addition of the Nortel WLAN Handset 6100 Series Administration Tool Software. For more information about this tool for the WLAN Handset 6120/6140, including personal computer requirements, how to install the USB driver, and how to install and use the software, see "WLAN Handset configuration" (page 39).

The self-healing software enhancement functionality requires WLAN IP Telephony Manager 2245 minimum software release 174.034, WLAN Handset 2210/2211/2212 minimum firmware version 97.071, and WLAN Handset 6120/6140 minimum firmware of 115.015.

You configure wireless handsets with the IP address of a designated WLAN Telephony Manager 2245. As the wireless handsets register, they receive a list of IP addresses of other WLAN Telephony Manager 2245 in the network and they distribute among other WLAN Telephony Manager 2245 to share the load. The list of addresses automatically updates each time the wireless handset powers on.

If the WLAN Telephony Manager 2245 fails, the wireless handset drops active calls, then re-registers with another WLAN IP Telephony Manager 2245 in their list. The wireless handsets return to active state after this registration period. This failure does not affect other wireless handsets registered on the other WLAN IP Telephony Manager 2245 units. The recovery period for the wireless handsets on the failed WLAN IP Telephony Manager 2245 is approximately 60 seconds.

This release also includes support for Real-Time Location System (RTLS). RTLS is a wireless radio frequency solution that continually monitors and reports real-time locations of tracked resources.

Other
Revision history

January 2009	Standard 03.02. This document is up-issued to support Nortel Communication Server 1000 Release 5.5. This document includes an update to Regulatory domain, 802.11 configuration, and transmit power section.
December 2007	Standard 03.01. This document is issued to support Nortel Communication Server 1000 Release 5.5.
December 2007	Standard 02.01. This document is issued to support Nortel Communication Server 1000 Release 5.0.
September 2007	Standard 01.04. This document is up-issued to support Communication Server 1000 Release 5.0. This document includes an update to WLAN Handset Standby menu and WLAN Handset Configuration menu sections.
June 2007	Standard 01.03. This document is up-issued to support Communication Server 1000 Release 5.0. This document includes a table of factory default settings for the WLAN Handsets 6120/6140.
June 2007	Standard 01.02. This document is up-issued to reflect changes in technical content.
May 2007	Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: *WLAN IP Telephony: Installation and Configuration (553-3001-304)* () .

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins

- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues

- arrange for automatic notification of new software and documentation for Nortel equipment

- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the current ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Regulatory and safety information

This chapter includes regulatory and safety information about the following topics:

- "European Union Directives Conformance Statement" (page 13)
- "FCC Rules - Part 15" (page 13)
- "Industry Canada Notice" (page 14)
- "Nortel WLAN Handset 6100 Series Dual Slot Charger information" (page 15)
- "Operational warnings" (page 15)
- "Electromagnetic interference and compatibility" (page 16)
- "Handset operation normal position" (page 18)
- "Handset operation body-worn position" (page 18)

European Union Directives Conformance Statement

The WLAN Handsets 2210/2211/2212/6120/6140 comply with the essential requirements and other relevant provisions of R&TTE directive 1999/5/EC. You can obtain a copy of the Declaration from Nortel GmbH address: Ingolstaedter Strasse 14-18, 80807 Munich Germany or from www.nortel.com/corporate/community/environment/life_cycle/declarations.html.

FCC Rules - Part 15

The WLAN Handsets 2210/2211/2212/6120/6140 comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement: This portable device with its antenna complies with FCC's RF radiation exposure limits set forth for an uncontrolled environment. To maintain compliance this transmitter must not be colocated or operating in conjunction with any other antenna or transmitter.

Industry Canada Notice

This device complies with RSS-210 of Industry Canada (IC). Operation is subject to the following two conditions: 1) This device may not cause interference, and 2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

⚠	**WARNING** Changes or modifications to this equipment not approved by Nortel can cause this equipment to not comply with Part 15 of the FCC rules and void the user's authority to operate this equipment.
⚠	**CAUTION** This equipment contains no user-serviceable parts inside. Refer servicing to qualified service personnel.
⚠	**WARNING** • Follow standard acceptance procedures before operating the WLAN Handsets 2210/2211/2212/6120/6140 near life-support systems. • To minimize risk of interference, pacemaker users should not carry the WLAN Handsets 2210/2211/2212/6120/6140 next to the pacemaker. • Avoid placing the handset near small metallic objects. The handset earpiece attracts magnetic objects. • The WLAN Handset 6120 and 6140 produce noise noticeable to hearing aid users. Use a headset compatible with hearing aids. • The WLAN Handsets 2210/2211/2212/6120/6140 comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. • Privacy of communications cannot be ensured when using the WLAN Handsets 2210/2211/2212/6120/6140.

- To prevent radio interference to the licensed service, the WLAN Handsets 2210/2211/2212/6120/6140 must be operated only indoors and kept away from windows to provide maximum shielding.

Nortel WLAN Handset 6100 Series Dual Slot Charger information

This equipment has been tested and complies with the limits for a Class A digital device, pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, can cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This Class A digital apparatus complies with Canadian ICES-003.

Operational warnings

This section contains operational warnings.

> **WARNING**
> **For vehicles equipped with an air bag:** Do not place a portable radio product in the area over the air bag or in the air bag deployment area. An air bag inflates with great force. If a portable radio is placed in the air bag deployment area and the air bag inflates, the radio product can be propelled with great force and cause serious injury to occupants of the vehicle.

> **WARNING**
> **Potentially explosive atmospheres:** Turn off your radio product prior to entering any area with a potentially explosive atmosphere, unless it is a radio product type especially qualified for use in such areas (for example, Factory Mutual Approved). Do not remove, install, or charge batteries in such areas. Sparks in a potentially explosive atmosphere can cause an explosion or fire resulting in bodily injury or even death.
>
> Areas with potentially explosive atmospheres include fueling areas such as below decks on boats, fuel or chemical transfer or storage facilities, areas where the air contains chemicals or particles such as grain, dust, or metal powders, and any other area where you are normally advised to turn off your vehicle engine. Areas with potentially explosive atmospheres are often but not always posted.

> **CAUTION**
> **Loud noise environment:** The WLAN Handsets 2210/2211/2212/6120/6140 are designed to produce optimal voice quality. However, when used in extremely loud noise environments (for example, close to working heavy machinery), users can experience degradation in call quality performance due to echo. Avoid using the handset when traversing these types of environments.

Batteries

All batteries can cause property damage and bodily injury, such as burns, if a conductive material such as jewelry, keys, or beaded chains touch exposed terminals. The conductive material can complete an electrical circuit (short circuit) and become quite hot. Exercise care in handling any charged battery, particularly when placing it inside a pocket, purse, or other container with metal objects.

Cleaning and drying considerations

A leather carrying case can help to protect the surfaces of the radio product and help prevent liquids (for example, rain) from entering into its interior. This product is not waterproof and exposing it to liquids can result in permanent damage.

If your handset interior gets wet, do not try to accelerate drying with the use of an oven or a blow dryer, as this will damage the handset and void the warranty. Instead, do the following: 1. Immediately power off the handset. 2. Remove the battery pack from handset. 3. Shake excess liquid from the handset. 4. Place the handset and battery pack in an area that is at room temperature with good airflow. 5. Let the handset and battery pack dry for 72 hours before you reconnect the battery pack and/or power on the handset. If the handset does not work after following the steps listed above, contact your dealer for servicing information.

Electromagnetic interference and compatibility

This section provides information about electromagnetic interference and compatibility.

> **ATTENTION**
> Nearly every electronic device is susceptible to electromagnetic interference (EMI) if inadequately shielded, designed, or otherwise configured for electromagnetic compatibility.

Facilities

To avoid electromagnetic interference and compatibility conflicts, turn off your radio product in any facility where posted notices instruct you to do so. Hospitals or health care facilities can be using equipment that is sensitive to external RF energy.

Medical devices

This section provides information about EMI and some medical devices.

Pacemakers

The Health Industry Manufacturers Association recommends that you maintain a minimum separation of 6 inches (15 cm) between a handheld wireless radio product and a pacemaker. These recommendations are consistent with the independent research by, and recommendations of Wireless Technology Research.

> **WARNING**
>
> Persons with pacemakers should:
>
> - always keep the radio product more than 6 inches (15 cm) from their pacemakers when the radio product is turned on
>
> - not carry the radio product in a breast pocket
>
> - use the ear opposite the pacemaker to minimize the potential for interference
>
> - turn the radio product off immediately if they suspect the occurrence of interference

Hearing aids

Some digital wireless radio products can interfere with some hearing aids. In the event of such interference, consult your hearing aid manufacturer to discuss alternatives.

Hearing Aid Compatibility (HAC) as per FCC Part 68

Other medical devices

If you use any other personal medical device, consult the manufacturer of your device to determine if it is adequately shielded from external RF energy. Your physician can assist you in obtaining this information.

Use while driving

Check the laws and regulations on the use of radio products in the area where you drive. Always obey them. When using the radio product while driving:

- Give full attention to driving and to the road.

- Use handsfree operation, if available.

- Pull off the road and park before making or answering a call, if driving conditions so require.

Handset operation normal position

Hold the handset as you would any other telephone, with the earpiece to your ear and speak into the microphone. The internal antenna is then positioned properly.

Handset operation body-worn position

To maintain compliance with RF energy exposure guidelines, if you wear a handset on your body when transmitting, always use the handset with a Nortel-supplied accessory as described in the user guide for the handset. Nortel supplies belt clips, holsters, and lanyards for body-worn operation. Use of accessories not supplied by Nortel can cause the handset emissions to exceed RF energy exposure guidelines.

Overview

This chapter contains information about the following topics:

Subject

This document describes configuration, maintenance, and troubleshooting for the Nortel WLAN Handsets:

- Nortel WLAN Handset 2210
- Nortel WLAN Handset 2211
- Nortel WLAN Handset 2212
- Nortel WLAN Handset 6120
- Nortel WLAN Handset 6140

For information about planning, or installation, see WLAN IP Telephony Installation and Commissioning (NN43001-504)

Note on legacy products and releases

This document contains information about systems, components, and
features that are compatible with Nortel Communication Server 1000
Release 5.0 software. For more information about legacy products and
releases, click the **Technical Documentation** link under **Support &
Training** on the Nortel home page:

www.nortel.com

Terminology

In this document, the following systems are referred to generically as
system:

- Communication Server 1000M (CS 1000M)

- Communication Server 1000E (CS 1000E)

Resources

This section lists information sources that relate to this document.

- *WLAN Handset 2210 User Guide (NN10300-077)* ()

- *WLAN Handset 2211 User Guide (NN10300-078)* ()

- *WLAN Handset 2212 User Guide (NN10300-071)* ()

- *WLAN Handset 6120 User Guide (NN43150-100)* ()

- *Features and Services Fundamentals (NN43001-106)* ()

- *Main Office Configuration Guide for the Survivable Remote Gateway
  50 (NN43001-307)* ()

- *Branch Office Installation and Commissioning (NN43001-314)* ()

- *IP Line Fundamentals (NN43001-500)* ()

- *WLAN IP Telephony Installation and Commissioning (NN43001-504)* ()

Online

To access Nortel documentation online, click the **Technical
Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer
representative.

WLAN Handset 2210/2211/2212 and WLAN Handset 6120/6140

The WLAN Handsets 2210/2211/2212 and WLAN Handsets 6120/6140 use Voice over IP (VoIP) technology on IEEE 802.11-compliant Wireless Local Area Networks (WLANs). Access points (AP) use radio frequencies to transmit signals to and from the wireless handsets.

In this document, handsets means the WLAN Handset 2210/2211/2212, and WLAN Handset 6120/6140. Where the feature refers only to a specific handset, the full handset name is used.

Employees carry wireless handsets to make and receive calls as they move throughout the building. The handsets are used only on the premises; they are not cellular phones. The handsets communicate with the CS 1000 system and with the WLAN IP Telephony Manager 2245. Just like wired telephones, the wireless handsets receive calls directly, receive transferred calls, transfer calls to other extensions, and make outside and long-distance calls (subject to corporate restrictions).

The frequencies that are allocated are governed by IEEE guidelines for WLANs and are part of the free spectrum. The WLAN Handset 6120/6140 use a, b, and g frequencies, and the WLAN Handset 2210/2211/2212 use the b frequency.

The handsets work only in a Nortel Succession 3.0 (and later) environment coordinated with a Communication Server (CS) 1000. These handsets communicate with the Nortel call server through the Unified Network IP Stimulus (UNIStim) protocol. The media path of the voice call goes from the handset directly to the destination device (through the WLAN Telephony Manager 2245). In addition, the handset encapsulates all traffic in the SpectraLink Voice Priority (SVP) protocol. The WLAN Telephony Manager 2245 deencapsulates the VoIP traffic from SVP and passes it onto the network—it does not translate between UNIStim and SVP. Therefore, the Telephony Manager 2245 is in the path of all communication to and from the handset. Likewise, signaling goes from the handset to the Telephony Manager 2245 to the call server.

The WLAN Handset 2211 and the WLAN Handset 6140 are the most durable and they are the only handsets that support Push-to-talk (PTT).

Components

The WLAN Handset Series 2200 offers the following components for local configuration:

- Nortel WLAN Handset 2200 Series Configuration Cradle Software—software only

- Nortel WLAN Handset 2200 Series Configuration Cradle—required hardware (serial cable included)

The WLAN Handset 6100 Series offers the following components for local configuration:

- Nortel WLAN Handset 6100 Series Administration Tool Software— software only

- Nortel WLAN Handset 6100 Series Dual Slot Handset Charger— required hardware (USB cable not included)

- USB Cable for the Nortel WLAN Handset 6100 Series Dual Slot Handset Charger

---

ATTENTION

For the purposes of this document

- Configuration Cradle refers to the Nortel WLAN Handset 2200 Series Configuration Cradle.

- Handset Administration Tool refers to the Nortel WLAN Handset 6100 Series Administration Tool Software.

- Dual Slot Handset Charger or Handset Charger refers to the Nortel WLAN Handset 6100 Series Dual Slot Handset Charger.

Language

The handset menus and screens that originate from the Call Server are displayed in the languages supported on the Call Server. The administration and configuration menus, and all other local handset prompts are English-only.

Licenses

The handset appears to the Call Server as a standard IP Phone 2004. Therefore, each wireless handset requires one IP User License and is subject to the same feature packaging requirements as the existing IP Phone 2004.

Wi-Fi Multimedia

The handsets support basic Wi-Fi Multimedia (WMM) to improve Quality of Service (QoS), as defined in the 802.11e specification. WMM provides prioritized QoS capability when concurrent applications, each with unique latency requirements, are competing for network resources.

When WMM is used, all voice traffic originating from the wireless handset is assigned the WMM Voice Access Category, making it the highest priority application. If the wireless network supports WMM, the handsets enable WMM support automatically; otherwise, SpectraLink Voice Prioritization (SVP) is used.

Wired Equivalent Privacy

The handsets support Wired Equivalent Privacy (WEP) as defined by the 802.11a, b, and g specification. Nortel offers the product with both 40-bit and 128-bit encryption. WEP increases the security of the wireless LAN to a level similar to a wired Ethernet LAN.

Wi-Fi Protected Access

The handsets support Wi-Fi Protected Access (WPA) using Preshared Key (PSK), as defined by the 802.11i specification. WPA increases the security of the wireless LAN, using key encryption, key rotation, authentication and message integrity checking.

Wi-Fi Protected Access2

The handsets support Wi-Fi Protected Access2 (WPA2) using Preshared Key (PSK) and Advanced Encryption Standard (AES), as defined by the 802.11i specification. WPA2 increases the security of the wireless LAN, using key encryption, key rotation, data encryption, authentication and message integrity checking.

Virtual Private Network

The WLAN Handset 2212 supports Virtual Private Network (VPN) security. VPN security provides a secure tunnel for the transfer of unencrypted information. A two-phase approach is used to negotiate the tunnel, with Phase 1 protecting Phase 2. Phase 1 uses preshared keys, Diffie-Hellman group, hashing, and encryption. Phase 2 uses hashing and encryption. Both phases have limited, configurable lifetimes.

Push-to-talk feature

With the Push-to-talk (PTT) feature, the WLAN Handset 2211 and the WLAN Handset 6140 can operate in a PTT group-broadcast mode like a two-way radio, in addition to the standard telephone operation.

For more information, see "Push-to-talk" (page 74).

Text-messaging feature

All WLAN handsets support text messaging applications through the WLAN Application Gateway 2246. The application server communicates to the WLAN Application Gateway 2246 through a proprietary Open Application Interface (OAI) messaging protocol. The WLAN Application Gateway 2246 forwards the messages to the WLAN IP Telephony Manager, which encapsulates the message for delivery to the handset.

If text messaging functions are programmed, the handset can receive text messages. While you access text messages, the handset is in messaging mode. Incoming calls ring with the second call ringing sound.

Loud noise environments

The handsets are designed to provide optimal voice quality. However, when used in extremely loud noise environments, (for example, close to working heavy machinery), degradation in call quality can be experienced due to echo. Avoid using the handsets in loud noise environments

Real-Time Location System

The WLAN Handset 6120/6140 supports Real-Time Location System (RTLS). RTLS monitors and reports real-time locations of tracked wireless handsets anywhere within the Wireless Fidelity (WiFi) network. RTLS uses a combination of client software, tags, APs, and system software to locate, track, and monitor wireless headsets within the coverage area.

If you activate RTLS, the following icon appears in the Ring Indicator location on the handset.

Figure 1
RTLS icon

DHCP options

If you use a DHCP Server, configure the following options:

- DHCP Option 3—the Default Gateway
- DHCP Option 7—the Syslog Server
- DHCP Option 42—the Time Server
- DHCP Option 60—the Class Identifier
- DHCP Option 66—the IP address of the TFTP Server
- DHCP Option 151—the IP address of the WLAN IP Telephony Manager 2245
- DHCP Option 152—the IP address for the optional WLAN Application Gateway 2246

For more information about DHCP options, see *WLAN IP Telephony Installation and Commissioning (NN43001-504)* () .

Handset switchover

If a user on an active call is moving about, the call switches from AP to AP in the subnet. This changeover is transparent to the user.

Loss of signal

If a wireless handset is out of range of all APs, it waits 20 seconds for a signal to return. If a signal is not reacquired within 20 seconds, the wireless handset loses connection to the Call Server and any calls are dropped. When the wireless handset comes back into range of an AP, it reestablishes a connection to the Call Server and goes through the system registration process.

ATTENTION

If a wireless handset is out of contact with the system for four seconds (worst case scenario) during UNIStim messaging, a UNIStim failure could occur and cause the wireless handset to lose the UNIStim association with the Line Telephony Proxy Server (LTPS).

Virtual Office

The handsets support Virtual Office. For more information, see *Features and Services Fundamentals (NN43001-106)* () and *IP Line Fundamentals (NN43001-500)* () .

Branch Office

The handsets are supported in a branch office location using the Branch Office feature. Branch Office refers to the Media Gateway (MG) 1000B and the Survivable Remote Gateway (SRG). A WLAN IP Telephony Manager 2245 and supported APs must be installed at the branch office location. Branch office wireless handsets do not require wireless handset infrastructure in the main office.

The wireless handsets in a branch office configuration behave like an IP Phone 2004 in the Branch Office feature. The wireless handsets are administered in the same manner as the IP Phone 2004. The display on the wireless handsets is almost the same as the display on the IP Phone 2004, with one exception—the Local mode display.

Local mode display

The default state of the wireless handset is Standby. To determine whether the wireless handset is in Local mode, press the off-hook (Green) or the MENU keys on the WLAN Handset 2210/2211/2212 or the soft keys and the Nav keys on the WLAN Handset 6120/6140. Pressing these keys changes the state of the handset to Active Idle or Active Off-Hook, therefore putting the handset in communication with the primary Signaling Server.

For the MG 1000B, if a wireless handset is registered to the Small System Controller (SSC) in Local mode, the local-mode license information appears on the wireless handset on the second line of the display. Since the maximum number of display characters on the wireless handset is 19

characters, the local-mode license information about the wireless handset display is truncated. See .

Table 1
IP Phone 2004 and handset Local mode license display (MG 1000B only)

IP Phone 2004	Handset
Licensed days left x	Licensed days lft x
Licensed days left xx	Licensed ds lft xx
Beyond licensed period	Beyond licensd prd

For more information about Branch Office, see *Branch Office Installation and Commissioning (NN43001-314)* () .

Survivable Remote Gateway

The handset can be deployed in a Survivable Remote Gateway (SRG) configuration for both SRG 1.0 and SRG50.

The handset supports Virtual Office in SRG for Normal mode. It is not supported in Local mode.

Test Local mode is not accessible because the Services key is not supported in Local mode.

The navigation keys are supported in Normal mode and not in Local mode.

Since the default state of the wireless handset is Standby, it is only possible to determine if the wireless handset is in Local mode by pressing the off-hook (Green) or MENU keys. Pressing these keys changes the state of the handset to Active Idle or Active Off-Hook, therefore putting it in communication with the primary Signaling Server in the main office.

For more information, see WLAN IP Telephony Installation and Commissioning (NN43001-504). For more information about SRG, see *Main Office Configuration Guide for the Survivable Remote Gateway 50 (NN43001-307)* () .

External Applications Server

The External Applications Server (XAS) applications are not available on the handsets.

CS 1000 features

Nearly all CS 1000 features are supported on the wireless telephone system and WLAN Handsets 2200 Series. For a list of partially supported features, see Table 2 "Partially supported CS 1000 features" (page 27). For a list of the features that are not supported, see Table 3 "CS 1000 features not supported" (page 27).

Table 2
Partially supported CS 1000 features

Feature	Feature full name	Description
DIG	Dial Intercom Group	Handsfree call option is not supported.
HOT I	Intercom Hotline	Voice Intercom Hotline (default) is not supported. The Ringing option is supported.
RGA	Ring Again	Since the handsets cannot buzz, there is no Ring Again tone. The only way to use the Ring Again feature is to determine if the Ring Again indicator is flashing, which is possible only when the wireless handset is in the active state.

Table 3
CS 1000 features not supported

Feature	Feature full name	Description
AAB	Automatic Answerback	Cannot automatically enable Handsfree.
VCC	Voice Call	Cannot automatically enable Handsfree.
	Active Call Failover	Not supported.

IP Phone 2004 features

Table 4 "IP Phone 2004 features" (page 27) provides information about the IP Phone 2004 features for the WLAN Handsets 2200 Series.

Table 4
IP Phone 2004 features

Feature	Supported on the WLAN handsets	Description
Keypad	Yes	

Table 4
IP Phone 2004 features (cont'd.)

Feature	Supported on the WLAN handsets	Description
Navigation keys	Yes	Up—Volume Up button Down—Volume Down button Left button— Right button—
6 feature keys	Yes	
4 soft-labelled keys	Yes	
Display	Partially	IP phone 2004: 5x24 display Handsets: 4x19 display
Message Waiting Indicator	Yes	Small envelope icon in the top right of the handset LCD display
Branch Office	Yes	
Survivable Remote Gateway	Yes	
Virtual Office	Partially	No Services key. Use FCN+7 for the Services key to support Virtual Office.
XAS	No	No Expand key.
Personal Directory Callers List Redial List	Yes	

Table 4
IP Phone 2004 features (cont'd.)

Feature	Supported on the WLAN handsets	Description
Password Admin	No	The handsets can be password-protected, but this is different from the IP Phone 2004 password protection mechanism. The IP Phone 2004 password protection is supported, in addition to the handset password protection.
KEM	No	

Handset firmware

This chapter contains information about the following topics:

- "Wireless handset firmware" (page 31)

- "View the software or firmware version" (page 35)

- "Software updates" (page 35)

- "Wireless handset download messages" (page 37)

Wireless handset firmware

All handsets ship with a generic firmware load that allows them to associate to a wireless LAN and download the functional firmware from a TFTP Server. The wireless handsets do not function properly without the appropriate firmware.

Predownload checklist

The following requirements must be met to download firmware by over-the-air file transfer:

- The wireless LAN must be properly configured and operational through the use of 802.11a, b, and g SVP-compliant wireless APs.

- The Nortel WLAN IP Telephony system must be connected to the network and completely operational.

- A TFTP Server must be available on the network in order to load the appropriate firmware into the wireless handsets.

- The battery pack on the wireless handsets must be fully charged.

- For the WLAN Handset 6120/6140, the Handset Administration Tool must be installed on the PC to which the Dual Charger is connected.

  For more information, see "Handset Administration Tool for the WLAN Handset 6120/6140" (page 57).

To download the wireless handset firmware for the

- WLAN Handset 2210/2211/2212, follow the steps in Procedure 1 "Downloading the firmware for the WLAN Handset 2210/2211/2212" (page 32)

- WLAN Handset 6120/6140, follow the steps in Procedure 2 "Downloading the firmware for the WLAN Handset 6120/6140" (page 33).

> **ATTENTION**
> Without the appropriate firmware, the handsets do not function properly.

Procedure 1
Downloading the firmware for the WLAN Handset 2210/2211/2212

Step	Action
1	Download the latest handset firmware from the Nortel Web site: www.nortel.com/support
2	Follow the instructions http://www.nortel.com/downloadingcontent at to download the following file: • Product Category: Wireless LAN • Product Name: WLAN Handset 2210, WLAN Handset 2211, or WLAN Handset 2212 • Content Type: Releases
3	Ensure the TFTP Server is started.
4	Load the latest version of the handset UNIStim code firmware and place it on the TFTP Server. The five required files are: • slnk_cfg.cfg • pd11gl3.bin • pd11usd.bin • pd11usd3.bin • pi110006.bin
5	If you are assigning static IP addresses, ensure that the wireless handset IP address, TFTP Server IP address, Subnet Mask, and Default Gateway information are accurate in the wireless handset Admin menu. **OR** If you are using a DHCP server, ensure that the DHCP options are configured. For more information, see "DHCP options" (page 24).

6   Ensure the wireless handset has properly configured ESSID and Reg Domain Information within the Admin menu.

If broadcast ESSIDs are accepted at the APs, the handset automatically learns the ESSID information when powering on.

7   Using the Admin menu on the wireless handset, ensure that the License Management menu option is configured to 010.

This ensures the handset checks for the proper UNIStim firmware files each time it powers on.

8   Power on the wireless handset.

The firmware now downloads to the wireless handset. The status bar increments fully across the wireless handset display for each function that is performed in the download process.

Upon completion of the update process, the wireless handset reboots with the new firmware.

9   Register the wireless handset with the CS 1000 system as if it were an IP Phone 2004.

10   Properly label the wireless handset with the appropriate extension number.

For future firmware upgrades, update the firmware files that are stored on the TFTP Server. Each time the wireless handset is powered on, it checks with the TFTP Server to ensure that it has the proper firmware version, and downloads the new firmware if necessary.

--End--

Procedure 2
Downloading the firmware for the WLAN Handset 6120/6140

Step	Action
1	Download the latest handset firmware from the Nortel Web site: www.nortel.com/support.
2	Follow the instructions http://www.nortel.com/downloadingcontent at to download the following file:
	• Product Category: Wireless LAN
	• Product Name: WLAN Handset 6120 or WLAN Handset 6140
	• Content Type: Releases
3	Ensure the TFTP Server is started.
4	Load the latest version of the handset UNIStim code firmware and place it on the TFTP Server.

The five required files are:

- slink_cfg.cfg
- pi1400us.bin
- pd14cus.bin
- pd14odus.bin
- pd14udus.bin

5 If you are assigning static IP addresses, ensure that the wireless handset IP address, TFTP Server IP address, Subnet Mask, and Default Gateway information are accurate in the wireless handset Admin menu.

   OR

   If you are using a DHCP server, ensure that the DHCP options are configured. For more information, see "DHCP options" (page 24).

6 Ensure the wireless handset has properly configured SSID and Reg Domain Information within the Admin menu.

   If broadcast SSIDs are accepted at the APs, the handset automatically learns the SSID information when powering on.

7 Using the Admin menu on the wireless handset, ensure the Telephony Protocol menu option is configured to 032.

   This ensures the handset checks for the proper UNIStim firmware files each time it powers on.

8 Power on the wireless handset.

   The firmware now downloads to the wireless handset. The status bar increments fully across the wireless handset display for each function that is performed in the download process, and the file name appears.

   Upon completion of the update process, the wireless handset reboots with the new firmware.

9 Register the wireless handset with the CS 1000 system as if it were an IP Phone 2004.

10 Properly label the wireless handset with the appropriate extension number.

   For future firmware upgrades, update the firmware files that are stored on the TFTP Server. Each time the wireless handset is powered on, it checks with the TFTP Server to ensure that it has the proper firmware version, and downloads the new firmware if necessary.

--End--

View the software or firmware version
For the WLAN IP Telephony Manager 2245

To view the firmware versions for the WLAN IP Telephony Manager 2245, follow the steps in Procedure 3 "Viewing the software version" (page 35).

Procedure 3
Viewing the software version

Step	Action
1	From the WLAN IP Telephony Manager 2245 **NetLink SVP-II System** screen, select **System Status** and press **Enter**.
2	On the **System Status Menu** screen, scroll down to **Software Versions** and press **Enter**.
	The Software Version Numbers screen displays the software version for each WLAN system component.

--End--

For a wireless handset

To display the firmware versions running on a wireless handset, power on the wireless handset and hold down the **Power On/Start Call** key

For the WLAN Handset 6120/6140, Firmware Version is also an option on the Config menu.

Software updates

Nortel provides information about software updates. If you do not already know the Product Category, Product Name, and Content Type of the software that you must download, get them from your next level of support. Otherwise, follow the instructions at http://www.nortel.com/downloadingcontent to download the software.

After obtaining the software updates from Nortel, transfer them to the TFTP Server accessed by the WLAN IP Telephony Manager 2245.

Over-the-air transfer of software updates

With the WLAN system, you can perform over-the-air transfer of firmware updates from the designated TFTP Server to the wireless handsets.

The download function in the wireless handset checks the firmware version every time the wireless handset is turned on. If there is any difference in the firmware version, the wireless handset immediately begins to download the update.

On a clear 802.11a, b, or g channel, the download process takes one minute or less to complete.

If the TFTP Server cannot be reached at the time the wireless handset is powered on, resets, or comes back into a WLAN service area, the wireless handset tries a few times to contact the TFTP Server, and then gives up and uses the existing firmware.

If more wireless handsets are requesting TFTP service than the TFTP Server has ports available, or if the TFTP Server is unreachable or unavailable, the wireless handsets try a few times to reach the TFTP Server, and then continues to use the existing firmware. In other words, it is not possible to guarantee that a wireless handset is using the latest firmware. For example, it is not possible to guarantee that all wireless handsets are upgraded as a result of an **isetResetAll** command. To verify that a wireless handset is running the intended version of firmware, use the **isetShow** command to determine the firmware version.

From the Signaling Server or Voice Gateway Media Card, use the oam> or IPL> **isetGet** command to display a list of all currently registered wireless handsets that are running the old firmware version. Use this command on all LTPS Signaling Servers or Voice Gateway Media Cards that have IP Phones and wireless handsets currently registered:

oam> isetGet fwvsn==<old 221022112212 firmware version>

Firmware update (version 97.071) for WLAN Handsets 2210/2211/2212

To download version 97.071 of the firmware for the WLAN Handsets 2210/2211/ 2212, follow the steps in Procedure 4 "Updating firmware for the WLAN Handsets 2210/ 2211/ 2212" (page 36). Version 97.07 1 is compatible with new or existing wireless handsets.

Procedure 4
Updating firmware for the WLAN Handsets 2210/ 2211/ 2212

Step	Action
1	Go to www.nortel.com.
2	Follow the instructions http://www.nortel.com/downloadingcontent at to download the following file: • Product Category: Wireless LAN • Product Name: WLAN Handset 2210, WLAN Handset 2211, or WLAN Handset 2212 • Content Type: Releases
3	Select **Find Products > A-Z**.

4   Select **W**.

5   Scroll to **WLAN Handset 2210/2211/2212** and select **Software**.

6   Select **WLAN – Handsets 2210/2211 Firmware version 97.070**.

--End--

Displays

When the wireless handset is powered on, it displays a series of messages indicating that it is searching for new firmware, checking the versions, and downloading the firmware. During the download, a progress bar on the wireless handset display screen displays the progress of the download.

> **ATTENTION**
> While the wireless handset is updating the firmware, the NO SVC message displays, and the wireless handset should not be powered off. For approximately 10 seconds, the wireless handset cannot be powered off. A warning message appears during that time. If the warning message is not displayed, the wireless handset can be powered off without damage.

When the update is complete, the wireless handset displays the extension number, and is ready for use.

Wireless handset download messages

The following sections describe wireless handset download messages.

Normal download messages

When the wireless handset is powered on, it displays a series of messages indicating that it is searching for new firmware, checking the firmware versions, and downloading. The normal message progression is listed in Table 5 "Normal download messages" (page 37).

Table 5
Normal download messages

Message	Description
Checking Code	Wireless handset is contacting the TFTP Server to determine if the server has a newer version of firmware that should be downloaded.
Erasing Memory	Wireless handset has determined that a download should occur and is erasing the current firmware from memory. This message also displays a progress bar. When the progress bar fills the display line, the erase operation is complete.
Updating Code	Wireless handset is downloading new firmware into memory. 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 wireless handset displays the extension number, and is ready for use.

Download failure or recovery messages

Table 6 "Failure and recovery messages" (page 38) lists the display messages for the wireless handset that indicate a failure or recovery situation during the firmware download process.

Table 6
Failure and recovery messages

Message	Description
Server Busy	Wireless handset is attempting to download from a TFTP Server that is busy downloading other handsets and refusing additional downloads. The wireless handset automatically retries the download every few seconds.
TFTP Error (x):yy	A failure occurred during the TFTP download of one of the files. **(x)** = the file number that was being downloaded. **yy** = an error code describing the particular failure. Possible error codes are: • 01 = TFTP Server did not find the requested file. • 02 = Access violation (reported from TFTP Server). • 07 = TFTP Server reported No such user error. Check the TFTP Server configuration. • 81 = File put into memory did not CRC. The wireless handset attempts to download the file again. • FF = Timeout error. TFTP Server did not respond within a specified period of time.
Erase Failed	Download process failed to erase the memory in the wireless handset. This operation retries.
Waiting	Wireless handset has attempted an operation several times and failed, and is now waiting for a period of time before attempting that operation again.
Internal Error OE	OE = Error while writing the Flash (return wireless handset to Nortel).

WLAN Handset configuration

This chapter contains information about the following topics:

System provisioning

Provision the handset on the CS 1000 system in the same manner as an IP Phone 2004. For detailed information, see *IP Line Fundamentals (NN43001-500)* () .

Configuration tasks

Perform wireless handset configuration after the WLAN IP Telephony Manager 2245 is installed and configured. The steps to configure a wireless handset must be performed for each wireless handset.

To enable the handsets to operate on the WLAN system, perform the following tasks:

1. Configure the wireless handset. For more information, see "Handset configuration" (page 40) and "Configuration Cradle for the WLAN Handset 2210/2211/2212" (page 46) and "Handset Administration Tool for the WLAN Handset 6120/6140" (page 57).

2. Program the features on the wireless handset. For more information, see "WLAN Handset 2210/2211/2212" (page 119) and "WLAN Handset 6120/6140" (page 123).

3. Test the wireless handset. For more information, see "Wireless handset testing" (page 133).

The handsets require special configuration to enable them to communicate with the optional WLAN Application Gateway 2246. Ensure that these settings are correct. See "Open and use the Admin menu on the handset" (page 41).

The Configuration Cradle is an accessory to the handsets. Use the Configuration Cradle to create and save configuration snapshots, save the configuration from an already-programmed handset, and write a saved configuration to a handset. For more information, see "Configuration Cradle for the WLAN Handset 2210/2211/2212" (page 46).

The Handset Administration Tool is a software utility for the WLAN Handsets 6120/6140. Use the Handset Administration Tool to configure options on the Admin Menu and the Config Menu, to assist with troubleshooting, and to upgrade the handset firmware. For more information, see "Handset Administration Tool for the WLAN Handset 6120/6140" (page 57).

Handset configuration

Use the following tools to configure the WLAN Handsets:

- Configuration Cradle for the WLAN Handset 2210/2211/2212

- Handset Administration Tool for the WLAN Handset 6120/6140

- Administration Menu on the handset

Configure the WLAN Handset 2210/2211/2212 using the Configuration Cradle

The Configuration Cradle and its software provide an automated method to configure multiple handsets. For a full description, see "Configuration Cradle for the WLAN Handset 2210/2211/2212" (page 46).

Configure the WLAN Handset 6120/6140 using the Handset Administration Tool

The Handset Administration Tool is a software utility designed for rapid administration and configuration of a number of handsets. For a full description, see "Handset Administration Tool for the WLAN Handset 6120/6140" (page 57).

Open and use the Admin menu on the handset

The Admin menu contains configuration options that are stored locally on each wireless handset. Every wireless handset is independent. If the default settings are not desired, the Admin options must be configured in each separate wireless handset that requires different settings.

To open and use the Admin menu

- on the WLAN Handset 2210/2211/2212, follow the steps in Procedure 5 "Opening and using the Admin menu on the WLAN Handset 2210/2211/2212" (page 41).

- on the WLAN Handset 6120/6140, follow the steps in Procedure 6 "Opening and using the Admin menu on the WLAN Handset 6120/6140" (page 42).

Procedure 5
Opening and using the Admin menu on the WLAN Handset 2210/2211/2212

Step	Action
1	With the wireless handset powered off, simultaneously press and hold the **Power On/Start Call** and **Power Off/End Call** keys.
2	Release the **Power On/Start Call** key, and then release the **Power Off/End Call** key. The first option on the Admin menu displays.
	If an Admin password is configured, you must enter the password to open the Admin menu. If no password is configured, the display proceeds directly to the Admin menu.
3	Press the **Up, Down**, and **Select** side buttons, and the soft keys on the wireless handset to scroll through the menu options.
	An asterisk (*) next to an option indicates that it is selected.

- Press the **Up/Down** buttons to display the previous/next menu items.

- Press the **Select** button to select the menu option or item. Alternatively, press the **OK** soft key to select the menu option or item.

- Press the **Save** soft key to save the entry.

- Press the **Bksp** key to backspace when editing the entry.

- Press the **Up** soft key to return to the previous menu level.

- Press **Cncl** to cancel the entry and return to the previous menu level.

- Press the **Exit** soft key to exit the menus.

--End--

Procedure 6
Opening and using the Admin menu on the WLAN Handset 6120/6140

Step	Action
1	With the wireless handset powered OFF, press and hold the **Start** key.
2	While you press the **Start** key, press the **End** key.
3	Release the End key, and then release the **Start** key.
	The first option on the Admin menu appears.
	If an Admin password is configured, you must enter the password to open the Admin menu. The default password is 123456. If no password is configured, the display proceeds directly into the Admin menu.
4	Press the navigation keys and the soft keys on the wireless handset to scroll through the menu options.
	Figure 2 "Navigation keys on the WLAN Handset 6120/6140" (page 43) illustrates the navigation keys.

Figure 2
Navigation keys on the WLAN Handset 6120/6140
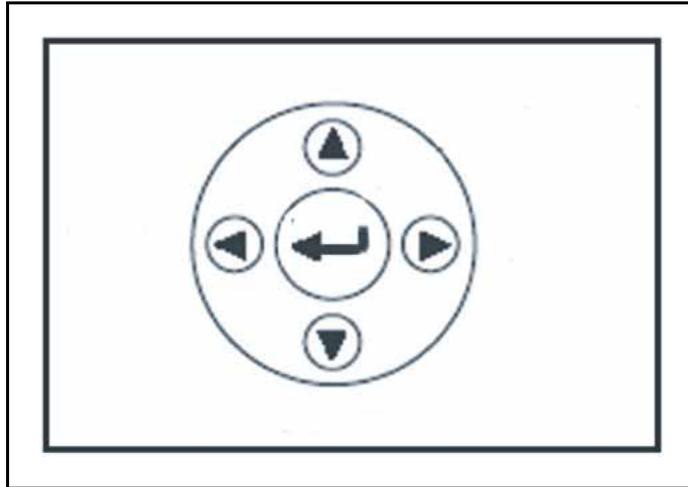
An asterisk (*) beside an option indicates that it is selected.

- Press **Nav** up or down, to display the previous and next menu options.

- Press **Enter** to select a menu option or item.

- Press **Nav <** to backspace when editing an entry.

- Press **Back** soft key to return to the previous menu level.

- Press the **Clr** soft key to delete an entry and then enter new data.

- Press the **Del** soft key to cancel the entry and return to the previous menu level.

- Press the **Exit** soft key to exit the menus.

--End--

Alphanumeric string entry

To make an alphanumeric string entry

- on the WLAN Handset 2210/2211/2212, follow the steps in Procedure 7 "Making an alphanumeric entry on the WLAN Handset 2210/2211/2212" (page 44).

- on the WLAN 6120/6140 Handset, follow the steps in Procedure 8 "Making an alphanumeric entry on the WLAN Handset 6120/6140" (page 44).

Procedure 7
Making an alphanumeric entry on the WLAN Handset 2210/2211/2212

Step	Action
1	On the keypad, press the **Select** button to change the entry.
2	Press the number key of the desired letter.
	The number appears on the display.
3	Press the number key again to display the first letter associated with that key.
4	Press the key again to scroll through the letters associated with that key.
	Example: if **2** is pressed repeatedly, 2, A, B, C, a, b, and c are displayed.
	The following table shows which keys to use to enter nonnumeric characters or other characters not represented on the keypad.

To enter	Press
. - _ ! # $ % & ' ( ) , : ; \ = @ ~	1
Space	0
Q q	7
Z z	9

Step	Action
5	When the correct entry displays, press the right arrow to move to the next character, and repeat for each digit and letter of the entry.
6	Press the **Save** soft key to save the entry and return to the menu. Press the **Exit** soft key to abort and return to the menu without saving any changes.

--End--

Procedure 8
Making an alphanumeric entry on the WLAN Handset 6120/6140

Step	Action
1	Enter a number by pressing any keypad button.
2	Press the number key again to display the first letter associated with that key.
3	Press the **CAPS/caps** soft key to toggle the case.
4	Press the key again to scroll through the letters associated with that key.

Example: if you press 2 repeatedly, 2, A, B, C (CAPS on) or 2,a, b, c (CAPS off) appear on the display.

Use the following keys to enter nonnumeric characters or other characters that are not represented on the keypad.

To enter	Press
. - _! # $ % & ' ( ) , : ; \ = @ ~	*
Space	#

5   After the correct entry appears, press **Nav >** to move to the next character, and repeat for each digit and letter of the entry.

6   Press the **Save** soft key to save the entry and return to the menu.

OR

Press the **Exit** soft key to abort and return to the menu without saving any changes.

--End--

Toggle options for the WLAN Handset 6120/6140

Some menu options on the WLAN Handset 6120/6140 have only two possible selections and operate on a toggle basis. The current setting appears on the second row of the display; this is called the info line. Press Enter to toggle between the selections. For example, when Enable PTT is the menu option, PTT Disabled appears on the info line. If Enable PTT is selected, PTT Enabled appears on the info line and the menu option toggles to Disable PTT.

Partial DHCP configuration

You can use the standard DHCP requirements for Nortel. The handsets that are configured for partial DHCP ignore the call server information from the DHCP server.

To configure partial DHCP, open the Admin menu on the handset and enter the following information:

- Call server 1 IP addr

- Call server 1 port

- Call server 2 IP addr

- Call server 2 port

For more information, see Table 14 "Admin menu options for the WLAN Handset 2210/2211/2212" (page 91) and Table 16 "Admin menu options for the WLAN Handset 6120/6140" (page 106).

Configuration Cradle for the WLAN Handset 2210/2211/2212

The Configuration Cradle is an optional accessory. It is designed to automate the configuration of the wireless handsets.

The cradle is connected to a personal computer (PC) through one of the communication (COM) ports. You can download the software for the PC from Product Category: Wireless LAN, Product Name: WLAN Configuration Cradle for WLAN Handset 2210, 2211, 2212, Content Type: Releases. Obtain the precise Release, Status, and Title of the file from your next level of support. See http://www.nortel.com/downloadingcontent for download instructions. The software is installed on the PC and configured to read from the COM port.

You can configure only one handset at a time.

> **ATTENTION**
> Nortel does not recommend the use of adapters or port replicators because they do not properly handle the communications between the cradle and the PC.

Personal computer requirements

The software runs on Windows NT, Windows 2000, and Windows XP.

Configuration Cradle safety notes

- Do not expose to freezing temperatures or sunlight. The Configuration Cradle operating environment is between 50 to 85 degrees F (10 to 30 degrees C) .

- Use only the original Nortel plug-in power adapter.

- Place only one phone in the cradle at a time.

- Do not place a phone in the cradle with a battery installed.

- Do not immerse the cradle in water or other liquid.

- Do not pour liquids into the telephone slots.

- Only use Nortel telephones in the Configuration Cradle. Do not place anything in the cradle other than the WLAN Handsets 2210/2211/2212, or you can damage the contacts. The cradle cannot work correctly with damaged contacts.

Install and configure the Configuration Cradle

Follow the steps in to install and configure the Configuration Cradle on the PC.

Procedure 9
Installing and configuring the Configuration Cradle

Step	Action
1	On the PC, create a folder for the software.
2	Using a Web browser, connect to www.nortel.com/support.
3	Follow the instructions http://www.nortel.com/downloadingcontent to download the following file to your local terminal:
	• Product Category: Wireless LAN
	• Product Name: WLAN Configuration Cradle for WLAN Handset 2210, 2211, 2212
	• Content Type: Releases
	Obtain the precise Release, Status, and Title of the file from your next level of support.
4	Locate the entry for the NetLink Configuration Cradle.
5	Click the product link and save the Configuration Cradle.exe file to the folder created in Step 1.
6	(Optional) Copy the release notes to the folder created in Step 1.
7	Double-click on the Configuration Cradle.exe file to install the software, putting the files into the folder created in Step 1.
	The tool does not require any additional installation and does not show up in the Programs menu or in the Windows registry.
8	(Optional) To aid in locating the tool quickly, create a shortcut on the computer desktop to the PhoneConfig.exe file.
9	Place the cradle on a flat horizontal surface and plug the power supply into the cradle and into an appropriate power outlet.
10	Connect the cradle, using a serial cable with a DB-9 connector, to one of the COM ports of the PC.
11	Double-click the PhoneConfig.exe file or the shortcut created in Step 8.
12	From the menu at the top of the Config Cradle screen, select **Settings > COM port**.
13	Enter the port number of the COM port that the cradle is uses.
14	Press **OK**.

--End--

If software updates are required, overwrite the installed files with the new files. The existing configuration files are retained.

Use the Configuration Cradle and software

The cradle contains two slots, one for the WLAN Handset 2210 and WLAN Handset 2212 and the other for the WLAN Handset 2211. For more information, see Figure 3 "Configuration Cradle" (page 48). After a handset is placed in the appropriate slot in the cradle, its configuration can be read using the software, and stored as a file on the personal computer. Handset profiles that are saved on the PC can be downloaded to the handset. Profiles can also be created independent of the handset.

Figure 3
Configuration Cradle

WLAN Handset 2211

WLAN Handset 2210
and WLAN Handset 2212

A series of master configuration files can be planned and created using the software. See "Plan the configuration files" (page 49) for a description of files. Planning should be done before any handsets are configured.

After the planning is complete, use the following procedures to:

● Read and save a handset configuration—see "Read and save a handset configuration" (page 52).

● Create a new master configuration file—see "Create a new master configuration file" (page 53).

- Create a new configuration file using the master files—see "Create a new configuration using the master files" (page 53).

- Change an existing configuration file—see "Change an existing configuration file" (page 54).

- Change a configuration from a handset—see "Change a configuration obtained from a handset" (page 55)

- Download a configuration to a handset—see "Download a configuration to a handset" (page 55).

Plan the configuration files

Careful planning of the configuration files reduces the number of custom changes that have to be done on the individual handsets. The software for the Configuration Cradle allows any number of files to be saved.

Settings can be categorized into four types:

- **System (Sys)**—options that are stable across the system. Typically, these include:
  - **License Option**
  - **Network Config**
  - **IP Addressing**
  - **ESSID**
  - **Security**
- **Group (Grp)**—options that are common to groups of users. Typically, these include:
  - **Push-to-talk Allow/Disallow**
  - **Push-to-talk Channel**
  - **Zones**
- **User (Usr)**—options that are default values or can be changed later by the user. Typically, these include:
  - **Ring Options**
  - **Phone Options**
- Custom user options—options that vary on an individual handset basis. Typically, these include:
  - **Static IP Address**
  - **Extension**

Use the available options listed in Table 14 "Admin menu options for the WLAN Handset 2210/2211/2212" (page 91) to determine which options belong in each master category (Sys, Grp or Usr). Each option should be in only one category. Custom user options do not require any additional planning.

After the different categories are determined, each category should have a separate copy of the worksheet, located in "Configuration Cradle worksheet" (page 56). Assign a different descriptive file name to each worksheet.

After the category worksheets are created, use "Create a new master configuration file" (page 53) to create each of the required master configuration files. Create the master files in the following order:

1. System options

2. Group options

3. User options

Finally, when the planning and master files are completed, use the "Create a new configuration using the master files" (page 53) to create the profile for each individual handset and use the cradle to download the profile to the handset.

Configuration Cradle software

Using the software, you can

- name, open and save configuration files

- download and upload configuration settings to and from the handset in the cradle.

- configure options in the Sys, Grp and Usr categories.

The top of the screen is shown in Figure 4 "Configuration Cradle software toolbar" (page 51).

Figure 4
Configuration Cradle software toolbar
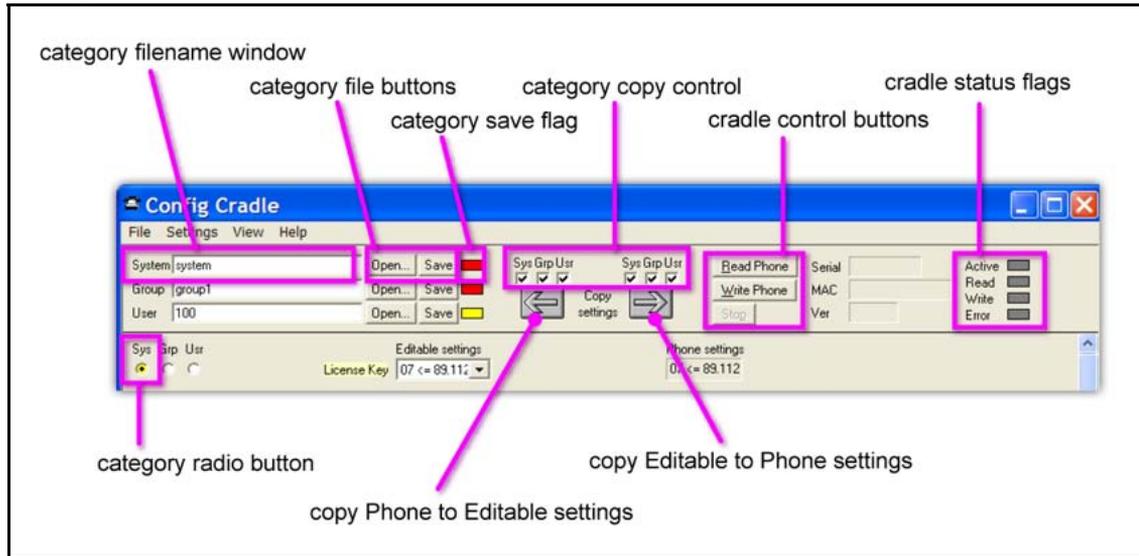
The top portion of the screen is the toolbar, and the bottom portion is the configuration area. Only part of the configuration area is shown in Figure 4 "Configuration Cradle software toolbar" (page 51).

On the left side of the screen is the category file control area. Each category (System, Group and User) has a file name window, file buttons (Open and Save) and a save flag. Each save flag displays different colors, depending on the status of the file:

- Red—file does not exist. The file name in the window is not yet created.

- Yellow—file not loaded. The file name in the window exists in the ConfigData folder but is not loaded into the Editable settings.

- Green—unsaved edits. After you make changes in the Editable settings fields, the green indicator indicates the changes are not saved.

- Gray—file up-to-date. The settings are saved.

To the right of the category file control area is the copy control area, made up of the category copy control boxes and the arrow buttons. The left arrow is used to copy the information in the Phone settings column to the Editable settings column. The right arrow is used to copy the information from the Editable settings column to the Phone settings column. The check boxes above these arrows control which categories are copied.

Next to the copy control area is the cradle control area, made up of the control buttons, flags and information area. The cradle control buttons (Read Phone, Write Phone and Stop) control the communication between the software and the cradle. If no handset is in the cradle when the buttons

are pressed, an error message appears. When the handset is read, its information (Serial number, MAC address and software version) are displayed in the boxes. The status flags display the action in progress with the cradle (Active, Read, Write, Error).

Below the toolbar is the configuration area. Each configurable option appears, with a set of category radio buttons. The category radio buttons are used to indicate which category the option is assigned to. An option can exist in only one category. The option box in the Editable settings column is where changes can be made. The option box in the Phone settings column is read-only.

When entering security keys, the cradle displays the key as entered. This is different from the way the handset handles the display through the Admin menu (key is not displayed).

Read and save a handset configuration

Follow the steps in Procedure 10 "Reading and saving the configuration of an existing handset" (page 52) to read and save the configuration of an already-configured handset. Before performing the following procedure, the Configuration Cradle must be installed. For more information, see Procedure 9 "Installing and configuring the Configuration Cradle" (page 47).

Procedure 10
Reading and saving the configuration of an existing handset

Step	Action
1	Start the **Config Cradle** software by double-clicking the PhoneConfig.exe file of the tool.
2	Remove the battery from the handset.
3	Place the handset in the proper slot in the cradle. See Figure 3 "Configuration Cradle" (page 48).
4	Press the **Read Phone** soft key in the **Config Cradle** screen. The configuration of the phone is read and appears in the right hand column, labeled **Phone settings**.
5	Press the left arrow button: The configuration data is copied from the **Phone settings** column to the **Editable settings** column.
6	(Optional) Press the radio button associated with each item to designate in which category (**Sys, Grp, Usr**) the item belongs.

Category	Description
System (Sys)	System-wide settings
Group (Grp)	Settings for a particular group
User (Usr)	Unique settings for a particular user

7 Enter a file name in the name box beside the category.

8 Press the **Save** button for the appropriate category to save the settings.

The red box beside the Save button changes to green after the save is complete.

--End--

Create a new master configuration file

Use Procedure 11 "Creating a new master configuration file" (page 53) to create a new master configuration file, starting from a worksheet.

Procedure 11
Creating a new master configuration file

Step	Action

1 Start the **Config Cradle** software by double-clicking the PhoneConfig.exe file of the tool.

2 Using the worksheet, enter the options for the category and press the appropriate category radio button.

3 After you enter all of the options, change the name beside the file buttons to match the name entered in the worksheet.

For example, if the options are for a group, enter the name of the group in the box beside Group.

4 Press the **Save** button associated with the category.

5 The configuration is saved to the named file.

--End--

Create a new configuration using the master files

Use Procedure 12 "Creating a new configuration using the master files" (page 54) to create a new configuration file using the master files.

Procedure 12
Creating a new configuration using the master files

Step	Action
1	Start the **Config Cradle** software by double-clicking the PhoneConfig.exe file of the tool.
2	Press the **Open** button for the System options and select the name of the master system file.
3	Press the **Open** button for the Group options and select the name of the master group file.
4	Press the **Open** button for the User options and select the name of the master user file.
5	Configure any custom user options.
6	Enter a name in the User box and press the associated **Save** button.
7	(Optional) Download the configuration to a handset. For more information, see Step 3 from Procedure 15 "Downloading a configuration to a handset" (page 55).

--End--

Change an existing configuration file

Use Procedure 13 "Changing an existing configuration" (page 54) to change an existing configuration file.

Procedure 13
Changing an existing configuration

Step	Action
1	Start the **Config Cradle** software by double-clicking the PhoneConfig.exe file of the tool.
2	Press the **Open** button associated with the category required and select the name of the file to be opened. The file is read and the settings appear in the **Editable settings** column.
3	Make the changes necessary.
4	Press the **Save** button to update the configuration file.

--End--

Change a configuration obtained from a handset

Use Procedure 14 "Changing a configuration obtained from a handset" (page 55) to change a configuration uploaded from a handset to the PC.

Procedure 14
Changing a configuration obtained from a handset

Step	Action
1	Start the **Config Cradle** software by double-clicking the PhoneConfig.exe file of the tool.
2	Remove the battery from the handset.
3	Place the handset in the proper slot in the cradle. See Figure 3 "Configuration Cradle" (page 48).
4	Press the **Read Phone** soft key in the **Config Cradle** screen. The configuration of the phone is read and appears in the right-hand column, labeled **Phone settings**.
5	Press the left arrow button. ⇐ The configuration data is copied from the **Phone settings** column to the **Editable settings** column.
6	Change the data as required.
7	(Optional) Save the configuration to a file.
8	(Optional) Download the configuration to a handset. For more information, see Step 3 from Procedure 15 "Downloading a configuration to a handset" (page 55).

--End--

Download a configuration to a handset

Use Procedure 15 "Downloading a configuration to a handset" (page 55) to download a configuration file to a handset.

Procedure 15
Downloading a configuration to a handset

Step	Action
1	Start the **Config Cradle** software by double-clicking the PhoneConfig.exe file of the tool.
2	Open the files required for the handset.

3   Remove the battery from the handset.

4   Place the handset in the proper slot in the cradle.

See Figure 3 "Configuration Cradle" (page 48).

5   Press the right arrow button.

$\Longrightarrow$

The configuration data is copied from the Editable settings column to the Phone settings column.

6   Press the **Write Phone** button.

7   After the download is complete, remove the handset from the cradle, replace the battery, and test the handset configuration.

For more information, see Procedure 30 "Testing the WLAN Handset 2210/2211/2212" (page 133).

--End--

Configuration Cradle worksheet

Complete one copy of this worksheet for each category in the configuration plan before using the Configuration Cradle for the WLAN Handset 2210/2211/2212. Label each worksheet with the plan category and file name.

Table 7
Plan category:_____ **File name:** _____

Sys	Grp	Usr	Label	Editable Setting

Handset Administration Tool for the WLAN Handset 6120/6140

The Handset Administration Tool for the WLAN Handset 6120/6140 is a software utility that you install on a PC that has a USB port that can be cabled to the USB port of the Dual Charger. Configuration options include:

- configuring all options on the Admin Menu
- configuring all options on the Config Menu
- assisting with troubleshooting by recording error information
- upgrading the handset firmware

To install the Handset Administration Tool, perform the following tasks:

1. Install the USB driver as described in Procedure 16 "Installing the USB driver" (page 57).

2. Install the software utility as described in Procedure 17 "Installing the Handset Administration Tool" (page 59).

Personal computer and hardware requirements

- Personal computer (PC) running Windows 2000 or Windows XP with a USB port
- Dual Charger for the WLAN Handset 6120/6140
- Power supply for the appropriate country or region
- Dual Slot Handset Charger USB Cable or comparable cable (with 5-pin mini-B connector)

> **ATTENTION**
> USB cables vary in the ability to make a proper connection to the Dual Charger USB port. Use the USB cable recommended by Nortel to ensure compatibility.

USB driver

To install the USB driver, follow the steps in Procedure 16 "Installing the USB driver" (page 57).

Procedure 16
Installing the USB driver

Step	Action
1	On the PC, create a folder for WLAN Handset 6120/6140 configuration.
2	Use a Web browser to connect to:
	www.nortel.com/support

3   Use the Product Finder to locate the Handset Administration Tool software:

- **Wireless LAN—Adapters, Phones & Applications**
- **WLAN Handset 6120 or WLAN Handset 6140**
- **Software**

4   Follow the instructions http://www.nortel.com/downloadingconten t to download the following file to your local terminal:

- Product Category: Wireless LAN
- Product Name: WLAN Handset 6120 or WLAN Handset 6140
- Content Type: Supporting Software

Obtain the precise Release, Status, and Title of the file from your next level of support.

5   Download the USB .zip file to the folder you created in Step 1.

6   Create a folder for the USB files and extract the two files from the zip file into the folder.

The two files are named slnkusb.sys and slnkusb.inf.

7   Place the Dual Charger on a flat, horizontal surface and plug the power supply into the Dual Charger and into an appropriate wall outlet.

8   Plug the USB cable into the Dual Charger and into an available USB port on the PC.

9   Power off a WLAN Handset 6120/6140 and place it into the charger.

The handset automatically powers on in USB mode.

The Microsoft Found New Hardware Wizard opens and asks if it can connect to Windows Update to search for software.

10   Select the **No, not at this time** radio button and click **Next**.

11   On the next dialog box, which prompts you for information about installing the USB device, select **Install from a list or specific location (Advanced)** and click **Next**.

12   On the next dialog box, which prompts you for the location, select **Search for the best driver in these locations**, clear the **Search removable media** check box, select the **Include this location in the search** check box and browse to the location of the USB driver files.

13   Click **Next**.

The Microsoft Wizard displays a warning message that states that the software you are installing has not passed Windows

Logo testing. The USB software has been fully tested and will not harm your system.

14 Click **Continue Anyway**.

15 After the USB driver is installed, click **Finish** to close the wizard, and then proceed with handset configuration.

--End--

Handset Administration Tool installation

To install the Handset Administration Tool for the WLAN Handset 6120/6140, follow the steps in Procedure 17 "Installing the Handset Administration Tool" (page 59).

> **ATTENTION**
> You cannot uninstall the Handset Administration Tool because it runs from its current location and stores its settings locally. It does not modify your system or registry.

Procedure 17
Installing the Handset Administration Tool

Step	Action

1 Use a Web browser to connect to:

www.nortel.com/support

2 Use the Product Finder to locate the Handset Administration Tool software:

- **Wireless LAN—Adapters, Phones & Applications**

- **WLAN Handset 6120 or WLAN Handset 6140**

- **Software**

3 Follow the instructions http://www.nortel.com/downloadingcontent to download the following file to your local terminal:

- Product Category: Wireless LAN

- Product Name: WLAN Handset 6120 or WLAN Handset 6140

- Content Type: Supporting Software

Obtain the precise Release, Status, and Title of the file from your next level of support.

4 Download the Handset Administration Tool software .zip file to the folder you created in Step 1 of Procedure 16 "Installing the USB driver" (page 57) for WLAN Handset 6120/6140 configuration.

5 Extract the individual files from the .zip file to the same folder.

6 Double-click the **HandsetAdminXxyy_yy_yy_yy.exe** file to run the utility.

7 Read and accept the **SpectraLink Software License Agreement**.

8 In the HandsetAdmin Setup window, select one of the following buttons:

- **Update Application**—click to check for and download updates to the Handset Administration Tool. You must be running the tool from a writable location.
  For more information, see "Update application" (page 60).

- **Setup Instructions**—click to display instructions to help you to create Start Menu shortcuts, or to copy HandsetAdmin.exe to another location.

- **Run From Current Location**—click to start the Handset Administration Tool.

--End--

Update application

Use the Update Application button to retrieve a more recent version of the Handset Administration Tool from a local folder or from an FTP server. Nortel recommends that you download the updated versions after you install the program.

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

Package files are located under the /pub/nortel folder on the SpectraLink FTP server. The files have a version number with a .pkg extension in this format:

HandsetAdminXxyy_yy_yy_yy.pkg

You can specify the folder to which the update .pkg is saved; you can then copy the file to the network or other media for use on other PCs.

Procedure 18
Updating the Handset Administration Tool

Step	Action
1	In the HandsetAdmin Setup window, select **Update Application**.
2	In the Select Upgrade method dialog box, select **Update from FTP server** and click **Continue**.
3	In the FTP upgrade configuration window, verify the configuration and click **Connect to Server**. After the connection is established, a list of available files appears.
4	Select a file and click **Update application**.

--End--

Local file update

If you select the Update from local file option, you can browse to the location of the update file. Before you can use this option, you must ensure that the file is downloaded or copied to the local PC.

Use the Handset Administration Tool

The Handset Administration Tool has two separate functional areas: the Administration Console and the Handset Settings Editor.

With the Administration Console, you can connect to the handset, configure and change the password, retrieve error messages, update handset firmware, and update the Handset Administration Tool software.

With the Handset Settings Editor, you can configure handsets and create, save and copy Admin menu options. For more information about using the Handset Settings Editor, see "Admin menu settings" (page 65).

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

- Green—the adjacent label is true and this state is desirable or required.

- Yellow—the adjacent label is true and this state requires caution or attention. For example, a yellow New folder indicator cautions that the file path is to be created. A yellow File exists indicator cautions that the file is to be overwritten.

- Red—the adjacent label is true and this state is undesirable or is accompanied by an error. A message, on the prompt line or in a dialog box, describes the nature of the error.

- Gray—the adjacent label is not true, for example, the handset is not connected.

- Blinking—file status indicators blink yellow when the file status is being queried but is not yet known (for example: when attempting to access slow drives or unresponsive network devices). File status indicators blink red when the path is invalid (mistyped). The Handset indicator blinks when the handset password must be entered.

A prompt line at the bottom of the window provides information about what action to take or the status of the utility.

To connect the handset, follow the steps in Procedure 19 "Connecting to the WLAN Handset 6120/6140 or WLAN Handset 6140" (page 62).

Procedure 19
Connecting to the WLAN Handset 6120/6140 or WLAN Handset 6140

Step	Action
1	In the Handset Administration Tool, select the **Connect** tab.
2	Power off the handset and insert it into the Dual Charger.
3	Type the password.

You must enter a password the first time you insert the handset. The default password is 123456.

> **ATTENTION**
> If you check the **Remember password** box, the password is retained as the default password for all handsets. Unique passwords for each handset are not remembered.

4   Click **Submit**.

After a connection is established between the program and the handset, the **Handset connected** indicator turns green and *Connected* appears on the prompt line. The handset is now ready for configuration.

--End--

Password configuration

Use the Handset Administration Tool to enable or disable the password requirement, or to change a current password. Connect to the handset and select the Password tab. If the Enable password check box is unchecked, no password is required to access Admin Settings in the handset Standby menu.

Procedure 20
Changing the password

Step	Action
1	In the Handset Administration Tool, select the Password tab.
2	Type the current password.
3	Type the new password.
4	Retype the new password.
5	Click **Change password**.

--End--

Error information

Use the Error info tab of the Handset Administration Tool to assist the customer service team in troubleshooting handset errors. Use this utility, as directed by customer service, to save any errors as a file that you can send to customer service for handling.

Use the Browse button to establish the path and then enter a file name. Future save operations point to this same location as the default; the same file can be overwritten if desired. A list box displays the most recently used file names. The File time window displays the modification timestamp of the file in the Save as window.

To save a file, click the Get file button. The file is copied from the handset to the location. The Read/Write indicators indicate each action as it occurs. A progress indicator above the prompt line shows file transfer progress.

Firmware updates

Select the Firmware tab and update the firmware in the handset by copying it from a location on your computer to the handset memory.

Each file must be individually downloaded into the handset. This is not an efficient method of updating any quantity of handsets, but it works for testing new code and in extremely small installations. If there is a TFTP server that is broadcasting older code, the handsets continue to download code over the air and revert to the older code after you power cycle them.

Procedure 21
Updating the WLAN Handset 6120/6140 firmware

Step	Action
1	Download the firmware update from www.nortel.com/support.
2	Follow the instructions http://www.nortel.com/downloadingcontent to download the following file to your local terminal: • Product Category: Wireless LAN • Product Name: WLAN Handset 6120 or WLAN Handset 6140 • Content Type: Releases Obtain the precise Release, Status, and Title of the file from your next level of support.
3	Create a new folder for the firmware update.
4	From the .zip file, extract the bin files to the folder that you created in Step 2.
5	Use the Handset Administration Tool to connect to the handset.
6	In the Handset Administration Tool, select the **Firmware** tab.
7	Click **Browse** to locate and select the firmware files. A list box displays the most recently used filenames. The File time indicator displays the modification timestamp of the selected file. The file version and handset version indicators display the version of the selected file and the version of the handset firmware for comparison.
8	Verify that the correct firmware update file is selected and click **Update**. The file is copied from the location to the handset. The Read/Write indicators indicate each action as it occurs. During a firmware update, you can open other tabs. The handset indicators on the tabs indicate the status of the update.
9	Repeat Step 6 and Step 7 for each of the .bin files.

--End--

If an Error indication occurs, ensure that the handset is properly seated and that the USB cable is in good condition and connected securely, and then retry the update. Contact Customer Service if an error persists.

Version
To view the serial number of the handset and the current firmware version, select the Version tab.

To update the Handset Administration Tool, click the Update Application button.

For more information, see .

Admin menu settings

Select the Settings tab in the Handset Administration Tool to configure required and optional settings in the Admin Menu. You can also assign end user Config Menu options such as user name. Which options are available depends on the firmware used by the handsets. For specific configuration requirements, see the Configuration and Administration document that pertains to the protocol used by the system at your site.

The handset serial number and firmware version appear on the Settings tab. To display the version of the Handset Administration Tool, click Show Tool Version.

To enter and modify menu settings, click Show Settings Editor. After the Handset Settings Editor appears, to close the Settings tab window, click Close this window. To reopen the Settings tab window from the Handset Settings Editor, select View>Admin functions.

Handset Settings Editor toolbar

With the Handset Settings Editor toolbar you can name, open, and save configuration files. You can also download and upload configuration settings to and from the handset in the charger.

Figure 5
Handset Settings Editor toolbar

Use the three file name windows to open and save settings by System, Group or User type as separate files. To assign a file name, type it into the field and click Save. By default, the files are saved in a new folder named ConfigData in the folder where the program is stored. The new folder is created automatically the first time a file is saved. To open an existing file, click Open and browse to the file. Use the File menu to customize the file structure.

The file indicators beside the Save buttons use four colors to indicate the status of the file displayed in the window:

- Red—file does not exist. The file name in the window is not yet created.

- Yellow—file not loaded. The file name in the window exists in the ConfigData folder but is not loaded into the Editable settings.

- Green—unsaved edits. After you make changes in the Editable settings fields, the green indicator indicates the changes are not saved.

- Gray—file up-to-date. The settings are saved.

There are two columns of configuration options. The Editable settings column shows settings that you can save as files. The Handset settings column shows settings that you can copy from or copy to the handset in the cradle. By using the Copy settings arrows and boxes, you can copy settings to the handset column and then write the settings to the handset in the charger.

You can also copy the configuration from a handset to the Editable settings area and then edit or save it. Use the Sys, Grp, and Usr check boxes to specify and copy only the settings that you require.

Use the Read Handset and Write Handset buttons to initiate the transfer of configuration data from or to the handset in the charger.

Four indicators (labeled Handset, Read, Write, and Error) indicate the status of the configuration transfer.

Create a configuration plan

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

ATTENTION
Do not create a plan that saves an option in two different categories. Be sure to establish option categories that do not overlap. For example, Speakerphone and Push-to-talk settings are typically tagged as Grp options and saved in Group files.

After you establish which options are categorized as System, Group, or User, enter the configuration information into the Editable settings fields. Begin with the System options and enter all system-level field values. Click the Sys category button on the left side of the window for each option. To save these settings as a System file, enter the file name in the System file name field and click Save.

To create each Group plan, enter the values in the fields designated as Group types. Click the Grp category button on the left side of the window for each option. Save each plan under a different name in the Group file name field.

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

> **ATTENTION**
> Although you need not save user settings for each handset, it is useful to do so. For example, you can save a user's ring preferences from a handset being replaced so that the new handset can be configured the same way. If you decide to save the configuration for each handset, it is easiest to do this during the configuration process. For more information, see Procedure 22 "Downloading a configuration plan to a WLAN Handset 6120/6140" (page 68).

Configuration planning worksheet

Use a worksheet similar to the one shown in Figure 6 "Sample planning worksheet" (page 67) to design your configuration plan.

Figure 6
Sample planning worksheet

Sys	Grp	Usr	Label	Editable Setting

Download or upload a configuration plan

After you establish your configuration plans, the settings can easily be downloaded to the handsets.

To download a configuration plan to a handset, follow the steps in Procedure 22 "Downloading a configuration plan to a WLAN Handset 6120/6140" (page 68).

To upload a configuration plan from a handset, follow the steps in Procedure 23 "Uploading a configuration plan from a WLAN Handset 6120/6140" (page 68).

Procedure 22
Downloading a configuration plan to a WLAN Handset 6120/6140

Step	Action
1	Use the Handset Settings Editor toolbar to open the System, Group, and User plans for this handset.
2	Enter information unique to the handset, for example, the Extension and User Name fields.
	The Extension field has a Next button that is useful for configuring a quantity of handsets.
3	Copy the settings to the Handset settings fields.
4	Click **Write Handset** to begin the download.
	After the Handset indicator turns off, the download is finished and you can remove the handset from the charger.
5	(Optional) To save the settings unique to this handset, ensure that the correct extension number or other file name exists in the User file name field and then click **Save**.
	You can also load files or edit settings for the next handset—Step 1 and Step 2 during the download.
6	Remove the handset from the charger.

--End--

Procedure 23
Uploading a configuration plan from a WLAN Handset 6120/6140

Step	Action
1	On the Handset Settings Editor toolbar, click **Read Handset.**
	After the Handset indicator turns off, the upload is complete and the handset settings appear in the Handset settings fields.
2	(Optional) Copy settings to **Editable settings** fields.
3	(Optional) Create configuration plans.
	OR
	Save the settings by user or extension.
	For more information, see "Create a configuration plan" (page 66).

--End--

Language configuration

To configure the language of the handset, you must make a configuration change while the handset is in the Idle state and another configuration change while it is in the Busy state.

Idle state

With the handset in the Idle state, press the FCN key and select Language. Choose a language from the list. This configuration controls the language in which the display information that is provided locally by the handset appears.

Busy state

With the handset in the Busy state, press the Menu key and then the FCN key. Choose Services > Telephone options > Language and choose a language from the list. This configuration controls the language that the CS 1000 uses to send display information to the handset.

ATTENTION

The handset does not translate display information received from the call server.

Trans, Conf, Frwr, and More are soft key labels that the handset receives from the call server. These labels appear in the language in which the call server sends them.

IP Phone 2004 mapping

This section describes the mapping between the emulated IP Phone 2004 and the handsets.

Voice Messaging Access

Voice mail access is obtained through the Inbox key. Voice mail is accessed on the wireless handset as FCN+ a digit that corresponds to the assigned key.

Codecs

The handsets are compatible with the G.711 and G.729A/AB codecs. No configuration is required on the wireless handsets.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a standardized protocol that enables clients to be dynamically assigned with various configuration parameters, such as an IP address, Subnet Mask, Default Gateway, and other critical network configuration information. DHCP servers centrally manage such configuration data, and are configured by network administrators with settings that are appropriate for a given network environment.

The wireless handset searches for server configuration in the options listed in Table 8 "DHCP options" (page 70). The wireless handset uses the DHCP options listed if DHCP use is enabled.

Table 8
DHCP options

Option	Meaning
1	Subnet Mask
3	Default Gateway
6	DNS Server
7	Syslog Server
15	Domain Name
42	Time Server
43	Vendor specific*
60	Class identifier
66	TFTP Server
128	Site specific *
144	Site specific *
151	WLAN IP Telephony Manager 2245
152	WLAN Application Gateway 2246
157	Site specific *
191	Site specific *
251	Site specific *
siaddr	Boot server or next server
* Could be used to find the CS 1000 device.	

TFTP

The handsets use TFTP to update the wireless handset firmware over the 802.11a, b, or g wireless LAN.

DNS

Domain Name System (DNS), an industry-standard protocol, locates computers on an IP-based network. IP networks rely on number-based addresses to move information about the network. However, it is easier to remember names than number-based addresses. DNS translates user-friendly names into IP addresses that the network can recognize. The wireless handsets can use DNS to automatically translate names into IP addresses for the TFTP Server and the WLAN IP Telephony Manager 2245.

Site certification

Certification is essential to ensure that the wireless handsets are adequately supported by the site.

Conduct a Site Survey of the installation. Note any areas where coverage is conflicting or inadequate. Note any system difficulties and work with the system administrator to determine the cause and possible remedy. For information about conducting a Site Survey, see "Diagnostic Tools" (page 135). For clues to possible sources of difficulties, see "Troubleshooting the handset" (page 147).

The testing must be performed in typical operating conditions, especially if heavy loads occur. Generally, organize the test according to area and volume, placing numerous calls to others who can listen while coverage tests are performed. Note any areas with excessive static or clarity problems and report it.

Testing signal strength with the handset

This test can be performed only if the Nortel WLAN IP Telephony system is installed and configured.

Follow the steps in Procedure 24 "Testing signal strength using the WLAN Handset 2210/2211/2212" (page 71) to test AP signal strength using the wireless handsets. For more information about the different handsets, see:

- "Run Site Survey for the WLAN Handset 2210/2211/2212" (page 135)
- "Run Site Survey for the WLAN Handset 6120/6140" (page 136)

Procedure 24
Testing signal strength using the WLAN Handset 2210/2211/2212

Step	Action
1	Test signal strength in the covered area by putting a handset in Site Survey mode, using **Any/Smry** ESSID.
	For more information, see "Run Site Survey for the WLAN Handset 2210/2211/2212" (page 135).
	The wireless handset remains in Site Survey mode until it is powered off.
2	Walk the entire coverage area while viewing the display, checking for any expected APs or other ESSIDs.
	For more information, see "Detect overlap or conflicts" (page 73).
3	Change the handset to **MyID/Smry** ESSID mode, and walk the site again, checking that every location has adequate coverage and good channel allocation.

For more information, see "Detect radio signal coverage" (page 73).

4 Change the handset to **MyID/Detl** (single AP mode) and walk the site again, checking each AP to ensure that it is configured for the correct data rates, beacon interval, 802.11 options enable, QoS method and security method.

For more information, see "Confirm supported data rates" (page 73).

5 Make any necessary adjustments to the AP locations and configuration, and then repeat this procedure, starting at Step 1, until the Site Survey shows adequate coverage and the correct configuration at every location.

6 After the testing is complete, press **Power Off/End Call** to power off the wireless handset.

--End--

Procedure 25
Testing signal strength using the WLAN Handset 6120/6140

Step	Action
1	Test signal strength in the covered area by putting a handset in Site Survey mode, using **Any/Smry** SSID.
	For more information, see "Run Site Survey for the WLAN Handset 6120/6140" (page 136).
	The wireless handset remains in Site Survey mode until it is powered off.
2	Walk the entire coverage area while viewing the display, checking for any expected APs or other SSIDs.
	For more information, see "Detect overlap or conflicts" (page 73).
3	Change the handset to **MyID/Smry** SSID mode, and walk the site again, checking that every location has adequate coverage and good channel allocation.
	For more information, see "Detect radio signal coverage" (page 73).
4	Change the handset to **MyID/Detl** (single AP mode) and walk the site again, checking each AP to ensure that it is configured for the correct data rates, beacon interval, 802.11 options enable, QoS method, and security method.
	For more information, see "Confirm supported data rates" (page 73).
5	Make any necessary adjustments to the AP locations and configuration, and then repeat this procedure, starting at Step 1,

until the Site Survey shows adequate coverage and the correct configuration at every location.

6   After the testing is complete, press **Power Off/End Call** to power off the wireless handset.

--End--

Detect radio signal coverage

Use the multiple ESSID mode in the Site Survey function to show the top four APs. Walk the perimeter of the site. The display on the wireless handset shows the top four APs that the wireless handset can contact.

Note any areas that have inadequate dBm readings.

Adequate coverage is when there is one AP with a stronger signal (more than 70dBm) in all areas.

Good channel allocation is when, at any point, the strongest AP shown is on a different channel than the next best choice.

Detect overlap or conflicts

Use the single ESSID mode in the Site Survey function. Use this information to detect overlaps or conflicts in AP signaling

Make note of any areas that have APs that are in contention for the same channel.

It is preferable that no overlaps exist anywhere in the site. If the Site Survey mode indicates two APs using the same channel, at least one other AP must be indicated that is at least 10dBm stronger than the other two APs to prevent channel conflicts.

Confirm supported data rates

Use the **Detl** soft key to displays details of the specific AP. Use this information to confirm signal strength and supported data rates.

Site Survey notes

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

Walk around the site to determine supported data rates, one AP at a time.

Each data rate (1, 2, 5.5, or 11 Mb/s) supported by the AP is shown. The rates that are in the Basic Rate set (sometimes referred to as required rates) are indicated by a b following the rate number. The Supported and Basic data rates should be the same on all APs for the site.

Push-to-talk

With the Push-to-talk (PTT) feature, the WLAN Handset 2211 and the WLAN Handset 6140 can operate in a PTT group-broadcast mode like a two-way radio, in addition to the standard telephone operation. The WLAN Handset 2211 supports eight multicast channels with the current channel saved in memory on the wireless handset. The WLAN Handset 6140 supports 24 multicast channels with the current channel saved in memory on the wireless handset.

> **ATTENTION**
> Push-to-talk is not supported on the WLAN Handset 2210, the WLAN Handset 2212, or the WLAN Handset 6120.

To initiate a PTT call, press the Talk button. All handsets that are monitoring the channel hear the transmission.

The two-way radio mode operates on the concept of a PTT session or call period. The PTT call period begins with the first transmission and ends when there is no two-way radio traffic on the channel for 10 seconds. The PTT mode controls the keypad during a PTT call period. Therefore, you cannot use the keypad for any other function such as accessing the on-hook menus or accessing an OAI application. However, you can place a PBX call.

The WLAN Handset 2211 and WLAN Handset 6140 join the IP multicast stream through Internet Group Management Protocol (IGMP) v1 reports. Each handset continues to send IGMP reports as long as PTT is enabled, so the IP multicast state is maintained in the network, even when there is no active use of the PTT feature. The multicast address used to support PTT is 224.0.1.116, and the port is 5001.

PTT operation

To use the PTT feature

- with the WLAN Handset 2211, follow the steps in

- with the WLAN Handset 6140, follow the steps in

Procedure 26
Initiating a PTT call with the WLAN Handset 2211

Step	Action
1	To initiate a PTT call, press and hold the **Talk** button.
2	Wait two seconds to activate the channel before talking.
3	Speak after you hear the start transmit sound. After you release the Talk button, you hear the end transmit sound. The WLAN Handset 2211 then enters the waiting state where it monitors the channel for up to 10 seconds.
4	Initiate subsequent transmissions by pressing the **Talk** button on any WLAN Handset 2211 that uses the same channel. The start transmit sound is played immediately and speech can begin. The display screen shows the current active channel. Because all phones on that channel are already in the receive state, there is no two-second delay. If no transmission occurs during the 10-second countdown period, the WLAN Handset 2211 plays the end call sound and reverts to the idle state.

--End--

Procedure 27
Initiating a PTT call with the WLAN Handset 6140

Step	Action
1	To initiate a PTT call, press and hold the Talk button.
2	Wait until the Transmitting message appears on the display.
3	Speak into the microphone. After you release the Talk button, you hear the end transmit sound. The WLAN Handset 6120 then enters the waiting state where it monitors the channel for up to 10 seconds.
4	Initiate subsequent transmissions by pressing the Talk button on any WLAN Handset 6120 that uses the same channel. The Transmitting message immediately appears on the display and speech can begin. The display screen shows the current active channel. Because all phones on that channel are already in the receive state, there is no two-second delay.

If no transmission occurs during the 10-second countdown period, the WLAN Handset 6120 plays the end call sound and reverts to the idle state.

--End--

Receiving a PTT transmission

Upon receiving a PTT transmission, the WLAN Handset 2211 plays the receiving alert sound and enters the receive state. In this state, the WLAN Handset 2211 receives all conversations on the selected channel. The WLAN Handset 2211 ignores the Talk key while in the receive state.

The WLAN Handset 2211 screen displays the current active channel, the Caller ID information of the current transmitter, and an indication that the WLAN Handset 2211 is receiving a broadcast transmission. At the end of a transmission, the WLAN Handset 2211 enters the waiting state, where it monitors the channel for up to 10 seconds and displays the Waiting message on the screen. If no other transmission occurs within 10 seconds, the WLAN Handset 2211 plays the end call sound and reverts to the idle state.

The user can push the Up and Down buttons to raise or lower the volume of the PTT transmission. A separate volume is maintained for PTT calls with the current volume selection retained in memory.

To exit a PTT broadcast, press the Terminate soft key and answer Yes to the confirmation prompt. PTT audio is immediately stopped and the WLAN Handset 2211 exits the PTT session. No other WLAN Handset 2211 is affected. Only the current PTT call is terminated for this WLAN Handset 2211. When another PTT call starts, the WLAN Handset 2211 is again in the receive state. A still-active session can be rejoined by initiating a PTT call. See Procedure 26 "Initiating a PTT call with the WLAN Handset 2211" (page 75).

Disable the PTT feature in the on-hook User Menu to prevent receiving any further PTT calls.

PTT dialog is interrupted when you answer an incoming telephone call. After the telephone call ends, PTT dialog resumes if an active PTT call is still transmitting. For more information, see "Interaction with telephone calls" (page 76).

Interaction with telephone calls

You can answer an incoming telephone call during a PTT call session. To announce an incoming call, the WLAN Handset 2211 rings with a low-volume ring and displays the system message. To answer the call,

press **Power On/Start Call**. The PTT call session is preempted and no PTT audio is heard. After the telephone call ends, press **Power Off/End Call** to go back on-hook, at which time PTT becomes active again. If an already active PTT call is ongoing, the PTT audio starts playing again.

If the user does not answer the telephone call by pressing **Power On/Start Call**, the PTT display appears again after the ring stops.

To start a telephone call during a PTT call session, press the **Power On/Start Call** key. This causes the two-way radio to be preempted until the telephone call is ended.

WLAN Handset 2210/2211/2212 Standby menu

You can configure user-defined preferences from the Standby menu. The wireless handset must be in contact with the system, no error messages displayed, and in Standby mode. For more information, see Table 9 "Standby menu" (page 77). An asterisk (*) indicates the default value.

With the handset in the standby state, press and hold FCN briefly to open the standby menu. Use the following keys to display and select options:

- **Up/Down** buttons: display previous or next menu item

- **Select** button: selects the menu item or option

- **OK** softkey: selects the menu item or option

- **Save** softkey: saves the entry

- **Bksp** softkey: backspaces to allow editing of entry

- **Cncl** softkey: cancels edit and returns to previous menu level

- **Up** softkey: returns to previous menu level

- **Exit** softkey: exits the menu (at the top level)

- **End** Call key: exits to standby state (from any level)

Table 9
Standby menu

Menu item	2nd level	3rd level	4th level
Lock Keys			
Language	*English Français Deutsch Español Português Norsk		

Menu item	2nd level	3rd level	4th level
Ring Options	Telephone Ring	Ring Cadence	Off *PBX Continuous Long Pulse Short Pulse
		Ring Tone	*Tone 1 Tone 2 Tone 3 Tone 4 Tone 5
		Ring Volume (WLAN Handset 2211 only)	Bars
		Vibrate Cadence	Off *PBX Continuous Long Pulse Short Pulse
		Ring Delay (appears if Ring Cadence and Vibrate Cadence are both set to a value other than Off)	*No Delay 5 Second Delay 10 Second Delay
	Auxiliary Ring 1		
	Auxiliary Ring 2		
Phone Options	Noise Mode	*Normal High Severe	
	Key Tones	*Enable Tones Disable Tones	
	Warning Tones	*Enable Warnings Disable Warnings	
	Display Contrast	Contrast %	
	Keypad Autolock	*Disable 5 seconds 10 seconds 20 seconds	
System Info	Phone IP Addr		
	Server IP Addr		
	Firmware Version		
Extension			

Menu item	2nd level	3rd level	4th level
Current Call Svr			
Terminal Type	i2004 3rd Party		
Push-to-Talk (WLAN Handset 2211 only)	Channel	Current Channel: X 1 2 3 4 5 6 7 8 New Channel = ?	
	Enable/Disable	PTT Enabled * PTT Disabled	
	Audio Volume		
	Tone Volume		

Lock Keys

If you enable the Keypad Lock option, the keypad locks immediately. To unlock the keypad, press FCN and then the # key.

Language

Select Language, to view the available languages and select a language from the list.

Ring Options

Select Ring to configure the ring for three separate functions. Use Telephone Ring for usual telephony functions. Use the Auxiliary Rings to configure different ringing patterns for OAI applications.

Telephone Ring

Select Telephone Ring to configure a distinctive ring style, volume and sequence. Select from an audible ring or a vibrate-only ring or a vibrate ring along with, or followed by an audible ring.

Ring Cadence

Select Ring Cadence to configure the rhythm of the ring. You can select a preprogrammed ring cadence or opt to obtain the cadence from the PBX. The PBX option utilizes any distinctive rings sent by the PBX while allowing you to configure unique rings for auxiliary applications.

- Off: silent
- PBX: PBX determines ring cadence

  (For example, the PBX can send rings that differentiate between internal and external calls.)

- Continuous: rings continually until answered
- Short Pulse: rings in short bursts
- Long Pulse: rings in long bursts

Ring Tone
Select Ring Tone to select from five available tones. You can use the Play softkey to preview the tones before selection. If you configure Ring Cadence to off, the Ring Tone option does not appear on the menu.

Ring Volume
(WLAN Handset 2211 only) Select Ring Volume to adjust the volume level. The graduated volume bar indicates the levels. This setting can be overridden by adjusting volume while the handset is ringing.

Vibrate Cadence
Select Ring Cadence to configure the rhythm of the ring. You can select a preprogrammed vibrate cadence or opt to obtain the cadence from the PBX. The PBX option utilizes any distinctive vibrate cadence sent by the PBX while allowing you to configure unique vibrate cadence for auxiliary applications.

- Off: silent
- PBX: PBX determines vibrate cadence

   (For example, the PBX can send vibrate cadences that differentiate between internal and external calls.)
- Continuous: vibrates continually until answered
- Short Pulse: vibrates in short bursts
- Long Pulse: vibrates in long bursts

Ring Delay
Select Ring Delay to specify how long the vibrate cadence plays before the audible ring begins. The Ring Delay option appears if both ring cadence and vibrate cadence are configured to PBX, Continuous, Short Pulse or Long Pulse. If Ring Cadence or Vibrate Cadence is turned off, the Ring Delay option does not appear on the menu.

Auxiliary Ring 1 and Ring 2
The Auxiliary rings are designed to be utilized by OAI applications. With Auxiliary Ring 1 and Ring 2 you can configure a distinctive ring for these applications.

Phone Options
The following sections describe the Phone Options menu options.

Noise Mode
Select Noise Mode to specify the noise level in your environment. Select Normal for most office environments; High: for moderate background noise; or Severe: for extremely noisy conditions. The High and Severe

modes adjust the microphone and in-ear speaker volume of the handset to account for background noise. If you use High or Severe mode in a quiet environment, the person on the other end of the line can find it difficult to hear your voice.

Key Tones
Select Key Tones to specify whether tones play when keys are pressed. Key Tones are enabled by default.

Warning Tones
Select Warning Tones to specify whether warning tones (such as system up or down, or out of range) play. Warning Tones are enabled by default.

Display Contrast
Select Display Contrast to adjust the display for different lighting conditions.

Keypad Autolock
Select Keypad Autolock to configure the keypad to lock automatically when the handset enters standby mode. You can disable the automatic locking function (the default) or adjust the autolock for a 5, 10, or 20 second delay before locking.

System Info
The following sections describe the System Info menu options.

Phone IP Addr
Select Phone IP Addr to view the IP address currently assigned to the handset.

Server IP Addr
Select Server IP Addr to view the IP address of the SVP Server and the OAI Server (if installed).

Firmware Version
Select Firmware Version to view the current firmware version of the handset—the MAC address (the hardware identification number configured at the factory) and the three files used by each version:

- Downloader: pd11gl3.bin

- Functional: pd11xxx3.bin

- Phintl: phintl24.bin or pi11xxx.bin

Extension
Select Extension to view the extension currently assigned to the handset. You cannot configure the extension with this option.

Current Call Svr

Select Current Call Svr to view the current Call Server IP address and port number.

Terminal Type

Select Terminal Type to view the type of PBX in use.

Push-to-Talk

From the Push-to-Talk menu, you can enable or disable the PTT feature locally. You can also configure the channel, tone volume and audio volume. The menu for Push-to-Talk does not appear if PTT is disallowed on the Admin menu or if no channel is enabled on the Admin menu.

For detailed information about the user-defined preferences in the Standby menu and how to configure them, see *WLAN Handset 2210 User Guide (NN10300-077)* () , *WLAN Handset 2211 User Guide (NN10300-078)* () , and *WLAN Handset 2212 User Guide (NN10300-071)* () .

WLAN Handset 6120/6140 Configuration menu

You can configure user-defined preferences from the Configuration menu. The wireless handset must be in contact with the system, no error messages displayed, and in Standby mode. For more information, see Table 10 "Configuration menu" (page 82). An asterisk (*) indicates the default value.

With the handset in the standby state, press the Cfg softkey to open the standby menu.

Table 10
Configuration 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 Cadence	Off PBX Continuous Short Pulse Long Pulse

Config menu	2nd level	3rd level	4th level	5th level	6th level
				Ring Tone	Tones 1–10
				Ring Volume	Volume (bars)
				Vibrate Cadence	Off PBX Continuous Short Pulse Long Pulse
				Ring Delay	No Delay 5 Second Delay 10 Second Delay
			Auxiliary Ring 1		
			Auxiliary Ring 2		
		Noise Mode	Normal High Severe		
		Ring in Headset Ring in Speaker			
		Warning Tones Disable/Enable			
		Key Tones Disable/Enable			
		Push-to-talk Disable/Enable (WLAN Handset 6140 only)			
Phone Settings	Keypad Autolock	Disable 5 seconds 10 seconds 20 seconds			
	Language	*English Français Deutsch Español Português Norsk			
	Display Contrast	Set Contrast			

Config menu	2nd level	3rd level	4th level	5th level	6th level
	Use Hearing Aid Use No Hearing Aid				
	Startup Song Play/Inhibit				
	Predial Disable/ Enable				
Push to Talk (WLAN Handset 6140 only)	Default Channel	Channel 1 …. Channel 24			
	Subscribed Channels	Channel 1 Channel 2 Channel 3 Channel 4 …. Channel 24			
	PTT Audio Volume	Audio Volume (bars)			
	PTT Tone Volume	Tone Volume (bars)			
System Info	Phone IP Address				
	Alias IP Address				
	SVP IP Address				
	Curr Call Server				
	Terminal Type				
	Firmware Version				
Extension	Enter Number **				
User Name	Enter User Name				
** CS 1000 —The extension number cannot be edited. The handset obtains the extension from the server and it appears on the info line when you select this option. BCM —You must configure the extension number here in the Config Menu for it to appear on the handset in standby mode and in Caller ID					

Lock Keys

If you enable the Keypad Lock option, the keypad locks immediately. To unlock the keypad, press FCN and then the # key.

User Profiles

Select and configure your user profile.

Ring Settings

From the Ring Settings menu, you can configure the ring for three separate functions. Use Telephone Ring for usual telephony functions. Use the Auxiliary Rings to configure different ringing patterns for OAI applications.

Telephone Ring

Select Telephone Ring to configure a distinctive ring style, volume and sequence. Select from an audible ring or a vibrate-only ring or a vibrate ring along with or followed by an audible ring.

Ring Cadence

Select Ring Cadence to configure the rhythm of the ring. You can select a preprogrammed ring cadence or opt to obtain the cadence from the PBX. The PBX option utilizes any distinctive rings sent by the PBX while allowing you to configure unique rings for auxiliary applications.

- Off: silent
- PBX: PBX determines ring cadence

   (For example, the PBX can send rings that differentiate between internal and external calls.)

- Continuous: rings continually until answered
- Short Pulse: rings in short bursts
- Long Pulse: rings in long bursts

Ring Tone

Select Ring Tone to choose from five available tones. You can use the Play softkey to preview the tones before selection. If you configure Ring Cadence to off, the Ring Tone option does not appear on the menu.

Ring Volume

(WLAN Handset 2211 only) Select Ring Volume to adjust the volume level. The graduated volume bar indicates the levels. This setting can be overridden by adjusting volume while the handset is ringing.

Vibrate Cadence

Select Ring Cadence to configure the rhythm of the ring. You can select a preprogrammed vibrate cadence or opt to obtain the cadence from the PBX. The PBX option utilizes any distinctive vibrate cadence sent by the PBX while allowing you to configure unique vibrate cadence for auxiliary applications.

- Off: silent
- PBX: PBX determines vibrate cadence

  (For example, the PBX can send vibrate cadences that differentiate between internal and external calls.)

- Continuous: vibrates continually until answered
- Short Pulse: vibrates in short bursts
- Long Pulse: vibrates in long bursts

Ring Delay

Select Ring Delay to specify how long the vibrate cadence plays before the audible ring begins. The Ring Delay option appears if both ring cadence and vibrate cadence are configured to PBX, Continuous, Short Pulse or Long Pulse. If Ring Cadence or Vibrate Cadence is turned off, the Ring Delay option does not appear on the menu.

Auxiliary Ring 1 and Ring 2

The Auxiliary rings are designed to be utilized by OAI applications. With Auxiliary Ring 1 and Ring 2 you can configure a distinctive ring for these applications.

Noise Mode
Select Noise Mode to specify the noise level in your environment. Select Normal for most office environments; High: for moderate background noise; or Severe: for extremely noisy conditions. The High and Severe modes adjust the microphone and in-ear speaker volume of the handset to account for background noise. If you use High or Severe mode in a quiet environment, the person on the other end of the line can find it difficult to hear your voice.

Ring in Headset Ring in Speaker

You can select to have the handset ring in the headset or the handset speaker.

Warning Tones

You can specify whether warning tones (such as system up or down, or out of range) play. Warning Tones are enabled by default.

Key Tones

You can specify whether tones play when keys are pressed. Key Tones are enabled by default.

Push-to-talk Disable/Enable

You can enable or disable the PTT feature locally.

Phone Settings

The following sections describe the Phone Settings menu options.

Keypad Autolock

You can configure the keypad to lock automatically when in standby mode. You can disable the automatic locking function (the default) or adjust the autolock for a 5, 10, or 20 second delay before locking.

Language

Select Language to view the available languages and select a language from the list.

Display Contrast

You can adjust the display for different lighting conditions.

Use Hearing Aid/Use No Hearing Aid

You can select whether you use a hearing aid.

Startup Song Play/Inhibit

You can select whether the startup song plays.

Predial Disable/Enable

Predial allows you to enter the number you want to predial, while the handset is in standby mode. You can select whether to enable the Predial feature.

Push-to-Talk

From the Push-to-Talk menu, you can configure the default channel, subscribed channels, tone volume and audio volume. The menu for Push-to-Talk does not appear if PTT is disallowed on the Admin menu or if no channel is enabled on the Admin menu.

System Info

The following sections describe the System Info menu options.

Phone IP Address

Select Phone IP Address to view the IP address currently assigned to the handset.

Server IP Address

Select Server IP Address to view the IP address of the SVP Server and the OAI Server (if installed).

Alias IP Address

Select Alias IP Address to view the alias IP address of the wireless handset (provided by the WLAN IP Telephony Manager 2245).

SVP IP Address

Select SVP IP Address to view the IP address of the SpectraLink Voice Priority (SVP) Server.

Current Call Svr

Select Current Call Svr to view the current Call Server IP address and port number.

Terminal Type

Select Terminal Type to view the type of PBX in use.

For detailed information about the user-defined preferences in the Configuration menu and how to configure them, see *WLAN Handset 6120 User Guide (NN43150-100)* () .

Firmware Version

Select Firmware Version to view the current firmware version of the handset.

Extension

Select Extension to view the extension currently assigned to the handset.

- CS1000 —The extension number cannot be edited. The handset obtains the extension from the server and it appears on the info line when you select this option.

- BCM —You must configure the extension number here in the Config Menu for it to appear on the handset in standby mode and in Caller ID.

User Name

Select User Name to enter or change the name that appears on the handset display, next to the extension, in standby mode.

Default configuration

Restore Defaults is an option available on the Admin Settings menu. For a list of the default configurations, see the following tables:

Table 11
User profiles

Profile	Loud	Soft	Vibrate	Silent	Custom
Ring Cadence	PBX	PBX	OFF	OFF	PBX
Ring Tone	Tone 1	Tone 1	Tone 1	Tone 1	Tone 1
Ring Volume	7	3	1	1	5
Vibrate Cadence	OFF	OFF	PBX	OFF	PBX
Ring Delay	none	none	none	none	5 seconds
Noise Mode	Normal	Normal	Normal	Normal	Normal
Headset or Speaker Ring	Speaker	Speaker	Speaker	Speaker	Speaker
Key Tones	Enabled	Enabled	Disabled	Disabled	Enabled

Table 12
Phone settings

Keypad Autolock	Disabled
Language	English
Set Extension	[blank]
Set User Name	[blank]
Display Contrast	Medium
Use Hearing Aid	No
Startup Song	Play

Table 13
Admin settings

Disable Password	123456
Change Password	123456
Restore Defaults	not applicable
Speakerphone	Enabled

Admin menu options

This chapter describes the options that are available from the Admin menu of the handsets:

-
-

WLAN Handset 2210/2211/2212

lists the Admin menu options for the WLAN Handset 2210/2211/2212. Detailed descriptions of each item follow the table.

The default settings are indicated with an asterisk (*).

Table 14
Admin menu options for the WLAN Handset 2210/2211/2212

Admin menu option	2nd level	3rd level	4th level	5th level
Phone Config	Language	*English French German Spanish Portuguese Norwegian		
	License Option	Set Current	[List per download]	
	Terminal Type	i2004 3rd Party		
	OAI On/Off	Enable OAI Disable OAI		
	Push-to-talk	Allowed Channels	*Channel 1 *Channel 2 *Channel 3 *Channel 4 *Channel 5	

Admin menu option	2nd level	3rd level	4th level	5th level
			*Channel 6 *Channel 7 *Channel 8	
		Allow/Disallow	*Allow PTT Disallow PTT	
	Admin Password	Enter PW	Reenter Password	
	Startup Keylock			
	Location Services	On * Off	Set transmission interval:	1 5 10
			IP address	*_ _ _._ _ _._ _ _._ _ _
Network Config	IP Addresses	*Use DHCP		
		Static IP	Phone IP TFTP Server IP Default Gateway Subnet Mask Syslog Server IP SVP IP Addr	
		Svr1	Srvr 1 IP Addr Srvr 1 Port Srvr 2 IP Addr Srvr 2 Port OIA Server IP	
	ESSID	*Learn Once Learn Always Static		
	Security	*None		
		WEP	Authentication	Open System Shared Key
			WEP On/Off	

Admin menu option	2nd level	3rd level	4th level	5th level
			Key Information	Default Key Key Length Key 1-4
			Rotation Secret	
		Cisco FSR	Username Password	
		WPA-PSK	Passphrase Direct Entry	
		WPA2-PSK	Passphrase Direct Entry	
		VPN	VPN Server IP	
			VPN Client IP	Static IP IKE Mode Config
			Phase 1—ISAK MP	Mode Authentication Diffie-Hellman Auth. Hash Encryption Local ID Lifetime (sec) Options
			Phase 2—ESP	Auth. Hash ESP Encryption Remote Network Lifetime (sec)
	Reg. Domain: none			
	Transmit Power	*Maximum 50 mW 30 mW 20 mW 15 mW 10 mW 5 mW (See Note)		

Admin menu option	2nd level	3rd level	4th level	5th level
Diagnostics	Run Site Survey			
	Diagnostics Mode	Diagnostics On *Diagnostics Off		
	Syslog Mode	*Disabled Errors Events Full		
Restore Defaults				

In the Transmit Power section, the 50 mW and 30 mW settings only appear if the Regulatory Domain is configured to None or 01.

Language

Choose a language from those on the list.

License Option

License Option enables selection of the VoIP protocol that the site is licensed to download and run. The UNIStim Protocol to use for the handsets is 010. Any other protocol causes the wireless handset to malfunction.

After selecting the correct protocol for the site, Nortel recommends upgrading the firmware for the wireless handsets. See .

Terminal Type

Select 2004P2. The Terminal type configures the wireless handset for the type of PBX in use. The CS 1000 requires the 2004P2 setting; the BCM requires the 3rd party setting.

OAI On/Off

The Nortel Open Application Interface (OAI) enables the wireless handset to connect with the optional WLAN Application Gateway 2246. With this device, third-party computer applications can display alphanumeric messages on the wireless handset display and take input from the wireless handset keypad. For more information, see WLAN IP Telephony Installation and Commissioning (NN43001-504).

If a WLAN Application Gateway 2246 is installed in the system, OAI can be optionally enabled in each wireless handset. Select whether the wireless handset should attempt to connect to the WLAN Application Gateway 2246 by choosing either the **Enable** or Disable options in this menu.

If OAI is enabled, and a WLAN Application Gateway 2246 IP address is available to the wireless handset (either through DHCP or Static IP configuration), the wireless handset communicates with the WLAN Application Gateway 2246 at power-on, and then periodically during the time the wireless handset is powered on.

If a WLAN Application Gateway 2246 is not installed at the site, disable the OAI feature to preserve network bandwidth and battery life.

Push-to-talk

All eight Push-to-talk channels are allowed by default. The Push-to-talk menu contains the following options:

- **Allowed Channels**—toggle the status of any allowed channel, by scrolling to the channel to be disallowed and pressing the Select button. Allowed channels are displayed with a star (*) in the left column. Only the allowed channels appears on the Standby menu, where they can be enabled or disabled by the user.

- **Allow/Disallow**—enables or disables Push-to-talk. Scroll to Disallow PPT and press the Select button to disable Push-to-talk.

Push-to-talk is available on the WLAN Handset 2211 and the WLAN Handset 6140. It is not available on the WLAN Handset 2210/2212 and the WLAN Handset 6120.

Admin Password

The optional Admin Password controls access to the administration functions in the Admin menu of the wireless handset. Configure the password in each wireless handset for which controlled access is desired. Wireless handsets are shipped without any Admin password.

Data entry for the password uses the alphanumeric string entry technique. Type the password and press the Save soft key. A confirmation prompt appears. Type the password again and press the Save soft key. If the passwords match, the Admin password is configured.

If this option is selected on a wireless handset that already has a configured password, and the Exit soft key is pressed with no entry, the password is erased. This means that the wireless handset does not require an Admin password to access the Admin menu.

ATTENTION

Record the wireless handset Admin password and store it in a safe place. If the password is lost or forgotten, contact Nortel Technical Support.

Startup Keylock

Startup Keylock deactivates the keypad during startup so that initialization cannot be interrupted. This is a toggle option; the info line displays whether the option is enabled or disabled. Select No Startup Keylock to disable and select Startup Keylock On to enable.

IP Addresses menu

There are three modes in which the wireless handset can operate: DHCP-enabled, Static IP or Svr1 (Server 1). Select the mode for operation from the IP Address menu:

- *** Use DHCP**—use Dynamic Host Configuration Protocol (DHCP) to assign an IP address each time the wireless handset is turned on. If DHCP is enabled, the wireless handset also receives all other IP address configurations from DHCP.

- **Static IP**—a fixed IP address can be manually configured. If this option is selected, the wireless handset prompts for the IP addresses of each configurable network component. When entering IP addresses, enter the digits only, including leading zeroes. No periods are required.

- **Server1 (Srvr1)**—the IP addresses and ports of the servers and OIA server can be configured either statically or through DHCP.

Regardless of the mode in which the wireless handset is operating, the following components must be configured:

- **Phone IP**—the IP address of the wireless handset. This is automatically assigned if DHCP is used. If using Static IP configuration, obtain a unique IP address for each wireless handset from the network administrator.

- **SVP Server IP**— If using Static IP configuration, this is simply the IP address of the WLAN IP Telephony Manager 2245. The WLAN IP Telephony Manager 2245 must be statically configured to have a permanent IP address. If DHCP is being used, the wireless handset tries the following, in order: the DHCP option 151, and then a DNS lookup of SLNKSVP2 if the DHCP options 6 (DNS Server) and 15 (Domain Name) are configured.

- **Server 1 IP**—the TLAN node IP address of the LTPS IP Telephony Node on the Call Server. If the wireless handset is using static IP address configuration, enter the TLAN node IP address of the LTPS IP Telephony Node on the Call Server. If the WLAN handset is using DHCP, the DHCP server must be configured to provide the TLAN node IP address (and UDP port number) of the LTPS IP Telephony Node on

the Call Server using one of the following DHCP options:
46, 128, 144, 157, 191, and 251.

- **Server 1 Port**—the UDP port number used by the wireless handset to contact the LTPS Node Connect Service to request registration with the LTPS and the Call Server. If the wireless handset is using static IP address configuration, enter port number 4100. If the WLAN handset is using DHCP, the DHCP server must be configured to provide the TLAN node IP address and UDP port number of the LTPS IP Telephony Node on the Call Server using one of the following DHCP options:
46, 128, 144, 157, 191, and 251.

The following components can be configured optionally:

- **TFTP Server IP**—the IP address of the TFTP Server on the network that holds firmware images for updating the wireless handsets. If this feature is configured (not configured to 0.0.0.0 or 255.255.255.255), either through Static IP configuration, through using DHCP option 66 (TFTP Server), or the Boot server/next server (siaddr) field, the wireless handset checks for different firmware each time it is powered on or comes back into range of the network. This check takes only five to seven seconds and ensures that all wireless handsets in the network are kept up-to-date with the same version of firmware.

It does not matter if the firmware version on the TFTP Server is newer or older; if the versions are different, the wireless handsets download the firmware from the TFTP Server.

- **OAI Server IP**—the IP address of the WLAN Application Gateway 2246 (if using). If using Static IP configuration, this is simply the IP address of the WLAN Application Gateway 2246. If DHCP is being used, the wireless handset tries DHCP option 152.

- **Default Gateway and Subnet Mask**—used to identify subnets when using a complex network that includes routers. Both of these fields must be configured (not configured to 0.0.0.0 or 255.255.255.255) to enable the wireless handset to contact any network components on a different subnet. They can be configured using Static IP configuration or through DHCP options 3 (Default Gateway) and 1 (Subnet Mask) respectively. Contact the network administrator for the proper settings for the network.

The wireless handsets cannot roam across subnets, because the wireless handsets cannot change their IP address while operational. Ensure that all the APs are attached to the same subnet for proper operation. The wireless handset can change subnets if DHCP is enabled, and the wireless handset is powered off, and then back on, when within range of APs on the new subnet.

- **Server 2 IP**—the IP address of a WLAN Telephony Manager 2245 unit. Currently, the wireless handset does not make use of this information. If using Static IP configuration, this is simply the IP address of the device. If DHCP is being used, the wireless handset tries to obtain the IP address and port information of the device using the following DHCP options: 46, 128, 144, 157, 191, and 251.

- **Server 2 Port**—the port number used by a WLAN Telephony Manager 2245 device to communicate with IP Phones. Currently, the wireless handset does not make use of this information. If you use Static IP configuration, consult the device documentation for port numbers. If you use DHCP, the wireless handset tries to obtain the IP address and port information of the device using the following DHCP options: 43, 128, 144, 157, 191, and 251.

- **Syslog Server IP**—the address of the Syslog Server. See "Diagnostic Tools" (page 135) for more information.

ESSID

Select the option that enables the wireless handset to acquire APs with the correct ESSID (Extended Service Set ID, or Extended SSID) each time it is turned on.

For Automatic Learn options, Broadcast ESSID must be enabled in the APs for ESSID learning to function (or contact the AP vendor for specifics). Overlapping wireless systems complicate the use of ESSID learning, as the wireless handset in an overlapping area could receive conflicting signals. If this is the situation at the site, use Static Entry or Learn Once in an area without overlapping ESSIDs.

- *** Learn Once**—the wireless handset to scan all ESSIDs for a DHCP server and TFTP Server. After either is found, the wireless handset retains the ESSID from whichever AP it associates with at that point. When overlapping wireless systems exist, the Learn Once feature allows the wireless handset to use only the ESSID established the first time at all subsequent power-ons. This ESSID is retained by the wireless handset until the ESSID option is reselected.

- **Learn Always**—the wireless handset to automatically learn the ESSID at each power-on or loss of contact with the wireless LAN (out of range). This can be useful if the wireless handset is used at more than one site.

- **Static Entry**—if the APs do not accept broadcast ESSID, or if there are overlapping wireless systems in use at the site, enter the correct ESSID manually.

Security

For authentication, the WLAN Handsets 2210/2211/2212 and WLAN Handsets 6120/6140 support open, WEP shared key, or WPA/WPA2 Preshared Key (PSK) mechanisms. The WLAN Handset 2212, in addition, also supports IPsec VPN.

For data encryption, the WLAN Handsets 2210/2211/2212 and WLAN Handsets 6120/ 6140 support 40-bit and 128-bit WEP, WPA, and WPA2 . In addition, the WLAN Handset 2212 supports 3DES for VPN encryption. If you use WEP, Nortel recommends that you configure the authentication type to open, because of a known weakness of the 802.11 shared key authentication algorithm.

For WPA and WPA2, the use of PSK does not pose the same security risk that WEP shared key authentication does. The choice of a WPA2 pass phrase is important; however, weak pass phrases can be broken through dictionary attacks. The Configuration Cradle for the WLAN Handsets 2210/2211/2212 and the Handset Administration Tool for the WLAN Handsets 6120/6140 are especially valuable for configuring complex and secure pass phrases.

Because the WEP encryption algorithm is compromised, it does not thwart determined attackers and eavesdroppers. Even 128-bit WEP is only roughly twice as secure as 40-bit WEP. Therefore, the effort to program many handsets with 128-bit keys may not be worth the effort put into it.

For the best security on the WLAN Handsets 2210/2211/6120/6140, use WPA2-PSK; for best handset security on the WLAN Handset 2212, use IPsec VPN.

The following are the security options:

- *** None**—disables any 802.11 encryption or security authentication mechanisms.

- **WEP** (Wired Equivalent Privacy)—a wireless encryption protocol that encrypts data frames on the wireless medium, providing greater security in the wireless network. If WEP Encryption is required at this site, each wireless handset must be configured to correspond with the encryption protocol configured up in the APs. Select the entries from the following options to enable the wireless handset to acquire the system.

  By default, WEP options are off. If WEP is desired, options must be configured in the wireless handset that match those configured in the APs.

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

WEP can be configured to optional at the AP if there are wireless devices in use that do not have WEP capability. All wireless devices must be upgraded to WEP capability for a fully secured WEP environment.

WEP settings must match the AP settings.

Configure each of the following options to match exactly the settings in the APs:

— **Authentication**—select either Open System or Shared Key.

— **WEP**—select either WEP Off or WEP On.

— **Key Information**—scroll through the options.

– **Default Key**—enter the preshared key number specified for use by the wireless handsets. This is 1 through 4.

– **Key Length**—select either 40-bit or 128-bit depending on the key length specified for use at this site.

– **Key 1-4**—scroll to the key option that corresponds to the Default Key that was entered above. Press Select and enter the encryption key as a sequence of hexadecimal characters. Use the 2 and 3 keys to access hexadecimal digits A-F; use soft keys to advance to the next digit and backspace. For 40-bit keys, enter 10 digits; for 128-bit keys, enter 26 digits. The display scrolls as needed.

– **Rotation Secret**—used for proprietary WEP key rotation if this feature is supported in the system.

• **Cisco FSR**—to provide the highest level of security without compromising voice quality on Cisco Aironet WLAN APs, the Fast Secure Roaming (FSR) mechanism is implemented. FSR is designed to minimize call interruptions for wireless handset users as they roam throughout a facility. Existing Aironet 350, 1100, and 1200 APs can require a firmware upgrade to support FSR. Cisco FSR requires advanced configuration of the Cisco APs in the site. See the Cisco representative for detailed documentation on configuring the APs and other required security services on the wired network. To configure Cisco FSR in the wireless handset, enter a Radius Server username and password into each wireless 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.

- **WPA-PSK** —Wi-Fi Protected Access (WPA) using Preshared Key (PSK) provides enhanced security and can be used, if supported by the APs. Select one of the following options:

    — **Passphrase**—enter a passphrase. The passphrase can be from 1 to 63 ASCII characters or 64 hexadecimal digits. Use a strong passphrase that cannot be discovered using password-cracking programs. A 20 to 30 character passphrase is recommended. For more information, see "Choosing a passphrase" (page 103).

        – Example: why2fear4WPA-is-DEPLOYED_HERE

    — **Direct Entry**—enter a preshared key code (hexadecimal number).

    For information about whether WPA-PSK is recommended for the AP, consult the Configuration Note for the installed APs, available from www.spectralink.com. Configure the recommended version on the AP and configure the corresponding option on the Admin menu.

    WPA-PSK settings must match the AP settings.

- **WPA2-PSK** —WPA2 with PSK provides enhanced security over WPA-PSK and can be used, if supported by the APs. Select one of the following options:

    — **Passphrase**—enter a passphrase. The passphrase can be from 1 to 63 ASCII characters or 64 hexadecimal digits. Use a strong passphrase that cannot be discovered using password-cracking programs. A 20 to 30 character passphrase is recommended. For more information, see "Choosing a passphrase" (page 103).

        – Example: why2fear4WPA2-is-DEPLOYED_HERE

    — **Direct Entry**—enter a preshared key code (hexadecimal number).

    Consult the Configuration Note for the installed APs for information about whether WPA2-PSK is recommended for the AP. Configure the recommended version on the AP and configure the corresponding option on the Admin menu.

- **VPN** —the selection of VPN for security requires that a secure tunnel be established for the transfer of information. The data itself no longer must be encrypted because the VPN tunnel is already encrypted. VPN security requires a number of configuration steps, and is easily configured using the Configuration Cradle. For more information, see "Configuration Cradle for the WLAN Handset 2210/2211/2212" (page 46). VPN security is also closely tied with the VPN server configuration. Only the WLAN Handset 2212 supports VPN security.

    The VPN server must support the handset configuration.

— **VPN Server IP**—the IP address of the VPN server on the public (unsecure) side of the network.

— **VPN Client IP**—the IP address that appears to be part of the private (or secure) network

– **Static IP**—the address can be statically programmed in the handset, in which case it must match the address assigned to the handset in the VPN server.

– **IKE Mode Config**—if the VPN server supports the ISAKMP Mode Configuration, it can assign the IP address automatically.

— **Phase 1—ISAKMP**—this is the first phase of the tunnel negotiation process. It establishes a set of security parameters (the ISAKMP Security Association) that is used to encrypt the negotiation of the actual tunnel parameters in Phase 2. In essence, Phase 1 protects Phase 2.

– **Mode**—VPNs can negotiate their parameters using two different modes. These are called Main Mode and Aggressive Mode. Aggressive Mode is the most flexible of the two and is the only one currently supported by the handsets.

– **Authentication**—enter a preshared key, which must match the shared secret key entered for the handset in the VPN server. The key can be an ASCII string or a hexadecimal string.

– **Diffie-Hellman**—choose Group 1, Group 2 or Group 5, depending on the level of security required and the level supported by the VPN server.

– **Auth. Hash**—choose either MD5 or SHA, depending on the VPN server setting.

– **Encryption**—chooses DES or 3DES, depending on the VPN server setting.

– **Local ID**—identifies the VPN user who is trying to connect to the server. The Local ID must match the VPN server setting.

– **Lifetime (sec)**—gives the lifetime, in seconds, of the ISAKMP security association. When the lifetime expires, the tunnel must be closed and a new one created. Nortel recommends a minimum of 12 to 24 hours (43 200 to 86 400 seconds). The maximum value for the lifetime setting is 31 days (2 778 400 seconds).

– **Options**—each of the options can be enabled individually.

Init Contact—by enabling this option, the handset sends an initial contact request message to notify the VPN server that the handset has relinquished the old tunnel and wants to open a new one.

> **Nortel features**—enabling this option makes the handset use Nortel-specific extensions to the standard IKE negotiation. The handset advertises itself as a Contivity-compatible client and hashes the Key ID before passing the information to the Contivity.

— **Phase 2—ESP**—this is the second phase of the tunnel, and is encrypted by the parameters established in Phase 1. Phase 2 negotiates the parameters used by Encapsulated Security Payload (ESP) to encrypt the actual traffic in the tunnel.

– **Auth. Hash**—choose either MD5 or SHA1 to match the settings in the VPN server.

– **ESP Encryption**—select DES or 3DES for the encryption algorithm for the tunnel traffic.

– **Remote Network**—enter an IP address and a network mask to specify the private (secure) network address range.

– **Lifetime (sec)**—configure a lifetime in seconds for ESP security associations. Typically, this setting is a few hours and must be no greater than the Phase 2 lifetime configured in the VPN server.

Choosing a passphrase

The choice of a strong passphrase ensures the privacy of the handset data and messages.

A good passphrase is:

- Known only to the administrator.

- Long enough so that it is difficult to guess or crack. For example, search programs often contain dictionary words and famous phrases. Some passphrase character lengths are

  — 8-character passphrase—weak

  — 20-character passphrase—minimum

  — 20 to 30-character passphrase—recommended

  — 63-character passphrase—very strong

- Difficult to guess by intuition—even by someone who knows the administrator well. Birth dates, for example, are a poor choice.

- Easy for the administrator to remember and type. Nortel does not recommend writing the password down.

Reg. (Regulatory) Domain

The Regulatory Domain defaults to None on the wireless handset display. FCC requirements dictate that the menu for changing the domain be available by password, which in this case is the LINE button. To change the domain, press LINE and then enter the digits that represent the domain for the site. You must enter both digits.

The following are domain digits:

- **01**—North America
- **02**—Europe (except Spain and France) and Japan
- **04**—Spain
- **05**—France
- **06**—Korea

As of this writing, Spain and France are adopting the general European Regulatory rules. Check with the wireless LAN administrator or supplier for the correct domain to enter in these countries.

Transmit Power

The Transmit Power selected must match the installed APs and all Wireless Handsets and is regulated by the domain. The maximum for North America is 100 mW, while other domains have a maximum of 30 mW. The following power settings are available:

- **Maximum** (default)
- **50 mW** (only available in the North American domain)
- **30 mW** (only available in the North American domain)
- **20 mW**
- **15 mW**
- **10 mW**
- **5 mW**

If the default is not used, ensure that the Transmit Power setting is the same for all handsets and all APs.

Run Site Survey

Run Site Survey is used to check the signal strength from APs. When Run Site Survey is selected, the wireless handset remains in this mode until it is powered off. During configuration, press the right arrow to skip this mode. For more information about using this mode, see WLAN IP Telephony Installation and Commissioning (NN43001-504). For a detailed

description of the survey results, see "Run Site Survey for the WLAN Handset 2210/2211/2212" (page 135) and "Run Site Survey for the WLAN Handset 6120/6140" (page 136).

Diagnostics Mode

After you select Diagnostics Mode from the menu, the handset enters the diagnostics function immediately. For more information, see "Diagnostics Mode" (page 138)for more information.

Syslog Mode

You can enable or disable Syslog Mode.

Configure Syslog Mode to one of the following:

- * **Disabled**—turns syslog off.
- **Errors**—causes the handset to only log events that are considered errors.
- **Events**—logs all errors, plus some events of interest.
- **Full**—logs all errors and all other events of interest.

Table 15 "Syslog message levels for the WLAN Handset 2210/2211/2212" (page 105) lists the syslog messages and which level of logging produces each message.

Table 15
Syslog message levels for the WLAN Handset 2210/2211/2212

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 error threshold exceeded	Yes	Yes	Yes
Audio stats	No	No	Yes (every 5s)
Radio error threshold exceeded	Yes	Yes	Yes
Radio stats	No	No	Yes (every 5s)

Restore Defaults

The Restore Defaults option resets all user and administrative parameters (other than Telephony Protocol) to their factory defaults. During configuration, press the right arrow to skip this mode.

WLAN Handset 6120/6140

Table 16 "Admin menu options for the WLAN Handset 6120/6140" (page 106) lists the Admin menu options for the WLAN Handset 6120/6140. Detailed descriptions of each item follow the table. An asterisk (*) beside a setting indicates the default setting.

Table 16
Admin menu options for the WLAN Handset 6120/6140

Admin menu option	2nd level	3rd level	4th Level	5th Level
Phone Config	Language	*English Française Deutsch Español Português Norsk		
	Telephony Protocol	*Type 032		
	Push-to-Talk	PTT Enable/Disable		
		Allowed Channels	*Channel 1 *Channel 2 *** *Channel 24	
		Name Channels	*Channel 1 *Channel 2 *** *Channel 24	
		Priority Channel On/Off	Name Channel	
	Time Zone	[list] *GMT		
	Daylight Saving	*DST No Adjust DST Auto <USA> DST Auto <Euro> DST Auto <AUS>		
	Protected Spd Dial	Enter Number	Enter Name	Assign Speed-dial
	Password [Disable/Enable]			
	Change Password			
	Set Terminal Type [2004/3rd Party]			

Table 16
Admin menu options for the WLAN Handset 6120/6140 (cont'd.)

Admin menu option	2nd level	3rd level	4th Level	5th Level
	Startup Keylock			
	Speakerphone [Disable/Enable]			
	OAI [Disable/Enable]			
	Location Services	On * Off	Set transmission interval:	1 5 10
			IP address	*___.___.___.___
Network Config	IP Addresses	*Use DHCP	*Full DHCP	
			Partial DHCP	Server1 IP Address Server1 Port Server2 IP Address Server2 Port
		Static IP	Phone IP	
			Default Gateway	
			TFTP Server IP	
			Subnet Mask	
			Syslog Server IP	
			Time Server IP	
			SVP IP	
			Call Server Info	Server1 IP Address Server1 Port Server2 IP Address Server2 Port
			OAI Server IP	
	SSID	[Enter]		

Table 16
Admin menu options for the WLAN Handset 6120/6140 (cont'd.)

Admin menu option	2nd level	3rd level	4th Level	5th Level
	Security	*None		
		WEP	Authentication	Open System Shared Key
			WEP On/*Off	*WEP Off WEP On
			Key Information	Default Key Key Length Key 1-4
			Rotation Secret	
		WPA2-PSK	Passphrase Pre-Shared Key	
		Cisco FSR	Username Password	
		WPA-PSK	Passphrase Pre-Shared Key	
	Reg. Domain: *none	01-02		
			[802.11 Config]	
			a →	802.11a 5.150-5.250 5.250-5.350 DFS 5.470-5.725 DFS 5.275-5.825 DFS
			*b and b/g mixed → g only →	[Transmit Power] *Maximum 5 mW <7dBm> 10 mW <10dBm> 20 mW <20dBm> 40 mW <40dBm> 50 mW <17dBm> 100 mW <20dbm>

Table 16
Admin menu options for the WLAN Handset 6120/6140 (cont'd.)

Admin menu option	2nd level	3rd level	4th Level	5th Level
Diagnostics	Run Site Survey			
	Diagnostics Mode [Disable/Enable]			
	Syslog Mode	*Disabled Errors Events Full		
	Error Handling Mode Halt on Error Restart on Error			
Restore Defaults				

Language

Choose a language from those on the list.

Telephony Protocol

Use Telephony Protocol to select the VoIP protocol that your site is licensed to download and run. The UNIStim Protocol to use for the WLAN Handset 6120/6140 is 032. Any other protocol causes the handset to malfunction.

Push-to-talk

All 24 Push-to-talk channels are allowed by default. The Push-to-talk menu provides the following options:

- Allowed Channels

  Toggle the allowed status of any allowed channel by scrolling to the channel to be disallowed and pressing Enter. Allowed channels are displayed with an asterisk (*) in the left column. Only those channels allowed in the Admin menu appear on the Config menu, where they can be subscribed to by the user.

- Named Channels

  You can name allowed channels. The name appears instead of the channel number when channel information appears on the handset. The name appears on the local handset only; it does not appear on target handsets.

- Priority Channel

You can configure the priority channel, also referred to as channel 25, which makes it available to all Push-to-talk handsets. When you make a Push-to-talk broadcast on the priority channel, it overrides any active Push-to-talk transmission on all other channels. You can name the priority channel.

Time zone

Worldwide time zone options are available. Select your time zone from the list. Greenwich Mean Time (GMW) is the default.

Daylight Saving

You can adjust the handset for daylight savings time. The following are the Daylight Savings menu options:

- DST No Adjust (Default)
- DST Auto (USA)
- DST Auto (AUS)
- DST Auto (EURO)

Protected Spd Dial

The protected speed-dial number appears as the first item on the speed-dial list and is specially marked with an asterisk (*) as the first character in its name. It is usually programmed to a number to be called in emergency situations.

If the Call Server offers directory services, Redial, Speed-dial, and Phonebook features in the handset are disabled, including the protected speed-dial number feature. Any entry here is overridden by the Call Server.

Password [Disable/Enable] and Change Password

The password option controls access to the administrative functions in the Admin menu of the wireless handset. Configure the password in each handset for which controlled access is desired. By default, the password is disabled when the handset is shipped.

To modify the password requirement, enter the default or previously configured password to verify the change. The Password option operates as a toggle between Enabled and Disabled. Press Enter to change the password protection state. Change Password appears only if the password is enabled.

ATTENTION
Record the wireless handset Admin password and store it in a safe place. Do not lose the Admin password! If the Admin password is lost or forgotten, you can be required to return the handset to Nortel to have the password reset.

Set Terminal Type

The terminal type configures the WLAN Handset 6120/6140 for the type of PBX in use. The CS 1000 system requires the 2004P1 or 2004P2 setting, the BCM system requires the 3rd Party setting. The current Terminal Type is shown on the information line. Press Enter to toggle to the alternate setting.

Startup Keylock

Startup Keylock deactivates the keypad during startup so that initialization cannot be interrupted. This is a toggle option; the info line displays whether the option is enabled or disabled. Select No Startup Keylock to disable and select Startup Keylock On to enable.

Speakerphone

You can disable the speakerphone when quiet handset operation is required. Disabling the speakerphone removes the speakerphone soft key from the active mode display. The current speakerphone setting is shown on the information line. Press Enter to toggle to the alternate setting.

OAI [Disable/Enable]

With the Nortel Open Application Interface (OAI), the wireless handsets can connect with the optional WLAN Application Gateway 2246. This device allows third-party computer applications to display alphanumeric messages on the wireless handset display and take input from the wireless handset keypad.

If a WLAN Application Gateway 2246 is installed in the system, OAI can be optionally enabled in the wireless handset. Select whether the wireless handset can attempt to connect to the WLAN Application Gateway 2246 by pressing Enter to toggle to the alternate setting.

If OAI is enabled, and a WLAN Application Gateway 2246 IP address is available to the wireless handset (either through DHCP or Static IP configuration), the wireless handset communicates with the WLAN Application Gateway 2246 at power-on, and then periodically during the time the wireless handset is powered on.

If a WLAN Application Gateway 2246 is not installed at the site, disable the OAI feature to preserve network bandwidth and battery life.

IP addresses

The WLAN IP 6120 handset can operate in three modes: DHCP enabled, either Full DHCP or Partial DHCP, and Static IP. Select the mode for operation from the IP Address menu:

- Use DHCP—uses 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.

  — Full DHCP—enables DHCP for all IP addresses.

  — Partial DHCP—enables static IP address configuration for Server 1, Server 1 Port, Server 2, and Server 2 Port. All other IP addresses are assigned by DHCP.

    Server 1 (2) IP address—the IP addresses of the Nortel device. If using Static IP configuration, this is the IP address of the device. If DHCP is used, the handset tries to obtain the IP address and port information by using the following DHCP options: 43, 128, 144, 157, 191, and 251.

    Server 1 (2) Port—the port number used by Nortel device to communicate with IP telephones. If using Static IP configuration consult your Nortel documentation for port numbers. If DHCP is used, the handset tries to obtain the IP address and port information by using the following DHCP options: 43, 128, 144, 157, 191, and 251.

- Static IP—allows you to manually set a fixed IP address. If selected, the handset prompts for the IP Addresses of each configurable network component. When entering addresses, enter the digits only, including leading zeroes. No periods are required.

Regardless of the mode in which the handset is operating, you must configure the following components:

- 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 that includes routers. Both of these must be configured either with an IP address under Static IP (not configured 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 your network administrator for the proper settings for your network.

> **ATTENTION**
> A WLAN Handset 6120/6140 cannot roam across subnets because it cannot change its IP address while it is operational. Ensure that all your access points are attached to the same subnet for proper operation. If DHCP is enabled, you can change the subnet of the handset by powering off the handset, and then powering it back on when it is within range of access points on the new subnet.

- TFTP Server IP—the IP address of a TFTP server on your network that holds firmware images for updating the handsets. If this feature is configured (not configured to 0.0.0.0 or 255.255.255.255), either by using Static IP configuration or by using DHCP option 66 (TFTP Server), or the Boot server/next server (siaddr) field, the handset checks for newer firmware 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 firmware.

- Syslog Server IP—the IP address of the Syslog Server. See the Diagnostics section for more information.

- Time Server IP—the IP address of the time server.

- SVP IP address—the IP address of the SVP Server. If using Static IP configuration, this is simply the IP address of the SVP Server. To have a permanent IP address, the SVP Server must be statically configured. If DHCP is used, the handset tries the following, in this order:

  — DHCP option 151

  — a DNS lookup of SLNKSVP2 if the DHCP options 6 (DNS Server) and 15 (Domain Name) are configured.

- Call Server Info—the IP addresses of the CS 1000 server. When setting static IP addresses, the IP addresses and Port addresses must be configured for Svr1 and Svr 2. For more information, see .

- OAI Server IP—the IP address of the NetLink (NL) OAI Gateway (if applicable). If using Static IP configuration, this is simply the IP address of the NL OAI Gateway. If DHCP is being used, the handset tries the DHCP option 152.

SSID
Enter the SSID.

Security
The following are the security options:

> **ATTENTION**
> For Wired Equivalent Privacy (WEP), WiFi Protected Access using PSK
> Preshared Key (WPA-PSK), and WPA2-PSK configure each of the following
> options to match exactly the settings in your APs. Encryption codes appear as
> they are entered. For security reasons, codes do not appear on the display
> when a user returns to the Admin menu, Encryption options.

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

- WEP—a wireless encryption protocol that encrypts data frames on the wireless medium, allowing for greater security in the wireless network. If WEP is used, you must configure each handset to correspond with the encryption protocol configured in the access points. 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—Configure the following:

    – Default Key—Enter the key # specified for use by the handsets. This is 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 you entered above. Enter the encryption key as a sequence of hexadecimal characters. (Use the 2 and 3 keys to access hexadecimal digits A-F.)

  — Rotation Secret—This is used for proprietary WEP key rotation. To determine whether this feature is supported in your system, see your custom document.

- WPA2-PSK—The security features of WPA2-PSK are available and can be used if supported by the access points in the facility. Select one of the following:

  — Passphrase—enter a passphrase between 8 and 63 characters in length.

  — Direct Entry—enter the 256-bit key code.

> **ATTENTION**
> For information about whether WPA2-PSK is recommended for an
> AP, consult the Configuration Note for the installed APs. Configure the
> recommended version on the AP and select the corresponding option on
> the Admin menu.

- Cisco FSR—To provide the highest level of security without compromising voice quality on Cisco Aironet WLAN APs, the Fast Secure Roaming (FSR) mechanism is implemented. FSR is designed to minimize call interruptions for wireless handset users as they roam throughout a facility. Existing Aironet 350, 1100, and 1200 APs can require a firmware upgrade to support FSR. Cisco FSR requires advanced configuration of the Cisco access points at your site. See the Cisco representative for detailed documentation about configuring your access points and other required security services on your wired network. To configure Cisco FSR in the wireless handset, you must enter a Radius Server username and password into each handset.

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

  — Password—Enter the password that corresponds to this Username.

- WPA-PSK—The security features of WPA-PSK are available and can be used if supported by the access points in the facility. Select one of the following:

  — Passphrase—enter a passphrase between 8 and 63 characters in length.

    – 8-character passphrase—weak

    – 20-character passphrase—minimum

    – 20 to 30-character passphrase—recommended

    – 63-character passphrase—very strong

  — Direct Entry—enter the 256-bit key code.

Regulatory domain, 802.11 configuration, and transmit power

Regulatory domain, 802.11 configuration, and transmit power are interdependent settings. After the domain and 802.11 type are established, you can configure the transmit power.

> **ATTENTION**
> The 802.11 options and the transmit power options, must be configured to match the corresponding settings used by the APs in the facility.

The FCC requirements dictate that the menu for changing the domain be available by password, which in this case is the LINE key. To configure the domain, press LINE and then select the domain:

- 01 North America

- 02 Europe

For the North America Domain, the following frequency ranges and channel numbers are supported on the handset based on U-NII regulatory domain:

Table 17
Frequency ranges and channel numbers

Band (GHz)	Channel Numbers
U-NII lower band (5.15-5.25)	36, 40, 44, 48
U-NII middle band (5.25-5.35)	52, 56, 60, 64
U-NII upper band (5.725-5.825)	149, 153, 157, 161

ATTENTION
The United States also allows for transmissions in the ISM regulatory domain on channel 165 whose center frequency is 5.825 GHz which is at the upper edge of the upper U-NII band however is not compatible with the handset. Therefore, it is important to not configure any WLAN Access Points for operation on channel 165.

After you establish the regulatory domain, the 802.11 Config options appear on the display. You can choose only one option; 802.11 (b and b/g mixed) is the default. If 802.11 (a) is selected, another menu opens so that you can select the 802.11a transmission frequency. Only those ranges that are allowed in the selected domain appear. You can select multiple ranges. The selected mode and ranges are marked with an asterisk (*). Press the Done soft key after you finish specifying the 802.11 mode.

After you press the Done soft key, the Transmit Power menu opens. Only those power levels that apply to the domain and 802.11 mode are listed. You can select only one level. The default varies with the domain and 802.11 mode. The selected level is marked with an asterisk (*).

Run Site Survey

Select this option to activate the Site Survey mode. Site Survey runs immediately upon selecting this option. For more information about Site Survey, see "Run Site Survey for the WLAN Handset 2210/2211/2212" (page 135) and "Run Site Survey for the WLAN Handset 6120/6140" (page 136).

Diagnostics Mode

For a detailed explanation of the Diagnostics Mode options, see "Diagnostics Mode" (page 138).

Syslog Mode

Configure Syslog Mode to one of the following options:

- Disabled—turns syslog off

- Errors—logs events that are considered errors

- Events—logs all errors, plus some events of interest

- Full—logs all errors and all other events of interest

Table 18 "Syslog message levels for the WLAN Handset 6120/6140" (page 117) lists the syslog messages and the level of logging produces each message.

Table 18
Syslog message levels for the WLAN Handset 6120/6140

Message type	Errors	Events	Full
Failed handoff	Yes	Yes	Yes
Successful handoff	No	Yes	Yes
Security error	Yes	Yes	Yes
Call start or end	No	Yes	Yes
Audio error threshold exceeded	Yes	Yes	Yes
Audio stats	No	No	Yes (every 5 s)
Radio error threshold exceeded	Yes	Yes	Yes
Radio stats	No	No	Yes (every 5 s)

For more information, see "Syslog Mode" (page 141).

Error Handling Mode

The Halt on Error option causes the handset to stop operating if an error message is received. Unless the error is a fatal one, normal operation can be resumed by power cycling the handset. Press START or remove and replace the Battery Pack. The Restart On Error option causes the handset to make every effort to reboot quietly and quickly to standby mode. In either scenario, a call in progress is lost.

Error detail can be captured by the Syslog Server and can also be available for downloading with the Handset Administration Tool.

Restore Defaults

The Restore Defaults option restores all user and administrative parameters, except Telephony Protocol, to the factory default configurations. For more information, see "Factory Defaults" (page 173).

Feature programming

This chapter contains information about feature programming for the handsets:

- "WLAN Handset 2210/2211/2212" (page 119)
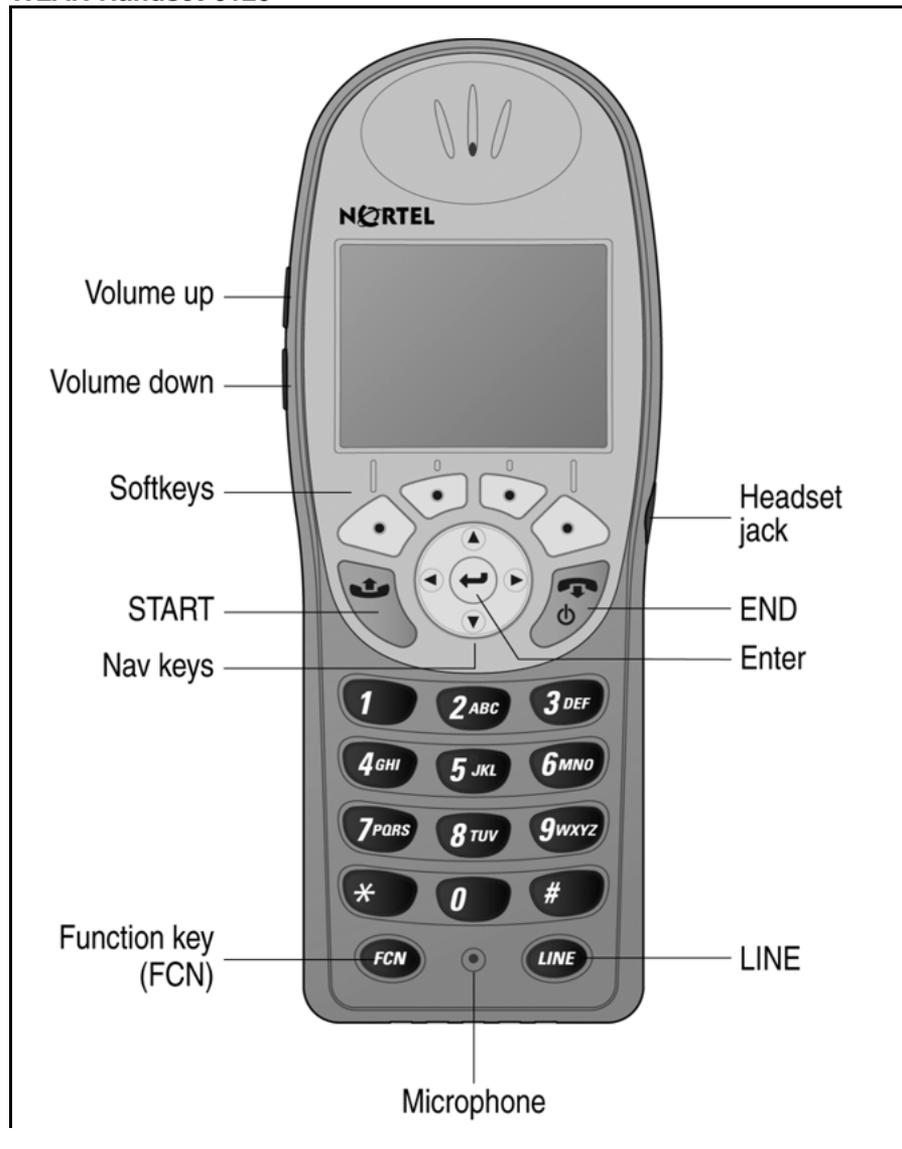- "WLAN Handset 6120/6140" (page 123)

WLAN Handset 2210/2211/2212

The WLAN Handset 2210/2211/2212 emulates the IP Phone 2004. All IP Phone 2004 functions and messaging features are supported where possible. Functions that require use of the volume keys and the speakerphone function are not supported.

The large screen area of the IP Phone 2004 and its numerous keys are mapped onto the smaller screen and fewer buttons of the wireless handsets. The button mapping from the IP Phone 2004 to the handsets was designed to preserve nearly all of the functionality of the IP Phone 2004 within a small, mobile device.

Feature and key assignment

The line keys, numbered 1, 2, 3, 4, 5, and 6, to the left and right of the display screen of the IP Phone 2004 are mapped to the LINE buttons on the handsets. See Figure 7 "WLAN Handset 2210" (page 121).

The IP Phone 2004 has several fixed feature keys. The handsets support the six features that are suitable to a mobile user through the Function (FCN) key on the wireless handset. After FCN is pressed, a screen that lists the features and the assigned keys appear. Press FCN again to display a second screen that lists more features and their assigned keys.

If a third-party application is assigned to a key, that information appears on the Feature list. For fixed feature keys supported by the handsets, see Table 19 "Supported fixed feature keys" (page 120). Keys not indicated are not supported.

Table 19
Supported fixed feature keys

Screen	Fixed feature key
First screen	1 Mute
	2 Hold
	3 Goodbye
	4 Directory
Second screen	5 Inbox
	6 Outbox
	7 Optional third-party application
	8 Optional third-party application
	9 Optional third-party application

If an OAI application is operational, a function key sequence is assigned in the OAI application configuration and overrides any function sequence established here. Therefore, FCN+7, FCN+8, or FCN+9 is a good choice for the OAI sequence.

Figure 7
WLAN Handset 2210

The WLAN Handset 2210/2211/2212 have the same button and screen layout.

Table 20 "IP Phone 2004 mapping to the WLAN Handset 2210/2211/2212" (page 122) lists how the keys of the IP Phone 2004 are mapped to key sequences on the wireless handsets.

Table 20
IP Phone 2004 mapping to the WLAN Handset 2210/2211/2212

IP Phone 2004 key	Feature	Wireless handset key sequence
1	Programmable	Line + 1
2	Programmable	Line + 2
3	Programmable	Line + 3
4	Programmable	Line + 4
5	Programmable	Line + 5
6	Programmable	Line + 6
Mute	Mute	Fcn + 1
Hold	Hold	Fcn + 2
Goodbye	Goodbye	Fcn + 3
Directory	Directory	Fcn + 4
Inbox	Inbox	Fcn + 5
Outbox	Outbox	Fcn + 6
Soft key	Programmable	Soft key A
Soft key	Programmable	Soft key B
Soft key	Programmable	Soft key C
Soft key	Programmable	Soft key D

WLAN Handset 2210/2211/2212 programming keys

The Line keys 1 to 6 on the handsets are programmable by the end user. These Line keys can be programmed in the wireless handset in the same manner they are programmed on the IP Phone 2004.

Follow the steps in to program keys on the wireless handset.

Procedure 28
Programming the keys on the WLAN Handset 2210/2211/2212

Step	Action
1	Place the wireless handset in the idle state by pressing **Power On/Start Call**.
2	Press **FCN + 3**. The wireless handset is in the Active (idle) state. The soft key display area is active but there is no dial tone.
3	Select the Line key to be programmed.

4   Enter the number and save the entry.

--End--

For information about using the wireless handset features, see *WLAN Handset 2210 User Guide (NN10300-077)* () , *WLAN Handset 2211 User Guide (NN10300-078)* () ,*WLAN Handset 2212 User Guide (NN10300-071)* () , and *WLAN Handset 6120 User Guide (NN43150-100)* () .

WLAN Handset 6120/6140

The WLAN Handset 6120/6140 emulates the IP Phone 2004. All IP Phone 2004 functions and messaging features are supported where possible.

The large screen area of the IP Phone 2004 and its numerous keys are mapped onto the smaller screen and fewer buttons of the wireless handsets. The button mapping from the IP Phone 2004 to the handsets was designed to preserve nearly all of the functionality of the IP Phone 2004 within a small, mobile device.

The line keys, numbered 1, 2, 3, 4, 5, and 6, to the left and right of the display screen of the IP Phone 2004 are mapped to the LINE button on the handset. See Figure 8 "WLAN Handset 6120" (page 124) and Figure 9 "WLAN Handset 6140" (page 125).

Figure 8
WLAN Handset 6120

Figure 9
WLAN Handset 6140

Soft key assignment

shows the soft keys that appear in standby mode.
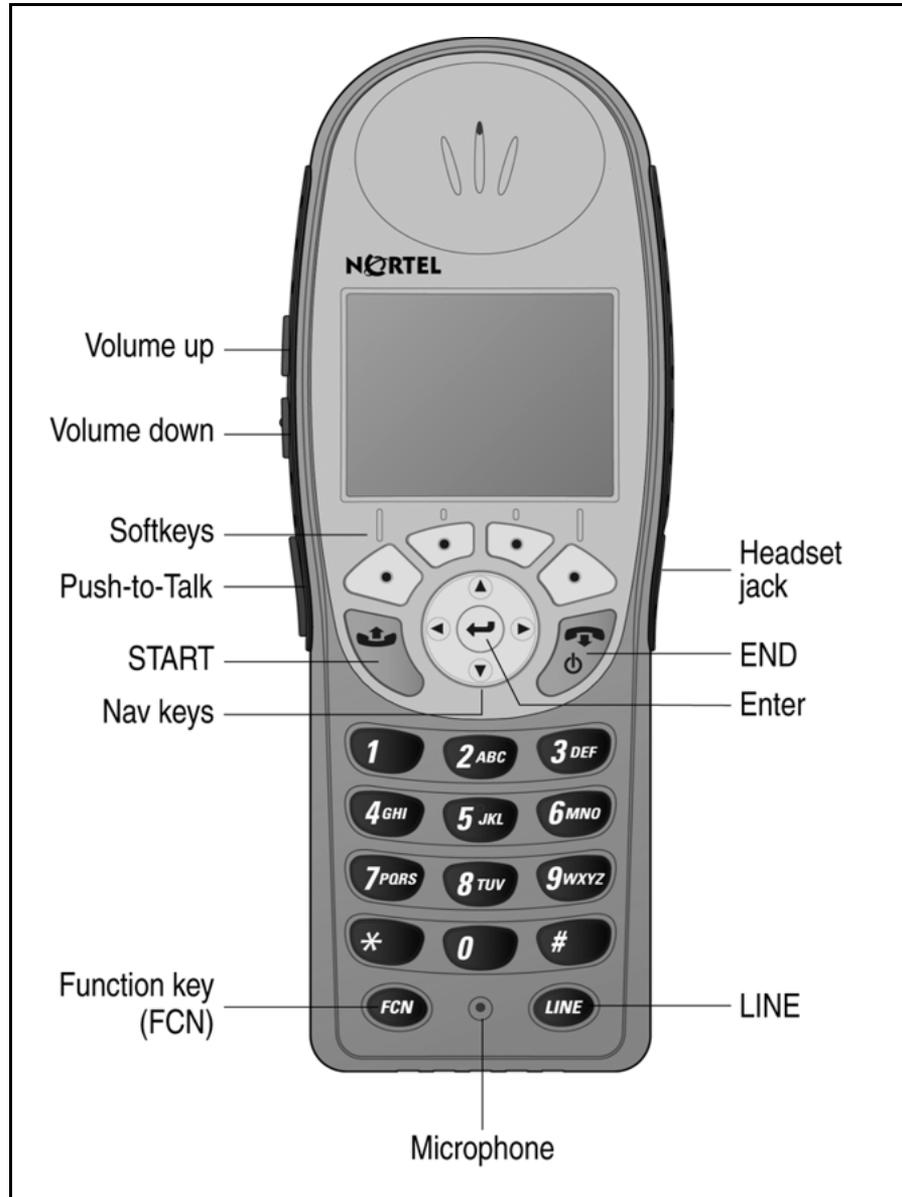
Figure 10
Soft keys in standby mode

| | Spkr | Prof | Cfg | Actv | |
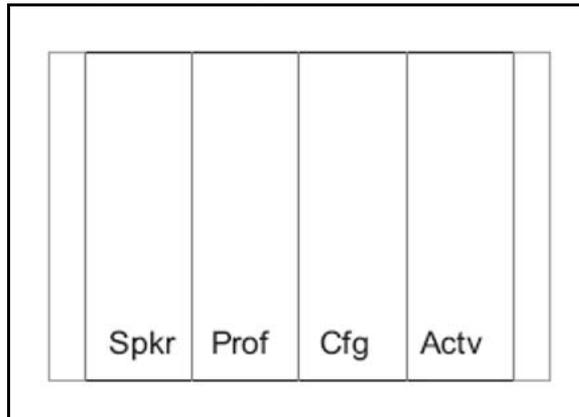
In the CS 1000, call server features include redial, speed-dial, and phonebook. These features are disabled in the handset. Access such CS 1000 features through the Directory Services option on the Feature List. Press FCN on the handset to display the Feature List.

Active idle mode and active mode
After you press the Actv soft key, the handset enters the active idle mode. The soft keys that are programmed from the CS 1000 replace the standby-mode soft keys so you can access features while the handset is still on-hook. The active idle mode times out if no keys are pressed. This same set of soft keys also appears when the handset is off-hook or in a call.

Figure 11 "Active idle or active mode" (page 126) illustrates the active idle mode or active mode soft keys.

Figure 11
Active idle or active mode

| Trns | Conf | Frwr | More | RngA | Park | Pckp | More | PrvR | Chrg | CPrt | More |
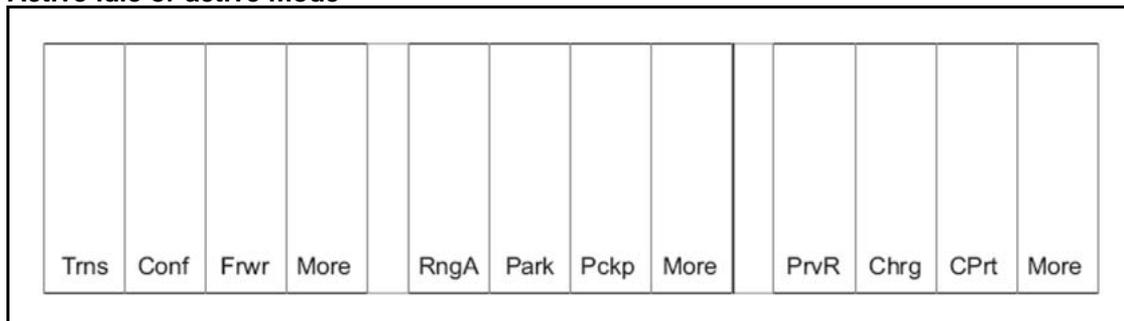
When in active idle or active mode, press **FCN** to display the Feature List and soft keys that activate the following handset features:

- **Spkr** (speaker)

- **Hold**

- **Mute**

- **Exit**

BCM standby mode

With the Business Communications Manager (BCM) Server, redial, speed-dial and phonebook are available in the handset and appear in the second set of soft keys. USB appears only during handset configuration.

When more than four soft keys are available, left and right arrows appear, as illustrated by . Use the **NAV >** and **NAV <** keys to toggle between sets.

Figure 12
Soft key sets

◄	Trns	Prof	Frwr	More	►	◄	RngA	Park	Pckp	More	►
	Set 1						Set 2				

BCM active idle mode

From standby, press Actv to enter the active idle mode. The Ftre (Feature) soft key provides access to programmed BCM system features while off-hook. Press keypad numbers to activate features just as you do on the IP Phone 2004.

BCM active mode

During a call, press FCN to display the Feature List and soft keys that activate the following handset features:

- **Spkr** (Speaker)

- **Hold**

- **Mute**

- **Exit**

Feature assignment

Table 21 "IP Phone 2004 mapping to the WLAN Handset 6120/6140" (page 128) describes how the keys of the IP Phone 2004 are mapped to key sequences on the WLAN IP 6120 handset.

Table 21
IP Phone 2004 mapping to the WLAN Handset 6120/6140

IP Phone 2004 key	Feature	Handset key sequence	Display location
1	Line 1 (usually)	Line +1	Line menu
2	Programmable	Line +2	Line menu
3	Programmable	Line +3	Line menu
4	Programmable	Line +4	Line menu
5	Programmable	Line +5	Line menu
6	Programmable	Line +6	Line menu
Goodbye		Fcn +1	Feature list
Directory		Fcn +2	Feature list
Inbox		Fcn +3	Feature list
Outbox		Fcn +4	Feature list
Services		Fcn +5	Feature list
Quit		Fcn +6	Feature list
Copy		Fcn +7	Feature list
	[OAI]	Fcn +8	Feature list

ATTENTION
If an OAI is operational, up to four function key sequences are assigned in the OAI configuration and override any function sequence established here. Use unassigned key sequences (for example, FCN + 8, 9, #, *) for OAI access.

Accessing features on the WLAN Handset 6120/6140

Some features can be accessed and activated by pressing a soft key. Examples are Hold, Mute, Park, and Conference. Others are only available through the Line Menu or the Feature List.

If the IP environment permits, you can program the line keys 1 to 6 to

- lines—called line appearances

- features—called line features

Line Menu

While off-hook, press the LINE key to view the key labels for line appearances and line features. This list is updated whenever the CS 1000 server updates the programmable key labels. To activate a line or a line feature, press the corresponding number key. Use the Nav buttons to scroll and select, use the LINE button to page between screens. Press the END key or the Cncl soft key to exit the Line menu.

Feature List

The IP Phone 2004 has several fixed feature keys. The CS 1000 implementation supports the features that are suitable to a mobile user through the Function (FCN) key on the handset. After you press FCN, the display lists the features and the assigned key. Press the END key or the Exit soft key to exit the list.

Activate the fixed features on the off-hook handset by pressing FCN + the assigned number key. You can also use the Nav keys to scroll through the items and activate the features on this list.

If an OAI application is assigned to a key, OAI information appears on the Feature List. For more information or for a list of features supported on the handset, see Table 21 "IP Phone 2004 mapping to the WLAN Handset 6120/6140" (page 128).

Lock and unlock the keypad

Because there is no Lock soft key, you must lock the keypad with the Cfg soft key. Cfg + 1 locks the keypad and displays the Unlk soft key. Press Unlk+ # to unlock the keypad.

Programmable keys on the WLAN Handset 6120/6140

In certain IP environments, the Line keys 1 to 6 on the handsets are programmable by the end user. Program the Line keys on the WLAN Handset 6120/6140 in the same manner they are programmed on the IP Phone 2004. Follow the steps in Procedure 29 "Programming the keys on the WLAN Handset 6120/6140" (page 129) to program keys on the handset.

Procedure 29
Programming the keys on the WLAN Handset 6120/6140

Step	Action
1	From the Standby state, press the **Actv** soft key.
	The wireless handset is in the Active (idle) state. The soft key display area is active but there is no dial tone.
2	Press the **Servcs** soft key.
3	Choose the **Program Key** option and press the Select soft key.

The display lists the unused line buttons that are available to program. Use the up and down navigation buttons to scroll through this list.

4 Choose the line button that you want to program and press the **Set** soft key.

5 Follow the prompts to enter the information to program this button.

--End--

For information about using the wireless handset features, see *WLAN Handset 6120 User Guide (NN43150-100)* () .

To record the function assigned to each programmed key, use a template similar to Figure 13 "Programmed key map" (page 131).

Figure 13
Programmed key map

```
            Feature   Key Press

           Transfer   FCN + _____

            Forward   FCN + _____

         Conference   FCN + _____

           Camp on    FCN + _____

             Redial   FCN + _____

          Voicemail   FCN + _____

              Flash   FCN + _____

   Application mode   FCN + _____

          _____   FCN + _____

          _____   FCN + _____

          _____   FCN + _____

          _____   FCN + _____

          _____   FCN + _____

          _____   FCN + _____
```

Troubleshooting

This chapter contains information about the following topics:

- "Wireless handset testing" (page 133)
- "Diagnostic Tools" (page 135)
- "Troubleshooting the handset" (page 147)
- "Dropped calls" (page 148)
- "Handset error messages" (page 169)
- "Before calling Nortel Technical Support" (page 171)

Wireless handset testing

Verify proper registration and operation of each wireless handset by performing the following tests on each wireless handset in an active wireless area, as follows:

- To test the WLAN Handset 2210/2211/2212, follow the steps in Procedure 30 "Testing the WLAN Handset 2210/2211/2212" (page 133).
- To test the WLAN Handset 6120/6140, follow the steps in Procedure 31 "Testing the WLAN Handset 6120/6140" (page 134).

Procedure 30
Testing the WLAN Handset 2210/2211/2212

Step	Action
1	Power on the wireless handset by pressing **Power On/Start Call**. A series of messages display as the wireless handset acquires the system. The wireless handset displays the user extension or displays dashes if no extension is programmed. Any error messages clear.
2	Press the **Power On/Start Call** key. The extension number is replaced by information from the Call Server and a dial tone is heard.

3   Place a call and listen to the audio quality.

4   End the call by pressing the **Power Off/End Call** key.

5   Place a call to the wireless handset and verify that ring, answer, clear transmit, and clear receive audio.

6   Use the **FCN** key to verify all programmed features on the wireless handset.

7   Press the **Power On/Start Call** key.

         Any line indicators turn off and the extension number display returns.

--End--

Procedure 31
Testing the WLAN Handset 6120/6140

Step	Action
1	Power on the wireless handset by pressing **End**.
	A series of messages display as the wireless handset acquires the system. The wireless handset displays the user extension or displays dashes if no extension is programmed. Any error messages clear.
2	Press the **Start** key.
	The extension number is replaced by information from the Call Server and dial tone is heard.
3	Place a call and listen to the audio quality.
4	End the call by pressing the **End** key.
5	Place a call to the wireless handset and verify that ring, answer, clear transmit, and clear receive audio.
6	Use the **FCN** key to verify the Features list.
7	Use the **Line** key to verify the Line appearances and Line Features list.
8	Press the **End** key.
	Any line indicators turn off and the extension number display returns.

--End--

Diagnostic Tools

Run Site Survey, Diagnostics Mode, and Syslog Mode are provided to assist the WLAN administrator to evaluate the functioning of the handset and the VoWLAN system. You enable these tools from the handset Admin menu.

Run Site Survey for the WLAN Handset 2210/2211/2212

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 ESSID. The information available through Site Survey includes:

- ESSID
- beacon interval
- information regarding support of various protocols and standards, as required
- current security configuration

When Run Site Survey begins, it is in single ESSID mode. Press the Any soft key to switch to all APs (regardless of ESSID) mode; the Any soft key changes to MyID. The display looks like the following in multiple AP mode:

111111 -22 33	444
111111 -22 33	444
111111 -22 33	444
111111 -22 33	444
MyID	Detl

where

111111 = last three octets of the ESSID for the
        discovered AP
22 = signal strength of the specified AP
33 = channel number of the specified AP
4444 = DTIM interval configured for the specified AP
MyID = soft key to toggle between single and any ESSID
        mode
Detl = soft key to toggle between summary and detail
        screens

Press the **Detl** soft key to view the details, as follows:

```
i:bbbbb sn ch bcn

eeeeeeeeee DGHI

rrrrrrrrrrrr+xxxx

mmm G:gggg P:pppp

Any                    Smry
```

where

i = index of selected AP (range: 0-3)
bbbbb = last three octets of the ESSID for a
      discovered AP
sn = signal strength in -dBm
ch = channel
bcn = beacon interval
eeeeeeeeee = ESSID (up to first 11 characters)
DGHI = standards supported
rrrrr = rates supported (example: 1b2b5b11b)
+ = more rates supported than displayed
xxxx = WMM or UPSD if supported
mmmm = security mode
G:gggg = group key security
P:pppp = pair-wise key security
Any = soft key to toggle between single and multiple
      ESSID mode
Smry = soft key to return to summary display

Run Site Survey for the WLAN Handset 6120/6140

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

- SSID

- beacon interval

- information regarding support of various protocols and standards, as
  required

- current security configuration

When Run Site Survey begins, it is in single SSID mode. Press the Any
soft key to switch to all APs (regardless of SSID) mode; the Any soft key
changes to MyID. The display looks like the following in multiple AP mode:

111111 -22 33	444	
111111 -22 33	444	
111111 -22 33	444	
111111 -22 33	444	
MyID	Detl	

where

111111 = last three octets of the SSID for the
    discovered AP
22 = signal strength of the specified AP
33 = channel number of the specified AP
4444 = DTIM interval configured for the specified AP
MyID = soft key to toggle between single and any SSID
    mode
Detl = soft key to toggle between summary and detail
    screens

The following display shows three APs configured with an SSID that
matches that of the handset. The first has a signal strength of −28dBm,
and is configured on channel 2 with a beacon interval of 100 ms. The
second has a signal strength of −48dBm, and is configured on channel
6 with a beacon interval of 200 ms. The third has a signal strength of
−56dBm and is configured on channel 11 with a beacon interval of 100 ms.

ab7bc8 -28 02	100
2ae578 -48 06	200
2ae596 -56 11	100
Any	Detl

When you select any Any SSID mode, the summary display contains the
first six characters of the APs SSID instead of the beacon interval, as
shown in the following example.

ab7b -28 02	ALPHA
2ae5 -48 06	WSMTES
2ae5 -56 11	voice
Any	Detl

In detail mode, the display appears as follows. The left and right arrow keys move between AP indices.

```
i:bbbbb sn ch bcn

eeeeeeeeee DGHI

rrrrrrrrrrrr+xxxx

mmm G:gggg P:pppp
Any                     Smry
```

where

i = index of selected AP (value is from 0 to 3 inclusive)

bbbbb = last three octets of the SSID for a discovered AP

sn = signal strength in -dBm

ch = channel

bcn = beacon interval

eeeeeeeeee = SSID (up to first 11 characters)

DGHI = standards supported

rrrrr = rates supported—basic rates have a b following the rate

+ = more rates supported than displayed

xxxx = WMM or UPSD if supported

mmmm = security mode

G:gggg = group key security

P:pppp = pair-wise key security

Any/MyID = soft key to toggle between single SSID and multiple SSID mode

Detl/Smry = soft key to toggle between the multiple AP display (summary) and the single AP display (detail)

ATTENTION

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

Diagnostics Mode

Diagnostics Mode evaluates the overall quality of the link between the handsets, the AP, and the infrastructure equipment (call server, WLAN IP Telephony Manager 2245, and gateways). Diagnostics Mode can be used when the handset is active.

When Diagnostics Mode is activated in the Admin menu, the handset enters the diagnostic state. The handset can display diagnostics any time it is on a call.

Pressing the Menu key displays a number of diagnostic counters. Five screens of counters can be displayed by pressing the Menu key to scroll through the following screens:

- Screen 1—displays counters for missed receive packets, missed transmit packets, receive retry count, and transmit retry count.

- Screen 2—displays jitter delta, last successful transmit data rate, and gateway type.

- Screen 3—displays a list of APs and some of their details.

- Screen 4—displays association and reassociation counts.

- Screen 5—displays security error count and sequence number for last security error.

After all the counters are displayed, the screen returns to the normal off-hook display.

The screen number appears on the top line of the screen.

Diagnostics Screen 1 displays the following information:

MissedRcvCnt	nnnnn
MissedXmtCnt	nnnnn
RxRetryCount	nnnnn
TxRetryCount	nnnnn

where

MissedRcvCnt is the missed receive packet count since power on.
MissedXmtCnt is the missed transmit packet count since power on.
RxRetryCount is the receive retry count since power on.
TxRetryCount is the transmit retry count since power on.

Diagnostics Screen 2 displays the following information:

Jitter	nnnnn
LastRate	nnnnn
GatewayType	mnemo

where

Jitter is the current delta from the desired jitter
buffer depth, in microseconds.

LastRate is the last successful transmit data rate.

GatewayType is a mnemonic that indicates the gateway
type. The mnemonic is one of the following.

SAWA2	all phones are rate limited to 2 Mb because an old 2 Mb handset is on the network (not applicable for the WLAN Handset 6120 and the WLAN Handset 6140)
2Mb	old style 2 Mb (not applicable for the WLAN Handset 6120 and the WLAN Handset 6140)
11Mb	New style 11 Mb (for all handsets)

Diagnostics Screen 3 displays a list of the APs that are heard, in the
following format:

C : mmmm ch - ss		aid
1 : mmmm ch - ss		mnem
2 : mmmm ch - ss		mnem
3 : mmmm ch - ss		mnem

where

C is the AP currently in use.

1, 2, and 3 are the candidate APs.

mmmm is the hexadecimal number comprised of the last
two octets of the AP MAC address.

ch is the channel number that the AP is configured on.

ss is the signal strength for the AP in dBm.

aid is the Association ID of the currently associated
AP.

mnem is a mnemonic that indicates why the handset
did not hand off. The mnemonic is one of the
following.

Unkn	reason unknown
Weak	signal strength too weak
Rate	One or more basic rates not supported
Full	AP cannot handle bandwidth requirements
AthT	Authentication Timeout
AthF	Authentication Failure
AscT	Association Timeout
AscF	Association Failure

SecT	Security Timeout
SecF	Security Failure
Cnfg	Configuration error—AP is not configured correctly (check security, QoS mode, or network infrastructure)

Diagnostics Screen 4 displays the following information:

AssocCount	nnnnn
ReAssocCount	nnnnn
AsssocFailure	nnnnn
ReAssocFail	nnnnn

where

AssocCount is the association count since power on.
ReAssocCount is the reassociation count since power on.
AssocFailure is the number of association failures since power on.
ReAssocFail is the number of reassociation failures since power on.

Diagnostics Screen 5 displays the following information:

Sec-ErrCount	nnnnn
LstSecErrSeq	nnnnn

where

Sec-ErrCount is the security error count since power on.
LstSecErrSeq is the MAC frame sequence number with the last security error.

Syslog Mode

A Syslog Server must be present on the network so that the handset can send log messages and have them saved. The Syslog Server IP address can be configured using DHCP or statically configured.

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 cannot send any syslog messages.

Each syslog message includes the following:

- Date and time (to 1100th of a second) since the handset power on (configured to January 1 00:0:00); requires an SNTP server
- WLAN Handset MAC address
- WLAN Handset IP address
- Sequence number
- plus, additional items, based on the message type, as shown in Table 22 "Syslog message contents" (page 142).

Message example:

Jan 1 00:01:26 0090.7a02.2a1b (172.16.0.46) [001a] RStat: AP 00:40:96:48:1D:0C (-56dBm), 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%).

Table 22 "Syslog message contents" (page 142) contains the contents of the syslog messages.

Table 22
Syslog message contents

Syslog message	Contents
Failed Handoff (sent whenever the handset decided to hand off, but failed trying)	Failed AP MAC Failed AP signal strength Current AP MAC Current AP signal strength Failure reason
Successful Handoff	New AP MAC New AP signal strength Old AP MAC Old AP signal strength Reason for handoff Other candidate APs:

Table 22
Syslog message contents (cont'd.)

Syslog message	Contents
	• MAC • Signal strength • Reason not used
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 ms) 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

Table 22
Syslog message contents (cont'd.)

Syslog message	Contents
Audio threshold exceeded (Sent if payloads missed rate or payloads late rate exceeds 2%, or if the average jitter is over 2 ms)	AP MAC AP signal strength Payload size (in ms) 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
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)

Table 22
Syslog message contents (cont'd.)

Syslog message	Contents
	RX retry count
	RX retry rate (over last 5 seconds)
Radio threshold exceeded (Sent if TX drop rate exceeds 2%, or TX or RX retry rate exceeds 5%)	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)
VPN: Established IKE phase1 SA, renew in xs VPN: Established IKE phase2 SA yy:yy, renew in xs (a phase1 message follows the phase 2 message, sent whenever a phase 1 or phase 2 security association completes)	Expiration time and security association identifiers, if applicable. sx is the number of seconds yy:yy stands for the two eight-digit SA numbers for send and receive
VPN: phase2 Unexpected message VPN: phase2 Initiated by VN server VPN: phase2 INFO Delete payload	none

Table 23
Syslog reason codes

Reason code number	Meaning
0	OK
1	TOO FEW AVERAGE PROBES
2	WORSE SIGNAL
3	INVALID SSID
4	NO PARAMS FOUND
5	BAD RATES
6	OFF CHANNEL PROBE RESP
7	AP TOO BUSY
8	AUTH TIMEOUT
9	ASSOC TIMEOUT
10	FAILED AUTHENTICATION
11	FAILED ASSOCIATION
12	SOFT NEIGHBOR
13	NO SIG IMPROVEMENT
16	NO KEEPALIVE
17	LOST AUDIO
18	NO RESPONSE
19	NO PRIVACY
20	APP UNHAPPY
21	DISASSOCIATED
22	NO HANDOFF
23	HANDOFF
24	INITIAL ASSOC
25	LOST AP
26	TX FAILURES
27	CHANGING RATES
28	UNDEFINED
29	EAP START TIMEOUT
30	LEAP CHALLENGE TIMEOUT
31	EAP SUCCESS TIMEOUT
32	LEAP CHALLENGE RESPONSE TIMEOUT

Table 23
Syslog reason codes (cont'd.)

Reason code number	Meaning
33	NONCE CCKM TIMEOUT
34	RSNIE AP TIMEOUT
35	NONCE GTK TIMEOUT
36	EAPOL LOGOFF
37	EAPOL FAILURE
38	NO WPA ELEMENT
39	BAD MIC
40	BAD PROBE RESP
41	BAD CAP INFO AD HOC
42	ACTION TIMEOUT
43	FAILED ACTION
44	DELTS
45	QOS REQUIRED
46	CHANGED LISTEN INTERVAL

Troubleshooting the handset

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

Context

When troubleshooting a problem with a wireless handset, it is important to determine the context of when and where the problem occurred. Context includes the following:

- Was the wireless handset on an active call?

- Was the wireless handset moving or stationary?

- Was the wireless handset powering on or powering off?

- Was PTT being used?

- At what location did the problem occur?

Record this information and provide it to the system administrator or Nortel Technical Support.

No ring

It is possible in certain situations for a voice mail message to be left on a wireless handset without the wireless handset ever ringing. This situation could occur when a wireless handset is out of range of an AP for even a few seconds. If during the time the wireless handset were out of AP range and an incoming call was received, the incoming call receives the Call Forward No Answer (CFNA) treatment configured for that wireless handset, such as forwarding the incoming call to voice mail. To prevent this situation from occurring, ensure adequate AP coverage in all areas where a wireless handset can be used.

- Allow the Config menu to time out. The Config menu times out after 20 seconds of inactivity.

- Press End or Exit soft key to exit the Config menu.

Far-end echo

Sometimes, when using the G.711 codec, echo might be perceptible at the far end, and be more severe when the wireless handset is in an environment with extreme background noise and the wireless handset volume is configured to maximum volume.

To correct this problem, reduce the volume setting on the wireless handset. Alternatively, if experiencing this problem, consider using the G.729 codec.

Dropped calls

If calls are dropping, use the Site Survey mode of the wireless handset in the area where the problem occurred to determine if there is inadequate AP coverage in that area.

Wireless handset status messages

Wireless handset status messages provide information about the handset communication with the AP and Call Server. Table 24 "Wireless handset status messages" (page 148) summarizes the status messages, in alphabetical order.

Table 24
Wireless handset status messages

Message	Description	Action
3 chirps	Wireless 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 is handed-off to the best AP after it becomes available.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Address Mismatch	Wireless handset firmware download files are incorrect or corrupted.	Download new firmware from the Nortel site. See "Software updates" (page 35).
ASSERT xxx.c Line yyy (For WLAN Handsets 2210/2211/2212 only.)	The handset has detected a fault from which it cannot recover.	Record the error information so that it can be reported. Turn the handset off, and then on again. If the error persists, try registering a different handset to this telephone port. If the error still persists, contact Nortel Technical Support and report the error.
Assoc Failed xxxxxxxxxxxx	x...x = AP MAC address Handset association was refused by the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.
Assoc Timeout xxxxxxxxxxxx	x...x = AP MAC address Handset did not receive an association response from the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.
Auth Failed xxxxxxxxxxxx	x...x = AP MAC address Handset authentication was refused by the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.
Auth Timeout xxxxxxxxxxxx	x...x = AP MAC address Handset did not receive an authentication response from the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Bad Code Type xx Expected Code Type yy	xx, yy = firmware license types Handset firmware does not match the current handset license selection.	Download new firmware from the Nortel site. See "Software updates" (page 35).
Bad Config	Some needed configuration parameter has not been configured.	Check all required wireless handset configuration parameters for valid settings.
Bad ESSID (For WLAN Handsets 2210/2211/2212 only.)	The wireless handset is configured for static ESSID (as opposed to Learn once or Learn always) and no ESSID is entered.	Enter an ESSID in the configuration settings or change to one of the Learn modes.
Bad SSID (For WLAN Handsets 6120/6140 only.)	The wireless handset is configured for static SSID (as opposed to Learn once or Learn always) and no SSID is entered.	Enter an SSID in the configuration settings or change to one of the Learn modes.
Bad Local ID	The value of the Phase 1 Local ID type entered in the handset through the menus or the Configuration Cradle is improperly configured.	Enter a valid ID value.
Bad Local ID Type	The Phase 1 Local ID type entered in the handset through the menus or the Configuration Cradle is missing or invalid.	Enter a valid ID type. KEY ID is the only valid choice.
Bad Network IP	The value of the Remote Network IP address entered in the handset through the menus or the Configuration Cradle is missing or invalid.	Enter a valid remote network IP address.
Bad Network Mask	The value of the network mask for the Remote Network entered in the handset through the menus or the Configuration Cradle is missing or invalid.	Enter a valid network mask.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Bad Payload Type	The VPN server is not accepting some of the parameters passed to it by the handset. One common instance would be it two handsets try to use the Client IP.	If the VPN Client IP is statically configured, ensure that the address assigned to the handset is unique. If using IKE Mode Config, ensure that the address entered in the VPN Server configuration for the handset or user is unique.
Bad Phintl File	The handset firmware download files are incorrect or corrupted.	Download new firmware from the Nortel site. See "Software updates" (page 35).
Bad Program File	The handset firmware download files are incorrect or corrupted.	Download new firmware from the Nortel site. See "Software updates" (page 35).
Bad Preshared Key	The value of the preshared key entered in the handset through the menus or Configuration Cradle is improperly configured.	Enter a valid preshared key value. For a Contivity VPN server, this is the password.
Bad Tunneled IP	The value of the VPN Client IP address entered in the handset through the menus or the Configuration Cradle is configured for static IP and is missing.	Enter a valid client IP address.
Bad VPN Server IP	The VPN Server IP address entered in the handset through the menus or the Configuration Cradle is invalid.	Enter the IP address of the VPN server.
(battery icon), Low Battery message, and beep Battery Low	Low battery	**In call**: the battery icon displays and a soft beep is heard when the user is on the wireless handset and the battery charge is low.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Battery Low		The **Battery Low** message indicates that the battery pack can be changed while the call is still in progress. For the WLAN Handsets 2210/2211/2212 only, do not press **Power Off/End Call**. Place the call on Hold or Park, quickly remove the discharged battery and replace with a charged battery, power on the handset and press **Power On/Start Call** to resume the call in progress. For the WLAN Handsets 6120/6140 only, do not press End. Place the call on Hold or Park, quickly remove the discharged battery and replace with a charged battery, power on the handset and press Start to resume the call in progress. **Not in call**: The battery icon displays whenever the battery charge is low. The message **Low Battery** and a beep indicate a critically low battery charge when the user is not on the wireless handset. The wireless handset does 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 battery pack. Only the approved battery pack works.
Battery Failed	Battery pack is damaged or incompatible with the handset.	Replace the battery pack with a new or confirmed battery pack. Only the approved battery pack works.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Can't renew DHCP yyy.yyy.yyy.yyy	y...y = DHCP server IP address DHCP server is not responding to the initial renewal attempt.	Configuration problem. Check the IP address configuration in the DHCP server.
Charging ...	The wireless handset is charging in the Desktop Charger.	No action needed.
Charge Complete	The wireless handset is now fully charged.	No action needed.
Checking Code	Wireless handset is contacting the TFTP Server to determine if it has a newer version of firmware that should be downloaded.	None. This message should only last for approximately one second. If message remains displayed, power off and contact Nortel Technical Support.
Checking DHCP IP	The wireless handset is retrieving DHCP information from the DHCP server.	None. This is for information only.
CRC Code Error	The firmware that is TFTP downloaded has a bad Cyclical Redundancy Code (CRC) check.	Try the download again. It is possible the firmware was corrupted during download. If the error repeats, check that the download image on the TFTP Server is not corrupted.
Code Mismatch!	The firmware loaded into the wireless handset is incorrect for this model of telephone.	Verify that the License Management value is correct. Replace the firmware image on the TFTP server with firmware that is correct for the handset model.
DCA Timeout	The handset has detected a fault from which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off, and then on again. If the error persists, contact Nortel Technical Support and report the error.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
DHCP Error (1-5)	DHCP Error 1	The wireless handset cannot locate a DHCP server. It tries every 4 seconds until a server is located.
	DHCP Error 2	The wireless handset has not received a response from the DHCP server to a request for an IP address. It retries until a DHCP server is found.
	DHCP Error 3	The server refuses to lease the wireless handset an IP address. It keeps trying.
	DHCP Error 4	The DHCP server offered the wireless handset a lease that is too short. The minimum lease time is 10 minutes. One hour is the minimum recommended lease time. The wireless handset stops trying. Reconfigure the DHCP server and power-cycle the wireless handset.
	DHCP Error 5	Failure during WEP Key rotation process (proprietary failure).
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 wireless handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration is changed by the administrator. The wireless handset attempts to negotiate a new lease or display one of the DHCP errors (1-5).
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 wireless handset is no longer valid, which forces the wireless handset to restart. This problem should resolve itself on the restart. If it does not, the problem is in the DHCP server.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
DL Not On Sector	The handset firmware download files are incorrect or corrupted.	Download new firmware from the Nortel site. See "Software updates" (page 35).
DO NOT POWER OFF	The wireless handset is in a critical section of the firmware update.	None. Do not remove the battery or attempt to power off the phone while this message is displayed. Doing so can require the wireless handset to be returned to Nortel to be recovered.
Duplicate IP	The wireless 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 wireless handset was assigned a unique address.
Erase Failed	Download process failed to erase the memory in the wireless handset.	Operation retries but can eventually report the error int. error: 0F. Power cycle the wireless handset.
Erasing memory	The wireless handset has determined that a download should occur and is erasing the current firmware 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.
Error! [error details] (For the WLAN Handset 6120/6140 only)	A fatal firmware error is detected. All handset operation is halted and any call is lost.	This message appears during the Halt on Error mode. To capture the error message, reboot the handset and write down the information that is on the display.
Files Too Big	The handset firmware download files are incorrect or corrupted.	Download new firmware from the Nortel site. See "Software updates" (page 35).

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Flash Config Error	Handset internal configuration is corrupt.	Perform the Restore Defaults operation from the administrator menu and reprogram, or reprogram using the Configuration Cradle.
Initializing	The wireless handset is performing a power-on initialization.	None. This is informational only.
Internal Err. # #	The wireless handset has detected a fault from which it cannot recover. OE=Error while writing the Flash (return handset to factory) OF = No functional code (contact Nortel Technical Support)	Record the error code so it can be reported. Turn the wireless handset off, and then on again. If error persists, try registering a different wireless handset to this telephone port. If error still persists, contact Nortel Technical Support and report the error.
Invalid ID Info	The VPN server did not recognize this user.	Make sure that the local ID (KEY ID) entered in the handset matches the key Id in the VPN server. For a Contivity VPN server, the local ID must match the username.
Multiple SVP Svr yyy.yyy.yyy.yyy	y...y = WLAN IP Telephony Manager 2245 IP address Handset received responses from multiple WLAN IP Telephony Managers 2245; displays the IP address of one responding WLAN IP Telephony Manager 2245.	Happens if the handset is reconfigured to use a different WLAN IP Telephony Manager 2245 and then powered-down before the previous server has had time to determine that the handset is no longer connected to it. The problem should correct itself in about 30 seconds.
Must upgrade SW!	Handset firmware is incompatible with the hardware.	Download new firmware from the Nortel site. See "Software updates" (page 35).
Net Busy xxxxxxxxxxxx	x...x = AP MAC address Handset cannot obtain sufficient bandwidth to support a call; displays the MAC of the failing AP.	Try call again later.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DHCP is operational and connected to the WLAN or use Static IP configuration in the handset.
No ESSID (For the WLAN Handsets 2210/2211/ 2212 only.)	Attempted to run the Site Survey application without an ESSID configured.	Let the handset come completely up. Statically configure an ESSID in the Admin menu.
No SSID (For the WLAN Handsets 6120/6140 only.)	Attempted to run the Site Survey application without an SSID configured.	Let the handset come completely up. Statically configure an SSID in the Admin menu.
No Func Code	Handset firmware download files are incorrect or corrupt.	Reconfigured the handset to gain access to the WLAN and download new code.
No Host IP (Addr)	The wireless handset is configured for static IP (as opposed to use DHCP) and no valid host IP address (the wireless handset IP address) is entered.	Enter a valid IP address in the configuration settings or change to use DHCP.
No IP Address	Invalid IP address.	Check the IP address of the wireless handset and reconfigure if required.
No Net Access	Cannot authenticate/associate with AP.	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.
No Net Found (For the WLAN Handsets 2210/2211/ 2212 only.)	This indicates any of the following:	
	• No radio link	Verify that the AP is turned on.
	• No ESSID—Autolearn not supported (or) incorrect ESSID	Verify the ESSID of the wireless LAN and enter or Autolearn it again, if required.
	• AP does not support appropriate data ranges	Check the AP configuration against the AP Configuration Note.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
	• Out of Range	Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the ESSID of the handset.
	• incorrect WEP settings	Verify that all the WEP settings in the handset match those in the APs.
	• Incorrect Security settings	Verify that all the Security setting in the AP.
No Net Found (For the WLAN Handsets 6120/6140 only.)	This indicates any of the following:	
	• No radio link	Verify that the AP is turned on.
	• No ESSID—Autolearn not supported (or) incorrect SSID	Verify the SSID of the wireless LAN and enter or Autolearn it again, if required.
	• AP does not support appropriate data ranges	Check the AP configuration against the AP Configuration Note.
	• Out of Range	Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the SSID of the handset.
	• incorrect WEP settings	Verify that all the WEP settings in the handset match those in the APs.
	• Incorrect Security settings	Verify that all the Security setting in the AP.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
No Net Found xxxxxxxxxxxx yy	x...x = AP MAC address yy = AP signal strength Handset cannot find a suitable AP; displays the MAC address and signal strength of the best nonsuitable AP found.	Check the AP and handset network settings, such as ESSID, (for the WLAN Handsets 2210/ 2211/2212), SSID (for WLAN Handsets 6120/6140), Security, Reg. domain, and Tx power. Ensure that the APs are configured per Configuration Note. Try Site Survey mode to determine a more specific cause.
No PBX Response	The wireless handset tried to send a message to the Call Server and failed to get a response.	Verify the Call Server is operational and connected to the network.
No Proposal	The handset and the VPN server could not agree on a set of configuration parameters.	Check that the Diffie-Hellman group, phase 1 and phase 2 hashes, and the encryption algorithms configured on the handset are acceptable to the VPN server.
No Reg Domain	Regulatory Domain not configured	Configure the Regulatory Domain of the handset.
No SVP IP	The wireless handset is configured for static IP (as opposed to use DHCP) and no valid WLAN IP Telephony Manager 2245 address is entered.	Enter a valid WLAN IP Telephony Manager 2245 IP address in the wireless handset configuration setting or change to use DHCP.
No SVP Response yyy.yyy.yyy.yyy	y...y = SVP Server IP address The handset has lost contact with the WLAN IP Telephony Manager 2245.	This can be caused by bad radio reception or a problem with the WLAN IP Telephony Manager 2245. The handset keeps trying to fix the problem for 20 seconds, and the message can clear by itself. If it does not, the handset restarts. Report this problem to the system administrator if it keeps happening.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
No SVP Server	Wireless handset can't locate WLAN IP Telephony Manager 2245.	IP address configuration of WLAN IP Telephony Manager 2245 is wrong or missing.
	WLAN IP Telephony Manager 2245 is not working.	Check error status screen on WLAN IP Telephony Manager 2245.
	No LAN connection at the WLAN IP Telephony Manager 2245.	Verify WLAN IP Telephony Manager 2245 connection to LAN.
No SVP Server No DNS Entry	The handset was unable to perform DNS lookup for the WLAN IP Telephony Manager 2245; server had no entry for SVP Server.	The network administrator must verify that a proper IP address is entered for the SVP Server DHCP option.
No SVP Server No DNS IP	The handset was unable to perform a DNS lookup for the WLAN IP Telephony Manager 2245; no IP address for DNS server.	The network administrator must verify proper DHCP server operation.
No SW Found	A required firmware component has not been properly identified.	Check that the handset license type has a corresponding entry in the slink_cfg.cfg file. Check that the pd11ccc.bin and pi110003.bin entries exist under this type in the slnk_cfg.cfg.
No UNIStim DHCP	The handset was unable to use DHCP to obtain the server information it requires to start up.	Verify the DHCP server configuration information. Verify network connectivity between the handset and the DHCP server.
No VPN Server	The handset could not find the VPN server.	Check that the value of the VPN Server IP address configured through the administration menu or the Configuration Cradle match the address of the VPN server.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Not Installed!	A required firmware component is missing.	Check that all required firmware files are on the TFTP Server, if over-the-air downloading is being used. If the error repeats, contact Nortel Technical Support.
Payload Malfmd	The handset could not understand an encrypted message from the VPN Server (or vice-versa). This is likely to be a mismatch in the security parameters such as preshared key, Diffie-Hellman group, hash and encryption algorithms.	Check the Diffie-Hellman group, the phase 1 and phase 2 hashes, and encryption configuration.
Press End Call	The call has ended.	Press the Power Off/End Call key to return to standby mode.
Restart Command	The wireless handset received a restart command from the Call Server.	None. The wireless handset automatically restarts in a few seconds.
RTP Open Failed	The handset was unable to open the requested RTP or RTCP socket.	Reboot the handset. If the error repeats, contact Nortel Technical Support.
Select License	The correct protocol has not been selected from the license set.	Using the administrative menus, select one license from the license set to allow the wireless handset to download the appropriate firmware.
Server Busy	Wireless handset is attempting to download from a TFTP Server that is busy downloading other devices and refusing additional downloads.	None. The wireless handset automatically retries the download every few seconds.
Server Unavailable. Restarting... (For the WLAN Handset 6120/6140 only)	An error caused the handset to lose the call. It is trying to restart and return to standby mode.	Occurs during Restart on Error mode. The handset is attempting to register with the PBX and resume normal operation. Error details are available through the Syslog Server and by download with the Handset Administration Tool.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
SKT Open Failed	Socket open fail. Occurs when the handset tries to connect to the call server, but there is not response. If resiliency is active, the handset keeps trying.	If the call server is inoperative and resiliency is not active, or the handset cannot locate a backup call server, turn off the handset and repair the primary call server. Note that it is advisable to reconfigure the backup call server to be the primary call server if the repair is more time-consuming than the reconfiguration.
Storing Config	Handset is storing changes to handset configuration.	None. Informational message only. The handset can display this briefly following a configuration change or firmware download.
SVP Service Rej.	The WLAN IP Telephony Manager 2245 has rejected a request from the wireless handset.	The wireless handset restarts and attempts to reregister with the WLAN IP Telephony Manager 2245, which should fix the problem. Report this to the administrator if it keeps happening.
System Busy yyy.yyy.yyy.yyy (with busy tone)	y...y = SVP or GW IP Address Gateway or WLAN IP Telephony Manager has reached call capacity; displays the IP address of the gateway SVP Server.	All call paths are in use; try call again in a few minutes.
System Locked (with busy tone)	WLAN IP Telephony Manager 2245 is locked. Gateway is locked.	Try call again later. System is locked for maintenance.

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
TFTP ERROR(x):yy	A failure has occurred during a TFTP firmware download. **(x)** = the file number that was being downloaded; **yy** = an error code describing the particular failure. Possible error codes are: • 01 = TFTP Server did not find the requested file. • 02 = Access violation (reported from TFTP Server). • 07 = TFTP Server reported No such user error. • 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 or 07—check the TFTP Server configuration. Error code 81—the wireless handset attempts to download the file again. For other messages, power off the wireless handset, and then turn it on again to retry the download. If the error repeats, note it and contact Nortel Technical Support.
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to Nortel.
Unknown xx:yy:zz	A phrase is missing from your phintl file.	Download new firmware from the Nortel site. See "Software updates" (page 35).
Updating Code	Wireless handset is downloading new firmware 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 off the handset during this operation.
VPN Error: xxxx	The VPN server returned an information message with a code of xxx.	

Table 24
Wireless handset status messages (cont'd.)

Message	Description	Action
Waiting	Wireless handset has attempted some operation several times and failed. It is now waiting for a period of time before attempting that operation again.	None. The wireless handset is waiting for a specified period of time before attempting that operation again.
Watchdog Timeout	The wireless handset failed to hear from the Call Server within the watchdog timeout interval.	Verify the Call Server is operational and connected to the network.
Wrong Code Type	The firmware loaded into the handset is incorrect for this model of handset.	Verify that the license type is configured correctly. If the license type is correct, replace the firmware image on the TFTP server with the firmware that is correct for the handset model.

Using Call Server overlay commands

The following sections provide information about Call Server overlay commands.

LD 32 IDU command

For the handsets, the IDU command outputs the following specific information:

- Release code: Rls: 6 (2210), Rls: 7 (2211) or Rls: 8 (2212)

- NT Code: NTTQ4010 (2210), NTTQ5010 (2211) or NTTQ69AA (2212)

- Software Version has different format: <Version>.<Issue> FWSW:097.059 (or later)

- The IP address is the alias IP address of the wireless handset that is provided by the WLAN IP Telephony Manager 2245. The MAC address is the MAC address of the wireless handset. In other words, the MAC address and the IP address are not related.

In the following example, 61 0 is an IP Phone 2004 and 62 2 is a WLAN Handset 2211.

```
.idu 61 0
I2004 TN: 061 0 00 00 V
TN ID CODE: i2004
ISET MAC ADR: 00:60:38:76:41:C7
ISET IP ADR: 192 .168 .010 .100
```

```
LTPS IP ADR: 047 .011 .214 .165
MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NT2K00GI
COLOR CODE: 66
RLS CODE: 0
SER NUM: 7641C7
FWSW VERSION: 0602B59
.idu 62 2
I2004 TN: 062 0 00 02 V
TN ID CODE: i2004
ISET MAC ADR: 00:90:7A:01:7E:47
ISET IP ADR: 192 .168 .010 .200
LTPS IP ADR: 047 .011 .214 .165
MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NTTQ5010
COLOR CODE: 66
RLS CODE: 7
SER NUM: 017E47
FWSW VERSION: 097.021
```

LD 32 STAT command

The wireless handsets are shown REGISTERED in the standby and active modes. In the following example, 61 0 is an IP Phone 2004 and 62 2 is a WLAN Handset 2211 in the standby mode.

```
.stat 61 0
IDLE REGISTERED 00
.stat 62 2
IDLE REGISTERED 00
```

LD 117 Inventory command

In the inventory report, the wireless handsets have a specific release code and NT code, similar to the IDU command output. In the following example, 61 0 is an IP Phone 2004 and 62 2 is a WLAN Handset 2211.

```
=> inv prt sets
Set inventory:
17 10 2003 8 17 21, 17 10 2003 8 17 22, 6
i2004, 61 00, i2004 NT2K00GI 66 0 7641C7, I2004 , 6000
i2004, 62 02, i2004 NTTQ5010 66 7 017E47, I2211 , 6502
```

LD 117 STIP command

The STIP command can be used for wireless handsets; however, the wireless handset alias IP address appears as the TERMIP in the command output, instead of physical IP address. In the following example, the 192.168.10.200 is an alias IP address assigned by the WLAN IP Telephony Manager 2245.

```
TN HWID STATUS HOSTIP TERMIP PORT

_____ _____ _____ _____
_____ _____
0x600a 0000000000000003000907a017e476607 REG 47.11.214.165
192.168.10.200 0x1450
CAPS

_____
0x00000000
-------------------------------
codec bdwth(k) codecCaps desc
-------------------------------
4 190 0x00000000 1
3 190 0x00000000 1
17 47 0x00000001 1
value = 537232412 = 0x2005841C
```

For information about more CLI commands, see "TPS CLI commands" (page 166).

TPS CLI commands

The following sections describe TPS command line interface (CLI) commands.

dsetShow command

In the **dsetShow** command output, the handsets have a specific Hardware ID. The alias IP address is output, not the physical wireless handset IP address.

In the following example, the IP Phone 2004 has an IP address of 192.168.10.100 and the WLAN Handset 2211 has an alias IP address of 192.168.10.200. The syntax of the Hardware ID is as follows:

- first two digits—Manufacturer Location. Manufacturer Location is 18 for the IP Phone 2004 and 30 for the WLAN Handset 2211.

- next six digits—Manufacturer Code. The Manufacturer Codes are defined as follows:

  — IP Phone 2004 Phase 1—006038

  — IP Phone 2004 Phase 2—000ae4

  — WLAN Handset 2210—00907a

— WLAN Handset 2211—00907a

— WLAN Handset 2212—00907a

- last two digits—Release Code. The Release Codes are defined as follows:

  — IP Phone 2004 Phase 1—0

  — IP Phone 2004 Phase 2—2

  — WLAN Handset 2210—0x06

  — WLAN Handset 2211—0x07

  — WLAN Handset 2212—0x08

```
-> dsetShow
TN IP Address Hardware ID TermType
---- --------------- ------------------- ----------
6004 192.168.10.100 180060387641c76600 i2004
600A 192.168.10.200 3000907a017e476607 i2004
value = 0 = 0x0
```

e2dsetShow command
The `e2dsetShow` command is used for the handsets in the same manner as for the IP Phones.

isetCount and isetGet
Use the alias IP address of the handsets in the expression string of the `isetCount` and `isetGet` commands, not the physical IP address. The following is an example of the `isetGet` output for the WLAN Handset 2211.

```
->isetGet "IP == 192.168.10.200"
IP Address Type RegType State Up Time Set-TN Regd-TN HWID
FWVsn
---------- ----- ------- ----- ------- ------- -----
------------ ---------
192.168.10.200 i2004 Regular online 0 00:12:00 062-02
062-02 3000907a017e476607 097.021

UNIStimVsn SrcPort DstPort
--------- ------ ------
2.6 5100 5000
```

isetReset and isetResetAll
The `isetReset` command can be used to reset the wireless handsets by specifying the wireless handset alias IP, not the physical IP address:

```
-> isetReset "192.168.10.200"
value = 0 = 0x0
```

isetShow, isetShowByTN, and isetShowByIP

Similar to the **dsetShow** command, the wireless handset outputs its specific hardware ID (see **dsetShow**) and alias IP, not the physical IP address. The FW version has a different format <Version>.<Issue> in this output.

In the following example, the telephone with TN 062-02 is the WLAN Handset 2211.

```
-> isetShow
Set Information
---------------
IP Address Type RegType State Up Time Set-TN Regd-TN
---------- ---- ----- ---- ----- ----- -------
192.168.10.100 i2004 Regular online 4 22:59:22 061-00
061-00

HWID FWVsn UNIStimVsn SrcPort DstPort
----------------- ---- -------- ----- -----
180060387641c76600 0602B59 2.8 5100 5000

IP Address Type RegType State Up Time Set-TN Regd-TN
---------- ---- ----- ---- ----- ----- -------
192.168.10.200 i2004 Regular online 0 02:03:22 062-02
062-02

HWID FWVsn UNIStimVsn SrcPort DstPort
----------------- ----- ------- ----- ------
3000907a017e476607 097.021 2.6 5100 5000
```

umsKernalJobsShow and umsUpgradeAll

The umsKernalJobsShow and umsUpgradeAll commands cannot be used to monitor and originate firmware upgrades for wireless handsets since the wireless handsets are upgraded using a different mechanism without the help of the UMS subsystem. For information about how to monitor and originate the firmware upgrade, see the documentation for the TFTP server used by the wireless handsets.

umsPolicyShow and umsUpdatePolicy

The IP Phone 2004 policy used in these commands is not applicable to handsets, even though they are configured as IP Phones 2004 in the IP Line software. The wireless handsets are upgraded using a different mechanism without the help of the UMS subsystem.

usiLibTrace

The `usiLibTrace` utility can be used to monitor UNIStim messages from the wireless handsets by entering the alias IP address, not the wireless handset physical IP address.

```
-> usiLibTraceOn "192.168.10.200", 255, 255
value = 0 = 0x0
```

Determining alias IP addresses

When diagnosing network problems, (for example, to ping the wireless handset), it is useful to know the mapping between the alias IP addresses as displayed by various Call Server commands and the physical IP address of the wireless handset. There is no single command that provides this information; however, the administrator can determine it in two ways:

1. If the wireless handset IP address is statically configured, the administrator can look at the IP address of the wireless handset using the Admin menu, which is available when the wireless handset is powered on. For more information, see "WLAN Handset 2210/2211/2212" (page 91).

2. After the wireless handset is operating and in standby mode, the administrator can look at the User Preferences menu to find the alias IP address of the wireless handset. For more information, see Table 9 "Standby menu" (page 77).

Handset error messages

Table 25 "Handset error messages" (page 169) shows error messages that appear on the liquid crystal diode (LCD) display of the wireless handsets.

Table 25
Handset error messages

Short	Error code	Description	Action
Assert	Assert Errors	The phone detects possible network errors and cannot recover without configuration modification.	Verify the AP settings: data rates and fragmentation threshold. Use the Configuration Cradle to capture the assert error and then send the error to Nortel GNTS.
Code	Bad Code Type	The license management setting on phone is incorrect.	Adjust the license management setting.

Table 25
Handset error messages (cont'd.)

Short	Error code	Description	Action
DHCP	DHCP Error(s)	A problem communicating with DHCP server exists.	Troubleshoot the DHCP server configuration and the network.
DHCP	Can't Renew DHCP	The DHCP server is not responding to a lease renewal attempt.	Troubleshoot the DHCP server configuration and the network.
Duplicate	Duplicate ID	Two phones are configured with the same IP address.	Configure a valid static IP address for the phone. Check the DHCP configuration.
ESSID	Bad ESSID	The ESSID on the phone does not match the SSID on the AP.	Configure the correct ESSID statically on the phone.
Flash Config	Flash Config Error	The internal configuration of the phone is corrupt.	Restore the phone defaults and enter the configuration information.
No Net	No Net Found	The ESSID on the phone does not match the SSID on the AP.	Configure the correct ESSID statically on the phone.
No Net	No Net Access	The security settings on the phone do not match the security settings on the AP.	Check the AP security settings and configure the security settings for the phone to match.
PBX	No PBX	The phone is not communicating with the PBX.	Check the cross connects, bridge clips, punch downs on demarcation block, amphenol tail and PBX (see if the extension is built correctly).
SVP	No SVP Response	The phone cannot communicate with the WLAN IP Telephony Manager 2245.	Configure the Ethernet switch port and SVP to 100/full. Forward the DHCP option 151 to the IP of the SVP server. Verify the settings on the AP. Verify that there is no 2.4Ghz interference of any kind.

Table 25
Handset error messages (cont'd.)

Short	Error code	Description	Action
SVP	No SVP IP	No static IP entered into the phone for the WLAN IP Telephony Manager 2245.	Check for a valid IP in the phone. Check the license management configuration. Compare a working phone code to the nonworking phone code.
SW	No SW Found	No phone code is found on the TFTP server.	Point the TFTP software to the correct directory that contains valid code.
System	System Locked	The WLAN IP Telephony Manager 2245 is locked.	Dial in and verify that system is locked. Soft reset the SpectraLink infrastructure through the menu system.
TFTP	TFTP Error(s)	A failure occurred during the TFTP firmware update.	Check the TFTP software (SolarWinds is not compatible). Check the TFTP configuration. Forward option 66 in the DHCP scope, to the IP address of the TFTP server.

Before calling Nortel Technical Support

To facilitate the handling of the call, obtain the following information and have it available when placing a call to Nortel Technical Support:

- firmware versions on the wireless infrastructure, such as the APs

- pre-installation Site Survey, including typical network information and the wireless Site Survey information from the Site Survey tool such as the Nortel Site Survey Tool

- paper-based layout of AP placement

- a more refined Site Survey of the area having issues using the wireless handset in Site Survey mode

- list of the PBX and LTPS software versions, including a list of patches

- WLAN IP Telephony Manager 2245 and handset firmware versions

- WLAN IP Telephony Manager 2245 configuration menu screen captures

- any error messages displayed in the Error Status screen of the System Status Menu of the WLAN IP Telephony Manager 2245

- any error messages displayed on the handset display screen

- content of the Syslog Server (if using)

- log of the DHCP Server (if available), if using DHCP

For more information about troubleshooting WLAN Telephony installations, see *WLAN IP Telephony Installation and Commissioning (NN43001-504)* ()
.

Appendix
Factory Defaults

This appendix provides the factory default configuration that is restored if you select the Restore Defaults menu option.

Items with an asterisk (*) beside them are minimum requirements for functionality after selecting the Restore Defaults option:

- Configure the SSID to an available access point (AP).
- Configure the Reg Domain to 01.

Table 26
Factory default configuration for the WLAN Handset 6120/6140

Admin menu option	2nd level	3rd level	4th Level	Default
Phone Config	Language			English
	Telephony Protocol			Type 032
	Push-to-Talk			Enable
		Allowed Channels		[All]
		Priority Channels	Name Channel	Off
	Time Zone			GMT
	Daylight Saving			DST No Adjust
	Protected Spd Dial			[None set]
	Password			Enable
	Set Terminal Type			i2004
	Startup Keylock			Disable
	Speakerphone			Enable

Admin menu option	2nd level	3rd level	4th Level	Default
	OAI			Disable
Network Config	IP Addresses			Full DHCP
	SSID*			[None set]
	Security			None
		[If Security set]		
		WEP	Authentication	[If selected:] Open System
			WEP	Off
			Key Information	[None set]
			Rotation Secret	[None set]
		WPA2-PSK	Pre-Shared Key	[None set]
		WPA-PSK	Pre-Shared Key	[None set]
		Cisco FSR	Username Password	[None set]
	Reg. Domain*			[None set]
		[If set]		b and b/g mixed
		Transmit Power		30 mW <15dBm>
Diagnostics	Run Site Survey			[n/a]
	Diagnostics Mode			Disable
	Syslog Mode			Disabled
	Error Handling Mode			Restart on Error
Restore Defaults				

Index

U
Update software   35

V
Virtual Private Network (VPN)   23, 101
voice mail   148

W
Wi-Fi Protected Access (WPA)   23, 101
Wi-Fi Protected Access2 (WPA2)   23, 101
Wired Equivalent Privacy (WEP)   23, 99

Nortel Communication Server 1000

WLAN Handsets Fundamentals

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com
Sourced in Canada

NORTEL