

TD61-2471A



# WirelessIP 5000 Administrator Manual (v2.0.0)

---

Hitachi Cable, Ltd.

<b>1. ADMIN MENU .....</b>	<b>1</b>
<b>1.1 Network.....</b>	<b>2</b>
1.1.1 Network.....	2
1.1.1.1 Basic Info .....	3
1.1.1.2 WLAN.....	3
1.1.1.3 WEP .....	4
1.1.1.4 Authentication .....	5
1.1.1.5 TCP/IP.....	6
1.1.1.6 SIP Outb Proxy .....	6
1.1.1.7 NAT Traversal .....	7
1.1.1.8 IP DiffServ .....	8
1.1.1.9 Coder.....	9
1.1.1.10 Jitter Buf Size.....	9
1.1.2 SIP.....	10
1.1.2.1 User Account.....	10
1.1.2.2 Server Settings .....	11
1.1.2.3 Outbound Proxy .....	11
1.1.2.4 Expire .....	12
1.1.3 Network Reload .....	12
1.1.4 Certs Manager .....	13
1.1.5 Site Scan.....	16
1.1.6 Ping Test .....	18
1.1.6.1 Manual .....	18
1.1.6.2 1st Proxy .....	18
1.1.6.3 2nd Proxy .....	19
1.1.6.4 Gateway .....	20
1.1.6.5 TFTP server.....	20
<b>1.2 Password .....</b>	<b>21</b>
1.2.1 Admin Password .....	21
1.2.2 User Pwd Reset .....	22
<b>1.3 Upgrade.....</b>	<b>23</b>
1.3.1 Program.....	23
1.3.2 Configuration .....	24
1.3.3 Setup.....	25
1.3.3.1 TFTP server.....	26
1.3.3.2 Auto Upgrade.....	26
<b>1.4 Syslog.....</b>	<b>27</b>
<b>1.5 Web Server .....</b>	<b>28</b>
<b>1.6 Phone Reset.....</b>	<b>29</b>
<b>1.7 Statistics .....</b>	<b>29</b>
<b>2. 802.1X (EAP-TLS) CERTIFICATE INSTALLATION METHODS.....</b>	<b>30</b>
<b>2.1 Installation Procedures 802.1x Certificate.....</b>	<b>30</b>
2.1.1 Root Certificate .....	30
2.1.2 Private Certificate.....	31
<b>3. BOOT-ROM MENU.....</b>	<b>34</b>

<b>3.1</b>	<b>Opening the boot-ROM menu.....</b>	<b>34</b>
<b>3.2</b>	<b>Network settings .....</b>	<b>34</b>
3.2.1	Manual IP .....	35
3.2.2	DHCP .....	37
<b>3.3</b>	<b>WLAN settings .....</b>	<b>38</b>
3.3.1	SSID .....	38
3.3.2	WEP key .....	39
<b>3.4</b>	<b>Boot-ROM upgrade .....</b>	<b>41</b>
<b>3.5</b>	<b>Software upgrade .....</b>	<b>43</b>
<b>3.6</b>	<b>Closing the Boot-ROM menu .....</b>	<b>44</b>
<b>4.</b>	<b><u>TROUBLESHOOTING .....</u></b>	<b><u>45</u></b>
<b>4.1</b>	<b>General.....</b>	<b>45</b>

# 1. Admin menu

Reference: Please refer to the “WirelessIP 5000 User’s Manual” for information on the names of the various WirelessIP 5000 buttons.

Required settings are made when using the phone. Only Administrators are able to set items on the Admin menu.

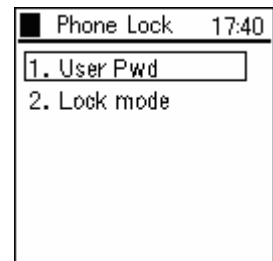
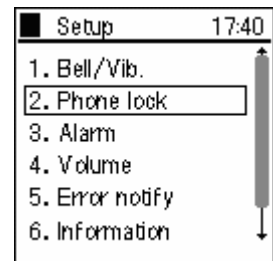
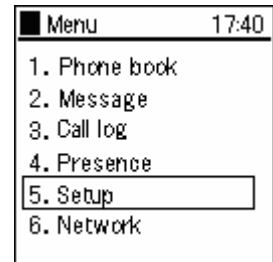
1 Press the **LeftSoft** key and select the menu.

Select "5. Setting".


From the Settings menu, select "2. Phone Lock".

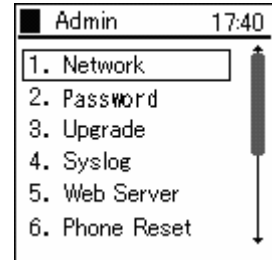
Select "1. KeyLock password".

When you select "1. KeyLock password", the system asks you for the current password. Enter the Admin password. The default value is 000000.



## 1.1 Network

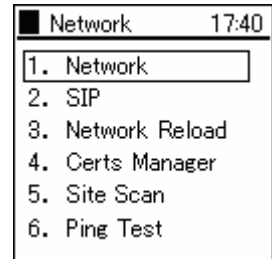
- 1 Either press the "1" on the number pad or select "1. Network", then press the  key.






### 1.1.1 Network

You can check the settings for the type of connected network as well as information about settings.

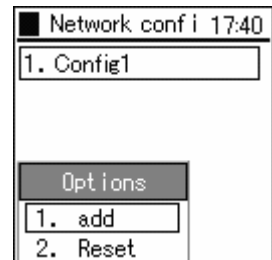
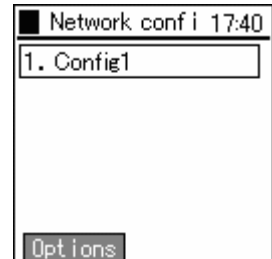
- 1 Select "1. Network" from the Network menu.



A list of the configurations is displayed.

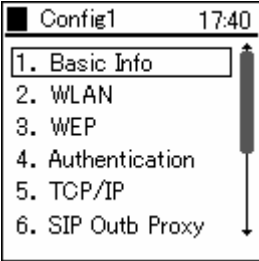

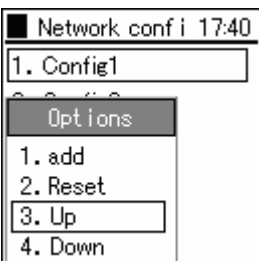
To add Config, press the  key to select the sub-menu, then select "1. Add" and press the  key. To reset Config, select "2. Reset" and press the  key.

At most five configurations can be stored.




### 1.1.1.1 Basic Info

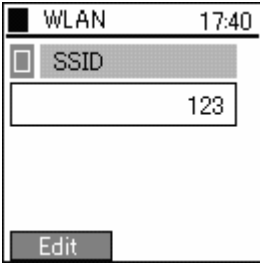
The WirelessIP 5000 can set the network for each AP (ESS-IS) (Dynamic Networking Binding function). You can set the priority of the various configurations here.

<p><b>1</b></p>	<p>Select "1. Basic Info" from the Config menu.</p>	 <p>The screenshot shows a menu titled 'Config1' with a time of 17:40. The menu items are: 1. Basic Info (highlighted), 2. WLAN, 3. WEP, 4. Authentication, 5. TCP/IP, and 6. SIP Outb Proxy.</p>
<p><b>2</b></p>	<p>Using the <b>LeftSoft</b> key, select "Edit" and "Join Method". Use the <b>◀▶</b> keys and select "AUTO" or "MANUAL".</p>	 <p>The screenshot shows the 'Basic Info' screen with a time of 17:40. It has fields for 'Name' (Config1) and 'Join Method' (AUTO). There is an 'Edit' button at the bottom.</p>
<p><b>3</b></p>	<p>When selecting "MANUAL", priority sequence can be changed by selecting "3. Up" or "4. Down" from the sub-menu on the Config list screen.</p>	 <p>The screenshot shows the 'Network config i' screen with a time of 17:40. It has a list of configurations: 1. Config1, 2. Config2, 3. Config3, 4. Config4. An 'Options' sub-menu is open, showing: 1. add, 2. Reset, 3. Up (highlighted), and 4. Down.</p>

### 1.1.1.2 WLAN

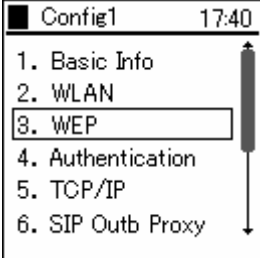
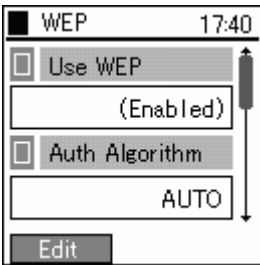
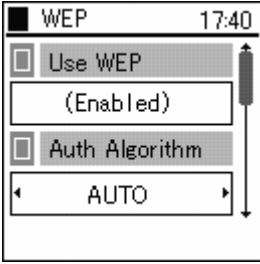
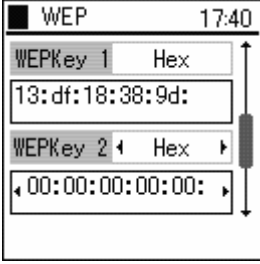
You can set the configuration for connection to wireless LAN, and create the SSID which identifies an access point.

<p><b>1</b></p>	<p>Select "2. WLAN" from the Config menu.</p>	 <p>The screenshot shows a menu titled 'Config1' with a time of 17:40. The menu items are: 1. Basic Info, 2. WLAN (highlighted), 3. WEP, 4. Authentication, 5. TCP/IP, and 6. SIP Outb Proxy.</p>
-----------------	---	--

<b>2</b>	<p>Displays SSID.</p> <p>When blank, the connection is made to the access point where the radio waves are the strongest.</p>	
----------	--	---

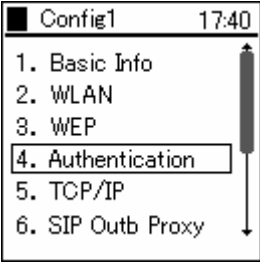

### 1.1.1.3 WEP

WEP key is used for authentication and encryption. WirelessIP 5000 supports 64/128/256 bit WEP key.

<b>1</b>	<p>Select "3. WEP" from the Config menu.</p>													
<b>2</b>	<p>Using the <b>LeftSoft</b> key, select "edit."</p> <p>For "Use WEP" use the <b>◀ ▶</b> keys to select "(Enable)" or "(Disable)".</p>													
<b>3</b>	<p>For "Auth Algorithm" use the <b>◀ ▶</b> keys to select either "AUTO", "Open System", or "Shared Key".</p>													
<b>4</b>	<p>Enter the WEP key in either hexadecimal or Asc format.</p> <table border="1" style="margin-left: 20px;"> <thead> <tr style="background-color: #e0ffff;"> <th>Bit</th> <th>Hex</th> <th>Asc</th> </tr> </thead> <tbody> <tr> <td>256 bit</td> <td>232 bit</td> <td>29 characters</td> </tr> <tr> <td>128 bit</td> <td>104 bit</td> <td>13 characters</td> </tr> <tr> <td>64 bit</td> <td>40 bit</td> <td>5 characters</td> </tr> </tbody> </table>	Bit	Hex	Asc	256 bit	232 bit	29 characters	128 bit	104 bit	13 characters	64 bit	40 bit	5 characters	
Bit	Hex	Asc												
256 bit	232 bit	29 characters												
128 bit	104 bit	13 characters												
64 bit	40 bit	5 characters												

### 1.1.1.4 Authentication


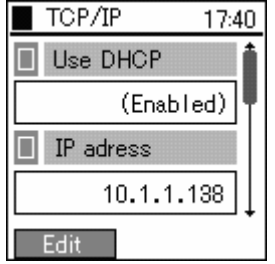
Authentication related settings

<p><b>1</b></p>	<p>Select “4. Authentication” from the Config menu.</p>	 <p>The screenshot shows a menu titled 'Config1' with a time of 17:40. The menu items are: 1. Basic Info, 2. WLAN, 3. WEP, 4. Authentication (highlighted with a box), 5. TCP/IP, and 6. SIP Outb Proxy. A vertical scrollbar is on the right side of the menu.</p>
<p><b>2</b></p>	<p>Using the <b>LeftSoft</b> key, select “edit.”</p> <p>For “Mode” use the <b>Left</b> <b>Right</b> keys and select “8021X-MD5”, 8021X-TLS”, 8021X-PEAP”, “8021X-TTLS”, “WEB” or “None” settings.</p>	 <p>The screenshot shows the 'Authenticatio' screen with a time of 17:40. It has two sections: 'Mode' with a dropdown menu currently showing 'None', and 'Username' with an empty text input field. An 'Edit' button is located at the bottom of the screen.</p>



### 1.1.1.5 TCP/IP


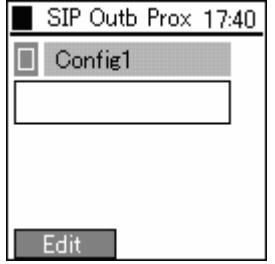
You can set the IP address, subnet mask, default gateway, and DNS.

<p><b>1</b></p>	<p>Select “ 5. TCP/IP” from the Config menu.</p>	
<p><b>2</b></p>	<p>TCP/IP Information displays: Use DHCP, IP Address, Netmask, Gateway, DNS1, and DNS2.</p> <p>If you want to set the IP address manually, deactivate DHCP. Enter the appropriate DNS (primary and secondary).</p>	

### 1.1.1.6 SIP Outb Proxy



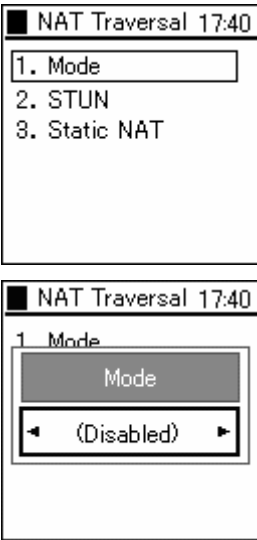
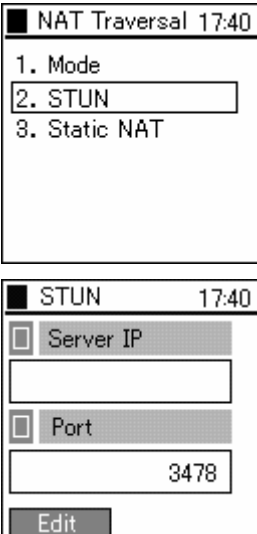
You can set the Outbound Proxy server settings.

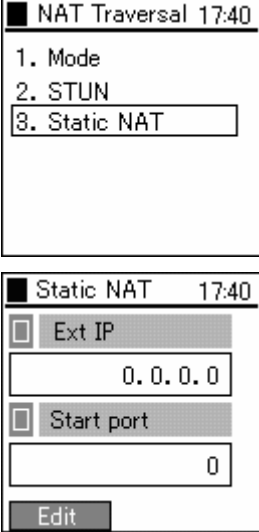
Depending on the system configuration, however, it sometimes is unnecessary to set it.

<p><b>1</b></p>	<p>Select “ 6. SIP Outb Proxy,” from the Config menu.</p>	
<p><b>2</b></p>	<p>A prompt will appear to enter the IP address for the SIP Outbound Proxy. Enter the IP address.</p>	

### 1.1.1.7 NAT Traversal



The WirelessIP 5000 supports both UPnP and StaticNAT, and it is possible to call from within the LAN to outside the LAN through NATBox. When doing so, you can set the UPnP and StaticNAT to match the settings of the NATBox being connected to.

<p><b>1</b></p>	<p>Select "7. NAT Traversal" from the Config menu.</p>	 <p>The screenshot shows a menu titled 'Config1' with a time of 17:40. The menu items are: 2. WLAN, 3. WEP, 4. Authentication, 5. TCP/IP, 6. SIP Outb Proxy, and 7. NAT Traversal. The '7. NAT Traversal' item is highlighted with a white background and a black border.</p>
<p><b>2</b></p>	<p>Select "1. Mode" from the NAT Traversal menu.</p> <p>Select SNAT, UPnP, STUN, or deactivate.</p> <p>When you press the  key, the selected value is applied.</p>	 <p>The top screenshot shows a menu titled 'NAT Traversal 17:40' with three items: 1. Mode, 2. STUN, and 3. Static NAT. '1. Mode' is selected. The bottom screenshot shows the '1 Mode' screen with a 'Mode' button and a selection box containing '(Disabled)'. There are left and right arrow buttons on either side of the selection box.</p>
<p><b>3</b></p>	<p>Select "2. STUN" from the NAT Traversal menu.</p> <p>Enter the Server IP and Port values.</p>	 <p>The top screenshot shows a menu titled 'NAT Traversal 17:40' with three items: 1. Mode, 2. STUN, and 3. Static NAT. '2. STUN' is selected. The bottom screenshot shows the 'STUN 17:40' configuration screen. It has a 'Server IP' field with a cursor, a 'Port' field with the value '3478', and an 'Edit' button at the bottom.</p>

4	<p>Select "3. Static NAT" from the NAT Traversal menu.</p>	 <p>The screenshot shows two windows. The top window is titled "NAT Traversal 17:40" and contains a list of options: "1. Mode", "2. STUN", and "3. Static NAT". The "3. Static NAT" option is selected and highlighted. The bottom window is titled "Static NAT 17:40" and contains two input fields: "Ext IP" with the value "0.0.0.0" and "Start port" with the value "0". There is also an "Edit" button at the bottom.</p>
<p>Enter the Ext IP and Start Port values.</p>		


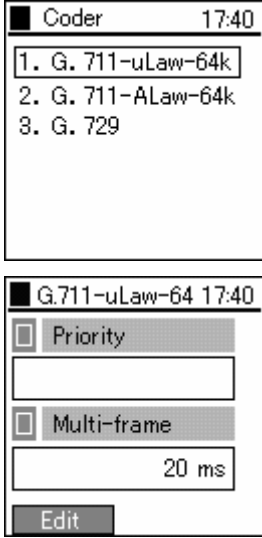
### 1.1.1.8 IP DiffServ

IP Diffserv sets the priority control settings.

1	<p>Select "8. IP DiffServ" from the Config menu.</p>	 <p>The screenshot shows a window titled "Config1 17:40" with a list of menu items: "3. WEP", "4. Authentication", "5. TCP/IP", "6. SIP Outb Proxy", "7. NAT Traversal", and "8. IP DiffServ". The "8. IP DiffServ" item is selected and highlighted.</p>
2	<p>Enter the value for the "Signal DSCP" and "Voice DSCP" setting using hexadecimal numbers.                  Note!!! Enter a value between the 0x00 and 0x3F.</p>	 <p>The screenshot shows a window titled "IP DiffServ 17:40" with two input fields: "Signal DSCP" with the value "0x0" and "Voice DSCP" with the value "0x0". There is also an "Edit" button at the bottom.</p>



### 1.1.1.9 Coder

You can set the CODEC (priority and transmission interval) to match the system configuration.

<p><b>1</b></p>	<p>Select “9. Coder” from the Config menu.</p>	
<p><b>2</b></p>	<p>Select the appropriate item from the Coder menu.</p> <p>Set Priority (1-3) and Multi-frame (20ms-40ms).</p>	


### 1.1.1.10 Jitter Buf Size

Taking into consideration your system configuration, you can optionally set the jitter buffer size.

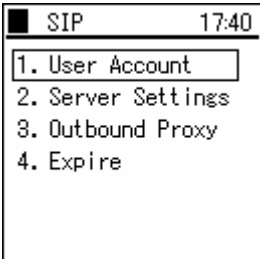
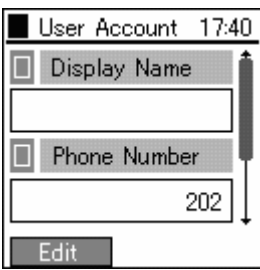
<p><b>1</b></p>	<p>Select “0. Jitter Buf size” from the Config menu.</p>	
<p><b>2</b></p>	<p>Configure Jitter Buf Size.</p>	

## 1.1.2 SIP

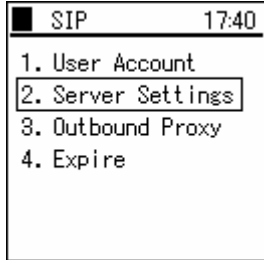
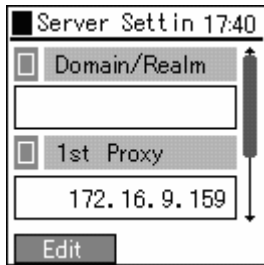
You can set items related to telephony. SIP configures call control.

<b>1</b>	Select "2. SIP" from the Network menu.	 <p>The screenshot shows a window titled "Network" with a timestamp of 17:40. It contains a list of menu items: 1. Network, 2. SIP (highlighted with a selection box), 3. Network Reload, 4. Certs Manager, 5. Site Scan, and 6. Ping Test.</p>
----------	--	--

### 1.1.2.1 User Account

<b>1</b>	Select "1. User Account" from the SIP menu.	 <p>The screenshot shows a window titled "SIP" with a timestamp of 17:40. It contains a list of menu items: 1. User Account (highlighted with a selection box), 2. Server Settings, 3. Outbound Proxy, and 4. Expire.</p>
<b>2</b>	<p>User Account Information displays: Display Name, Phone Number, User ID, and URL Scheme</p> <p>Although the Phone Number is required, enter the Display Name, User ID, and URL Scheme as deemed necessary.</p>	 <p>The screenshot shows a window titled "User Account" with a timestamp of 17:40. It contains two input fields: "Display Name" and "Phone Number". The "Phone Number" field contains the value "202". There is an "Edit" button at the bottom.</p>

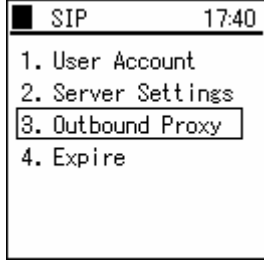
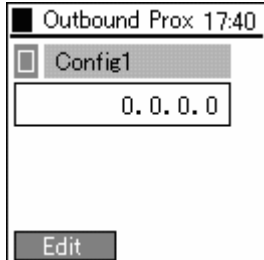
### 1.1.2.2 Server Settings

<p><b>1</b></p>	<p>Select "2. Server Settings" from the SIP menu.</p>	 <p>The screenshot shows a menu titled 'SIP' with a timestamp of '17:40'. The menu items are: 1. User Account, 2. Server Settings (highlighted with a box), 3. Outbound Proxy, and 4. Expire.</p>
<p><b>2</b></p>	<p>Server Settings Information displays: Domain/Realm, 1st Proxy, 1st Registrar, 2nd Proxy, and 2nd Registrar.</p>	 <p>The screenshot shows a form titled 'Server Settings' with a timestamp of '17:40'. It contains several input fields: 'Domain/Realm' (empty), '1st Proxy' (containing '172.16.9.159'), and '1st Registrar' (empty). There is an 'Edit' button at the bottom.</p>

### 1.1.2.3 Outbound Proxy

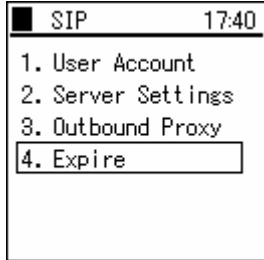
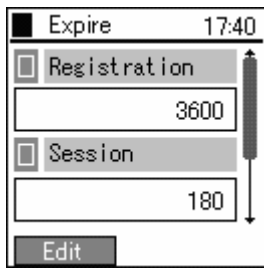
You can set the Outbound Proxy server settings.

Depending on the system configuration, however, it sometimes is unnecessary to set it.

<p><b>1</b></p>	<p>Select "3. Outbound Proxy" from the SIP menu.</p>	 <p>The screenshot shows a menu titled 'SIP' with a timestamp of '17:40'. The menu items are: 1. User Account, 2. Server Settings, 3. Outbound Proxy (highlighted with a box), and 4. Expire.</p>
<p><b>2</b></p>	<p>Enter the Outbound Proxy's IP Address.</p>	 <p>The screenshot shows a form titled 'Outbound Proxy' with a timestamp of '17:40'. It contains a 'Config1' section with an input field for the IP address, which is set to '0.0.0.0'. There is an 'Edit' button at the bottom.</p>

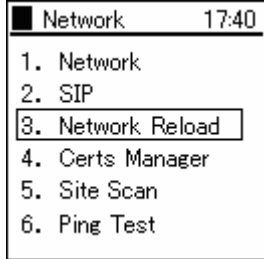



### 1.1.2.4 Expire

'Regist Expire Time', 'Session Timer', and 'Presence Expire Timer' can be set.

<p><b>1</b></p>	<p>Select "4. Expires" from the SIP menu.</p>	 <p>The screenshot shows a menu titled 'SIP' with a timestamp of 17:40. The menu items are: 1. User Account, 2. Server Settings, 3. Outbound Proxy, and 4. Expire. The '4. Expire' item is highlighted with a white background.</p>
<p><b>2</b></p>	<p>Set Regist Expire, Session Expire, and Presence Expire.</p>	 <p>The screenshot shows the 'Expire' settings screen with a timestamp of 17:40. It has two sections: 'Registration' with a value of 3600 and 'Session' with a value of 180. There is an 'Edit' button at the bottom.</p>

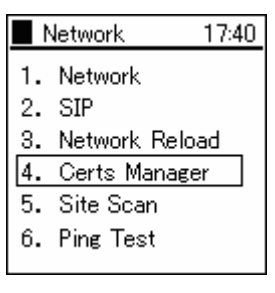
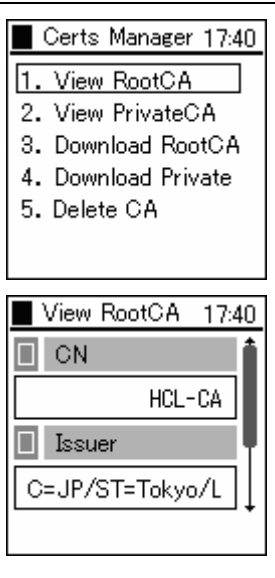
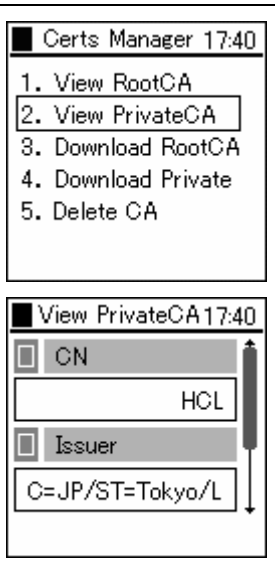
### 1.1.3 Network Reload

When taking various actions such as changing settings, adding and deleting configurations, you can manually perform a reload.

<p><b>1</b></p>	<p>Select "3. Network Reload" from the Network menu.</p>	 <p>The screenshot shows a menu titled 'Network' with a timestamp of 17:40. The menu items are: 1. Network, 2. SIP, 3. Network Reload, 4. Certs Manager, 5. Site Scan, and 6. Ping Test. The '3. Network Reload' item is highlighted with a white background.</p>
<p><b>2</b></p>	<p>Use the   keys and select "Auto" or "Config".</p>	 <p>The screenshot shows the 'Network reload' dialog with a timestamp of 17:40. It has a title bar 'Network reload' and a selection box containing 'AUTO' with left and right arrow keys on either side. Below the dialog, the menu item '6. Ping Test' is visible.</p>

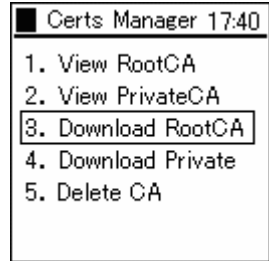
### 1.1.4 Certs Manager

When running 802.1x (EAP-TLS, PEAP, TTLS), root certificate and private certificate information can be imported and checked.

<p><b>1</b></p>	<p>Select "4. Certs Manager" from the Network menu.</p>	 <p>Network 17:40</p> <ol style="list-style-type: none"> <li>1. Network</li> <li>2. SIP</li> <li>3. Network Reload</li> <li>4. Certs Manager</li> <li>5. Site Scan</li> <li>6. Ping Test</li> </ol>
<p><b>2</b></p>	<p>Select "1. View RootCA" from the Certs Manager menu.</p> <p>View RootCA Information displays: CN, Issuer, Not Before, Not After, Serial, Signature, Subject, Version, and SPubKeyAlgorithm.</p>	 <p>Certs Manager 17:40</p> <ol style="list-style-type: none"> <li>1. View RootCA</li> <li>2. View PrivateCA</li> <li>3. Download RootCA</li> <li>4. Download Private</li> <li>5. Delete CA</li> </ol> <p>View RootCA 17:40</p> <p>CN: HCL-CA</p> <p>Issuer: C=JP/ST=Tokyo/L</p>
<p><b>3</b></p>	<p>Select "2. View PrivateCA" from the Certs Manager menu.</p> <p>View PrivateCA Information displays: CN, Issuer, Not Before, Not After, Serial, Signature, Subject, Version, and SPubKeyAlgorithm.</p>	 <p>Certs Manager 17:40</p> <ol style="list-style-type: none"> <li>1. View RootCA</li> <li>2. View PrivateCA</li> <li>3. Download RootCA</li> <li>4. Download Private</li> <li>5. Delete CA</li> </ol> <p>View PrivateCA 17:40</p> <p>CN: HCL</p> <p>Issuer: C=JP/ST=Tokyo/L</p>





4 Select "3. Download RootCA" from the Certs Manager menu.




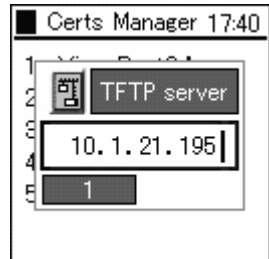
A warning message is displayed.



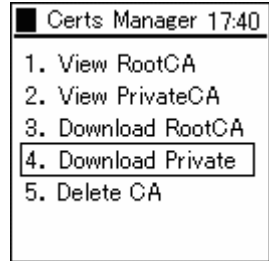
Use the   keys and select "Yes" or "No".



If "Yes" is selected, the IP Address of the download TFTP server will be asked to be entered. Download starts after entering the IP address and pressing the  key.



**5** Select "4. Download PrivateCA" from the Certs Manager menu.



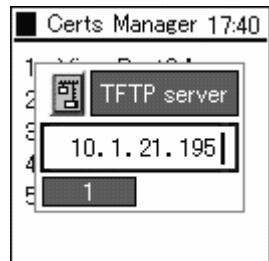
If the PrivateCA is not downloaded, a warning message as listed on the right will display.



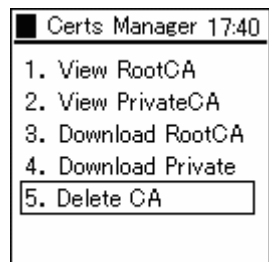
Use the keys and select "Yes" or "No".



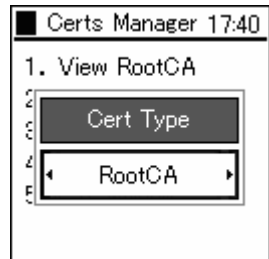
If "Yes" is selected, the IP Address of the download TFTP server will be asked to be entered. Download starts after entering the IP address and pressing the key.



**6** Select "5. Delete CA" from the Certs Manager menu.

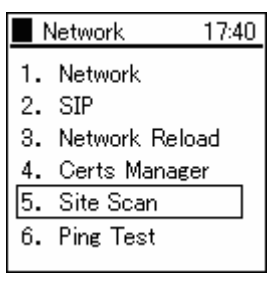

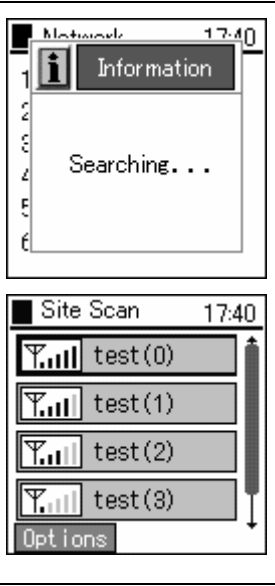
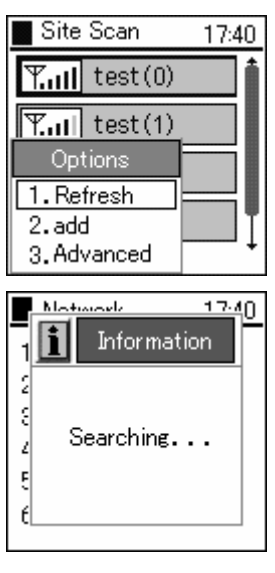


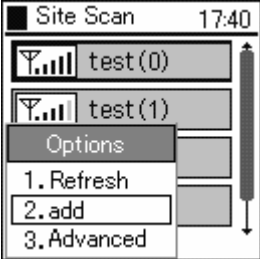

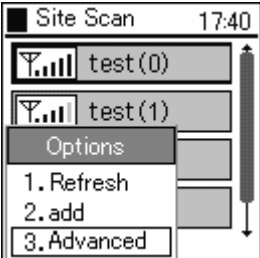
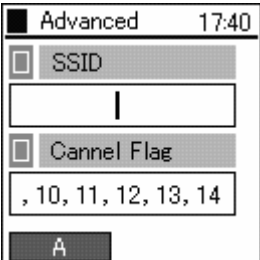
Use the keys and select "RootCA", "PrivateCA", "Delete All".



## 1.1.5 Site Scan

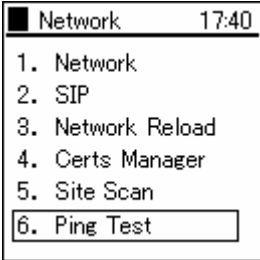
Information on signals detected can be displayed.

<p><b>1</b></p>	<p>Select "5. Site Scan" from the Network menu.</p>	 <p>A screenshot of a menu titled "Network" with a timestamp of 17:40. The menu items are: 1. Network, 2. SIP, 3. Network Reload, 4. Certs Manager, 5. Site Scan (highlighted with a white box), and 6. Ping Test.</p>
<p><b>2</b></p>	<p>A message is displayed during the search.</p> <p>The SSID for access points that were detected during the scan are displayed. If you want to see detailed information, select the SSID and press the .</p> <p>Note!!!) At most 10 access points can be displayed.</p>	 <p>Two screenshots are shown. The top one is a dialog box titled "Information" with a timestamp of 17:40, containing the text "Searching...". The bottom one is the "Site Scan" screen with a timestamp of 17:40, showing a list of four items: test(0), test(1), test(2), and test(3), each with a signal strength indicator. Below the list is an "Options" button.</p>
<p><b>3</b></p>	<p>To refresh the Site Scan Information, press the <b>LeftSoft</b> key to select the sub-menu, then select "1. Refresh".</p> <p>Site Scan reopens.</p>	 <p>Two screenshots are shown. The top one is the "Site Scan" sub-menu with a timestamp of 17:40, showing options: 1. Refresh (highlighted), 2. add, and 3. Advanced. The bottom one is the "Information" dialog with a timestamp of 17:40, containing the text "Searching...".</p>

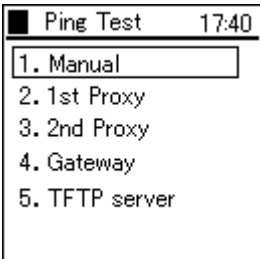

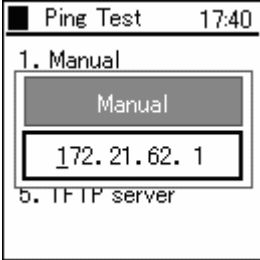
<p><b>4</b></p>	<p>Refer to the list of SSID's for detected access points, and select the SSID you would like to connect to (by moving the cursor). Select the submenu by pressing the <b>LeftSoft</b> key and choose "2.Addition".</p> <p>Follow the wizard as in the screen displayed to the right, and each of the network settings can be performed in order.</p> <p>For setting each item, refer to section 1.1.1.1 Basic Info (page 3).</p>	 
<p><b>5</b></p>	<p>When probing for particular SSIDs or Channels, press the <b>LeftSoft</b> key to select the submenu, then choose "3. Advanced".</p> <p>For example, when you enter the SSID displayed by the previously mentioned Scan in the SSID box on the right, and press <b>⊗</b>, a scan for that SSID commences and the results are displayed.</p> <p>Also, in the Channel Flag box, if you enter the number of the channel you would like to confirm and press the <b>⊗</b> key, a scan for that channel commences and the results are displayed.</p>	 

## 1.1.6 Ping Test

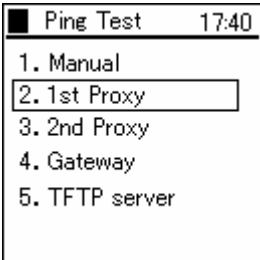
You can confirm a signal by using the PING command.


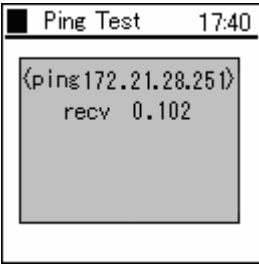
<b>1</b>	Select "2. Ping Test" from the Network menu.	 <p>Network 17:40</p> <ul style="list-style-type: none"> <li>1. Network</li> <li>2. SIP</li> <li>3. Network Reload</li> <li>4. Certs Manager</li> <li>5. Site Scan</li> <li>6. Ping Test</li> </ul>
----------	--	--

### 1.1.6.1 Manual

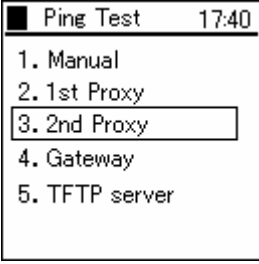

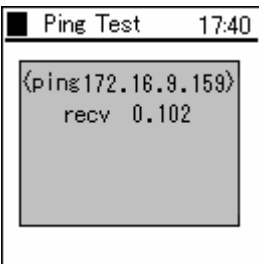
<b>1</b>	Select "1. Manual" from the Ping Test menu.	 <p>Ping Test 17:40</p> <ul style="list-style-type: none"> <li>1. Manual</li> <li>2. 1st Proxy</li> <li>3. 2nd Proxy</li> <li>4. Gateway</li> <li>5. TFTP server</li> </ul>
<b>2</b>	Enter the IP address for Ping and press the  key to start the Ping.	 <p>Ping Test 17:40</p> <ul style="list-style-type: none"> <li>1. Manual</li> <li style="background-color: #cccccc;">Manual</li> <li>172.21.62.1</li> <li>5. TFTP server</li> </ul>

### 1.1.6.2 1st Proxy


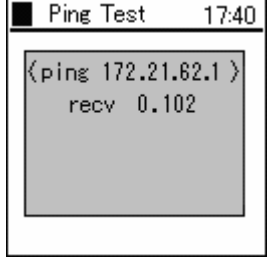
<b>1</b>	Select "2. 1st Proxy" from the Ping Test menu.	 <p>Ping Test 17:40</p> <ul style="list-style-type: none"> <li>1. Manual</li> <li>2. 1st Proxy</li> <li>3. 2nd Proxy</li> <li>4. Gateway</li> <li>5. TFTP server</li> </ul>
----------	--	--

<p><b>2</b></p>	<p>If the 1st Proxy is not configured, the message in the right diagram displays.</p>	 <p>The screenshot shows a window titled 'Ping Test' with a timestamp of 17:40. It features an 'Information' icon and the text 'No address set'.</p>
<p><b>3</b></p>		 <p>The screenshot shows a window titled 'Ping Test' with a timestamp of 17:40. It displays the output of a ping command: '&lt;ping 172.21.28.251&gt;' and 'rcv 0.102'.</p>



### 1.1.6.3 2nd Proxy

<p><b>1</b></p>	<p>Select "3. 2nd Proxy" from the Ping Test menu.</p>	 <p>The screenshot shows a window titled 'Ping Test' with a timestamp of 17:40. It displays a menu with five options: '1. Manual', '2. 1st Proxy', '3. 2nd Proxy' (which is highlighted with a selection box), '4. Gateway', and '5. TFTP server'.</p>
<p><b>2</b></p>	<p>If the 2nd Proxy is not configured, the message in the right diagram displays.</p>	 <p>The screenshot shows a window titled 'Ping Test' with a timestamp of 17:40. It features an 'Information' icon and the text 'No address set'.</p>
<p><b>3</b></p>		 <p>The screenshot shows a window titled 'Ping Test' with a timestamp of 17:40. It displays the output of a ping command: '&lt;ping 172.16.9.159&gt;' and 'rcv 0.102'.</p>


### 1.1.6.4 Gateway

<p><b>1</b></p>	<p>Select "4. Gateway" from the Ping Test menu.</p>	 <p>The screenshot shows a window titled "Ping Test" with a timestamp of 17:40. It contains a list of options: 1. Manual, 2. 1st Proxy, 3. 2nd Proxy, 4. Gateway (highlighted with a white box), and 5. TFTP server.</p>
<p><b>2</b></p>		 <p>The screenshot shows the same "Ping Test" window with the results of a ping to 172.21.62.1. The text displayed is: &lt;ping 172.21.62.1 &gt; recv 0.102.</p>




### 1.1.6.5 TFTP server

<p><b>1</b></p>	<p>Select "5. TFTP Server" from the Ping Test menu.</p>	 <p>The screenshot shows the "Ping Test" window with the timestamp 17:40. The list of options is: 1. Manual, 2. 1st Proxy, 3. 2nd Proxy, 4. Gateway, and 5. TFTP server (highlighted with a white box).</p>
<p><b>2</b></p>		 <p>The screenshot shows the "Ping Test" window with the results of a ping to 10.1.21.195. The text displayed is: &lt;ping10. 1. 21.195&gt; recv 0.102.</p>



## 1.2 Password

<p><b>1</b></p>	<p>Select "2. Password" from the Admin menu.</p>	 <p>The screenshot shows a terminal window titled 'Admin' with a timestamp of 17:40. A list of menu items is displayed: 1. Network, 2. Password, 3. Upgrade, 4. Syslog, 5. Web Server, and 6. Phone Reset. The '2. Password' option is highlighted with a rectangular selection box.</p>
-----------------	--	---





### 1.2.1 Admin Password

<p><b>1</b></p>	<p>Select "1. Admin Password" from the Password menu.</p>	 <p>The screenshot shows a terminal window titled 'Password' with a timestamp of 17:40. A list of menu items is displayed: 1. Admin Pwd and 2. User Pwd Reset. The '1. Admin Pwd' option is highlighted with a rectangular selection box.</p>
<p><b>2</b></p>	<p>When you select "1. Admin password", the system asks for the current password. Please enter the correct password. The default value is 000000.</p>	 <p>The screenshot shows the 'Password' terminal window at 17:40. It displays '1. Admin Pwd' at the top. Below it is a label 'Old password' next to a key icon, followed by a rectangular input field containing a vertical cursor.</p>
<p><b>3</b></p>	<p>When you input the correct password, the system asks you to input the new password.</p>	 <p>The screenshot shows the 'Password' terminal window at 17:40. It displays '1. Admin Pwd' at the top. Below it is a label 'New password' next to a key icon, followed by a rectangular input field containing a vertical cursor.</p>



<p><b>4</b></p>	<p>For verification, the system asks you to input the new password a second time.</p>	 <p>The screenshot shows a terminal window titled 'Password' with the time '17:40'. It displays a menu with '1. Admin Pwd' and '2. Retype Pwd'. A cursor is positioned at the start of the 'Retype Pwd' option.</p>
<p><b>5</b></p>	<p>When you input the password, a screen like that on the right is displayed for a few seconds.</p>	 <p>The screenshot shows a terminal window titled 'Password' with the time '17:40'. It displays a menu with '1. Information' and '2. Changed'. A cursor is positioned at the start of the 'Information' option.</p>

### 1.2.2 User Pwd Reset

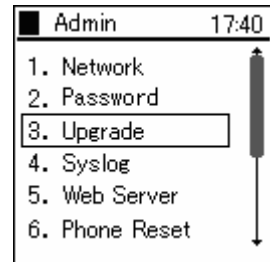
<p><b>1</b></p>	<p>Select "2. User Pwd Reset" from the Password menu.</p>	 <p>The screenshot shows a terminal window titled 'Password' with the time '17:40'. It displays a menu with '1. Admin Pwd' and '2. User Pwd Reset'. A cursor is positioned at the start of the 'User Pwd Reset' option.</p>
<p><b>2</b></p>	<p>With the   keys select either "Yes" or "No".</p>	 <p>The screenshot shows a terminal window titled 'Password' with the time '17:40'. It displays a 'Warning' dialog box with a question mark icon. The text inside the dialog box reads: 'Are you sure you want to reset user password?'. At the bottom of the dialog box, there are two buttons: 'Yes' and 'No'.</p>

## 1.3 Upgrade

You can upgrade the software and configuration.

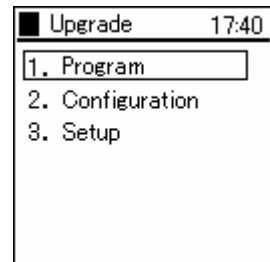
Warning: If there are major differences in the versions (i.e. Ver 1.x.x and Ver 2.x.x), the details of the old settings are not carried over.

- 1 Select "3. Upgrade" from the Admin menu.





### 1.3.1 Program

- 1 Select "1. Program" from the Upgrade menu.






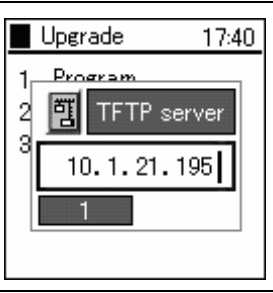



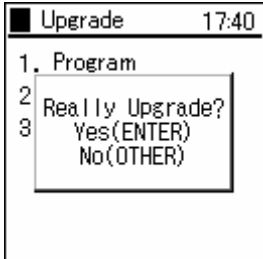


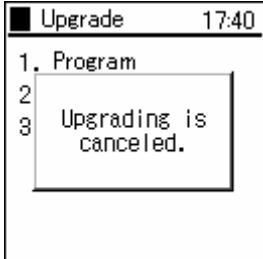
- 2 A warning message is displayed.

Use the   keys and select "Yes" or "No".  
(Refer to 1.3.2 Configuration)




### 1.3.2 Configuration



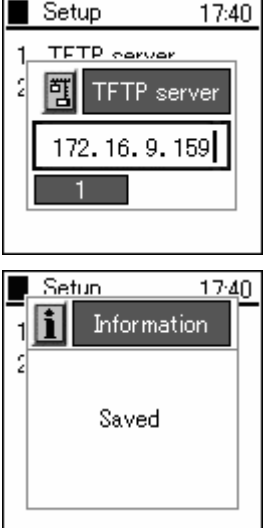
<p><b>1</b></p>	<p>Select “2. Configuration” from the Upgrade menu.</p> <p>When “2. Configuration” is selected, only the configuration is upgraded.</p>	 <p>The screenshot shows a menu titled 'Upgrade' with a time of 17:40. It lists three options: '1. Program', '2. Configuration' (which is highlighted with a rectangular box), and '3. Setup'.</p>
<p><b>2</b></p>	<p>A warning message is displayed.</p>	 <p>The screenshot shows a 'Warning' dialog box with a warning icon (exclamation mark). The text inside reads: 'Warning', 'Incorrect upgrading may cause phone to malfunction'.</p>
<p><b>3</b></p>	<p>Use the   and select “Yes” or “No”.</p>	 <p>The screenshot shows a 'Warning' dialog box with a question mark icon. The text inside reads: 'Warning', 'Upgrade Configuration?', 'Yes', and 'No'.</p>
<p><b>4</b></p>	<p>If “Yes” is selected, enter the IP address of the TFTP server using the dial pad and LeftSoft key.</p>	 <p>The screenshot shows the 'Upgrade' menu with '2. TFTP server' selected. Below it, the IP address '10.1.21.195' is entered in a text field. A '1' is shown in a small box at the bottom.</p>
<p><b>5</b></p>	<p>A download screen, like the one to the right, will appear.</p>	 <p>The screenshot shows the 'Upgrade' menu with '2. Downloading...' selected. Below it, the text 'ipphone.bz' and '205312' is displayed.</p>

<b>6</b>	After downloading, an upgrade confirmation screen will appear.	 <p>The screenshot shows a terminal window titled 'Upgrade' with the time '17:40'. It displays a menu with three options: '1. Program', '2. Really Upgrade?', and '3'. A box highlights the 'Really Upgrade?' option, which has sub-options 'Yes(ENTER)' and 'No(OTHER)'.</p>
<b>7</b>	Press the  key, and the program upgrade is performed  If you press any other button, the upgrade will be cancelled.	  <p>The first screenshot shows the 'Upgrade' terminal window with 'APP Upgrade is complete.' displayed. The second screenshot shows the 'Upgrade' terminal window with 'Upgrading is canceled.' displayed.</p>

### 1.3.3 Setup

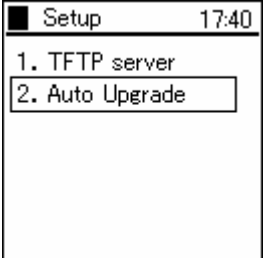
<b>1</b>	Select "3. Setup" from the Upgrade menu.	 <p>The screenshot shows a terminal window titled 'Upgrade' with the time '17:40'. It displays a menu with three options: '1. Program', '2. Configuration', and '3. Setup'. The '3. Setup' option is highlighted with a box.</p>
----------	--	---


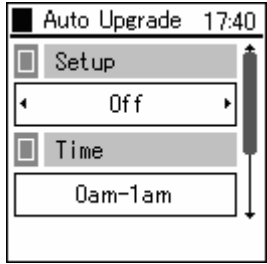
### 1.3.3.1 TFTP server

<p><b>1</b></p>	<p>Select “1. TFTP server” from the Upgrade menu.</p>	
<p><b>2</b></p>	<p>When the input box appears, enter the TFTP server IP address.</p> <p>Save the setting by pressing the  key</p>	

### 1.3.3.2 Auto Upgrade



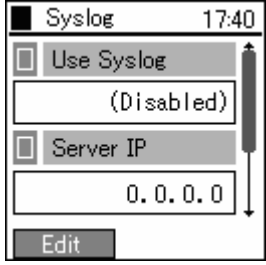
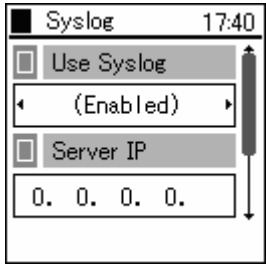
The firmware automatically upgrades randomly during the specified time intervals.



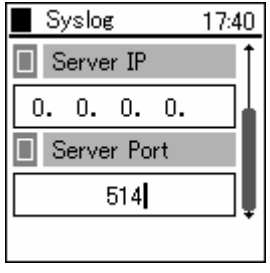
<p><b>1</b></p>	<p>Select “2. Auto Upgrade” from the Setup menu.</p>	
-----------------	--	---

<p><b>2</b> Select the settings using the  Key.</p> <p>The time can be set (0am-1am - 11pm-0am).</p> <p>The frequency can be set (Sun/Mon/Tue/Wed/ Thu/Fri/Sat/Daily)</p> <p>The settings can be configured (Enable/Disable)</p> <p>Warning!: When “1. Invalid” is selected in user.ini, the auto upgrade function will not operate even if the menu settings are configured to “Use”.</p> <p>Warning!: When a terminal version is not configured in loadrun.ini, upgrade is conducted automatically.</p> <p>Warning!: When the set time exceeds the WirelessIP time, the executed timing will be the following frequency.</p>	
---	---

## 1.4 Syslog






The WirelessIP 5000 can send information on the system log containing items such as events that occurred on the system and information to the Syslog server. Settings can be entered to match Syslog server configuration.

<p><b>1</b> Select “4. Syslog” from the Admin menu.</p>	
<p><b>2</b> Using the  key, select “edit.”</p>	
<p><b>3</b> After setting User-Syslog to “Enable,” the screen will look like the figure to the right and the Server IP can be entered.</p>	





- |  |   |
|--|---|
| <p><b>4</b> Using the  key scroll to the bottom of the screen and input an appropriate Server IP and Server Port.</p> <p>Apply this by pressing the  key</p> |  |
|--|---|

## 1.5 Web Server




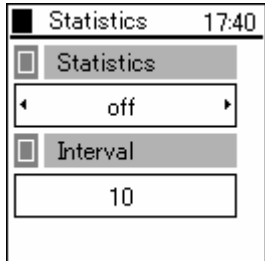
It is possible to configure and access the boot-ROM and software from the network using a Web browser. You can turn the Web Server function on/off from here.

- |  |   |
|--|---|
| <p><b>1</b> Select “5. Web Server” from the Admin menu.</p>  |   |
| <p><b>2</b> Using the   keys the web server can be turned on or off.</p> <p>Apply by pressing the  key.</p> |  |

## 1.6 Phone Reset

<p><b>1</b></p>	<p>Select “6. Phone Reset” from the Admin menu.</p>	 <p>The screenshot shows a terminal window titled 'Admin' with the time '17:40'. A list of menu items is displayed: 1. Network, 2. Password, 3. Upgrade, 4. Syslog, 5. Web Server, and 6. Phone Reset. The '6. Phone Reset' option is highlighted with a white background and a black border.</p>
<p><b>2</b></p>	<p>Use the  and  select “Yes” or “No”. Select “Yes” to clear setting details.</p>	 <p>The screenshot shows a terminal window titled 'Admin' with the time '17:40'. A warning dialog box is displayed with a question mark icon and the text: 'Warning', 'This will return the factory default.', and 'Are you sure?'. At the bottom of the dialog are two buttons: 'Yes' and 'No'.</p>

## 1.7 Statistics

<p><b>1</b></p>	<p>Select “2. SIP” from the Admin menu.</p>	 <p>The screenshot shows a terminal window titled 'Admin' with the time '17:40'. A list of menu items is displayed: 2. Password, 3. Upgrade, 4. Syslog, 5. Web Server, 6. Phone Reset, and 7. Statistics. The '7. Statistics' option is highlighted with a white background and a black border.</p>
<p><b>2</b></p>	<p>Use the   keys and select “Yes” or “No”.</p>	 <p>The screenshot shows a terminal window titled 'Statistics' with the time '17:40'. The screen displays configuration options for statistics. The 'Statistics' option is checked. Below it, there is a dropdown menu showing 'off' with left and right arrow keys. Further down, the 'Interval' option is checked, and a text input field below it contains the number '10'.</p>



## 2. 802.1x (EAP-TLS) Certificate Installation Methods

### 2.1 Installation Procedures 802.1x Certificate

[Requirements]

The following are required. Issue these in advance and place in the root directory of the tftp server.

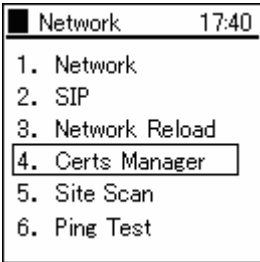
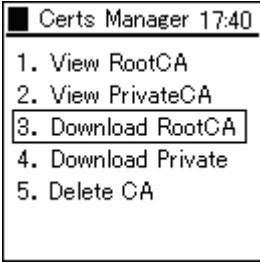


- Root Certificate (DER, CER [Base64 Encoding], PEM)
- Private Certificate (.pfx, p12)




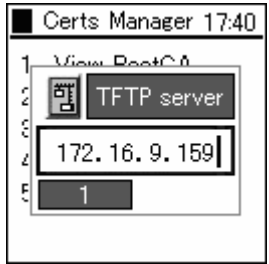
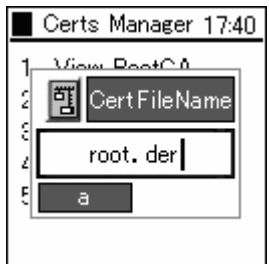
\* Please record and store the ID and Password when installing a Private Certificate.

\* Warning: Depending on the situation, the ID/Passwords developed for Private Certificates may differ from the ID/Passwords used for connection, please take particular care in these circumstances. The following describes when the ID/Password differs during the Private Certificate install and connection authentication.





\* The Root Certificate is necessary when using TLS, PEAP, and TTLS and the Private Certificate is necessary when using TLS.


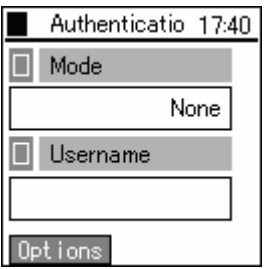
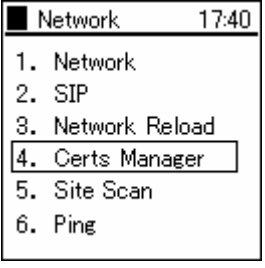
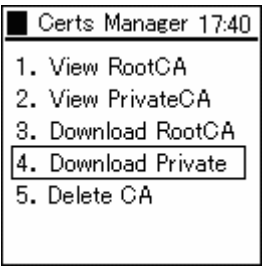


#### 2.1.1 Root Certificate




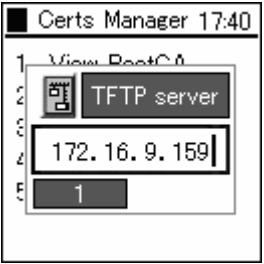
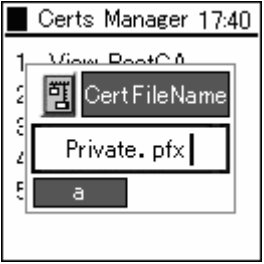
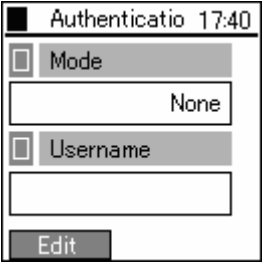
<b>1</b>	Select "4. Certs Manager" from the Network menu.	 <p>The screenshot shows a menu titled "Network" with a timestamp of 17:40. The menu items are: 1. Network, 2. SIP, 3. Network Reload, 4. Certs Manager (highlighted with a black box), 5. Site Scan, and 6. Ping Test.</p>
<b>2</b>	Select "3. Download RootCA" from the Certs Manager menu.	 <p>The screenshot shows a menu titled "Certs Manager" with a timestamp of 17:40. The menu items are: 1. View RootCA, 2. View PrivateCA, 3. Download RootCA (highlighted with a black box), 4. Download Private, and 5. Delete CA.</p>
<b>3</b>	Press the  key when the warning screen displays.	 <p>The screenshot shows a dialog box titled "Certs Manager 17:40" with a warning icon and the text: "Warning", "Incorrect upgrading may cause phone to malfunction." The dialog box has a list of options on the left, with the first option (1) selected.</p>

<p><b>4</b></p>	<p>A confirmation of whether to conduct an upgrade or not will appear. Use the   keys and select “Yes”.</p>	
<p><b>5</b></p>	<p>Enter the IP address for the TFTP server.</p>	
<p><b>6</b></p>	<p>Enter the file name to download.  (Wait a short while)  If an error messages displays, verify the environment and repeat 1 to 6.</p>	

### 2.1.2 Private Certificate

<p><b>1</b></p>	<p>Press the  key and select the menu. Either press the "6" on the number pad or select “6. Network”, then press the  key.</p>	
<p><b>2</b></p>	<p>A list of the configurations is displayed. Select the profile for use.</p>	

<p><b>3</b></p>	<p>Select "4. Authentication" from the Config menu.</p>	 <p>Config1 17:40</p> <ol style="list-style-type: none"> <li>1. Basic Info</li> <li>2. WLAN</li> <li>3. WEP</li> <li>4. Authentication</li> <li>5. TCP/IP</li> <li>6. SIP Outb Proxy</li> </ol>
<p><b>4</b></p>	<p>Configure as follows and restart.</p> <p>Mode</p> <p>    "None", "WEB", "8021X-TTLS", "8021X-TLS",     "8021X-MD5", "8021X-PEAP"</p> <p>Username</p> <p>    (User ID) blank space</p> <p>Password</p> <p>    (User Password) Password used for generating private certificates</p> <p>    (*Note) This becomes the password for generating Private Certificates, so it does not matter if the User ID is blank.</p>	 <p>Authenticatio 17:40</p> <p>Mode</p> <p>    None</p> <p>Username</p> <p>Options</p>
<p><b>5</b></p>	<p>Select "4. Certs Manager" from the Network menu.</p>	 <p>Network 17:40</p> <ol style="list-style-type: none"> <li>1. Network</li> <li>2. SIP</li> <li>3. Network Reload</li> <li>4. Certs Manager</li> <li>5. Site Scan</li> <li>6. Ping</li> </ol>
<p><b>6</b></p>	<p>Select "4. Download PrivateCA" from the Certs Manager menu.</p>	 <p>Certs Manager 17:40</p> <ol style="list-style-type: none"> <li>1. View RootCA</li> <li>2. View PrivateCA</li> <li>3. Download RootCA</li> <li>4. Download Private</li> <li>5. Delete CA</li> </ol>
<p><b>7</b></p>	<p>Press the  key when the warning screen displays.</p>	 <p>Certs Manager 17:40</p> <p>Warning</p> <p>Incorrect upgrading may cause phone to malfunction.</p>

<p><b>8</b></p>	<p>A question to whether conduct an upgrade will appear. Use the   keys and select “Yes”.</p>	
<p><b>9</b></p>	<p>Enter the IP address for the TFTP server.</p>	
<p><b>10</b></p>	<p>Enter the file name to download.  (Wait)  If an error messages displays, verify the environment and repeat 1 to 9.</p>	
<p><b>11</b></p>	<p>After downloading, the Username and Password used for generating Private Certificates that was set in “4” is changed to the User ID and Password used for certification that is recorded in Radius.  Mode Select the certification format ‘None’, ‘WEB’, ‘8021X-TTLS’, ‘8021X-TLS’, ‘8021X-MD5’, ‘8021X-PEAP’  Username (User ID) * ID for Certification that is recorded in RADIUS  Password (User Password) *Password for Certification that is recorded in RADIUS  (Caution)Please take care as the User ID and Password will become that which is recorded in Radius</p>	

### 3. Boot-ROM menu

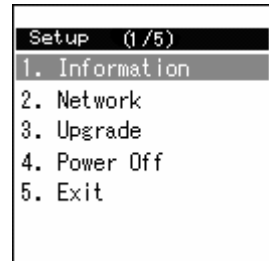
WirelessIP 5000 has both a normal mode and boot-ROM mode used for maintenance. In the boot-ROM mode, not only software but also a boot-ROM corresponding to the OS can be uploaded.

It is possible to upgrade from the boot-ROM menu on WirelessIP 5000. Upgrade using the following procedure.

Note!!!: Network settings on the boot-ROM menu are only valid in the boot-ROM menu. Network settings used during normal operation are set from the Admin menu.

#### 3.1 Opening the boot-ROM menu

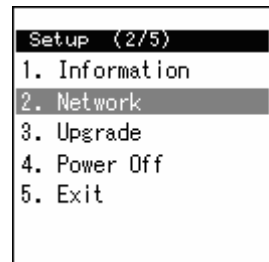
- 1 Press the **End** key and the **LeftSoft** key at the same time.  
Two seconds later, the boot-ROM menu will appear.



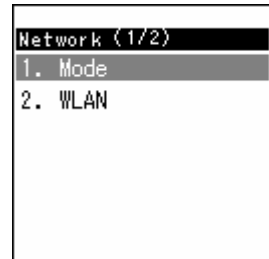
#### 3.2 Network settings

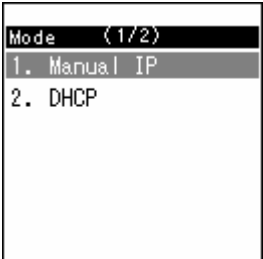
Before upgrading, it is necessary to set the network settings. Network settings are entered from the Boot-ROM menu; it is not necessary to enter the settings from the Admin menu. Boot-ROM menu network settings only allow wireless LAN and TCP/IP.

- 1 Select "2. Network."



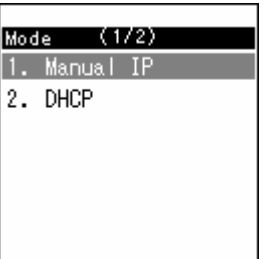
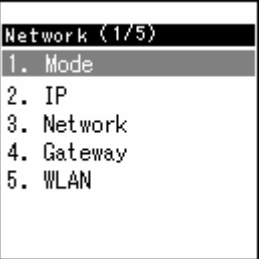
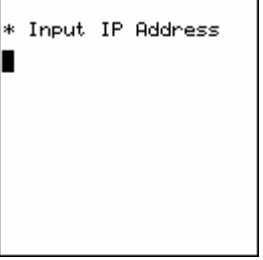


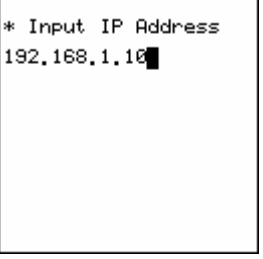
- 2 Select "1. Mode."



<b>3</b>	<p>You can select either manual IP or DHCP.</p> <ul style="list-style-type: none"> <li>- When selecting manual IP, refer to “3.2.1 Manual IP.”</li> <li>- When selecting DHCP, refer to “1.2.2 DHCP.”</li> </ul>	 <p>A screenshot of a terminal menu titled "Mode (1/2)". It lists two options: "1. Manual IP" and "2. DHCP". The "1. Manual IP" option is highlighted with a grey background.</p>
----------	--	--

### 3.2.1 Manual IP



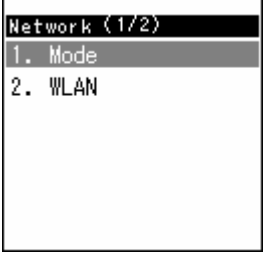
When using manual IP, values for the IP address, sub-network mask, and default gateway are necessary.

<b>1</b>	<p>Select “1. Manual IP.”</p>	 <p>A screenshot of a terminal menu titled "Mode (1/2)". It lists two options: "1. Manual IP" and "2. DHCP". The "1. Manual IP" option is highlighted with a grey background.</p>
<b>2</b>	<p>The following items have been added to the “Network” menu: When using manual IP, enter these values.</p>	 <p>A screenshot of a terminal menu titled "Network (1/5)". It lists five options: "1. Mode", "2. IP", "3. Network", "4. Gateway", and "5. WLAN". The "1. Mode" option is highlighted with a grey background.</p>
<b>3</b>	<p>Select “2. IP.”</p>	 <p>A screenshot of a terminal prompt titled "* Input IP Address". A cursor is visible at the beginning of the line.</p>
<b>4</b>	<p>Enter the IP address. Enter a period using the  key. Press the  key after entering the IP address.</p>	 <p>A screenshot of a terminal prompt titled "* Input IP Address". The IP address "192.168.1.10" has been entered, and the cursor is at the end of the line.</p>

<p><b>5</b></p>	<p>Press the <b>End</b> key.</p>	<pre>* Automatic update   Netmask &amp; Gateway   Yes  : [ENTER]   No   : [ OTHER ]</pre>
<p><b>6</b></p>	<p>Select “3. Netmask.”</p>	<pre>Network (3/5) 1. Mode 2. IP 3. Network 4. Gateway 5. WLAN</pre>
<p><b>7</b></p>	<p>Enter the netmask. Enter a period using the <b>*</b> key. Press the <b>Enter</b> key after entering the netmask.</p>	<pre>* Input Netmask 255.255.255.0</pre>
<p><b>8</b></p>	<p>Select “4. Gateway.”</p>	<pre>Network (4/5) 1. Mode 2. IP 3. Network 4. Gateway 5. WLAN</pre>
<p><b>9</b></p>	<p>Enter the gateway. Enter a period using the <b>*</b> key. Press the <b>Enter</b> key after entering the gateway.</p>	<pre>* Input Def. Gateway 192.168.1.1</pre>

### 3.2.2 DHCP

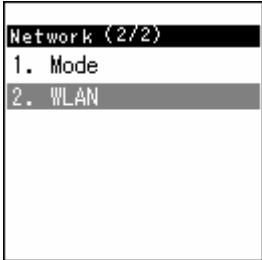
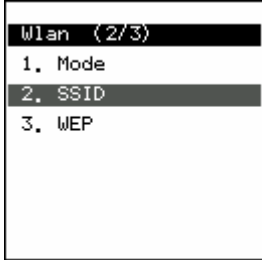
When using DHCP, the values for the IP address, netmask, and default gateway are automatically retrieved from the DHCP server.

<b>1</b>	Select "2. DHCP."	
<b>2</b>	A screen similar to the one to the right will appear.	
<b>3</b>	The following items are deleted from the "Network" menu: "IP", "Netmask", and "Gateway".	



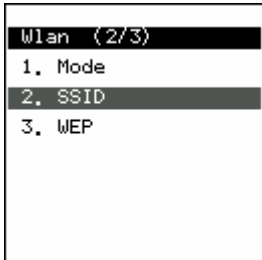

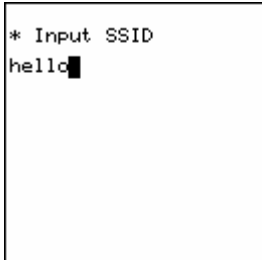
### 3.3 WLAN settings

Enter the settings for wireless LAN. When not using SSID and WEP key, go to section 1.4.

<p><b>1</b></p>	<p>Select "2. WLAN".</p>	 <pre> Network (2/2) 1. Mode 2. WLAN                     </pre>
<p><b>2</b></p>	<ul style="list-style-type: none"> <li>- When setting SSID, refer to "3.3.1 SSID."</li> <li>- When setting WEP key, refer to "3.3.2 WEP key."</li> </ul> <p>Note!!!: Change the setting after reading about the various features of each Mode in "1. Mode". While it is possible to select "Infra/Ad-hoc", it is possible that normal operation and network connections will be negatively affected if you make mistakes with the procedure.</p>	 <pre> Wlan (2/3) 1. Mode 2. SSID 3. WEP                     </pre>

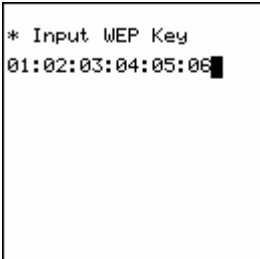
#### 3.3.1 SSID

SSID is used to connect to a specific access point.

<p><b>1</b></p>	<p>Select "2. SSID".</p>	 <pre> Wlan (2/3) 1. Mode 2. SSID 3. WEP                     </pre>
<p><b>2</b></p>	<p>Enter the SSID value for the access point you want to connect to. After entering the value, press the  key.</p>	 <pre> * Input SSID hello                     </pre>

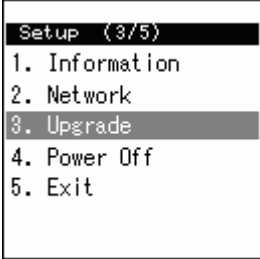
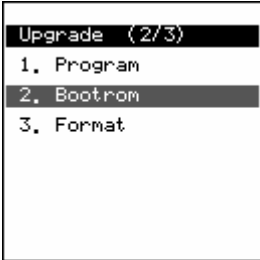
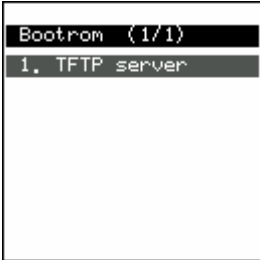




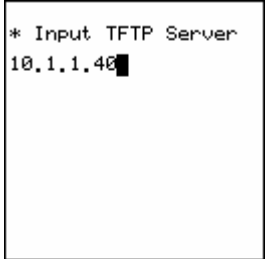


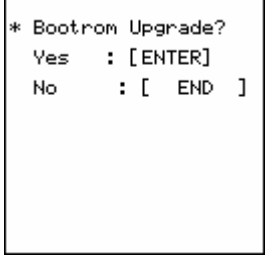
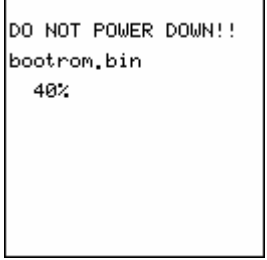
<p><b>5</b></p>	<p>Select "WEP Bit".</p> <p>WirelessIP 5000 supports 64/128/256 bit.</p>	<div data-bbox="1139 282 1401 539"> <p>WLAN (3/6)</p> <ul style="list-style-type: none"> <li>1. Mode</li> <li>2. SSID</li> <li style="background-color: #cccccc;">3. WEP</li> <li>4. WEP Bit</li> <li>5. Default KeyId</li> <li>6. WEP-Key</li> </ul> </div> <div data-bbox="1139 560 1401 817"> <p>WEP Bit (1/3)</p> <ul style="list-style-type: none"> <li style="background-color: #cccccc;">1. 64 Bit</li> <li>2. 128 Bit</li> <li>3. 256 Bit</li> </ul> </div>
<p><b>6</b></p>	<p>Select "Default KeyID", and enter the Index number. The default KeyID is connected to the WEP-Key.</p> <p>When the Default KeyID is set to 1, it is necessary to enter "WEP-key 1 for the WEP-Key in step 8.</p>	<div data-bbox="1139 851 1401 1108"> <p>WLAN (5/6)</p> <ul style="list-style-type: none"> <li>1. Mode</li> <li>2. SSID</li> <li>3. WEP</li> <li>4. WEP Bit</li> <li style="background-color: #cccccc;">5. Default KeyId</li> <li>6. WEP-Key</li> </ul> </div> <div data-bbox="1139 1128 1401 1386"> <p>* Input Index(1-4)</p> <p>1</p> </div>
<p><b>7</b></p>	<p>Select "6. WEP-Key".</p>	<div data-bbox="1139 1415 1401 1673"> <p>WLAN (6/6)</p> <ul style="list-style-type: none"> <li>1. Mode</li> <li>2. SSID</li> <li>3. WEP</li> <li>4. WEP Bit</li> <li>5. Default KeyId</li> <li style="background-color: #cccccc;">6. WEP-Key</li> </ul> </div>
<p><b>8</b></p>	<p>Select one of the following for the "WEP-Key": 1, 2, 3, or 4.</p>	<div data-bbox="1139 1702 1401 1960"> <p>WEP-Key (1/4)</p> <ul style="list-style-type: none"> <li style="background-color: #cccccc;">1. WEP-Key1</li> <li>2. WEP-Key2</li> <li>3. WEP-Key3</li> <li>4. WEP-Key4</li> </ul> </div>

<p><b>9</b></p>	<p>Using the dial pad, enter the WEP Key. Pressing the # key enters a “:”.</p> <p>Note!!!: Enter the WEP Key using hexadecimal numbers.</p> <p>Warning!: Enter “:” after every 2 characters.</p>	
-----------------	--	---

### 3.4 Boot-ROM upgrade

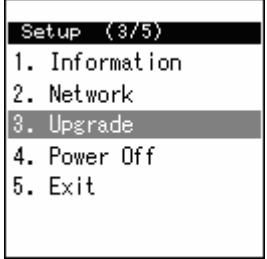

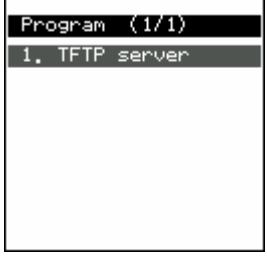

When upgrading the boot-ROM through a TFTP server, it is necessary to un-zip the boot-ROM folder on the TFTP server beforehand.

<p><b>1</b></p>	<p>Select “3. Upgrade”.</p>	
<p><b>2</b></p>	<p>Select “2. Boot-ROM”.</p>	
<p><b>3</b></p>	<p>Select “1. TFTP server”.</p>	

<p><b>4</b></p>	<p>Using the dial pad, enter the IP address for the TFTP server. (Use the  key to enter a period.) After entering the IP address, press the  key.</p> <p>If you enter an incorrect IP address for the TFTP server, a screen like the one in the figure to the right will appear.</p>	 <pre>* Input TFTP Server 10.1.1.40</pre>  <pre>* ERROR * Fail to download bootrom.bin</pre>
<p><b>5</b></p>	<p>After downloading, a screen, like the one to the right, will appear. Pressing the  key will write the contents into flash memory.</p> <p>Warning!: If the boot-ROM for WirelessIP 5000 is upgraded by an inappropriate or damaged file, it might not be possible to restore it. Upgrade after carefully checking that the TFTP settings are correct.</p> <p>Warning!!!: Do not turn off the power when writing the boot-ROM into flash memory. It may not be possible to restore it.</p> <p>If one of the above situations occurs, contact the store or dealer you purchased the product from.</p>	 <pre>* Bootrom Upgrade? Yes  : [ENTER] No   : [ END ]</pre>  <pre>DO NOT POWER DOWN!! bootrom.bin 40%</pre>

### 3.5 Software upgrade

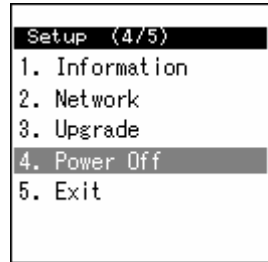
When upgrading software through the TFTP server, it is necessary to un-zip the software on the TFTP server beforehand.

<p><b>1</b></p>	<p>Select "3. Upgrade".</p>	 <pre> Setup (3/5) 1. Information 2. Network 3. Upgrade 4. Power Off 5. Exit                     </pre>
<p><b>2</b></p>	<p>Select "1. Program".</p> <p>Selecting "3. Format" deletes the software settings.</p>	 <pre> Upgrade (1/3) 1. Program 2. Bootrom 3. Format                     </pre>
<p><b>3</b></p>	<p>Select "1. TFTP server".</p>	 <pre> Program (1/1) 1. TFTP server                     </pre>
<p><b>4</b></p>	<p>After downloading, the software will automatically start up.</p>	 <pre> Now Downloading... qstr.bin 512  Running...                     </pre>

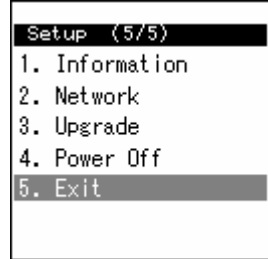
### 3.6 Closing the Boot-ROM menu

---

- 1** After selecting “4. Power off”, the power can be turned off after closing the boot-ROM menu.



Selecting “5. Exit” closes the boot-ROM and restarts the terminal.



## 4. Troubleshooting

### 4.1 General

Phenomena	Response
WirelessIP 5000 does not start.	The battery is dead. If the battery is dead, WirelessIP 5000 will not start and the LED will not light up. After recharging the battery using the AC adapter, try to restart it again.
A key will not work.	Remove the battery, and then reconnect it.
You can hardly see the screen.	Adjust the contrast using the Menu>Setting>Brightness adjustment.
There is a vertical line on the screen.	If it has not been used for a long time, there are cases when the line appears right after starting it up. This can also occur if the battery has been improperly removed.
Communication is bad, or phone suddenly disconnects.	It is possible that you are too far from the access point, the signal is being weakened by an obstruction such as a wall, or there is electromagnetic interference. Check the signal level and interference using Menu>Admin>Network>SITESCAN.
The standby time is different to that in the specifications.	The battery standby time can be different from that noted in the specifications on account of the access point configuration or settings. Also, the standby time can be shortened due to a high or low temperature environment.
WirelessIP 5000 heats up.	When the WirelessIP 5000 is located outside the range of the access point, there are situations when the device consumes power as when telephoning. The device can heat up slightly on account of this. The heat will not effect operation.
The sound level is too low.	Using the volume button, adjust the sound level.
After restarting, the time reverts to the default value.	Since WirelessIP 5000 cannot maintain the time when the power is off, it is necessary to retrieve time information from the NTP server.
The battery becomes unusable.	When the WirelessIP 5000 will not be used for more than a month please remove the battery from the handset and store it. The battery pack may become unusable due to self-discharge.  Please store the battery at less than 20°C in a low-humidity environment that is clean and free of dust.

\* When problems other than those discussed above occur, consult the store or dealer from whom you purchased the product.



Copyright© 2005

Hitachi Cable, LTD.

Otemachi Building, 6-1 Otemachi 1-chome,  
Chiyoda-ku, Tokyo 100-8166, Japan

(First Edition, February 2005)

(Second Edition, July 2005)