Preface
This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions
With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).

- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.

- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning. Also, do not use the telephone to report a gas leak in the vicinity of the leak.

⚠️ WARNING

- Disconnect the PLC from the power source before servicing.

Copyright
Copyright©2014 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

NOTE: This document is subject to change without notice.
Protect Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this PLC can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.
Table of Contents

Chapter 1 Product Information ................................................................. 6
  1.1 Front Panel and LED indicators ....................................................... 6
  1.2 Bottom Panel ............................................................................... 7
  1.3 How to understand the COVERAGE LED colors ................................ 8
  1.4 Point-to-Point Network ................................................................. 9
  1.5 Point to Multipoint Network ....................................................... 10
Chapter 2 Log In Procedure ................................................................. 11
  2.1 Configure STATIC IP MODE ......................................................... 11
  2.2 Logging In ............................................................................... 12
Chapter 3 G.hn Interface .................................................................... 13
  3.1 Basic Configuration .................................................................... 13
  3.2 NDIM Configuration ................................................................... 14
  3.3 Encryption Configuration via WEB UI ........................................ 14
Chapter 4 IP Interface ........................................................................ 15
  4.1 IP config .................................................................................. 15
Chapter 5 Ethernet Interface ............................................................... 16
Chapter 6 Device Interface .................................................................. 17
  6.1 HW information ....................................................................... 17
  6.2 SW information ....................................................................... 18
Chapter 7 Multicast Interface ............................................................... 19
  7.1 MCAST Configuration .............................................................. 19
Chapter 8 QoS menu .......................................................................... 20
  8.1 QoS Configuration .................................................................... 20
Chapter 9 VLAN Interface .................................................................. 23
  9.1 VLAN Configuration ................................................................ 23
Chapter 10 G.hn spectrum Interface .................................................... 24
  10.1 Notches .............................................................................. 24
Chapter 11 Log file Interface ............................................................... 25
  11.1 Log File ............................................................................... 25
Chapter 12 Advanced Interface ........................................................... 26
Chapter 13 WiFi Log In Procedure ....................................................... 27
  13.1 Configure STATIC IP MODE ....................................................... 27
  13.2 Logging In ............................................................................ 28
Chapter 14 Wireless .......................................................................... 30
  14.1 Basic Settings ................................................................. 30
  14.2 Advanced Settings .................................................................. 33
  14.3 Security .............................................................................. 35
  14.4 Access Control .................................................................. 42
  14.5 Wireless Site Survey .............................................................. 43
  14.6 WiFi Protected Setup .............................................................. 44
Chapter 15 TCP/IP Settings ................................................................. 45
  15.1 LAN Interface ................................................................. 45
Chapter 16 IPv6 .................................................................................. 46
  16.1 IPv6 LAN Setting ................................................................. 46
Chapter 17 Management ..................................................................... 47
  17.1 Status ............................................................................... 47
Chapter 1 Product Information

1.1 Front Panel and LED indicators

**WPS Button:** Press for 2 – 10 seconds to start the WPS function. Press for over 10 seconds to reset to factory defaults.

**Power Button:** Push once to power up the PG-9171n
Push once to power down the PG-9171n

<table>
<thead>
<tr>
<th>LED</th>
<th>COLOR</th>
<th>MODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Green</td>
<td>On</td>
<td>Node is secure (it has either received or generated network keys)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>Node is not secure, it has neither received nor generated network key parameters (domain name and encryption key)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blink</td>
<td>Node is in configuration mode (able to exchange network keys)</td>
</tr>
<tr>
<td>COVERAGE</td>
<td>Green</td>
<td>On</td>
<td>The current connection (estimated throughput) is greater than 40 Mbps</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>On</td>
<td>The current connection (estimated throughput) is greater than 20 Mbps and less than 40 Mbps</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>On</td>
<td>The current connection (estimated throughput) is between 1 and 20 Mbps per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>No PLC connection exists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blink</td>
<td>Adapter in power saving mode (blinks twice every 5 seconds)</td>
</tr>
<tr>
<td>WLAN</td>
<td>Green</td>
<td>Off</td>
<td>WLAN is off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blink</td>
<td>Wireless is activity (tx/rx data and message)</td>
</tr>
<tr>
<td>WPS</td>
<td>Green</td>
<td>Off</td>
<td>WPS function is disabled or there is no activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blink</td>
<td>There is activity occurring</td>
</tr>
</tbody>
</table>
### Ethernet

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>LAN connection established</td>
</tr>
<tr>
<td>Off</td>
<td>LAN connection is not established</td>
</tr>
<tr>
<td>Blink</td>
<td>Data transmitting/receiving</td>
</tr>
</tbody>
</table>

### Power

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>The device is powered up</td>
</tr>
<tr>
<td>Off</td>
<td>The device is powered down</td>
</tr>
</tbody>
</table>

### 1.2 Bottom Panel

![Config LED](image)

**Item Name** | **Description**
--- | ---
Config | Press more than 2 seconds ("Security" LED starts slow blinking) and released: the “One Button Security Setup” (OBUS) procedure is started and configuration period is open.  
Press more than 5 seconds ("Security" LED starts quick blinking) and released: security settings are set to default values.  
Press more than 10 seconds ("Security" LED switches off) and released: a factory reset is performed.
1.3 How to understand the COVERAGE LED colors

The COVERAGE LED displays quality of the network and provides important information that will provide solutions to common questions, such as why a High Definition (HD) movie is not showing or shows with pixels. The COVERAGE LED indicator will vary its color depending on the estimated speed of the Powerline connection. The speed is measured in Megabits Per Second (Mbps).

<table>
<thead>
<tr>
<th>Color</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED</td>
<td>The current connection has standard quality, normal Internet activities ex. 20Mbps are possible but the Powerline is unable to transmit either a Standard Movie or High Definition (HD) Movie.</td>
</tr>
<tr>
<td>ORANGE</td>
<td>The current connection has good quality and Internet activities ex. greater than 20Mbps and less than 40Mbps to transmit Standard Movie and HD Movie.</td>
</tr>
<tr>
<td>GREEN</td>
<td>The current connection has excellent quality and Internet activities ex. greater than 40Mbps to transmit multiple Standard Movies and HD Movies.</td>
</tr>
</tbody>
</table>
1.4 Point-to-Point Network

- **CASE 1**: Estimated throughput is less than 20 Mbps. The PLC channel is not able to transmit an SDTV channel. The COVERAGE LED will be RED as shown in the following figure:

  ![Figure showing RED Coverage LED](image1)

  Estimated throughput < 20 Mbps

- **CASE 2**: Estimated throughput is greater than 20 Mbps but less than 40 Mbps. The PLC channel is able to transmit an SDTV channel, but not two SDTV channels simultaneously or one HDTV channel. The COVERAGE LED will be ORANGE as shown in the following figure:

  ![Figure showing ORANGE Coverage LED](image2)

  20 Mbps < Estimated throughput < 40 Mbps

- **CASE 3**: Estimated throughput is greater than 10 Mbps. The PLC channel is able to play at least two SDTV channels or 1 HDTV. The COVERAGE LED will be GREEN as shown here:

  ![Figure showing GREEN Coverage LED](image3)

  Estimated throughput > 40 Mbps
1.5 Point to Multipoint Network

In the case where the PLC network is composed of three or more adapters, similar situations could arise as with a point-to-point network.

- **CASE 1:** The COVERAGE LED in G.hn adapter 2 and G.hn adapter 3 will show the estimated level of the PLC link receiving from G.hn adapter 1.

- **CASE 2:** The COVERAGE LED in G.hn adapter 1 will show the estimated level of the PLC link from which it is receiving the most amount of traffic at any given time. For example, if G.hn adapter 1 is receiving traffic at 50Mbps from G.hn adapter 2 and is receiving 25Mbps from G.hn adapter 3, the COVERAGE LED will show the level with reference to the G.hn adapter 2 link, as shown in the following figure.
Chapter 2 Log In Procedure

2.1 Configure STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

Follow these steps to configure your PC IP address to use subnet 10.10.1.x.

**NOTE:** The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

**STEP 1:** From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the **Properties** button.

**STEP 2:** Select Internet Protocol (TCP/IP) and **click the** Properties button.

**STEP 3:** Change the IP address to the domain of 10.10.1.x (69<x<255) with subnet mask of 255.255.255.0. The screen should now display as below.

![Internet Protocol (TCP/IP) Properties](image)

**STEP 4:** Click **OK** to submit these settings.
2.2 Logging In

Perform the following steps to login to the web user interface.

**STEP 1:** Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 10.10.1.69, type [http://10.10.1.69](http://10.10.1.69)

**STEP 2:** A dialog box will appear, such as the one below. Input the default Authentication Password.

Authentication Password:  **paterna**

Click **OK** to continue.

**Note:**
The Factory Reset password is:  **betera**
Chapter 3 G.hn Interface

3.1 Basic Configuration

- **Domain Name** string of all nodes in the network.
- **Force node Type** force the modem to have a particular role (END POINT or DOMAIN MASTER)
- **G.hn profile** of all nodes in the network: selecting which G.hn profile must be applied to the network (PLC 50MHz, PLC 50MHz with MIMO, PLC 100MHz, COAX 100MHz and PHONE 100MHz).
3.2 NDIM Configuration

- **NDIM mode** set to Automatic for enabling automatic DOD selection functionality and set to Manual for manual configuration of DOD.
- **Domain ID (DOD)** manually set the DOD number from 1 to 15 to use a different preamble seed than the default 0.

3.3 Encryption Configuration via WEB UI

- **Pairing Password** used for authentication. Write a custom password to manually create a secure domain.

Available Connections

- In this tab table, all the available **G.hn connections** are presented. Remote node DID and MAC address, transmission and reception physical speeds.
Chapter 4 IP Interface

4.1 IP config

In the IP configuration tab of one G.hn node, the IPv4 and IPv6 settings can be read and changed.

IPv4 subsection:

- **DHCPv4 enabled**: in the case of choosing "No" (i.e. fixed) IP configuration in the previous option, the IPv4 Address, Subnet Mask, Default Gateway and DNS IPv4 Address should be configured; fill these fields in. In the case of choosing “Yes” (i.e. DHCP) they will be filled automatically when configuration is received from the DHCP server.

IPv6 subsection:

- **DHCPv6 enabled**: to enable the IPv6 DHCP configuration or choose not to.
- **DHCPv6 Address**: to read the node’s DHCPv6 address in case the DHCPv6 is enabled.
- **IPv6 Link Local Address**: to read the node’s Link Local address.
- **Manual IPv6 Manual Address**: to configure up to four IPv6 Manual Addresses for the node.
- **DNSv6 Address**: to configure the DNS address.
The Ethernet table shows the coverage & Info of the Ethernet interface; including Interface, Speed, Duplex, Interface Type, Mode, Internal PHY & Link.

**Powersaving**

Ethernet powersaving can be disabled, enabled by Ethernet link or enabled by Ethernet activity; idle timer can be configured as well.
6.1 HW information

In this tab, basic information such as MAC Address, Serial Number, HW Product and Revision, ASIC and Chipset of the selected node is shown. Other information about the Ethernet port is also shown.
6.2 SW information

Shows the FW version and system uptime.

Configuration password

The nodes in the network: to change the configuration password string from the default ("paterna") to another; decided by the user.

Software update:

Current loaded firmware and API version are shown. SW can be upgraded via FTP or TFTP. L2 is proprietary and is reserved for future use. Additionally, HTTP protocol can be also used for SW upgrade. Usually, a reboot should be performed afterwards to make sure the changes are effective.
7.1 MCAST Configuration

In the **MCAST Configuration** tab of "My Network", IGMP snooping and MLD features can be enabled or disabled. Also, IGMP multicast IP addresses ranges which the G.hn PLC network will sniff; can be configured.

- **IGMP Snooping**: Enable or Disable.
- **MLD Snooping**: Enable or Disable.
- **IGMP/MLD broadcast report (allowed)**: set to NO for enabling reports dropping until the video source is detected, this is a recommended setting when IGMP/MLD is enabled. Set to YES for broadcasting reports until the video source is detected; this implies the multicast video stream is sent as broadcast and it is the recommended state when IGMP/MLD is disabled.

**IGMP Multicast ranges configuration**: 4 multicast IP address ranges can be configured defining the minimum and maximum IP addresses of each range. Only multicast traffic within these ranges will be processed.
8.1 QoS Configuration

In the QoS configuration tab, the packet classifier can be managed to define a QoS rule for incoming Ethernet traffic, and assign a priority to be used in the G.hn network. Press the "Update" button for loading the newly configured settings:

- **QoS CRITERION**: a general criterion can be chosen among "None" (no QoS), "Custom" and "802.1p".
- **Type of Frame**: with this parameter the type of Ethernet traffic being transmitted by the G.hn network should be selected. Based on this parameter, the internal offsets in the system are adjusted. In the QoS tab, Ethernet frame offsets should be set counting number as they appear in the sniffer SW (for instance, the same field will be in a different position if normal Ethernet frames or 802.1Q tagged frames exist).
- **Packet detection 1**: first packet detection rule can be configured (offset, bitmask and pattern). Packets which accomplish it will be sent to the classification module.
- **Packet detection 2**: if second packet detection is also enabled, both, first and second detection criteria must be accomplished to pass packets to the classification module.
- **Packet classification**: up to 8 classification rules can be defined in this section for packets which have previously been correctly detected. For 802.1p only priorities can be managed, offset, bitmask and pattern are predefined to sniff the PCP field.
- **Default priority**: select default priority; which will be applied to non classified incoming packets. Priority 7 is the highest. Priority 0 is the lowest.
If QoS criterion: 802.1p, all other options are grayed out, and follow the QoS rules below.

According to G.9960 specs, the priority mapping recommended by [IEEE 802.1D] subclause 7.7.3 is presented in Table III.1. for four priority queues.

<table>
<thead>
<tr>
<th>PCP</th>
<th>Priority</th>
<th>Acronym</th>
<th>Traffic Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 (Third)</td>
<td>BK</td>
<td>Background</td>
</tr>
<tr>
<td>0</td>
<td>1 (lowest)</td>
<td>BE</td>
<td>Best Effort</td>
</tr>
<tr>
<td>2</td>
<td>2 (lowest)</td>
<td>EE</td>
<td>Excellent Effort</td>
</tr>
<tr>
<td>3</td>
<td>3 (Third)</td>
<td>CA</td>
<td>Critical Applications</td>
</tr>
<tr>
<td>4</td>
<td>4 (second)</td>
<td>VI</td>
<td>Video, &lt; 100 ms latency and jitter</td>
</tr>
<tr>
<td>5</td>
<td>5 (second)</td>
<td>VO</td>
<td>Voice, &lt; 10 ms latency and jitter</td>
</tr>
<tr>
<td>6</td>
<td>6 (highest)</td>
<td>IC</td>
<td>Internetwork Control</td>
</tr>
<tr>
<td>7</td>
<td>7 (highest)</td>
<td>NC</td>
<td>Network Control</td>
</tr>
</tbody>
</table>

In summary, the sequence of priority queue, (7,6) > (5,4) > (3,0) > (2,1)
**Note:** If the user selects “Custom” as the QoS criterion, there will be an inaccuracy after the user clicks the **OK** button at the bottom of the screen (i.e, the Offset value will increase by two (from 7-9 in the rule 1-8 boxes). In this case you can reset the factory defaults in the Advanced menu to recall Factory Resets if necessary. If you want to correct this inaccuracy, manually change the values in the Offset boxes to the number 5. Upon clicking the **OK** button the Offset values will all display 7 respectively.
9.1 VLAN Configuration

In the VLAN Configuration tab of one G.hn node, a VLAN tag can be added or removed per interface. Also, removing a tag at egress per interface can be also enabled or disabled:

- **Enable VLAN Configuration**: Select No from the drop down menu to disable completely the VLAN functionality, removing all tags.

- **Remove VLAN tag at egress**: Select Yes from the drop down menu for the port that you want to remove the VLAN tag from.

- **Ingress/Egress tag**: A tag value (from 1 to 4095) per interface can be added in this section. Set value to 0 for no tagging.
Chapter 10 G.hn spectrum Interface

10.1 Notches

In this tab a table with all configured Notches of selected node will be shown. The table is composed of next columns for every notch: Notch Number, Type of notch, Start Frequency (KHz), Stop Frequency (KHz), Depth (in dB) and Enabled. The "Refresh" button will update the table.

The first 22 notches (Regulation) are Read Only, RO, in the system and they can be neither removed nor modified. The next 40 notches (Vendor) are defined by the vendor using SDK and they are also RO. The last 10 notches (User) are R/W and they can be added/removed by user using this tool.

To add new notches the user should fill the "Add a new User Notch" fields, setting Start and Stop frequencies in KHz and depth in dB of notch and then press the "Add" button. They will be added in first User free position from number 1 to 10.

To remove a User Notch, the "Remove a User Notch" section should be used, setting notch number to be removed from 1 to 10 and pressing the "Remove" button.
Chapter 11 Log file Interface

In the **Log File** configuration tab the following settings can be read, and changed by clicking on the corresponding "Update" button for the selected node:

- **Enable Log File** set to YES for enabling Log File functionality in the node and set to NO for disabling it.
- **Data Capture Interval** sets the interval of time in seconds to capture data.
- **FTP Server URL** configures the url for the remote FTP server where the files will be uploaded.
- **FTP Server Login** configures the user for the FTP server.
- **FTP Server Password** configures the password for the FTP server.
- **Upload to Server Interval** sets the interval of time in minutes to send the captured file to the remote server.
Chapter 12 Advanced Interface

Broadcast suppression

In this tab the broadcast suppression feature can be managed. Broadcast traffic higher than the selected value will be dropped.

**Hardware Reset**: Click on this button to perform a reboot in the node.

**Factory reset**: Click the OK button to order a factory reset of the node.
Chapter 13 WiFi Log In Procedure

13.1 Configure STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

Follow these steps to configure your PC IP address to use subnet 192.168.0.x.

**NOTE:** The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

**STEP 1:** From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the **Properties** button.

**STEP 2:** Select Internet Protocol (TCP/IP) and click the **Properties** button.

**STEP 3:** Change the IP address to the domain of 192.168.0.x (9<x<255) with subnet mask of 255.255.255.0. The screen should now display as below.

![Internet Protocol (TCP/IP) Properties](image)

**STEP 4:** Click **OK** to submit these settings.
13.2 Logging In

Perform the following steps to login to the web user interface.

**STEP 1:** Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.0.9, type [http://192.168.0.9](http://192.168.0.9)

**STEP 2:** A dialog box will appear, such as the one below. Input the default Authentication Password.

![Dialog Box](image)

Authentication Username: **root**

Authentication Password: **12e45**
## Access Point Status

This page shows the current status and some basic settings of the device.

### System
- **Uptime**: 0day:20h:2m:42s
- **Firmware Version**: PG-9171n-WLAN-3464TCA-C01_R01

### Wireless Configuration
- **Mode**: AP
- **Band**: 2.4 GHz (B+G+N)
- **SSID**: Telecable_GbN
- **Channel Number**: 1
- **Encryption**: WPA2
- **BSSID**: f8:8e:85:f5:07:8f
- **Associated Clients**: 0

### TCP/IP Configuration
- **Domain Name**: [Removed]
- **IP Address**: 192.168.0.9
- **Subnet Mask**: 255.255.255.0
- **Default Gateway**: 192.168.0.1
- **MAC Address**: f8:8e:85:f5:07:8f

### LAN IPv6 Configuration
- **Link Type**: IP link
- **Connection Type**: DHCPv6
- **Global Address**: [Removed]
- **L.L. Address**: fe800000000000000000000000000000
- **Default Gateway**: f8:8e:85:f5:07:8f
- **MAC Address**: f8:8e:85:f5:07:8f

### PLC Configuration
- **Serial Number**: 14056800018
- **MAC Address**: f8:8e:85:f5:07:8f
- **Firmware Version**: gedw362f_WorksysEval_512M_v1_x_SPIRIT_v6_4_r398_51_cvs
- **Associated Devices**: 0

---

**Note**: The raw text was marked as [Removed] due to its inclusion of sensitive information.
Chapter 14 Wireless

14.1 Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface: Select the check box to disable the wireless LAN interface.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band</td>
<td>Select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 n, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. If you want to allow 802.11b, 802.11g, and 802.11 Draft-N clients to connect to this access point, select 2.4GHz (B+G+N).</td>
</tr>
<tr>
<td>Mode</td>
<td>PG-9171n only supports AP mode.</td>
</tr>
<tr>
<td>Network Type</td>
<td>In Infrastructure Mode, wireless clients can access the other networks (perhaps Internet) via this AP. For AP. Only Infrastructure Mode is allowed here.</td>
</tr>
<tr>
<td>SSID</td>
<td>Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>Select wireless channel width (bandwidth taken by wireless signals of this access point). It’s suggested to select ‘Auto 20/40MHz’. Do not change to ‘20 MHz’ unless you know what it is.</td>
</tr>
<tr>
<td>Control Sideband</td>
<td>Select Upper or Lower sideband when in 40MHz mode.</td>
</tr>
<tr>
<td>Channel Number</td>
<td>Drop-down menu that allows selection of a specific channel.</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>Select No to hide the SSID such that a station cannot obtain the SSID through passive scanning. Select Yes to make the SSID visible so a station can obtain the SSID through passive scanning.</td>
</tr>
<tr>
<td>WMM (Wi-Fi Multimedia)</td>
<td>The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.</td>
</tr>
<tr>
<td>Data Rate</td>
<td>Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, it’s not necessary to change this value unless you know what will happen after modification.</td>
</tr>
</tbody>
</table>

Click the Show Active Clients button to display the following.
**Active Wireless Client Table**

This table shows the MAC address, transmission, reception packet counts, and encrypted name for each associated wireless client.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Mode</th>
<th>Tx Packet</th>
<th>Rx Packet</th>
<th>Tx Rate (Mbit/s)</th>
<th>Power Saving</th>
<th>Expired Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

[Refresh][Close]
14.2 Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragment Threshold</td>
<td>Set the Fragment threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2346</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>Set the RTS threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2347</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>Set the beacon interval of wireless radio. Do not modify default value if you don’t know what it is, default value is 100</td>
</tr>
<tr>
<td>Preamble Type</td>
<td>Set the type of preamble of wireless radio, Do not modify default value if you don’t know what it is, default setting is ‘Short Preamble’</td>
</tr>
<tr>
<td>IAPP</td>
<td>Click to enable or disable the IAPP function.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protection</td>
<td>Click to enable or disable the Protection function.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Click to enable or disable the Aggregation function.</td>
</tr>
<tr>
<td>Short GI</td>
<td>Click to enable or disable the Short GI function.</td>
</tr>
<tr>
<td>STBC</td>
<td>Click to enable or disable the STBC function.</td>
</tr>
<tr>
<td>LDPC</td>
<td>Click to enable or disable the LDPC function.</td>
</tr>
<tr>
<td>20/40MHz Coexist</td>
<td>Click to enable or disable the 20/40MHz Coexist function.</td>
</tr>
<tr>
<td>TX Beamforming</td>
<td>Click to enable or disable the TX Beamforming function.</td>
</tr>
<tr>
<td>Multicast to Unicast</td>
<td>Click to enable or disable the multicast to unicast conversion function.</td>
</tr>
<tr>
<td>RF Output Power</td>
<td>You can set the output power of wireless radio. Unless you’re using this wireless power line access point in a really big space, you may not have to set output power to 100%. <strong>This will enhance security (malicious / unknown users in distance will not be able to reach your wireless access point).</strong></td>
</tr>
</tbody>
</table>
14.3 Security
This page allows you setup the wireless security. Turning on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Select which SSID's security settings to configure.

Encryption: Select an encryption type from the drop down menu (and refer to the appropriate section below for more details). Select “Disable” to disable wireless encryption for the network. This is not recommended - anyone within range can connect to the device's SSID.

Default security settings are:

SSID: Telecable_GhN
Encryption Type: WPA2-AES Personal
Pre-Shared Key Format: Passphrase
Pre-Shared Key: t3l3cabl32015!
14.3.1 802.1x Authentication

If you select “Disabled” or “WEP” as your encryption type, you can check the “Enable 802.1x Authentication” box to enable 802.1x authentication based on a RADIUS user authentication server.

<table>
<thead>
<tr>
<th>RADIUS Server IP Address</th>
<th>Input the IP address of the RADIUS authentication server here.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Server Port</td>
<td>Input the port number of the RADIUS authentication server here. Default value is 1812.</td>
</tr>
<tr>
<td>RADIUS Server Password</td>
<td>Input the password of the RADIUS authentication server here.</td>
</tr>
</tbody>
</table>

Click the Apply Changes button to display the following.

**Change setting successfully!**

Your changes have been saved. The router must be rebooted for the changes to take effect. You can reboot now, or you can continue to make other changes and reboot later.

Reboot Now  Reboot Later

Your changes have been saved. The router must be rebooted for the changes to take effect. You can reboot now, or you can continue to make other changes and reboot later.
14.3.2 WEP (Shared Key)

Wired Equivalent Privacy (WEP) is a basic encryption type.

**WPA encryption is recommended – though some legacy wireless devices may only support WEP. WEP supports data rates up to a maximum 54Mbps.**

![Wireless Security Setup](image)

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| Select SSID: RootAP · Comrend | Apply Changes | Reset |

**Encryption:**

**802.1x Authentication:**

**Authentication:**

- Open System
- Shared Key
- Auto

**Key Length:**

- 64-bit

**Key Format:**

- Hex (10 characters)

**Encryption Key:**

************

<table>
<thead>
<tr>
<th>Enable 802.1x Authentication</th>
<th>Check this box to enable 802.1x user authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>You can select Open System or Shared Key or Auto for your authentication method.</td>
</tr>
<tr>
<td>Key Length</td>
<td>Select “64-bit” or “128-bit” key length. “128-bit” is safer than “64-bit” but will reduce some data transfer performance.</td>
</tr>
<tr>
<td>Key Format</td>
<td>Select “ASCII” or “Hex” key format. The key length will also be displayed here - ASCII and Hex keys vary in length depending on “Key Length” (above).</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Enter WEP key here, the number of characters must be the same as the number displayed in the “Key Format” field. For “ASCII” key format, you can use any alphanumerical characters (0-9, a-z, and A-Z). For “Hex” format, you can use the characters 0-9, a-f, and A-F.</td>
</tr>
</tbody>
</table>

Click the Apply Changes button to display the following.
Your changes have been saved. The router must be rebooted for the changes to take effect. You can reboot now, or you can continue to make other changes and reboot later.

14.3.3 WPA2 or WPA Mixed+Personal (Pre-Shared Key)

WPA pre-shared key is the recommended and most secure encryption type.

<table>
<thead>
<tr>
<th>Authentication Mode</th>
<th>Select Personal (Pre-Shared Key).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA Cipher Suite</td>
<td>WPA (AES) is selected by default (and is the only option).</td>
</tr>
<tr>
<td>Pre-shared Key Format</td>
<td>Select the pre-shared key format from “Passphrase” (8 to 63 alphanumerical characters) or “Hex” (64 characters 0 to 9 and a to f.)</td>
</tr>
</tbody>
</table>
Pre-shared Key | Please enter the key according to the key format you selected above. For security reasons, it’s best to use a complex, hard-to-guess key.
---|---

TKIP supports a maximum data rate of 54Mbps.

Click the Apply Changes button to display the following.

### Change setting successfully!

Your changes have been saved. The router must be rebooted for the changes to take effect. You can reboot now, or you can continue to make other changes and reboot later.

- Reboot Now
- Reboot Later

Your changes have been saved. The router must be rebooted for the changes to take effect. You can reboot now, or you can continue to make other changes and reboot later.
14.3.4 WPA2 or WPA Mixed+Enterprise (Radius)

WPA RADIUS is a combination of WPA encryption and RADIUS user authentication. If you have a RADIUS authentication server, you can authenticate the identity of every wireless client against a user database.

![WLAN Access Point](image)

<table>
<thead>
<tr>
<th>Authentication Mode</th>
<th>Select Enterprise (RADIUS).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2 CipherSuite</td>
<td>Select from WPA2 (AES) or WPA-Mixed. AES is safer than TKIP, but not supported by all wireless clients. WPA2 (AES) or WPA2 is recommended if supported by your wireless client. Mixed is recommended if your client does not support AES.</td>
</tr>
<tr>
<td>RADIUS Server IP address</td>
<td>Enter the IP address of the RADIUS authentication server here.</td>
</tr>
<tr>
<td>RADIUS Server Port</td>
<td>Enter the port number of the RADIUS authentication server here. Default value is 1812.</td>
</tr>
<tr>
<td>RADIUS Server Password</td>
<td>Enter the password of the RADIUS authentication server here.</td>
</tr>
</tbody>
</table>

Click the Apply Changes button to display the following.
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.

[Reboot Now] [Reboot Later]
14.4 Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

**MAC Address:** Input a MAC address permitted to connect to the extender. Only enter characters 0 to 9 or a to f.

**Comment:** Enter an optional comment associated with the specified MAC address for reference/identification, consisting of up to 16 alphanumerical characters.
14.5 Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Click on the Site Survey to display the following.

<table>
<thead>
<tr>
<th>SSID</th>
<th>BSSID</th>
<th>Channel</th>
<th>Type</th>
<th>Encrypt</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTMG-INT</td>
<td>80:1f:02:57:23:31</td>
<td>1</td>
<td>AP</td>
<td>no</td>
<td>60</td>
</tr>
<tr>
<td>CTMG-INT</td>
<td>80:1f:02:66:34:01</td>
<td>4</td>
<td>AP</td>
<td>no</td>
<td>52</td>
</tr>
<tr>
<td>3345</td>
<td>02:1f:02:66:34:00</td>
<td>4</td>
<td>AP</td>
<td>WPA2-PSK</td>
<td>52</td>
</tr>
</tbody>
</table>

**SSID:** The SSID that the wireless client connected to.

**BSSID:** The BSSID that the wireless client connected to.

**Channel:** The connected channel number that the wireless client used to connect.

**Type:** PG-9171n’s type that the wireless client is connected to.

**Encrypt:** The encryption the connection is using.

**Signal:** The strength of the signal from the wireless client.
14.6 Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Click the **Start PBC** button to start the Push-Button style WPS setup procedure. The Pg-9171n will wait for WPS requests from another wireless device for 2 minutes. The ‘WPS’ LED on the PG-9171n will be blinking for 2 minutes when this PG-9171n is waiting for an incoming WPS request.

Click the **Stop WSC** button to cancel / deactivate the WPS setup procedure.
Chapter 15 TCP/IP Settings

15.1 LAN Interface

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

**IP Address:**  Specify an IP address here. This IP address will be assigned to your extender, and will replace the default IP address 192.168.0.9.

**Subnet Mask:**  Input the subnet mask of the new IP address.

**Default Gateway:**  Input the network’s gateway IP address.

**DNS:**  Input the Domain Name Server’s IP address.

**DHCP:**  Selecting Enable means this device will use DHCP client to get IP address. Selecting Disabled means this device will use the IP address input in this page.

Click the **Apply Changes** button to restart the system and make the changes take effect. Click the **Reset** button to clear and reset the data just inputted.
Chapter 16 IPv6

16.1 IPv6 LAN Setting

This page is used to configure the parameters for IPv6 in the local area network.

Click the Enable IPv6 checkbox if you want to enable IPv6 addressing in the LAN of your extender. By default, IPv6 is disabled.

Configure DHCPv6 or Static addressing depending on your network.

**IP Address:** Specify an IPv6 address and Prefix Length here.

**Default Gateway:** Input the network’s gateway IPv6 address and Prefix Length.

**DNS:** Input the Domain Name Server’s IPv6 address and Prefix Length.

Click the **Apply Changes** button to restart the system and make the changes take effect.

Click the **Reset** button to clear and reset the data just inputted.
Chapter 17 Management

17.1 Status

This page shows the current status and some basic settings of the device.
17.2 Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Click the **Refresh** button to get the latest statistics.
17.3 Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

**Time Zone Setting**

**Time Zone Select**: Choose your preferred time zone.

**Automatically Adjust Daylight Saving**: Tick the box if appropriate for your region.

**Enable NTP client update**: Enable the NTP function here (date and time can be synchronized with a time server).

Click the **Apply Change** button to save the changes.

Click the **Reset** button to clear or reset the Web page.

Click the **Refresh** button to reload the data on the Web page.
17.4 Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

**STEP 1:** Obtain an updated software image file from your ISP.

**STEP 2:** Enter the path and filename of the firmware image file in the **Select File** field or click the Browse button to locate the image file.

**STEP 3:** Click the **Upload** button once to upload and install the file.
17.5 Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Click the **Save** button to save current settings to PC.

Click the **Browse** button to locate the desired file.

**Upload**: update the device’s setting from PC’s file.

Click the **Reset** button to reset the PG-9171n to factory default settings.
17.6 TR-069 Configuration

This page is used to configure the TR-069 protocol settings, including the settings for the ACS’s parameters.

<table>
<thead>
<tr>
<th>TR-069 Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS’s parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TR069</td>
<td>Enabled</td>
</tr>
<tr>
<td>ACS URL</td>
<td><a href="https://main.acs.telecable.es:7005/ac/">https://main.acs.telecable.es:7005/ac/</a></td>
</tr>
<tr>
<td>User Name</td>
<td>ACSGHN</td>
</tr>
<tr>
<td>Password</td>
<td>b313cab315!</td>
</tr>
<tr>
<td>Periodic Inform Enable</td>
<td>Enabled</td>
</tr>
<tr>
<td>Periodic Inform Interval</td>
<td>86400</td>
</tr>
</tbody>
</table>

**Connection Request:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>GhN</td>
</tr>
<tr>
<td>Password</td>
<td>GhN15!</td>
</tr>
<tr>
<td>Path</td>
<td>0</td>
</tr>
<tr>
<td>Port</td>
<td>80005</td>
</tr>
</tbody>
</table>

Please note that this system will be reboot after new TR-069 configuration is set.

**STUN:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enabled</td>
</tr>
<tr>
<td>Server Address</td>
<td></td>
</tr>
<tr>
<td>Server Port</td>
<td>2478</td>
</tr>
<tr>
<td>Server User Name</td>
<td></td>
</tr>
<tr>
<td>Server Password</td>
<td></td>
</tr>
<tr>
<td>Maximum Keep Alive</td>
<td>20</td>
</tr>
<tr>
<td>Minimum Keep Alive</td>
<td>10</td>
</tr>
</tbody>
</table>

Please note that this system will be reboot after new STUN configuration is set.

**Certificate Management:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Certificate</td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>CA Certificate</td>
<td><img src="image" alt="Image" /></td>
</tr>
</tbody>
</table>

No se ha seleccionado ningún archivo.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TR-069</td>
<td>Tick the radio button to enable. Enabled by default.</td>
</tr>
<tr>
<td>URL</td>
<td>URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The “host” portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.</td>
</tr>
<tr>
<td>ACS User Name</td>
<td>Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.</td>
</tr>
<tr>
<td>ACS Password</td>
<td>Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.</td>
</tr>
<tr>
<td>Periodic Inform Enable</td>
<td>If enabled, CPE MUST periodically send CPE information to the ACS using the Inform method call.</td>
</tr>
<tr>
<td>Periodic Inform Interval</td>
<td>The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method if Periodic Inform Enable is true.</td>
</tr>
<tr>
<td><strong>Connection Request</strong></td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>Username used to authenticate an ACS making a Connection Request to the CPE.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to authenticate an ACS making a Connection Request to the CPE.</td>
</tr>
<tr>
<td>Path</td>
<td>It’s part of HTTP URL for an ACS to make a Connection Request Notification to the CPE.</td>
</tr>
<tr>
<td>Port</td>
<td>It’s part of HTTP URL for an ACS to make a Connection Request Notification to the CPE.</td>
</tr>
</tbody>
</table>
17.7 Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Input the **User Name**. Then input the **New Password** and Confirm the New Password. Click the **Apply Changes** button to save the new password.
Chapter 18 Logout

This page is used to logout from PG-9171n.

Click the Apply Change button to logout from the PG-9171n.