COMTREND

PowerGrid-9182AC

Powerline Ethernet WiFi Adapter

User Manual

261072-044

Version A1.0, April 02, 2019

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 lightening. 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
- For indoor user only
- Do NOT open the casing
- Do NOT use near water
- Do NOT insert sharp objects into the adapter's socket
- Socket maximum output is 15A

Power Specifications:

I/P : 100-125Vac, 50/60Hz, 15A

O/P : 100-125Vac, 50/60Hz, 15A

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Caution: Exposure to Radio Frequency Radiation.

1. To comply with the Canadian RF exposure compliance requirements, this device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.
2. To comply with RSS 102 RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Attention: exposition au rayonnement radiofréquence.

1. Pour se conformer aux exigences de conformité RF canadienne l'exposition, cet appareil et son antenne ne doivent pas être co-localisés ou fonctionnant en conjonction avec une autre antenne ou transmetteur.
2. Pour se conformer aux exigences de conformité CNR 102 RF exposition, une distance de séparation d'au moins 20 cm doit être maintenue entre l'antenne de cet appareil et toutes les personnes.

Operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
La bande 5 150-5 250 MHz est réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Copyright

Copyright©2019 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.

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.

CATALOG

The setup images used in this manual are for reference only. The contents of these images may vary according to firmware version. The official image contents are based on the newest firmware version.

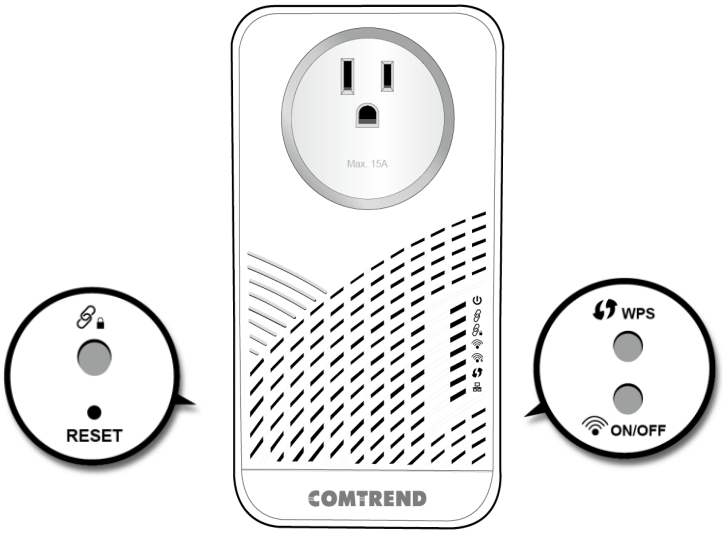
Chapter 1 Product Information

1.1 Front Panel and LED indicators

LED	Color	Mode	Description
Power LED	**Green**	On	The Adapter is powered on.
	Off	Off	The Adapter is powered off or faulty.
Connection LED	**Green**	On	The current connection (line rate) is more than 40Mbps.
	Orange	On	The current connection (line rate) is between 5Mbps and 40Mbps.
	Red	On	The current connection (line rate) is less than 5Mbps.
	Off	Off	An Adapter connection does not exist.
Security LED	**Green**	On	The Adapter is secure (it has received or generated network keys).
		Blinking	The Adapter is in the process of being secure.
	Off	Off	The Adapter is not secure.
2.4GHz LED	**Green**	On	2.4GHz WLAN is on.
	Off	Off	2.4GHz WLAN is off.
5GHz LED	**Green**	On	5GHz WLAN is on.
	Off	Off	5GHz WLAN is off.
WPS LED	**Green**	On	WPS is enabled.
	Green	Blinking	A WPS connection is in process.
	Off	Off	WPS is not enabled.

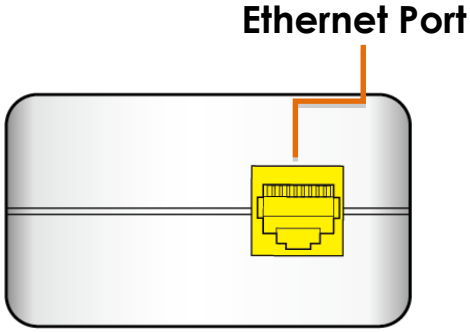
Etherent LED	**Green**	On	An Ethernet LAN connection is established.
		Blinking	Data over the Ethernet LAN connection is being transmitted.
	Off	Off	An Ethernet LAN connection is not established.

1.2 Side Panels



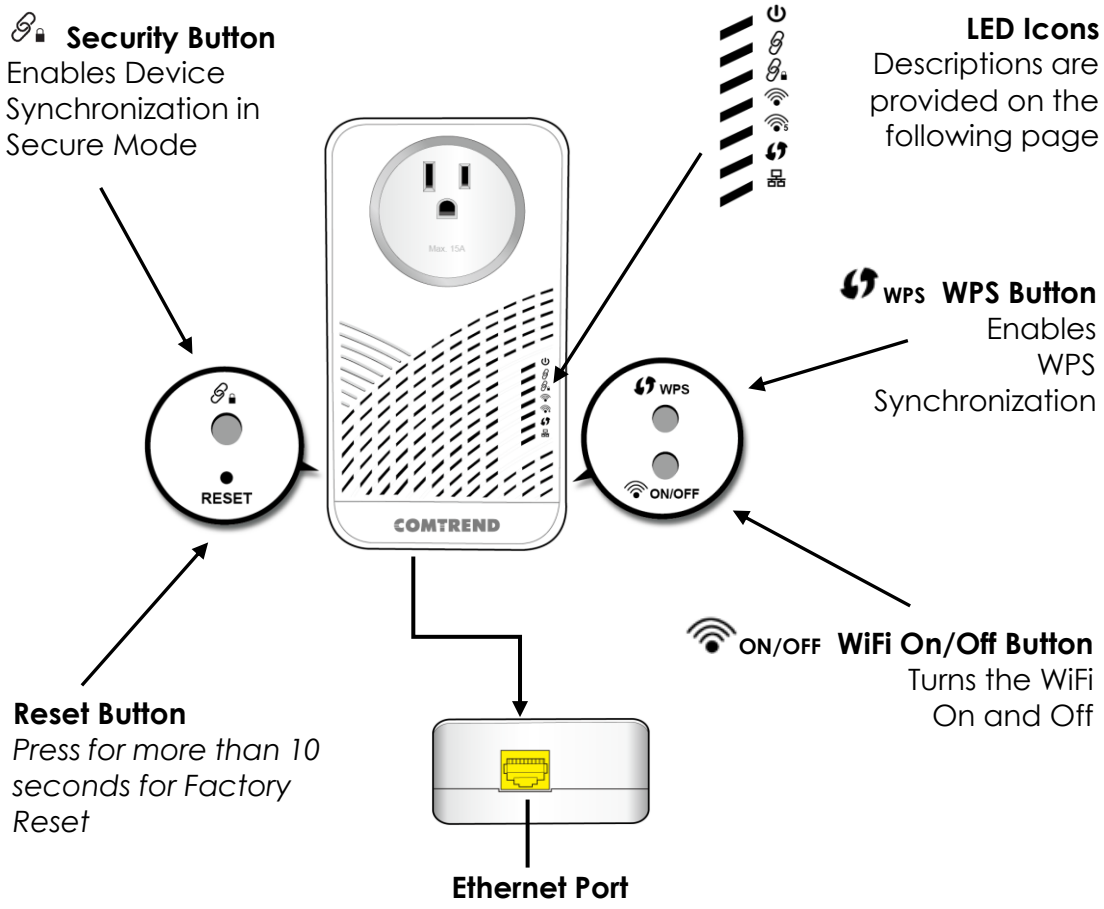
Item Name	Description
Security	Push the button for 2-5 seconds to securely synchronize the devices (i.e. both devices will get a random domain name and password).
Reset	Press more than 10 seconds (until all four LED's are ON) and release: a factory reset is performed.
WPS	Press and hold the **WPS Button** for more than 2 seconds on the PG-9182AC to activate its WPS.
ON/OFF	Push the button for 2-5 seconds to enable/disable the WiFi.

1.3 Bottom Panel



1.4 Quick Install Guide

A Understanding Your Powerline Adapter



LED	Color	Mode	Description
Power LED	**Green**	On	The Adapter is powered on.
	Off	Off	The Adapter is powered off or faulty.
Connection LED	**Green**	On	The current connection (line rate) is more than 40Mbps.
	Orange	On	The current connection (line rate) is between 5Mbps and 40Mbps.
	Red	On	The current connection (line rate) is less than 5Mbps.
	Off	Off	An Adapter connection does not exist.
Security LED	**Green**	On	The Adapter is secure (it has received or generated network keys).
		Blinking	The Adapter is in the process of being secure.
	Off	Off	The Adapter is not secure.
2.4GHz LED	**Green**	On	2.4GHz WLAN is on.
	Off	Off	2.4GHz WLAN is off.
5GHz LED	**Green**	On	5GHz WLAN is on.
	Off	Off	5GHz WLAN is off.
WPS LED	**Green**	On	WPS is enabled.
	Green	Blinking	A WPS connection is in process.
	Off	Off	WPS is not enabled.
Etherent LED	**Green**	On	An Ethernet LAN connection is established.
		Blinking	Data over the Ethernet LAN connection is being transmitted.
	Off	Off	An Ethernet LAN connection is not established.

B

Initial Powerline Adapter Setup

NOTE: A minimum of <u>two</u> G.hn Powerline Adapters are required. We suggest using the PG-9182AC as the primary Adapter that connects to your Network Device (Modem, Router, Access Point).

→ If you are setting up a G.hn Powerline network for the first time, then follow the below steps starting at Step 1.

→ If you are adding to an existing G.hn Powerline network, then skip to Steps 3-4.

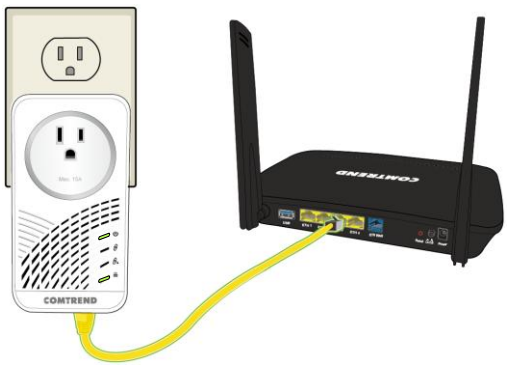
1. Plug the PG-9182PT* Powerline Adapter into a power outlet near your Network Device (Modem, Router, or Access Point).

   *We suggest using a PG-9182AC as the primary Adapter that connects to your Network Device, however, you can use any G.hn Powerline Adapter.

PG-9182PT

For maximum performance, please plug the Powerline Adapter directly into the wall outlet. Do not plug into a power strip or surge protector, as network performance could degrade significantly.

2. Connect the PG-9182AC to your Network Device (Modem, Router, or Access Point) with an Ethernet (RJ-45) cable. Wait 10 seconds for the **Ethernet LED** to light up **GREEN**, which indicates a connection is established. A flashing **GREEN** light indicates that the device is sending data.

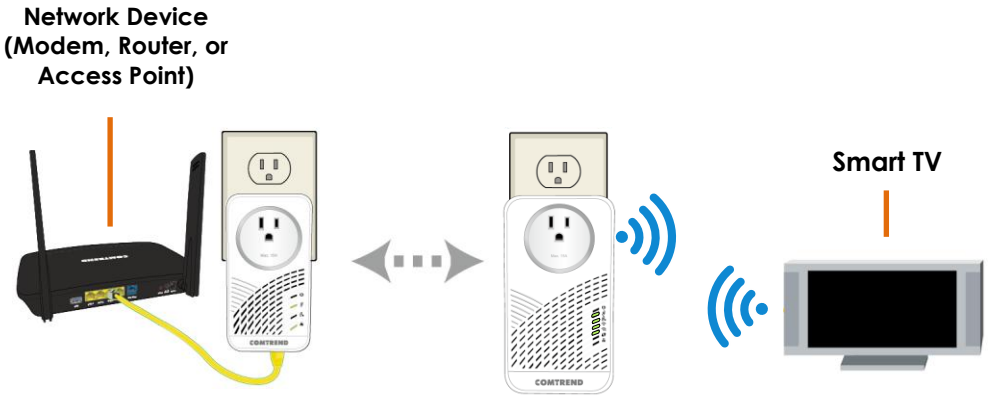


3. Plug the PG-9182AC Powerline Adapter into a power outlet near the location you want to add Wireless.

PG-9182AC

C Pairing the Powerline Adapters

4. Press the **Security Button** on one Adapter until you see the **Security LED** start blinking **GREEN**. Then press the **Security Button** on the other Adapter until you see the **Security LED** start blinking **GREEN**. The **Security LED** and the **Connection LED** should be solid **GREEN** on both Adapters when they are successfully paired.



Note: If you are adding to an existing G.hn Powerline network, then press the **Security Button** on any Adapter in the existing G.hn Powerline network until you see the **Security LED** start blinking **GREEN**. Repeat this on the Powerline Adapter you are adding. The **Security LED** and the **Connection LED** will light up **GREEN** on all adapters within the G.hn Powerline network.

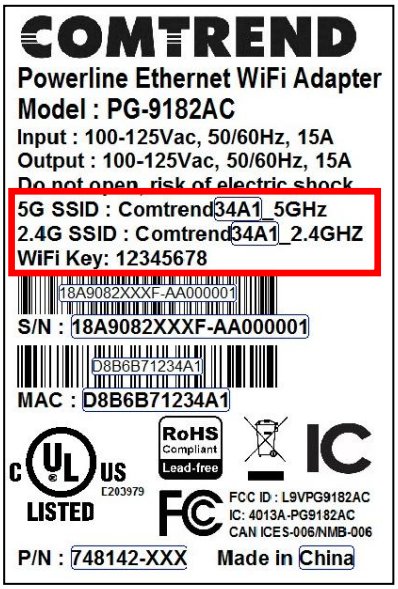
5. Repeat Steps 3 to 4 to add additional Powerline Adapters. Please note that up to 16 devices can be connected within a Powerline G.hn Network.

D Connect Your WiFi Devices to the New PG-9182AC Access Point

Note: The WiFi network behavior can vary based on different deployment scenarios. If WifiXtend™ or HARMONY technologies are being utilized, then the WiFi network will automatically become a single network with one SSID and Password per band. This occurs when there are two or more PG-9182AC adapters being used/when the Gateway is a WifiXtend™ or HARMONY enabled Comtrend Gateway.

6. For some devices (E.g. laptops, cameras, set-top-boxes, etc.) Wireless connectivity can be done via WPS (Wireless Protected Setup). WPS allows you to simply connect devices to the new Access Point without entering a username/password manually. To do this, please follow the instructions in Section E below.

7. To connect your WiFi devices to your new PG-9182AC WiFi Access Point, select the PG-9182AC Access Point using your WiFi device's standard network list. The Network Name (SSID) and Password (WiFi Key) can be found on the bottom of the PG-9182AC.



8. Go to Section F.

E

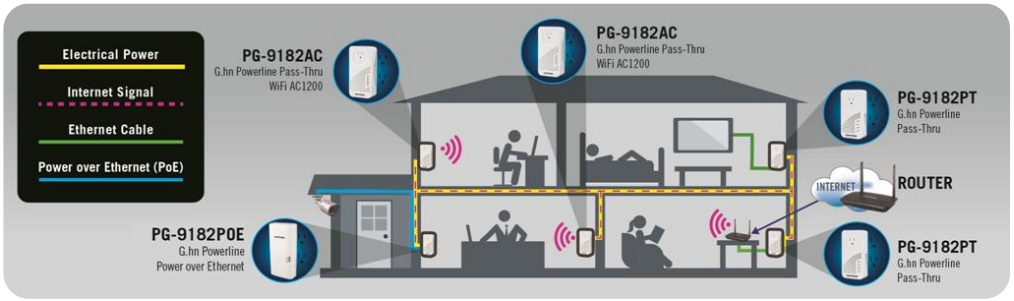
Setup of WiFi Devices via WPS (WiFi Protected Setup)

9. Press and hold the **WPS Button** for more than 2 seconds on the PG-9182AC to activate its WPS. The PG-9182AC's **WPS LED** should blink **GREEN** to indicate a WPS connection is in progress.

10. Within two minutes, press the **WPS Button** (often the WPS/Reset Button) on your remote Internet-Enabled Devices to activate WPS.
11. The devices will establish a secure WiFi connection.

F

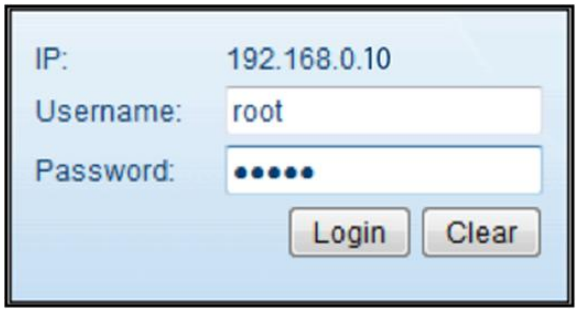
You Have Succesfully Set Up Your G.hn Powerline Adapter with WiFi!



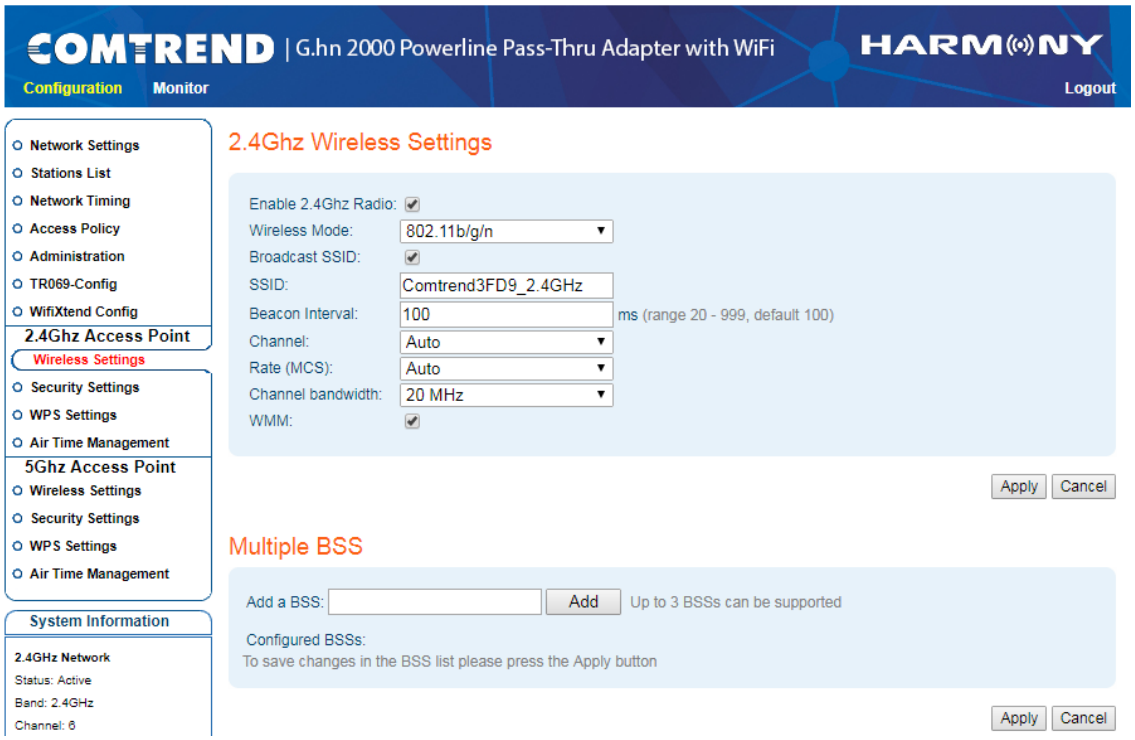
Creating a Custom SSID & Password

12. If you would like a different SSID and Password than what is provided, you will need to change it via the Web management interface. Start your Web browser and input "192.168.0.10" in the address bar. Then press the "Enter" key.

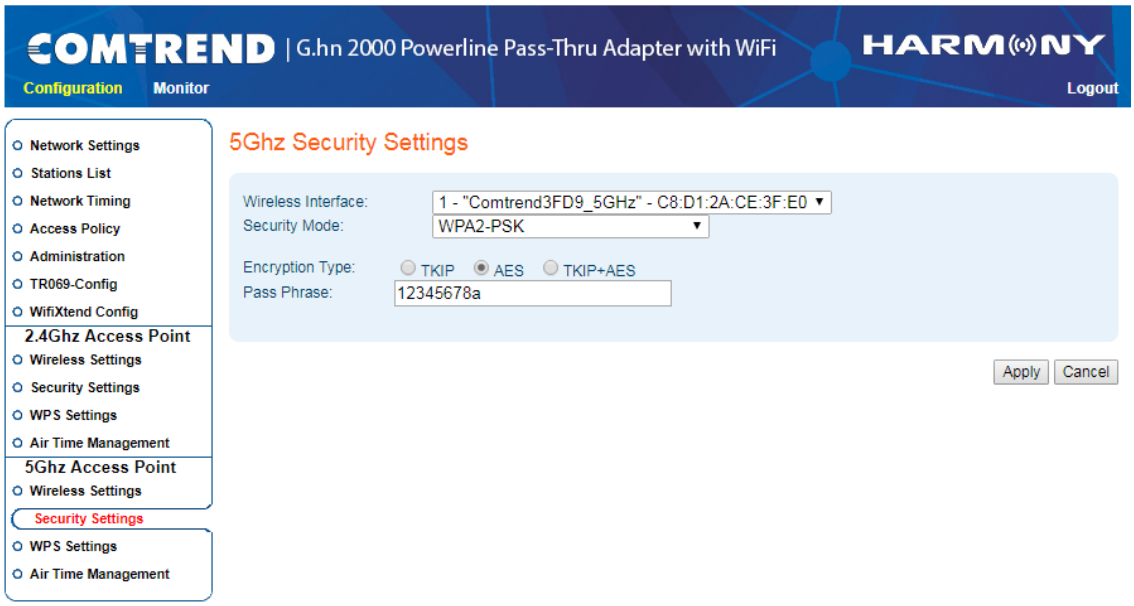
13. You will then see the following displayed. Input the Username "**root**" and default password "**12345**". Then press the Login button to view the Web management interface.



14. Press the "Wireless Settings" section in the left-hand sidebar. Here you can adjust the SSID for the two Wireless bands.



15. Press the "Security Settings" section to adjust the Wireless security settings for the wireless bands.



H

Troubleshooting

The following information should help you diagnose basic set up or installation problems.

Connection LED is OFF: The **Connection LED** shows that the Powerline Adapter is connected to the G.hn Network. If the indicator is off, then plug both Powerline Adapters that you are attempting to pair into power outlets that are located within the same room. The **Connection LED** should light up **GREEN**. If not, then press the **Reset Button** on each adapter for more than 10 seconds. Afterwards, you can plug the units back into their original location.

Ethernet LED is OFF: If the **Ethernet LED** fails to light up, check that the LAN port of the Powerline Adapter is connected firmly to the LAN port of the other device. To check the condition of the Ethernet cable, use another cable to test the same connection.

Security LED is OFF: If the **Security LED** is off, then it means the Powerline Adapter is not securely paired. Press the **Security Button** on the Powerline Adapter for 3 seconds until you see the **Security LED** start flashing **GREEN**. Repeat this on the other Powerline Adapter. The **Security LED** and the **Connection LED** will light up **GREEN** on both adapters. This means the adapters are now securely paired and have a strong connection.

2.4GHz LED /5GHz LED is OFF: If the **2.4GHz LED/5GHz LED** are off, then it means the WiFi is not enabled. You can turn on both indicators, (i.e. enable WiFi) by pressing the **WiFi Button** ON/OFF on the side of the device. You can also login to the PG-9182AC Web Interface to enable the WiFi. Please refer to the User Manual for additional details.

To join an existing G.hn Powerline network, press the **Security Button** on any Powerline Adapter in the existing G.hn Powerline network for 3 seconds until you see the **Security LED** start flashing **GREEN**. Then press the **Security Button** on the ***additional*** Powerline Adapter. The **Security LED** and the **Connection LED** will light up **GREEN** on both adapters.

*If you have tried the above and are still experiencing problems, you can reset all devices to factory default by pushing the **Reset Button** for more than 10 seconds (until all the LEDs of the device blink).

1.5 System Requirements

- Computer or network devices with wired or wireless network interface card.
- Any connected devices must feature a network port.
- Web browser (Microsoft Internet Explorer 4.0 or above, Google Chrome web browser, Opera web browser, or Safari web browser).

Chapter 2: System and Network Setup

2.1 Connecting to power line access point by web browser

PG-9182AC supports two kinds of management IP simultaneously.

(1) DHCP client, which gets dynamic IP address from Modem/Broadband Router/Home Gateway.

(2) Static IP, **192.168.0.10** by default, which can be configurable in web UI.

Before you can connect to the power line access point and start configuration procedures, your computer must be able to get an IP address automatically (dynamic IP address). PG-9182AC gets dynamic IP address from Modem/Broadband Router/Home Gateway that it is connected to by default. However, the current IP info of PG-9182AC would be displayed at Modem/Broadcom Router/Home Gateway.

On other side, Static IP of PG-9182AC can be accessed. The default static IP address of PG-9182AC is 192.168.0.10, subnet mask 255.255.255.0. Please use static IP address 192.168.0.100, subnet mask 255.255.255.0 for accessing web UI management.

2.2 Connecting to Web Management Interface

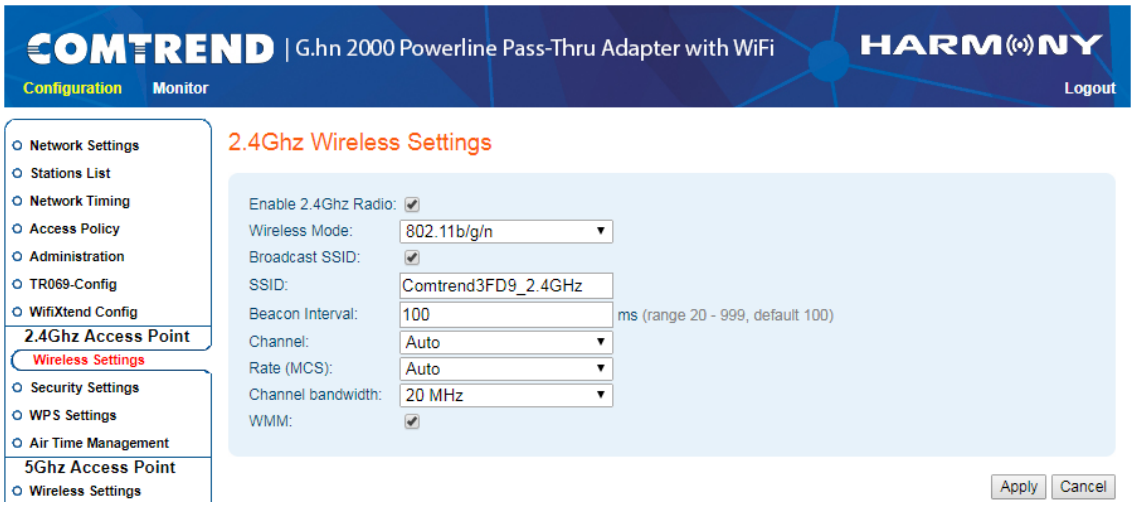
All functions and settings of WiFi AP of PG-9182AC must be configured via web management interface. Please start your web browser, and input '192.168.0.10' in the address bar, then click the 'Enter' key. The following window will pop up:

Please input user name and password in the field respectively, default user name is '**root**', and default password is '**12345**', then click 'OK' button, and you can see the web management interface of this access point:

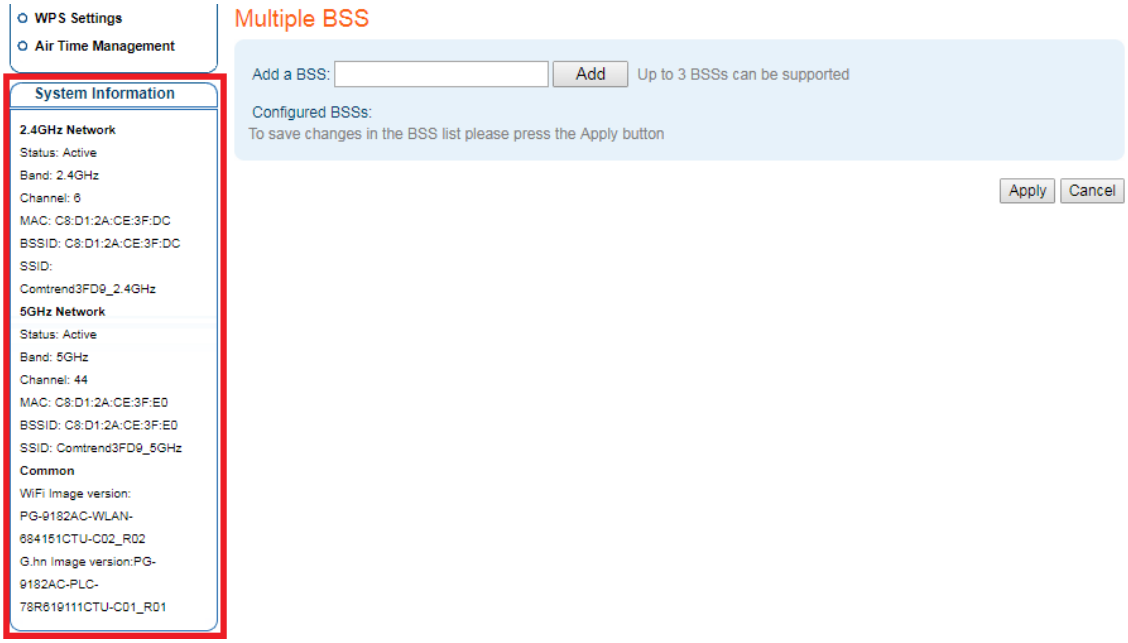
NOTE: If you can't see the web management interface, and you're being prompted to input user name and password again, it means you didn't input username and password correctly. Please retype user name and password again. If you're certain about the user name and password you type are correct, please go to 2.8 Administration, to perform a factory reset or to set the password back to the default value.

2.3 View System Information

The page will be displayed after login:



The system information is on the left-side corner of the web page.



Here are descriptions of every item:

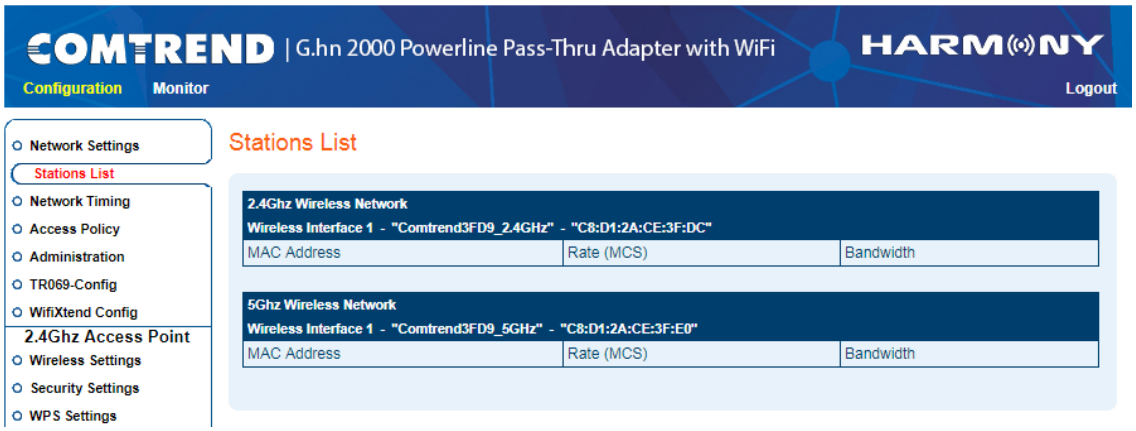
2.4GHz Network	*Displays 2.4GHz AP status, Channel, SSID string and BSSID.*
5GHz Network	*Displays Firmware version of Wireless. This information is helpful when you need online help from the dealer of purchase.*
Common	*WiFi and G.hn Image version information.* *WiFi Image version:* PG-9182AC-WLAN-684151CTU-C02_R02 *G.hn Image version:* PG-9182AC-PLC-78R619111CTU-C01_R01

2.4 Network Settings

The static IP for local management. Click "Apply" will reboot system for new modifications activation.

2.5 Station List

This is page shows the information of wireless Stations that are connected to PG-9182AC.



Here are descriptions of every item:

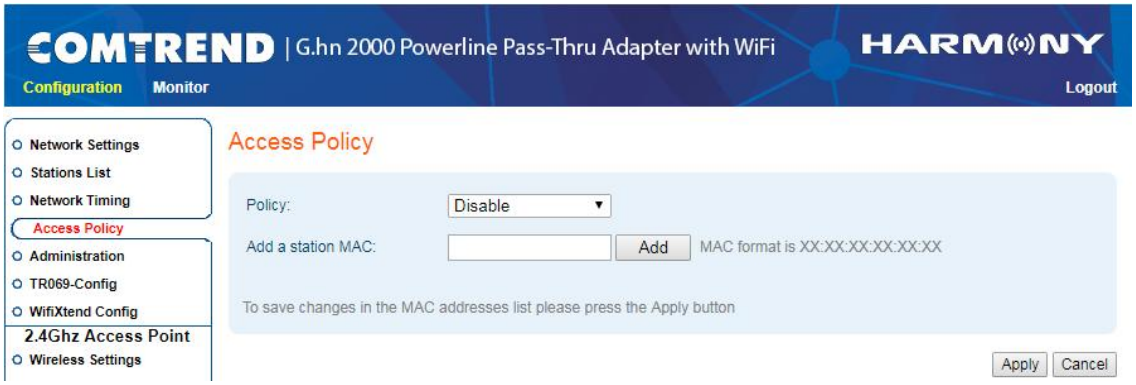
MAC address	This option will disable your Wireless station connecting to PG-9182AC at 2.4G or 5GHz Interface.
Rate (MCS)	MCS# on wireless interface with the station.
Bandwidth	Bandwidth, 20/40MHz for 2.4GHz, 20/40/80MHz for 5GHz.

2.6 Time Settings

This page is used to set the local time zone for TR069 management; in the current version local time zone is not configurable through web UI.

The current setting is (GMT-8, U.S).

2.7 Access Policy



Here are descriptions of every item:

Policy:	This option will allow/reject the list of wireless stations.
Add a station MAC	MAC format is XX:XX:XX:XX:XX:XX

A maximum 32 entries can be configured.

To save changes in the MAC addresses list please click the Apply button.

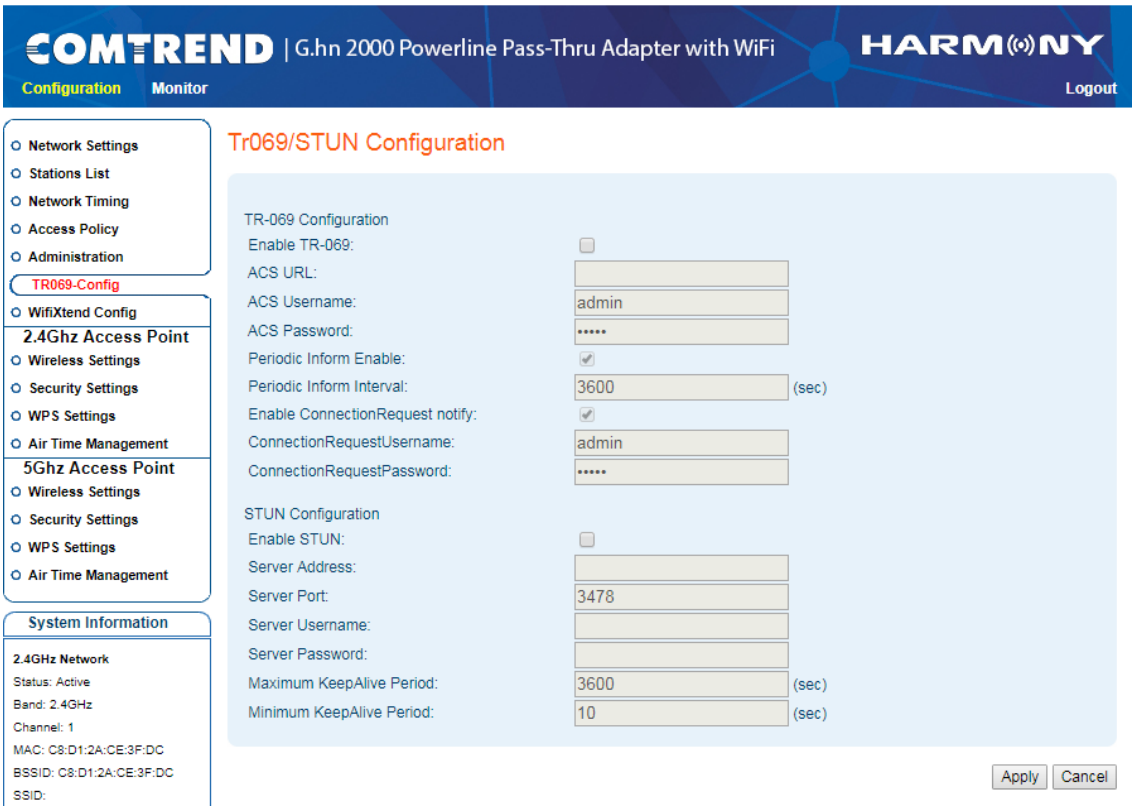
2.8 Administration

Here are descriptions of every setup item:

Software Upgrade	Select the firmware file of WiFi AP of PG-9182AC at the local driver of the laptop. The PG-9182AC is supporting a single TR069 entity for both WiFi and G.hn PLC.
Components Versions	Wi-Fi Image version: PG-9182AC-WLAN-684151CTU-C02_R02 G.hn Image version: PG-9182AC-PLC-78R619111CTU-C01_R01
Change Password	Click the Change Password button to change the web login password.
Download Log Files	Reserved for debugging purpose.
Restore Defaults	Factory reset of the PG-9182AC (WiFi & G.hn PLC)
System Reboot	System reboot by software.

2.9 TR069/STUN Configuration

This page allows the user to configure the settings for this CPE to communicate with ACS for management.



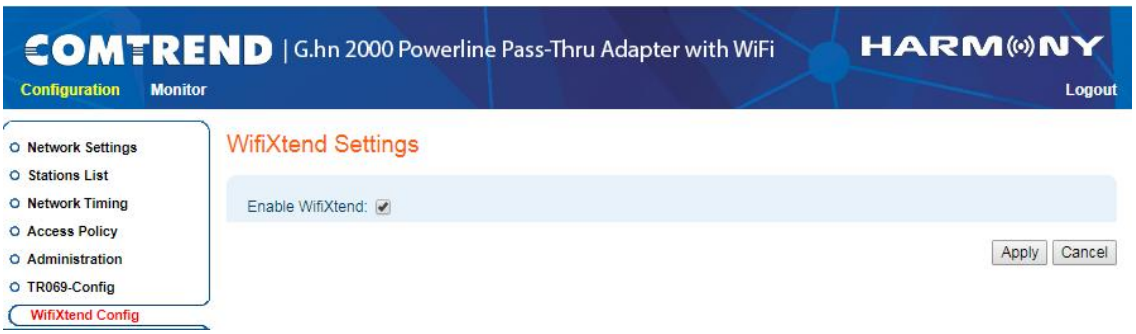
Here are descriptions of every setup item:

TR-069 Configuration	
Enable TR-069	Tick the checkbox to enable
ACS URL	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.
ACS Username	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.
ACS Password	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.
Periodic Inform Enable	When set to YES, the modem should periodically send information to the ACS using the Inform method call.
Periodic Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS.
Enable Connection Request notify	Tick the checkbox to enable.

Connection Request Username	Username used to authenticate an ACS making a Connection Request to the modem.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the modem.
STUN Configuration	
Enable STUN	Tick the checkbox to enable
Server Address	Host name or IP address of the STUN server to send Binding Requests if STUN is enabled via STUN_ENABLE parameter. If is an empty string and STUN_ENABLE is YES, the modem should use the address of the ACS extracted from the host portion of the ACS URL.
Server Port	Port number of the STUN server to send Binding Requests if STUN is enabled via STUN_ENABLE. By default, this should be equal to the default STUN port, 3478.
Server Username	If it is not an empty string, the value of the STUN USERNAME attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server).If it is an empty string, the modem will not send STUN Binding Requests with message integrity.
Server Password	The value of the STUN Password to be used in computing the MESSAGE-INTEGRITY attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server).
Maximum KeepAlive Period	If STUN is enabled, the maximum period, in seconds, that STUN Binding Requests must be sent for the purpose of maintaining the binding in the Gateway. This applies specifically to Binding Requests sent from the UDP Connection Request address and port. A value of -1 indicates that no maximum period is specified.
Minimum KeepAlive Period	If STUN is enabled, the minimum period, in seconds, that STUN Binding Requests can be sent for the purpose of maintaining the binding in the Gateway. This limit applies only to Binding Requests sent from the UDP Connection Request address and port, and only those that do not contain the BINDING-CHANGE attribute. This limit does not apply to retransmissions following the procedures defined in [RFC3489].

2.10 WiFiXtend Config

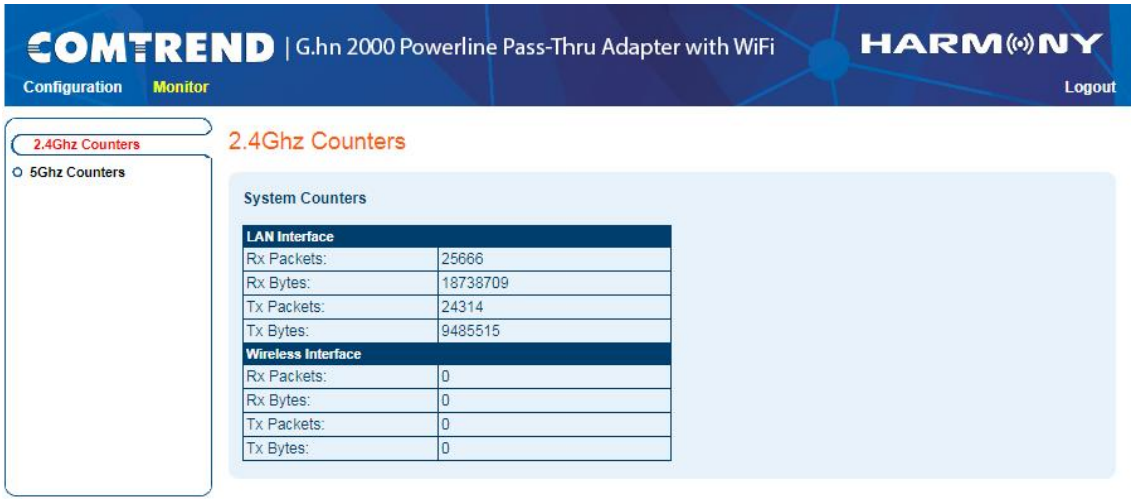
WifiXtend allows one or more Access Points to be deployed without configuration.

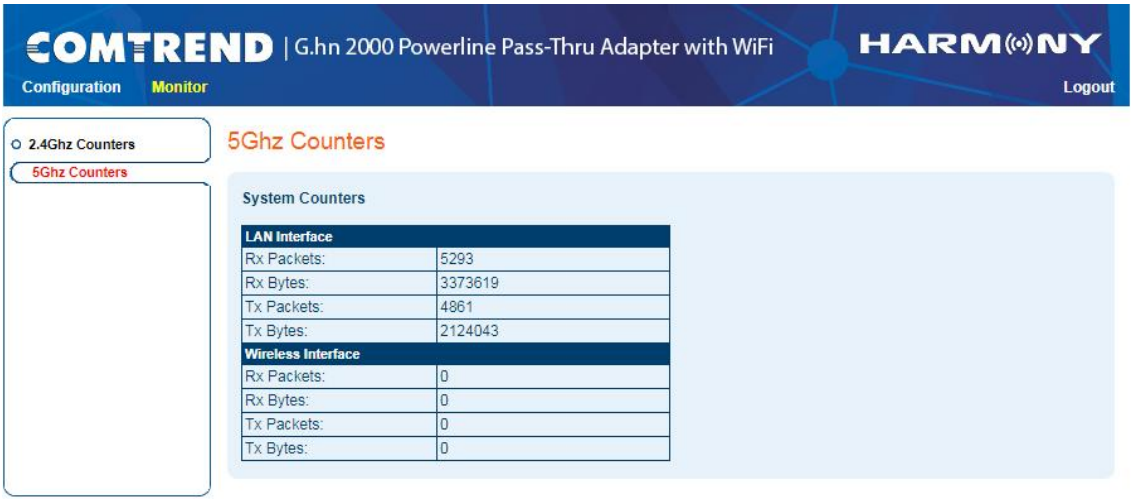


Tick the checkbox to enable.

2.11 Monitor

Monitor is to show the statistics on LAN, 2.4G & 5G interfaces.





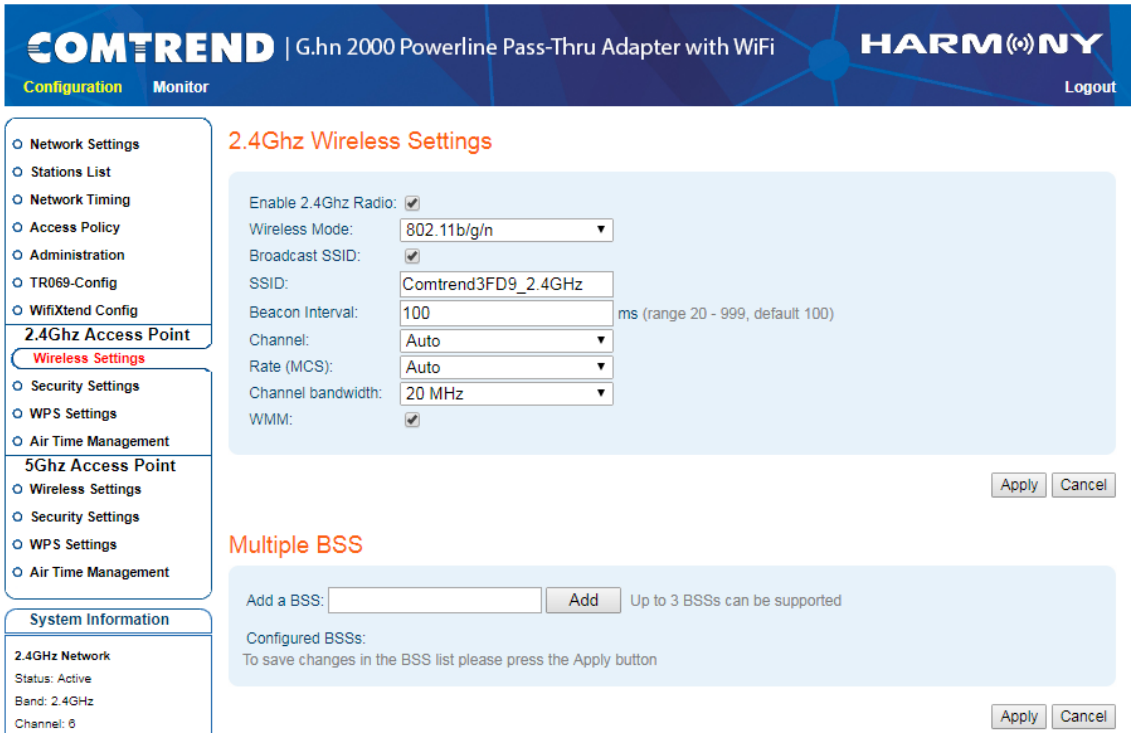
2.12 Logout

Log out of web management.

Chapter 3: Wireless Configurations

3.1 2.4G Wireless Settings

This page is to configure basic setting for 2.4GHz interface of access point.



Here are descriptions of every setup item:

Enable 2.4Ghz Radio	Ticked is enabling 2.4GHz radio.
Wireless Mode	802.11b/g legacy: auto selection of 802.11b/g. 902.11b/g/n: auto selection of 802.11b/g/n
Broadcast SSID	Decide if the wireless power line access point will broadcast its own SSID or not. You can hide the SSID of your wireless power line access point (set the option to 'Disable'), so only people those who know the SSID of your wireless power line access point can get connected.
SSID	Please input the SSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **PLEASE NOTE THAT ESSID IS CASE SENSITIVE.**
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 20 – 999. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Channel	Auto or manually select any channel from 1-13.
Rate	Modulation and Coding Scheme. It's safe to select Auto and it's not necessary to change unless you know the effect.

Channel Bandwidth	Select wireless channel width (bandwidth taken by wireless signals of this access point). It's suggested to select Auto for 'Auto 20/40MHz' & '20 MHz' only.
WMM	WMM (Wi-Fi Multimedia) technology, which can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When you enable WMM function, the power line access point will define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.
Multiple BSS	Two more SSID are required.

3.2 2.4G Security Settings

This page allows you to configure the Security Settings for 2.4Ghz interface of the access point.

Here are descriptions of every setup item:

Security Mode	Select the encryption supported over wireless access. The encryption method can be None, WPA-PSK, WPA2-PSK or WPA-PSK+WPA2-PSK.
Encryption Type	There are three types of Cipher :TKIP, AES, TKIP+AES
Passphase	8 to 63 alphanumerical characters

3.3 2.4G WPS Settings

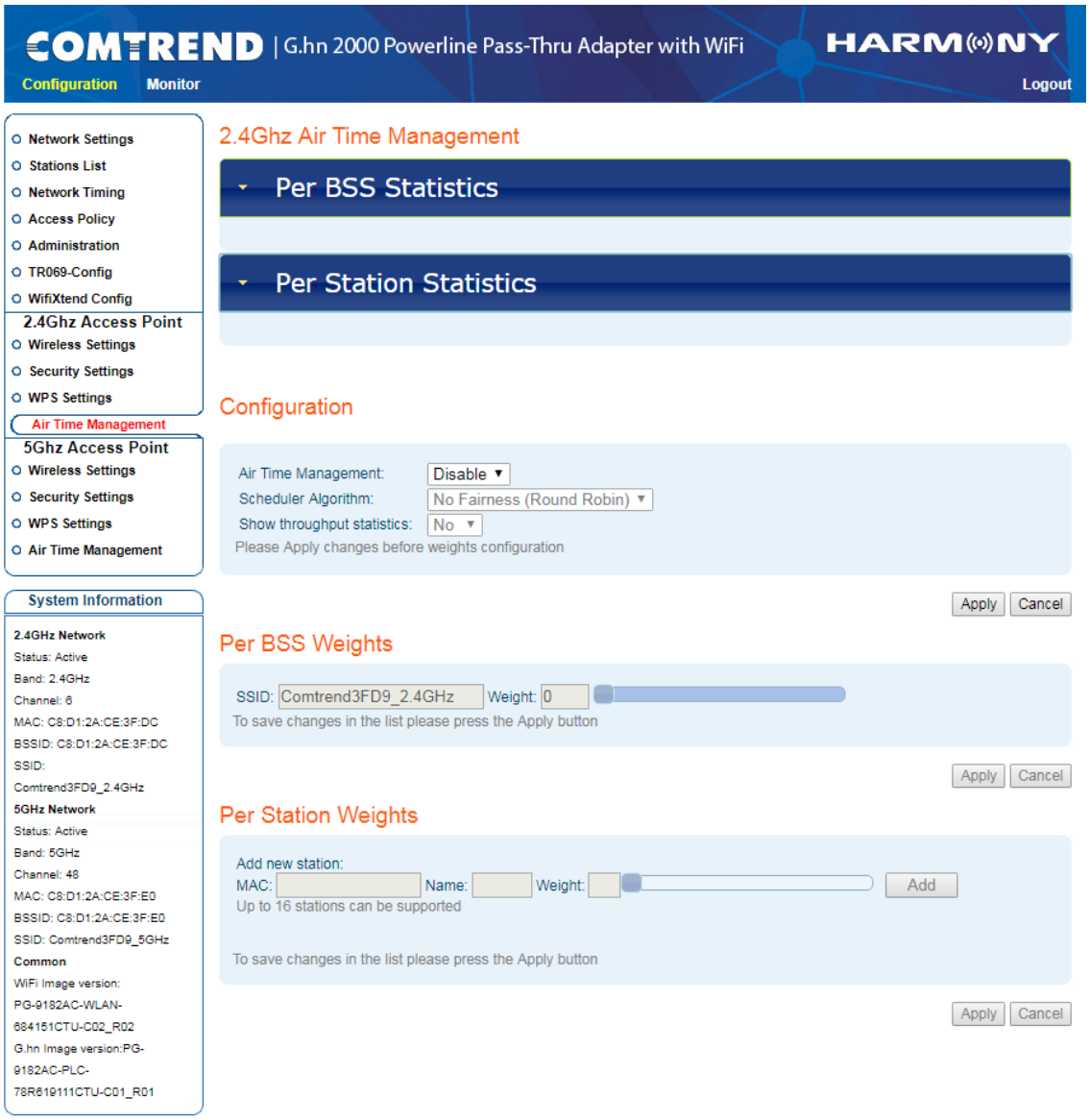
This page allows you to configure the WPS Settings for 2.4Ghz interface of the access point.
Wi-Fi Protected Setup allows that each time you want to set up a connection, there is no need to select the encryption mode and enter the encryption password.

Heading	Description
WPS	Select to Enable/Disable WPS from the drop-down menu. Then click the **Apply** button to implement your selection.
Configure Enrollee	Click 'Activating WPS' to start the Push-Button style WPS setup procedure. This Wireless AP will wait for WPS requests from wireless clients.
WPS Status	Shows the current WPS status.

Click the **Activating WPS** button to confirm your choice.

3.4 2.4G Air Time Management

This page allows you to configure the setting for Air Time Management of the 2.4GHz Access Point.



Configuration

Heading	Description
Air Time Management	Select to Enable/Disable Air Time Management from the drop-down menu.
Scheduler Algorithm	Select to No Fairness(Round Robin)/Fairness/Weighted Fairness Scheduler Algorithm from the drop-down menu. No Fairness(Round Robin): The order will decide the transmission, so the longer the device is connected, the longer the wait time. Fairness: Each device occupies the same transmission time. Weighted Fairness: According to the Weight you give to decide the priority of transmission.
Show Throughput statistics	Select to YES/NO to Show Throughput Statistics.

Per BSS Weights

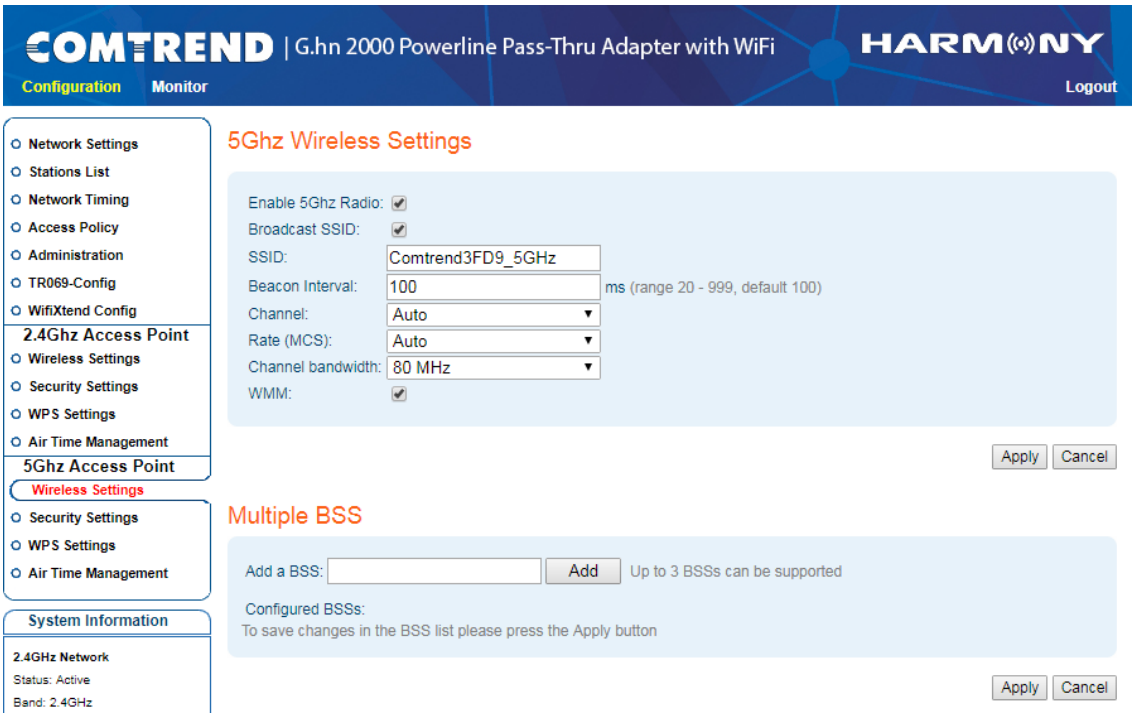
Heading	Description
SSID	Please input the SSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **PLEASE NOTE THAT THE ESSID IS CASE SENSITIVE.**
Weight	Set the Weights for Station from 0 to 100 by scrolling the scroll or Input the number.

Per Station Weights

Heading	Description
MAC	Input the MAC address from the device which you want to add on.
Name	Input an ID for the station (Not supported on this release)
Weight	Set the Weights for Station from 0 to 100 by scrolling the scroll or Input the number.

3.5 5G Wireless Settings

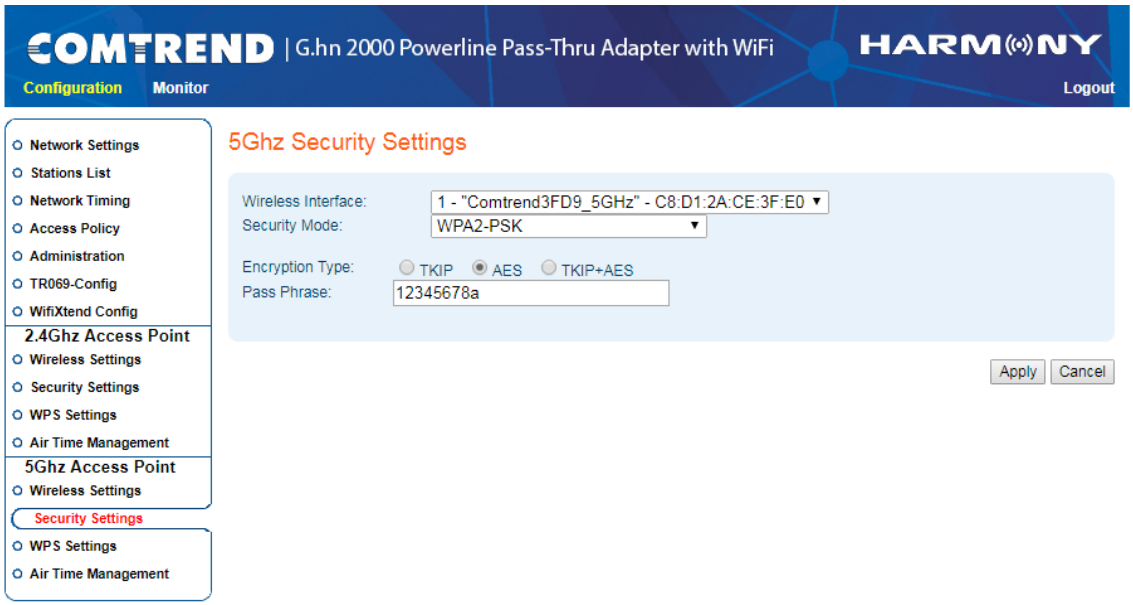
This page is to configure basic setting for 5GHz interface of access point.



Here are descriptions of every setup item:

Enable 5Ghz Radio	Ticked is enabling 5GHz radio.
Broadcast SSID	Decide if the wireless power line access point will broadcast its own SSID or not. You can hide the SSID of your wireless power line access point (set the option to 'Disable'), so only people those who know the SSID of your wireless power line access point can get connected.
SSID	Please input the SSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **PLEASE NOTE THAT ESSID IS CASE SENSITIVE.**
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 20 – 999. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Channel	Auto, Or manually select either of channel
Rate (MCS)	MCS# on wireless interface with the station.
Channel Bandwidth	Select wireless channel width (bandwidth taken by wireless signals of this access point). It's suggested to select for '20MHz', 40MHz, and 'Auto' (20/40/80MHz).
WMM	WMM (Wi-Fi Multimedia) technology, which can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When you enable WMM function, the power line access point will define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.
Multiple BSS	Two more SSID are required.

3.6 5 G Security Settings



Here are descriptions of every setup item:

Security Mode	Select the encryption supported over wireless access. The encryption method can be None, WPA-PSK, WPA2-PSK or WPA-PSK+WPA2-PSK.
Encryption Type	There are three types of Cipher :TKIP, AES, TKIP+AES
Passphase	8 to 63 alphanumerical characters

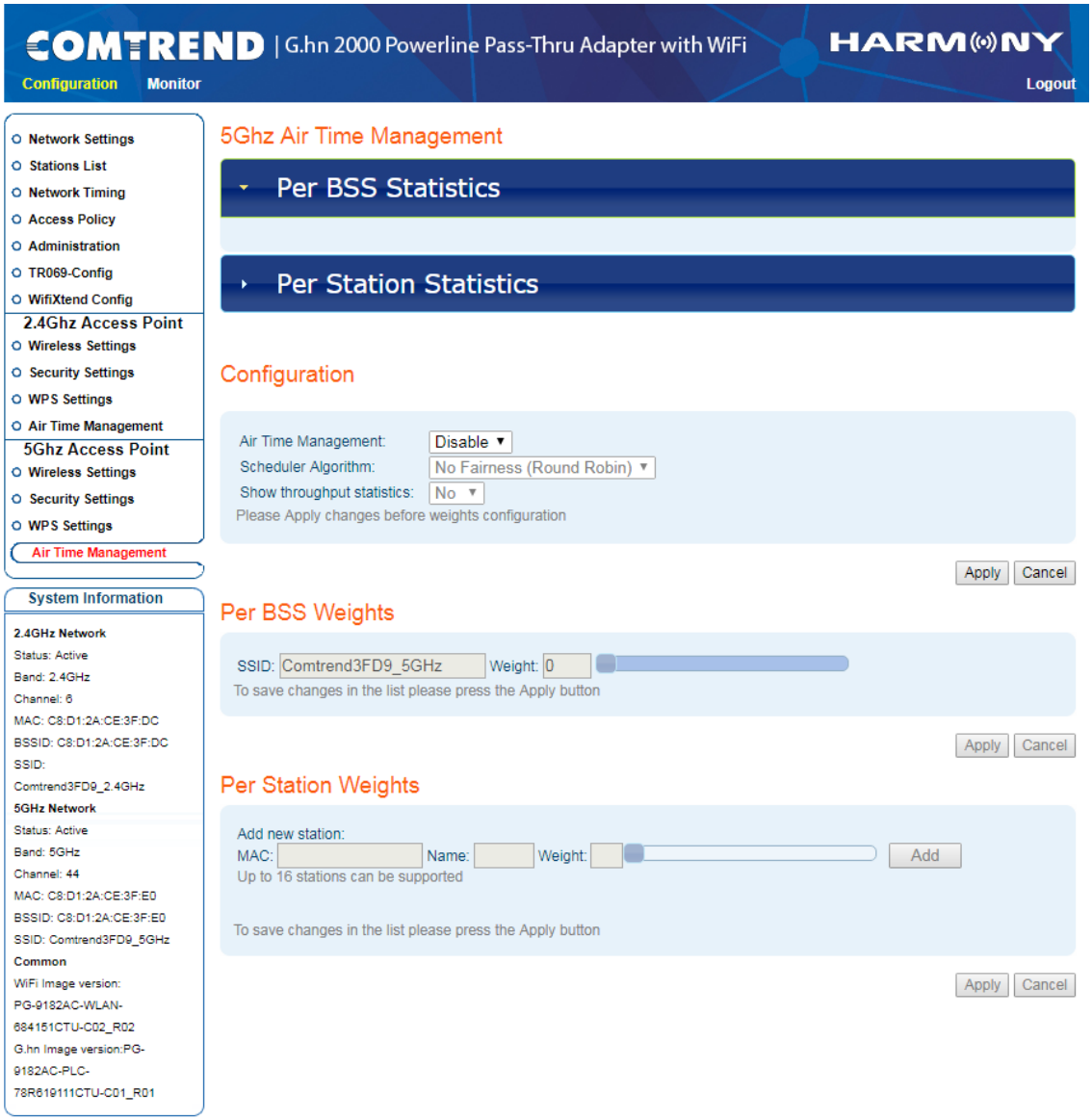
3.7 5G WPS Settings

Heading	Description
WPS	Select to Enable/Disable WPS from the drop-down menu. Then click the **Apply** button to implement your selection.
Configure Enrollee	Click 'Activating WPS' to start the Push-Button style WPS setup procedure. This Wireless AP will wait for WPS requests from wireless clients.
WPS Status	Shows the current WPS status.

Click the **Activating WPS** button to confirm your choice.

3.8 5G Air Time Management

This page allows you to configure the setting for Air Time Management of the 5GHz Access Point.



Configuration

Heading	Description
Air Time Management	Select to Enable/Disable Air Time Management from the drop-down menu.
Scheduler Algorithm	Select to No Fairness(Round Robin)/Fairness/Weighted Fairness Scheduler Algorithm from the drop-down menu. No Fairness(Round Robin): The order will decide the transmission, so the longer the device is connected, the longer the wait time. Fairness: Each device occupies the same transmission time. Weighted Fairness: According to the Weight you give to decide the priority of transmission.

Show Throughput statistics	Select to YES/NO to Show Throughput Statistics.

Per BSS Weights

Heading	Description
SSID	Please input the SSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **PLEASE NOTE THAT THE ESSID IS CASE SENSITIVE.**
Weight	Set the Weights for Station from 0 to 100 by scrolling the scroll or Input the number.

Per Station Weights

Heading	Description
MAC	Input the MAC address from the device which you want to add on.
Name	Input an ID for the station (Not supported on this release)
Weight	Set the Weights for Station from 0 to 100 by scrolling the scroll or Input the number.

PG-9182AC uses DHCP mode. It means PG-9182AC has to get IP address via DHCP server. You should check what IP address is assigned to PG-9182AC via your DHCP server and configure you PC IP address according to the IP address that was assigned to PG-9182PT.

4.1 Logging In

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

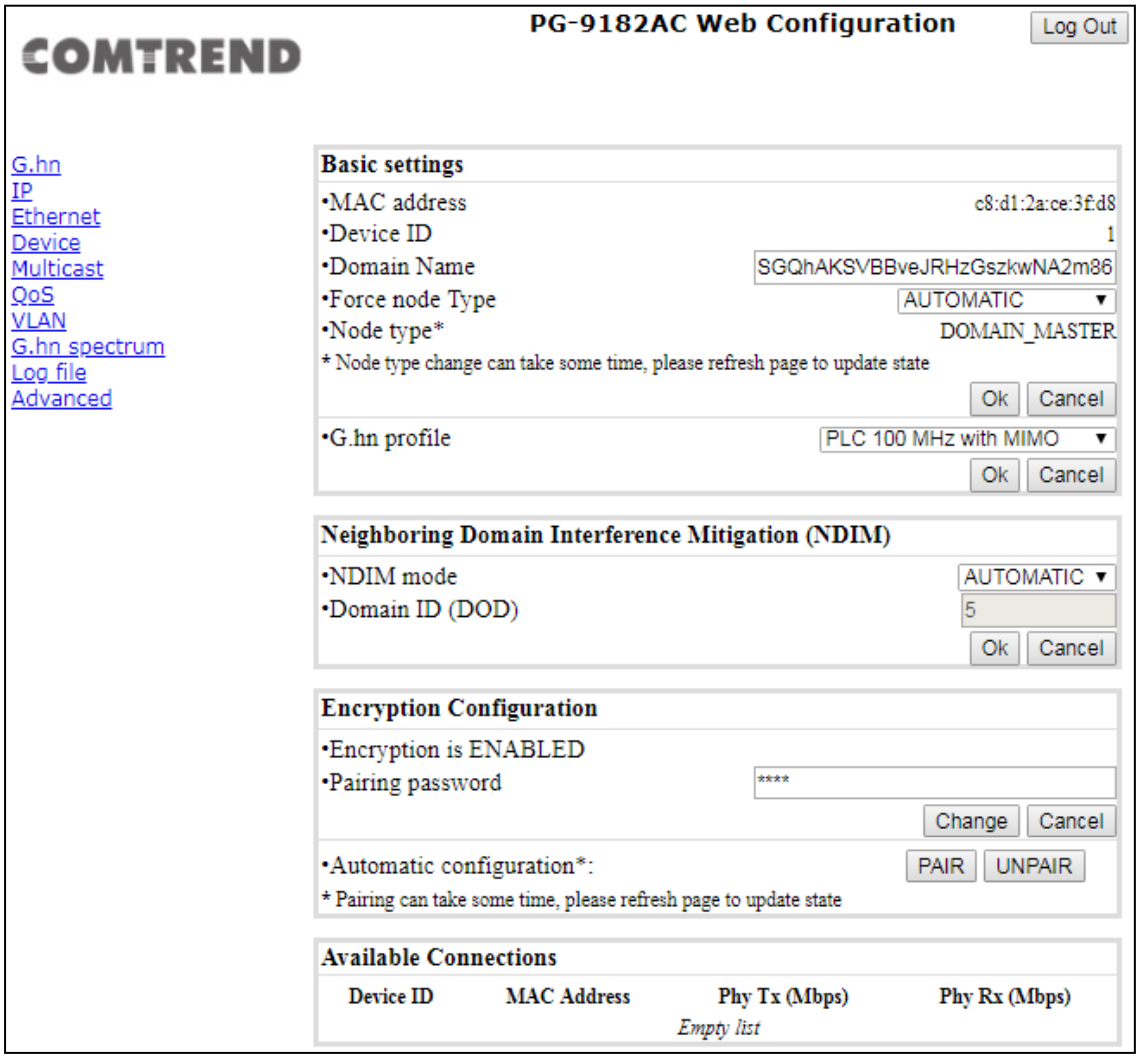
STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.0.5, type http://192.168.0.5

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

Authentication Password: **admin**

Click **OK** to continue.

Note:
The Factory Reset password is: **betera**



5.1 Basic Configuration

- **MAC Address** Displays the MAC address of the device.
- **Device ID** Device ID of this node.
- **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)
- **Node Type**
  Shows the current status of the device.
- **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).

5.2 NDIM Configuration

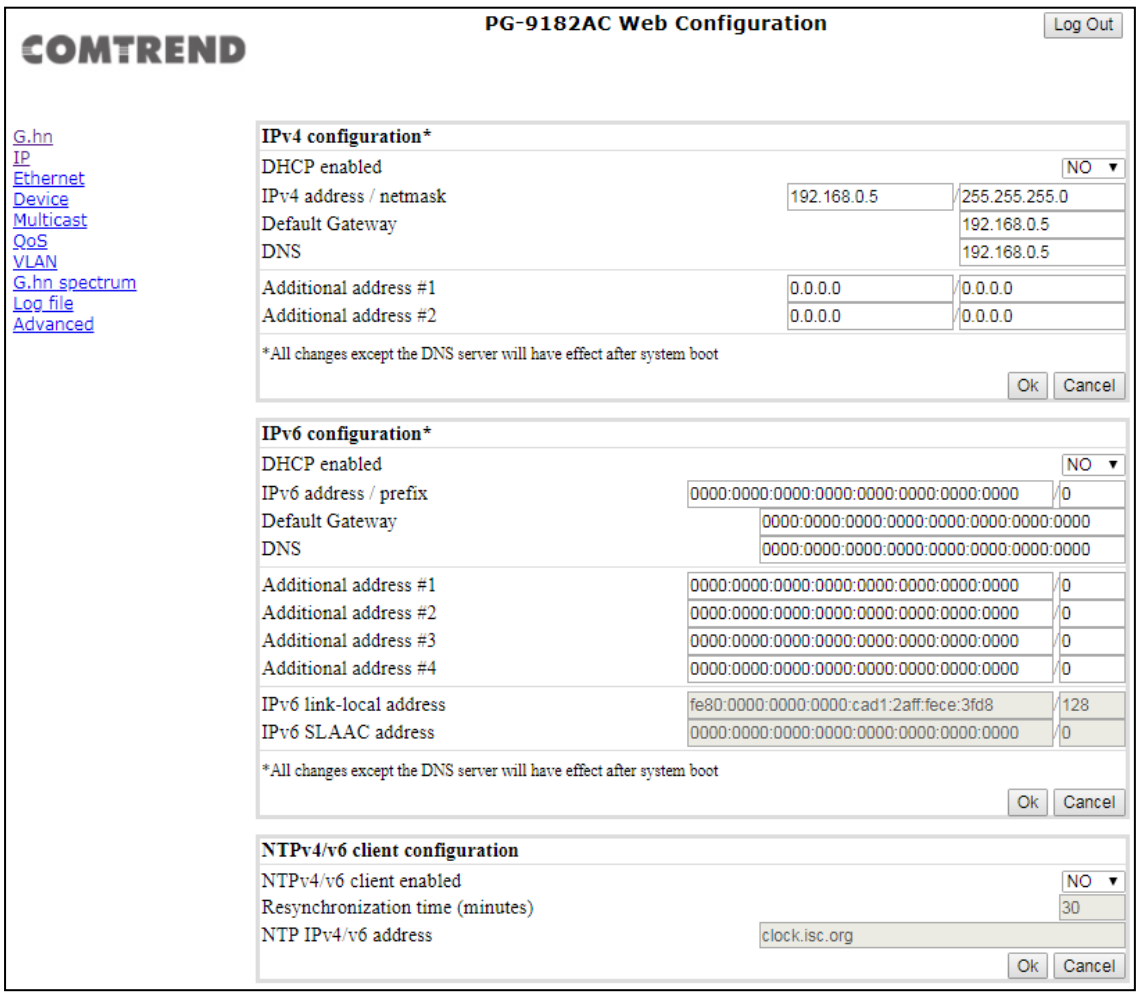
- **NDIM mode** set to Automatic for enabling automatic DOD selection functionality and set to Manual for manual configuration of DOD.
- **Domain ID (DOD)** manually set the DOD number from 1 to 15 to use a different preamble seed than the default 0.

5.3 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.



6.1 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**" IP configuration in the following parameters, the IPv4 Address, Subnet Mask, Default Gateway and DNS should be configured; fill these fields in. In the case of choosing "**YES**" they will be filled automatically when configuration is received from the DHCPv4 server.
- **IPv4 address/netmask:** IPv4 address / netmask of this device.
- **Default Gateway:** IPv4 gateway to connect the device to other LAN segments.
- **DNS:** Domain Name Server IP (IPV4).
- **Additional address #1/2**: additional fixed IPv4 addresses that will always be configured at boot time.

IPv6 subsection:

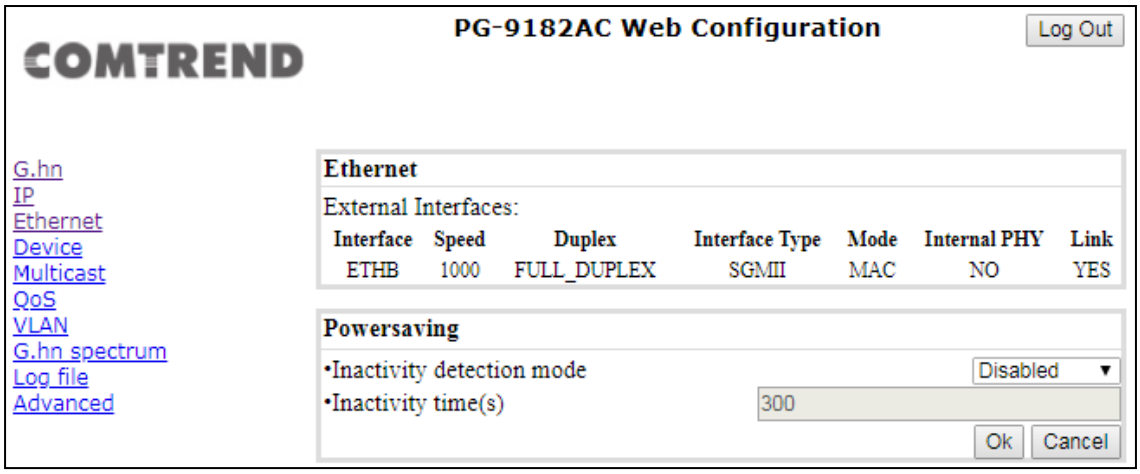
- **DCHPv6 enabled**: in the case of choosing "**NO**" IP configuration in the following parameters, the IPv6 Address, prefix, Default Gateway and DNS should be configured; fill these fields in. In the case of choosing "**YES**" they will be filled automatically when configuration is received from the DHCPv6 server.

- **IPv6 Address / prefix**: IPv6 address / prefix of the device to read the node's DHCPv6 address in case the DHCPv6 is enabled**.**
- **Default Gateway:** IPv6 gateway to connect the node to other LAN segments.
- **DNS:** Domain Name Server IP (IPV6).
- **Additional address #1/2/3/4**: additional fixed IPv6 addresses that will always be configured at boot time.
- **IPv6 Link-Local Address**: to read the node's Link Local address.
- **IPv6 SLAAC address:** IPv6 address, automatically obtained by means of the SLAAC mechanism.

NTPv4/v6 subsection:

- **NTPv4/v6 client enabled**: Enable/disable NTP client.
- **Resynchronization time**: Configure re-synchronization interval time in minutes.
- **NTP IPv4/v6 address:** Hostname or IP (IPv4 or IPv6) of NTP server.

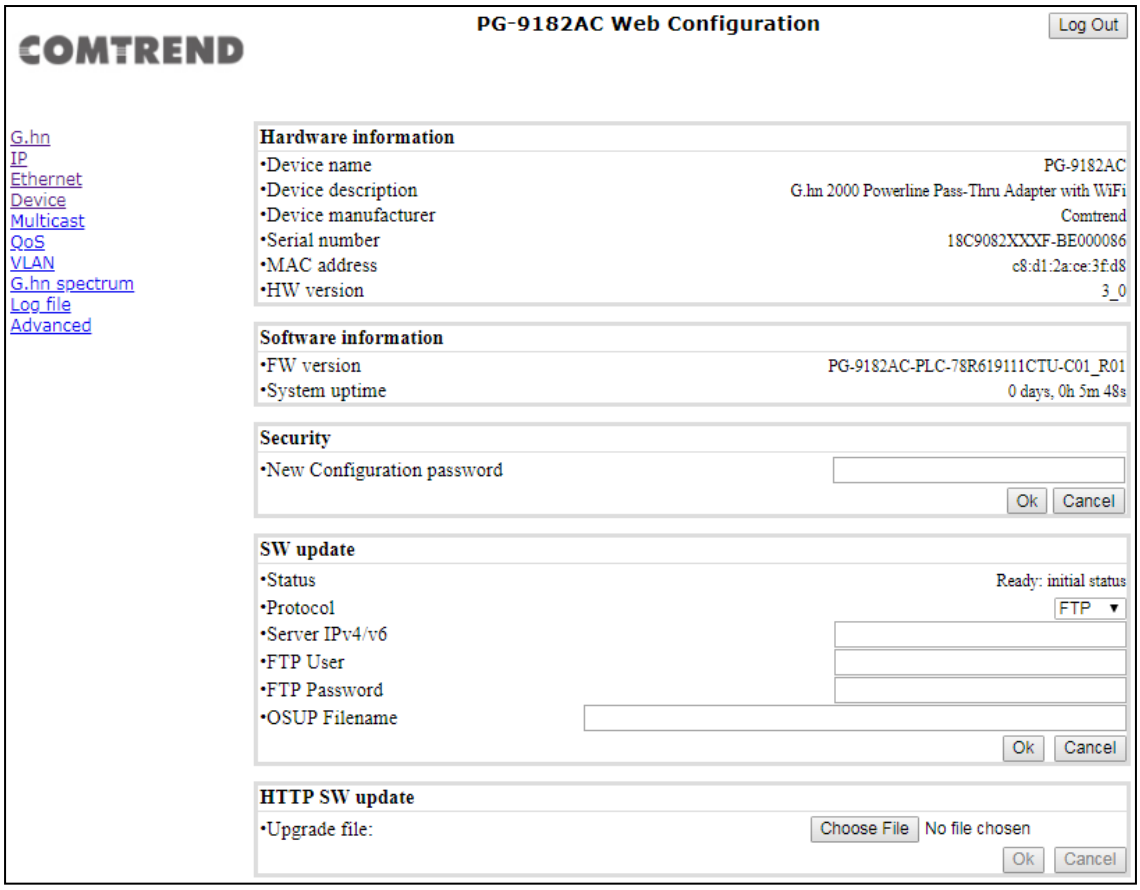
Chapter 7 Ethernet Interface



The Ethernet table shows the status & 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.



8.1 Hardware information

In this tab, basic information such as MAC Address and Serial Number of the selected node is shown.

8.2 Software information

Shows the FW version and system uptime.

8.3 Security

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

8.4 SW update

Current loaded firmware version is shown. Any flash section can be upgraded; the first flash section should be selected and after clicking on the "**OK**" button the corresponding file should be chosen. Usually, a reboot should be performed afterwards to make sure the changes are effective.

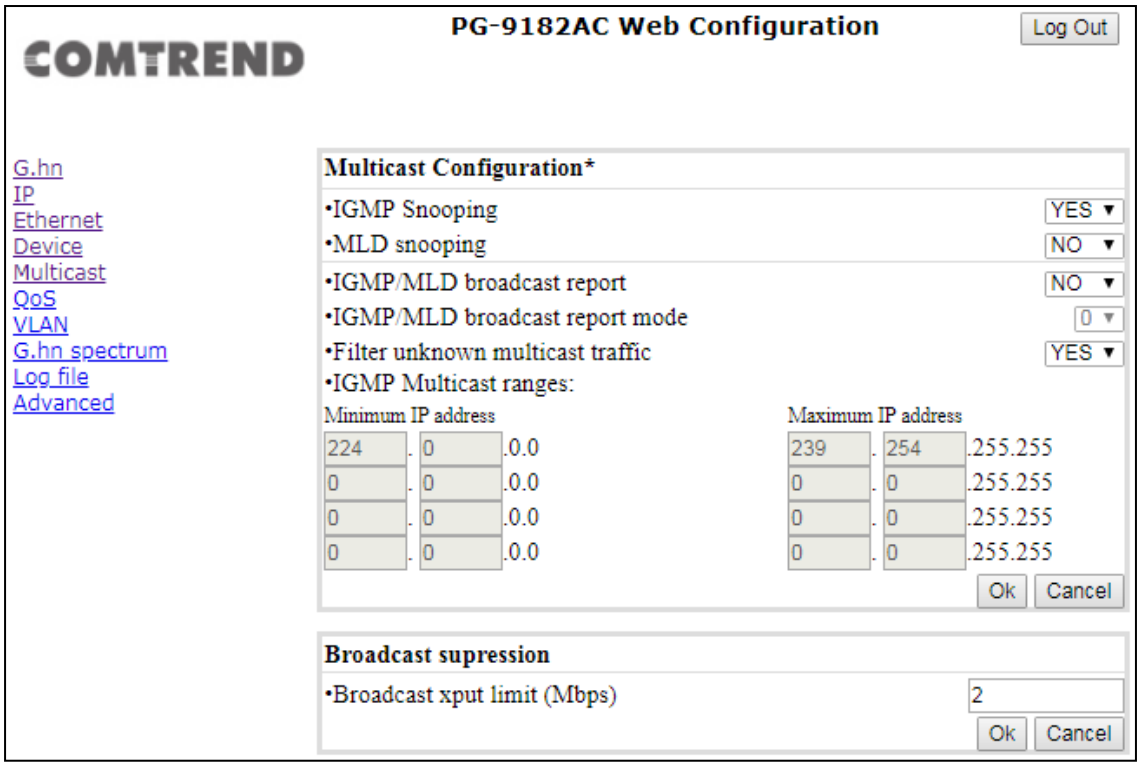
The protocol is by FTP client or TFTP client. L2 is proprietary and is reserved for future use.

8.5 HTTP SW update

STEP 1: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 2: Click the **OK** button once to upload and install the file.

NOTE1:	The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the Device screen with the firmware version installed, to confirm the installation was successful.
NOTE2:	The Power LED indicates the status of firmware update progress. Please **DO NOT** power off the device when Power LED is flashing or the device will be damaged.



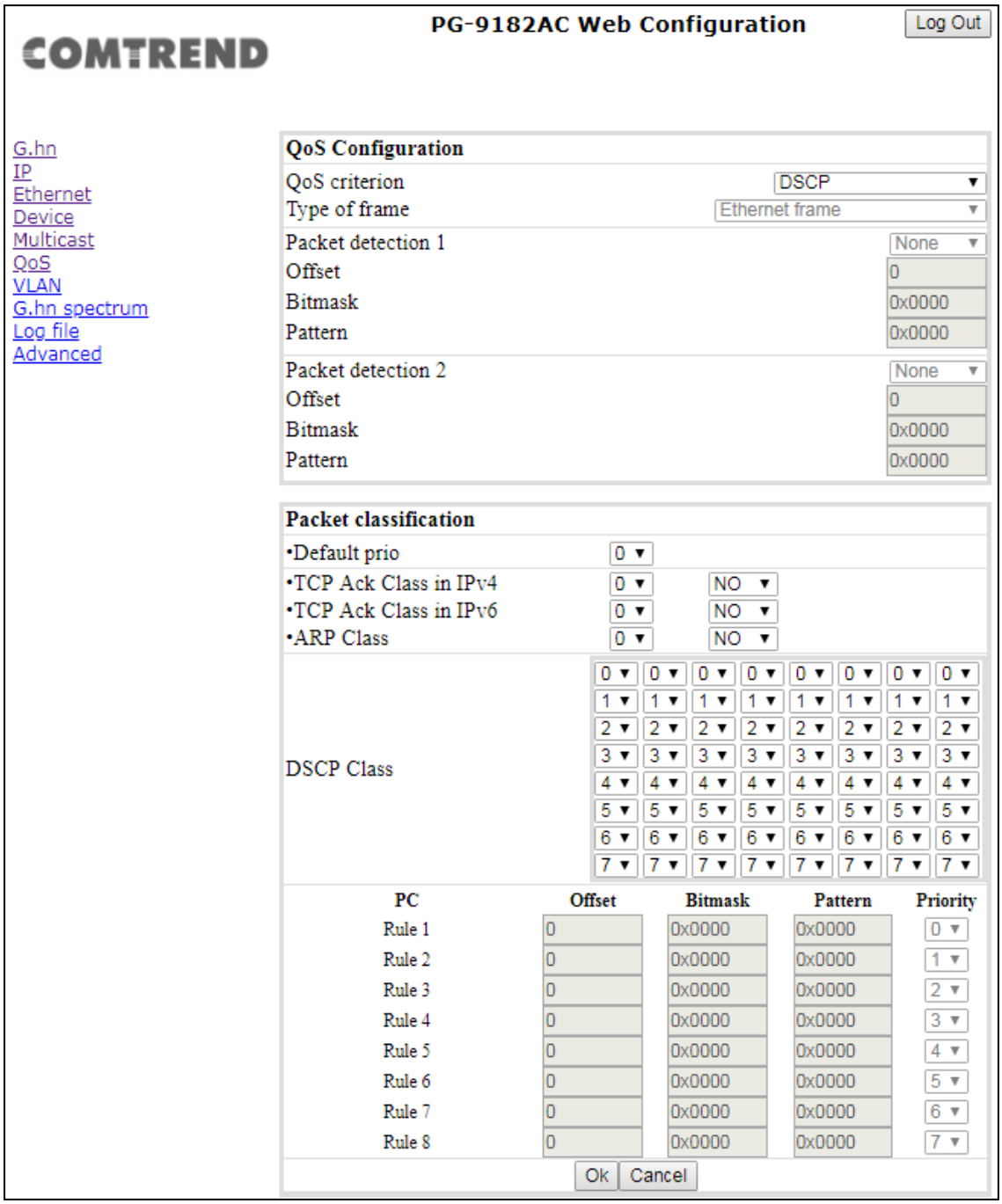
9.1 MCAST Configuration

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/MLD broadcast report mode:** Report broadcast forwarding behavior when the MCAST.GENERAL.REPORT_BROADCAST_ALLOWED is enabled.
  - If 0 then broadcast reports only when the video source is unknown.
  - If 1 then broadcast reports always.
  - If 2 then broadcast reports always if IGMPv3 and only when video source is unknown in others.

  The term 'video source' refers to the node whose Ethernet port is connected directly to the Home Gateway.
- **Filter unknown multicast traffic:** Enables the Multicast Filtering feature.
  If enabled, all the unsolicited multicast traffic will be blocked.
  In IPv4 multicast traffic, only the traffic between the IP ranges defined in the MCAST.GENERAL.IGMP_IP_RANGES_DEF and the packets are unsolicited, these packets will be dropped.
  Warning: This feature implies a higher CPU load, so it is advisable to enable it only in the Video Source.
  Only 100 Kbps of broadcast traffic could be managed in this mode.

- **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.
- **Broadcast Suppression:** Maximum throughput allowed without suppressing broadcast traffic. The accuracy of this parameter depends on size of packets (big packets -> more accuracy). Value 0 deactivates this functionality.



10.1 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 "**Ok**" 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).

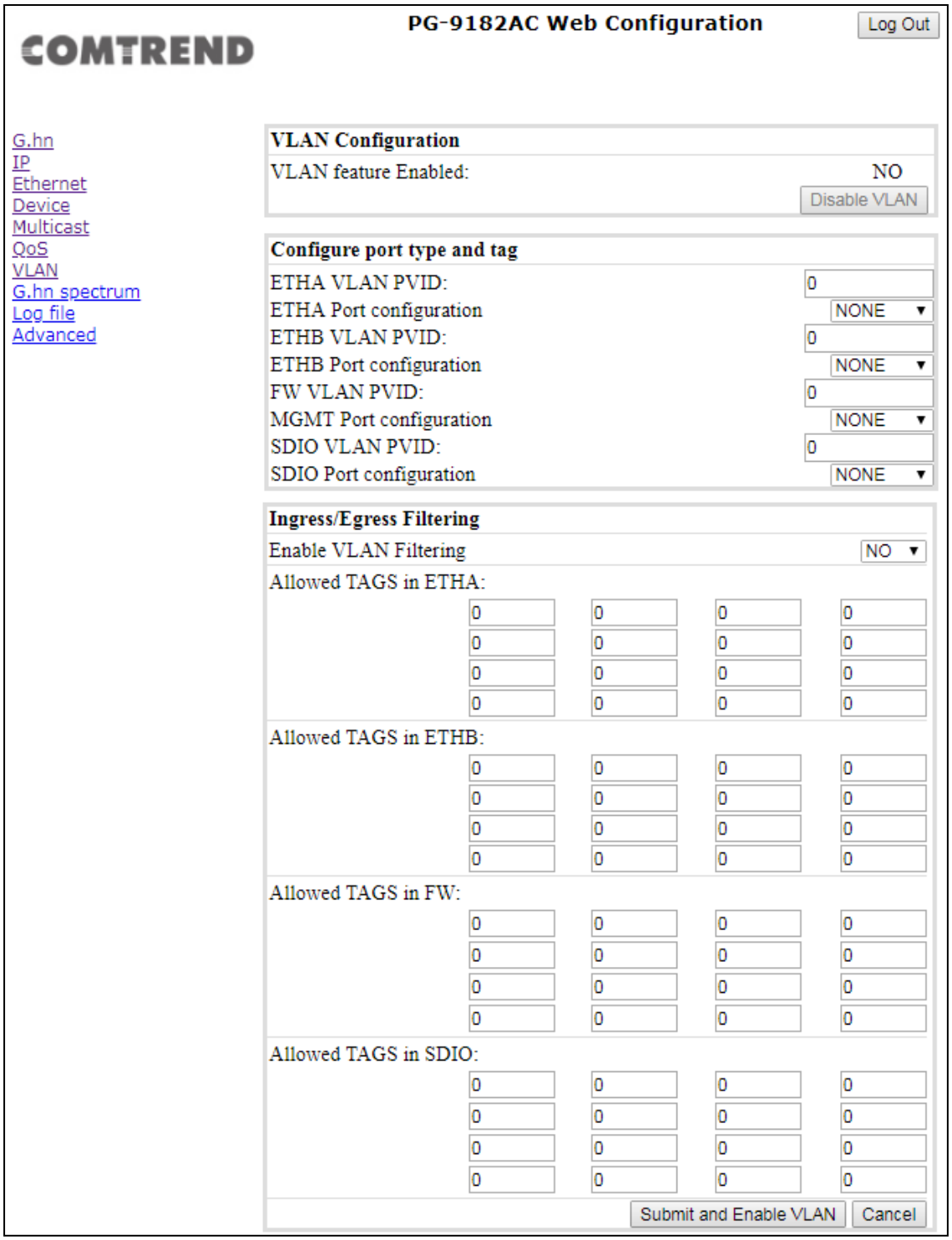
- **Packet detection 1**: first packet detection rule can be configured (offset, bitmask and pattern). Packets which accomplish it will be sent to the classification module.
- **Packet detection 2**: if second packet detection is also enabled, both, first and second detection criteria must be accomplished 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.
- **TCP Ack Class in IPv4:** Mapping TCP ACK (IPv4) to a Class Value.
- **TCP Ack Class in IPv6:** Mapping TCP ACK (IPv6) to a Class Value.
- **ARP Class:** Mapping ARP to a Class Value.
- **DSCP Class:** Mapping of each DSCP value to a Class Value.

As shown above, if QoS criterion: DSCP, 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.

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

In summary, the sequence of priority queue, (7,6) > (5,4) > (3,0) > (2,1)

Chapter 11 VLAN Interface



11.1 VLAN Configuration

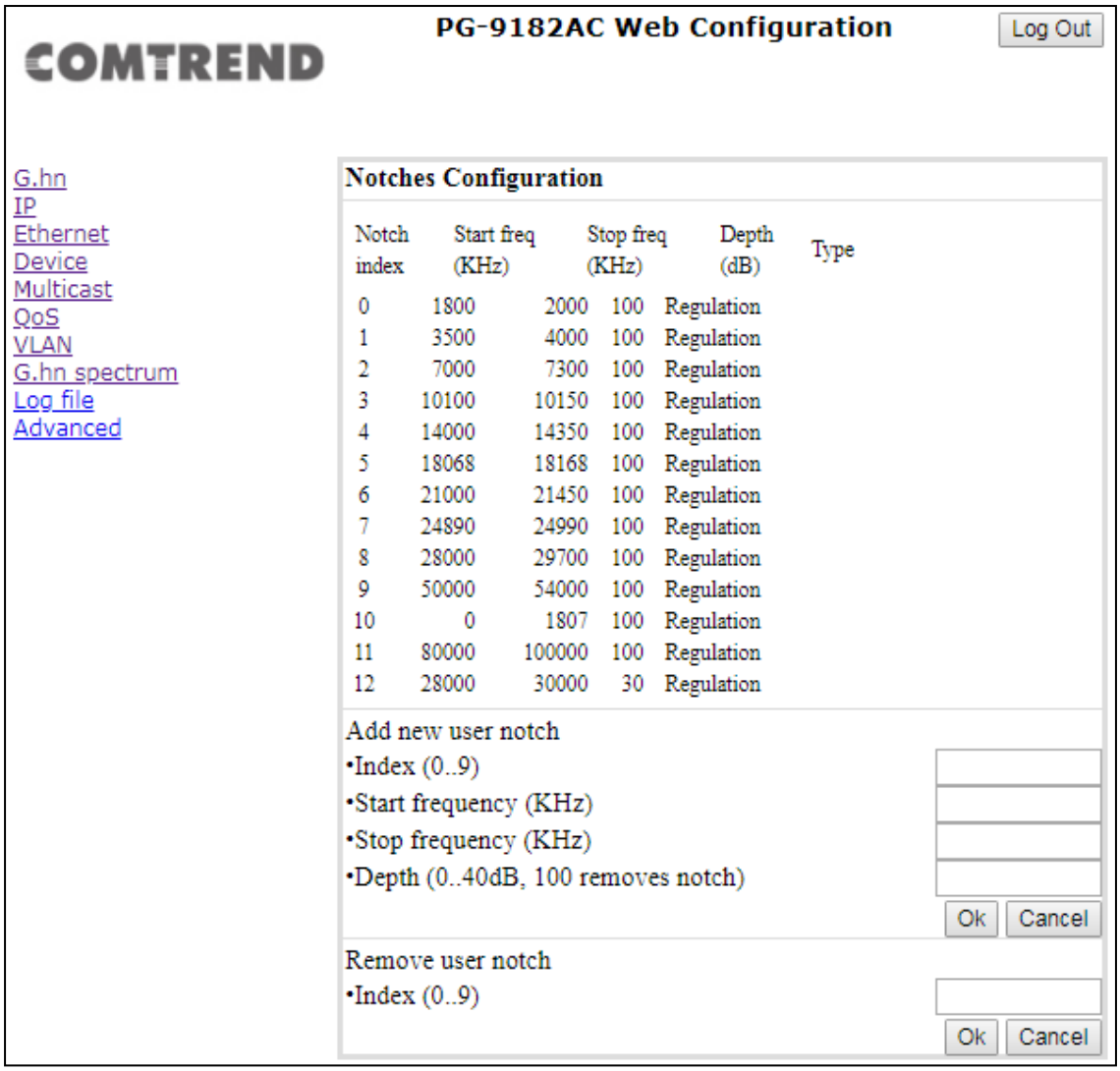
VLAN configuration has been improved allowing the definition of access, trunk and hybrid VLAN ports.

- **VLAN Feature Enabled**: To activate/deactivate VLAN (IEEE 802.1Q) tagging/untagging traffic.
- **ETHA VLAN PVID:** VLAN identifier for Ethernet A port (if it is set to 0, tagging is deactivated).
- **ETHA Port configuration:** Port Configuration for Ethernet A port (ACCESS, TRUNK, NONE).
- **ETHB VLAN PVID:** VLAN identifier for Ethernet B port (if it is set to 0, tagging is deactivated).
- **ETHB Port configuration:** Port Configuration for Ethernet B port (ACCESS, TRUNK, NONE).
- **FW VLAN PVID:** VLAN identifier for Ethernet A port (if it is set to 0, tagging is deactivated).
- **MGMT Port configuration:** Port Configuration for management port (ACCESS, TRUNK, NONE).
- **SDIO VLAN PVID:** VLAN identifier for SDIO port (if it is set to 0, tagging is deactivated).
- **SDIO Port configuration:** Port Configuration for SDIO port (ACCESS, TRUNK, NONE).

Ingress/Egress Filtering

- **Enable VLAN Filtering:** To enable/disable VLAN ingress and egress filtering.
- **Allowed TAGS in ETHA:** Tags allowed on Ethernet A interface.
- **Allowed TAGS in ETHB:** Tags allowed on Ethernet B interface.
- **Allowed TAGS in FW:** Tags allowed on firmware interface.
- **Allowed TAGS in SDIO:** Tags allowed on SDIO interface.

Chapter 12 G.hn spectrum Interface



12.1 Notches

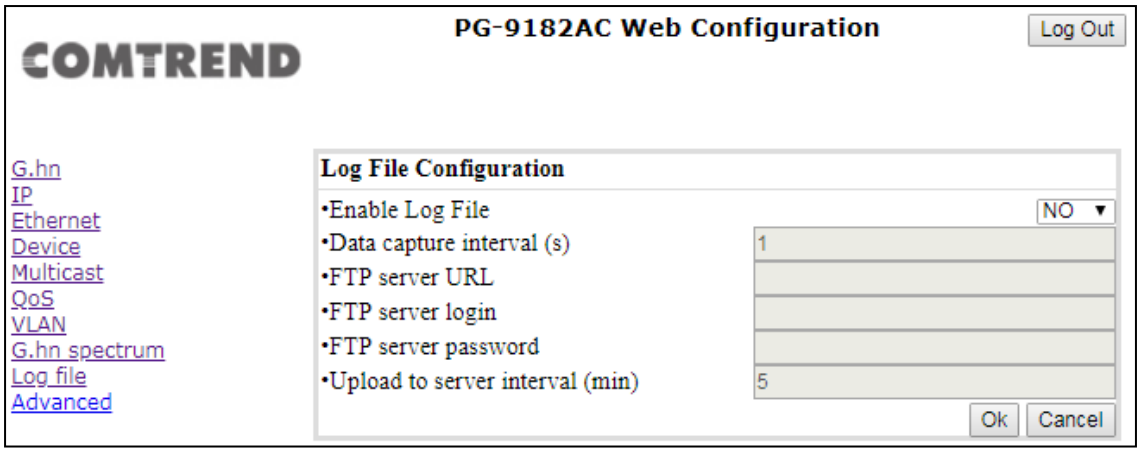
In this tab a table with all configured **Notches** of selected node will be shown. The table is composed of next columns for every notch: Notch Number, Type of notch, Start Frequency (KHz), Stop Frequency (KHz), Depth (in dB).

The first 13 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 "**Ok**" button. They will be added in first User free position from number 0 to 9. (If successful, you can see a record in the Type column)

To remove a User Notch, the "**Remove a User Notch**" section should be used, setting notch number to be removed from 0 to 9 and pressing the "**Ok**" button.

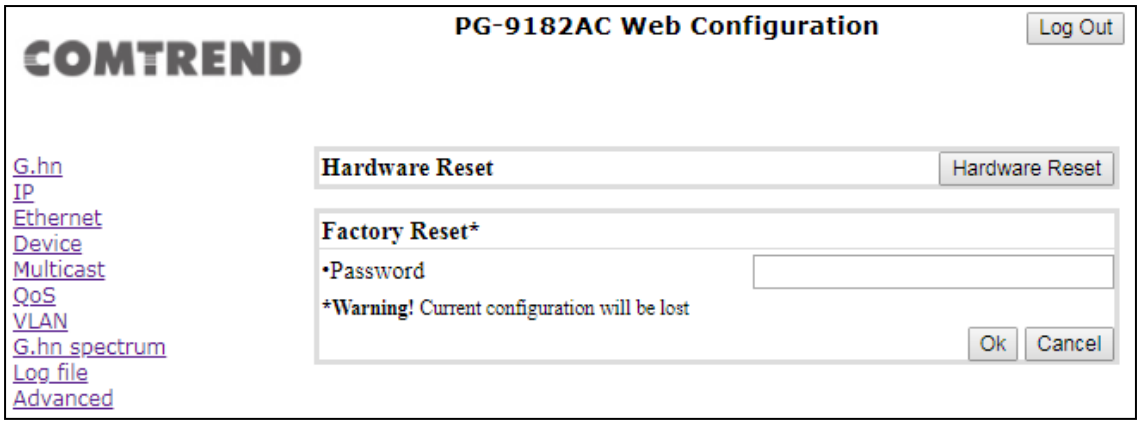
Chapter 13 Log file Interface



13.1 Log File

In the **Log File** configuration the following settings can be read, and changed by clicking on the corresponding "**OK**" 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.



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

Factory Reset: Input the password: **betera** and click the **OK** button to perform a factory reset. The current configuration will be lost.