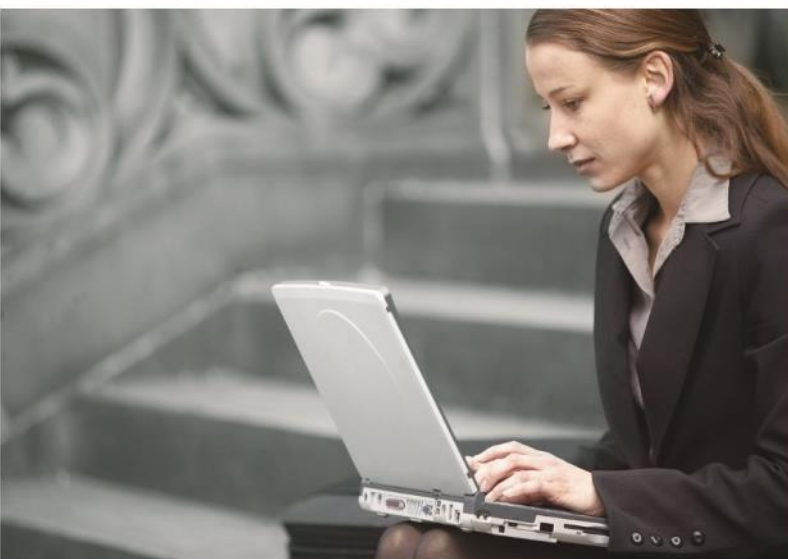




User's Manual

802.11ah Halow Wi-Fi Bridge/Station

- ▶ HLB-100-US915
- ▶ HLB-100-EU868



Copyright

Copyright (C) 2025 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means, electronic or mechanical including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET.

PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements and/or changes to this User's Manual at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

Federal Communication Commission Interference Statement



This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To assure continued compliance, for example, use only shielded interface cables when connecting to computer or peripheral devices.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

CE Compliance Statement

This device meets the RED 2014/53/EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection. The device complies with RF specifications when it is used at a safe distance of 20 cm from your body.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User Manual of PLANET 802.11ah Halow Wi-Fi Bridge/Station

Model: HLB-100-US915 HLB-100-EU868

Rev: 1.0 (June, 2025)

Part No. EM-HLB-100_v1.0

Table of Contents

Chapter 1.	Product Introduction.....	7
1.1	Package Contents.....	7
1.2	Product Description.....	8
1.3	Product Features.....	11
1.4	Product Specifications	12
Chapter 2.	Physical Descriptions.....	14
2.1	Product Outlook	14
Chapter 3.	Preparation	16
3.1	System Requirements.....	16
3.2	Hardware Installation	17
3.2.1	Stand-alone Installation	17
3.2.2	Wall-mount Installation.....	18
3.2.3	Media Chassis Installation	19
3.3	Manual Network Setup -- TCP/IP Configuration	20
3.3.1	Configuring the IP Address Manually	21
3.4	Logging on to the HaLow Network Device.....	24
3.5	Planet Smart Discovery Utility.....	27
3.6	Pair Button Connection Setup (To Be Supported in Future Firmware).....	28
Chapter 4.	Web-based Management	29
4.1	System	31
4.1.1	Operation Mode	32
4.1.2	Gateway Mode (Router)	33
4.1.3	Dashboard	40
4.1.4	System Status.....	41
4.1.5	System Service.....	42
4.1.6	Statistics.....	43
4.1.7	Connection Status	44
4.1.8	SNMP.....	45
4.1.9	NMS	46
4.1.10	Remote Syslog	47
4.1.11	Event Log.....	48
4.2	Network.....	49
4.2.1	WAN.....	50
4.2.2	LAN	53
4.2.3	UPnP.....	54
4.2.4	Routing.....	55

4.2.5	RIP	56
4.2.6	OSPF	57
4.2.7	IGMP	58
4.2.8	IPv6	59
4.2.9	DHCP	61
4.2.10	DDNS	63
4.2.11	MAC Address Clone	65
4.3	Security	66
4.3.1	Firewall	67
4.3.2	MAC Filtering	70
4.3.3	IP Filtering	71
4.3.4	Web Filtering	73
4.3.5	Port Forwarding	74
4.3.6	QoS	76
4.3.7	DMZ	77
4.4	Wireless	78
4.4.1	HaLow Wi-Fi	79
4.4.2	MAC ACL	80
4.4.3	Wi-Fi Advanced	81
4.4.4	Wi-Fi Statistics	82
4.4.5	Connection Status	83
4.5	Maintenance	84
4.5.1	Administrator	85
4.5.2	Date and Time	86
4.5.3	Saving/Restoring Configuration	87
4.5.4	Firmware Upgrading	88
4.5.5	Reboot / Reset	89
4.5.6	Auto Reboot	90
4.5.7	Diagnostics	91
Appendix A: DDNS Application		93
Appendix B: Troubleshooting		94
Appendix C: Note on EU Regulatory Compliance		96

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for purchasing PLANET 802.11ah HaLow Wi-Fi Bridge/Station. Unless specified, “HaLow Network Device” mentioned in this Quick Installation Guide refers to the HLB-100.

Model	Description
HLB-100	802.11ah HaLow Wi-Fi Bridge/Station

Open the box of the HaLow Network Device and carefully unpack it. The box should contain the following items:

- HLB-100
- QR Code Sheet
- DC 5V/2A Power Adapter
- Sub-1G Antenna

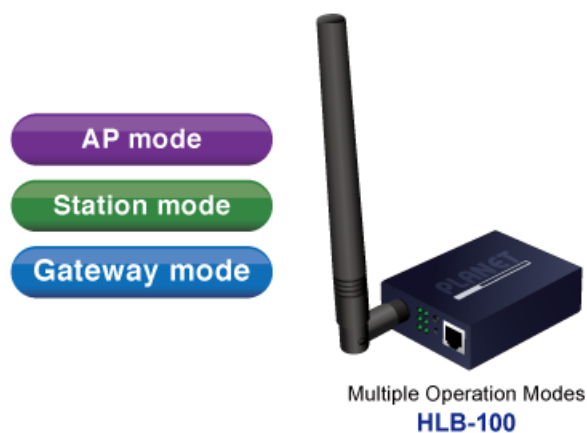
If any item is found missing or damaged, please contact your local reseller for replacement.

1.2 Product Description

Outstanding Features of PLANET HaLow AP

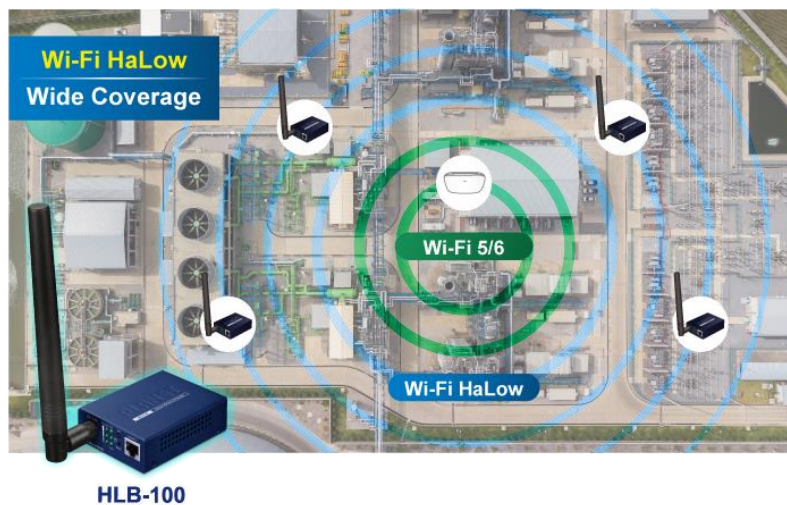
PLANET HaLow Wireless Access Point combines advanced technology with exceptional versatility, making it the ideal choice for demanding network applications. Its key features include:

- **Flexible Deployment Options:** Supports wireless **AP**, **Station**, and **Gateway** modes to meet various network demands.
- **Extreme Environmental Adaptability:** Operates reliably in temperatures ranging from -20°C to 60°C, ideal for industrial applications.
- **Advanced Data Encryption:** Equipped with WPA3 technology to ensure secure data transmission, suitable for enterprise and public networks.
- **Powerful Centralized Management:** Seamlessly integrates with PLANET NMS-AIoT platform, enabling management of over 3,000 devices for IoT and smart city applications.
- **Reliable IoT Solution:** Delivers high stability and scalability for scenarios like smart cities and industrial automation.



Benefits of HaLow Technology

With its exceptional range and stable transmission, PLANET HaLow Wireless AP is ideal for large-area applications. Whether for smart city deployments, industrial automation, or wide-area surveillance, it ensures reliable connectivity even in challenging environments. Its WPA3 encryption further enhances security, protecting data transmissions from potential breaches and ensuring peace of mind for users.

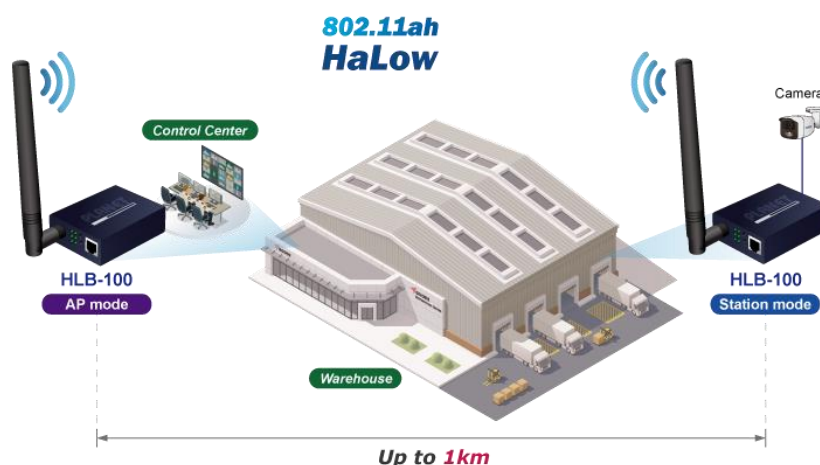


Long Range, Low Power Solution for IoT Connectivity

PLANET HaLow Wireless AP redefines IoT connectivity with its ultra-long range of up to 1km and energy-efficient design. Operating on low power, it ensures extended device runtime, making it ideal for IoT applications in smart cities, agriculture, and industrial automation.

With support for **AP**, **Station**, and **Gateway** modes, the HaLow AP offers versatile deployment options, while its advanced WPA3 encryption safeguards data transmission across networks.

Designed to withstand extreme environments and equipped with wall-mount installation, it delivers reliable, secure, and flexible connectivity for a wide range of IoT use cases.



Robust and Versatile Design

PLANET HaLow Wireless AP supports wall-mount installation, making it suitable for indoor use. The device's ability to adapt to diverse conditions and environments is further enhanced by its energy-efficient and low-power design, delivering long-lasting performance.

Enhanced Security with WPA3

By adopting the advanced WPA3 encryption protocol, PLANET HaLow Wireless AP ensures that data remains secure and protected from unauthorized access. This makes it a perfect fit for enterprises and public deployments where security is paramount.

Seamless Integration with NMS-AIoT for Enhanced IoT Management

PLANET HaLow Wireless AP is fully compatible with PLANET NMS-AIoT platform, enabling centralized management of IoT networks. By integrating with NMS-AIoT, users can monitor and manage over 3,000 sensing devices across wide areas through an intuitive dashboard and map-based interface.

The HaLow AP's long-range capabilities and energy-efficient design perfectly complement NMS-AIoT's AI edge computing, ESG energy management, and cybersecurity features. Together, they provide a robust and scalable solution for enterprises looking to optimize IoT operations with sustainability and security at the forefront.



1.3 Product Features

➤ **Hardware**

- Supports IEEE 802.11ah wireless technology.
- 1 x 10/100 RJ45 port
- 1 x RS485 serial interface
- 1 x pair button
- 1 x reset Button
- 3 x LED indicators for the Strength Signal
- LED indicators for Station, Power and LNK/ACT statuses

➤ **Multiple Operation Modes and Wireless Features**

- Multiple operation modes: AP, gateway and station
- Low power wide area network (LPWAN) connectivity
- Supports WPA3 personal encryption.
- Supports up to 1km wireless range.

➤ **Router Features**

- Bandwidth control per IP address to increase network stability
- Supports NAT Routing, IP Routing or Bridge mode.
- Supports routing / dynamic routing (RIPv1/v2) and VLAN tagging (802.1Q).
- Supports DHCPv6 and DHCP client/server.

➤ **Easy Deployment and Management**

- Supports management by using PLANET NMSViewerPro and CloudViewerPro app.
- Easy discovery by PLANET Smart Discovery
- Self-healing mechanism through system auto reboot setting
- System status monitoring through remote syslog server

1.4 Product Specifications

Product	HLB-100 802.11ah HaLow Wi-Fi Bridge/Station																												
Hardware Specifications																													
Interfaces	1 10/100BASE-TX RJ45 port including 1 LAN/WAN port Supports WAN mode and LAN mode, configurable via software.																												
Antenna Connector	1 × 50 Ω SMA Connector (Center Pin: SMA Female)																												
Serial Interface	1 x RS485 serial interface																												
Button	1 x reset button Press over 5 seconds to reset the device to factory default																												
	1 x pair button																												
Dimensions (W x D x H)	94 x 70.3 x 26.2 mm																												
Weight	223g																												
Power Requirements	5V 2A																												
Power Consumption	2W																												
Installation	Wall-mount																												
LED Indicators	Power, SYS, station, strength signal																												
Wireless Interface Specifications																													
Standard	IEEE 802.11ah (Wi-Fi HaLow) Compliance with regional regulatory requirements (FCC, ETSI)																												
Band Mode	Sub-1 GHz frequency operation																												
Frequency Range	868 MHz: European Union 902–928 MHz: North America																												
Operating Channels	Sub1G: 1MHz 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51 (Channels) 2MHz 2,6,10,14,18,22,26,30,34,38,42,46,50 (Channels) 4MHz 8,16,24,32,40,48 (Channels) 8MHz 12,28,44 (Channels)																												
Max. Transmit Power (dBm)	<table><tr><th>Bandwidth</th><th>MCS 0 Typ. (dBm)</th><th>MCS 7 Typ. (dBm)</th><th>MCS 0 Range (dBm)</th><th>MCS 7 Range (dBm)</th></tr><tr><td>1MHz</td><td>21</td><td>17</td><td>20 ~ 22</td><td>16 ~ 18</td></tr><tr><td>2MHz</td><td>21</td><td>17</td><td>20 ~ 22</td><td>16 ~ 18</td></tr><tr><td>4MHz</td><td>21</td><td>17</td><td>20 ~ 22</td><td>16 ~ 18</td></tr><tr><td>8MHz</td><td>21</td><td>17</td><td>20 ~ 22</td><td>16 ~ 18</td></tr></table>				Bandwidth	MCS 0 Typ. (dBm)	MCS 7 Typ. (dBm)	MCS 0 Range (dBm)	MCS 7 Range (dBm)	1MHz	21	17	20 ~ 22	16 ~ 18	2MHz	21	17	20 ~ 22	16 ~ 18	4MHz	21	17	20 ~ 22	16 ~ 18	8MHz	21	17	20 ~ 22	16 ~ 18
Bandwidth	MCS 0 Typ. (dBm)	MCS 7 Typ. (dBm)	MCS 0 Range (dBm)	MCS 7 Range (dBm)																									
1MHz	21	17	20 ~ 22	16 ~ 18																									
2MHz	21	17	20 ~ 22	16 ~ 18																									
4MHz	21	17	20 ~ 22	16 ~ 18																									
8MHz	21	17	20 ~ 22	16 ~ 18																									

Receive Sensitivity	Bandwidth	MCS 0 (dBm)	MCS 1 (dBm)	MCS 2 (dBm)	MCS 3 (dBm)	MCS 4 (dBm)	MCS 5 (dBm)	MCS 6 (dBm)	MCS 7 (dBm)
	1MHz	-105	-102	-99	-96	-93	-89	-88	-87
	2MHz	-103	-100	-97	-94	-90	-87	-85	-84
	4MHz	-101	-97	-95	-91	-88	-84	-83	-81
	8MHz	-97	-93	-91	-88	-85	-80	-79	-77
Software Features									
LAN	Static IP / Dynamic IP								
Wireless Mode	<div><div></div> Gateway</div> <div><div></div> Access Point</div> <div><div></div> Station</div>								
Channel Width	1MHz, 2MHz, 4MHz, 8MHz								
Encryption Security	WPA3 Personal								
Wireless Security	Enable/Disable SSID Broadcast								
Status Monitoring	Device status, wireless client List PLANET Smart Discovery DHCP client table System Log supports remote syslog server								
Management									
Basic Management Interfaces	Web browser SNMP v1/v2c PLANET Smart Discovery utility and NMS controller supported								
Secure Management Interfaces	TLSv1.2, SNMP v3								
System Log	System Event Log								
Others	Setup wizard Dashboard System status/service Statistics Connection status Auto reboot/Diagnostics Remote management through PLANET DDNS/Easy DDNS Configuration backup and restore Supports IGMP Proxy. Supports UPnP. Diagnostics								
Central Management	PLANET NMSViewerPro, PLANET CloudViewerPro								
Environment & Certification									
Temperature	Operating: -20~ 60 degrees C Storage: -40 ~ 70 degrees C								
Humidity	Operating: 10 ~ 90% (non-condensing) Storage: 5 ~ 90% (non-condensing)								
Regulatory	CE, FCC, RoHS								

Chapter 2. Physical Descriptions

2.1 Product Outlook

HLB-100

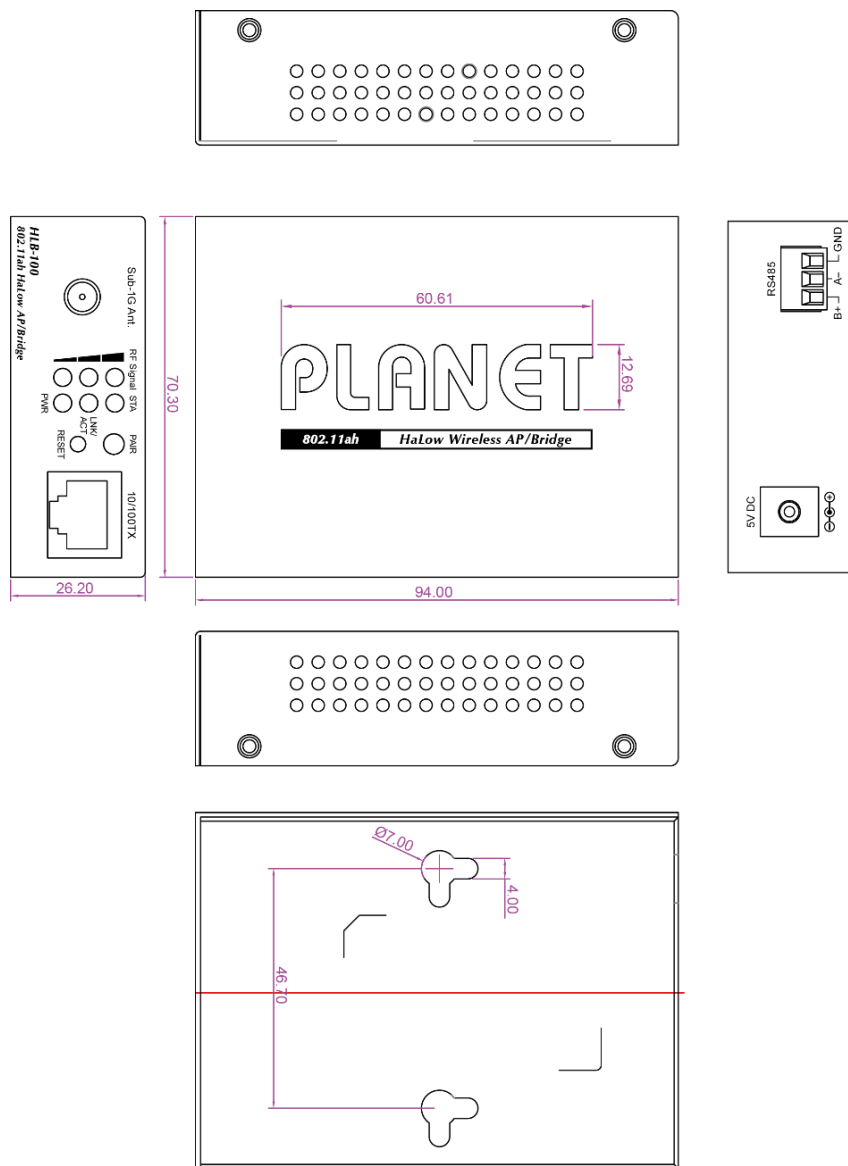
Dimensions

94 x 70.3 x 26.2 mm

Weight

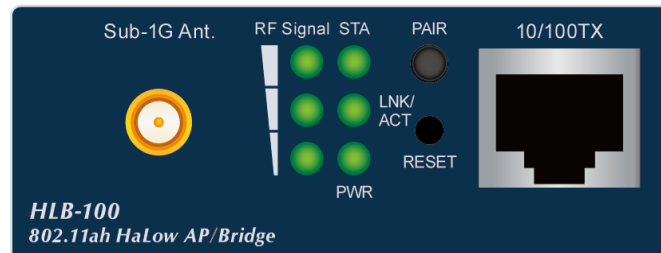
223g

Triple View



Dimensions (W x D x H): 94 x 70.3 x 26.2 mm

Front Side



LED definition

LED	STATUS	FUNCTION
PWR	On	The HLB-100 is on.
	Off	System is operating.
LNK/ACT	On	The HLB-100 is link-up.
	Off	The HLB-100 is link-down.
SYS	On	Lights to indicate the system is working.
	Off	Off to indicate the system is booting.
STA	On	HLB-100 operates in Station Mode.
	Off	HLB-100 operates in AP or Gateway Mode.

H/W Interface definition

Object	Description
LAN	10/100Mbps RJ45 port
Pair Button	Press the Pair button to be connected in 2 minutes.
Reset	Press the Reset button for over 5 seconds and then release it to restore system to the factory default settings.

Rear Side



Chapter 3. Preparation

Before getting into the device's web UI, user has to check the network setting and configure PC's IP address.

3.1 System Requirements

- Workstations running Windows 7/8/10/11, MAC OS 10.12 or later, Linux Kernel 2.16.18 or later, or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with **Ethernet NIC** (Network Interface Card)
- **Ethernet Port Connection**
 - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
 - The above PC is installed with Web browser.



It is recommended to use Chrome 98.0.xxx or above to access the HaLow Network Device. If the Web interface of the HaLow Network Device is not accessible, please turn off the anti-virus software or firewall and then try it again.

3.2 Hardware Installation

3.2.1 Stand-alone Installation

Step 1: Unpack the HLB-100 unit and accessories.

Step 2: Connect the 5V DC power adapter to the HLB-100 and verify that the Power LED lights up.

Step 3: Use a twisted-pair, straight-through Category 5e/6/7 UTP cable to connect the HLB-100 LAN port (RJ45) to the network equipment (e.g., switch, router, PC, or gateway device).

Step 4: When the LAN cable is properly connected, the LNK/ACT LED on the HLB-100 will light up, indicating successful Ethernet connection.

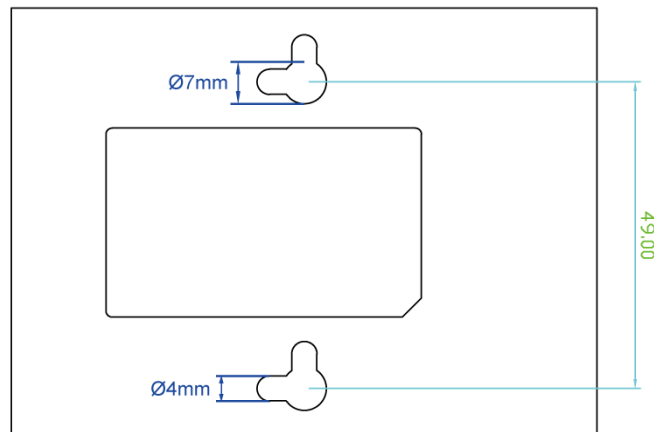
(Refer to the LED Indicators section for LED behavior descriptions.)

Step 5: Verify that all LED indicators are functioning correctly to complete the hardware installation.

3.2.2 Wall-mount Installation

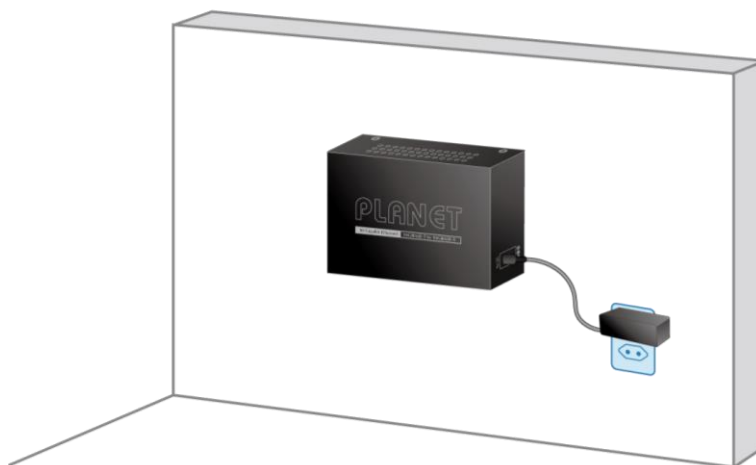
Step 1: Please find the wall that can mount the HLB-100

Step 2: Screw two screws on the wall.



Step 3: Hang the HLB-100 on the screws from the wall.

Step 4: Connect the 5V DC power adapter to the HLB-100 and verify the Power LED lights up.



Note

Before mounting the device to the wall, please check the location of the electrical outlet and the length of the Ethernet cable.



Note

The illustrations in this section are based on Media Converter models for reference. The mounting procedure is identical for the HLB-100.

3.2.3 Media Chassis Installation

To install the HLB-100 in a **10-inch** or **19-inch** standard rack, follow the instructions described below.

Step 1: Place your HLB-100 on a hard flat surface, with the front panel positioned towards your front side.

Step 2: Carefully slide in the module until it is fully and firmly fitted into the slot of the chassis; the Power LED of the HLB-100 will turn ON.



Figure 3-1: Insert HLB-100 into an available slot

Caution:

1. Never push the converter into the slot with force; it could damage the chassis.
2. The Media Converter Chassis supports hot-swap; there is no need to turn off the whole chassis before sliding in the new converter.



The illustrations in this section are based on Media Converter models for reference. The mounting procedure is identical for the HLB-100.

3.3 Manual Network Setup -- TCP/IP Configuration

The HLB-100 IP address default is [DHCP Client](#) mode. The fallback IP address is [192.168.1.253](#), and the default subnet mask is 255.255.255.0. These values can be changed as needed. In this guide, the default values are used for description.

Connect the HLB-100 to your PC by plugging one end of an Ethernet cable into the LAN port of the HLB-100, and the other end into the Ethernet port of the PC. The HLB-100 is powered by a 5V DC power adapter.

In the following sections, we will introduce how to configure the TCP/IP settings in Windows 11. The procedures for other operating systems are similar. Please ensure that your Ethernet Adapter is properly installed and functioning. Refer to your Ethernet adapter's manual if necessary.

3.3.1 Configuring the IP Address Manually

- Set up the TCP/IP Protocol for your PC.
 - Configure the network parameters. The IP address is 192.168.1.xxx (If the default IP address of the HLB-100 is 192.168.1.253, and the DSL router is 192.168.1.254, the "xxx" can be configured to any number from 1 to 252.) and subnet mask is 255.255.255.0.
- 1 Select **Use the following IP address**, and then configure the IP address of the PC.
 - 2 For example, the default IP address of the HLB-100 is 192.168.1.253 and the DSL router is 192.168.1.254, or you may choose from 192.168.1.1 to 192.168.1.252.

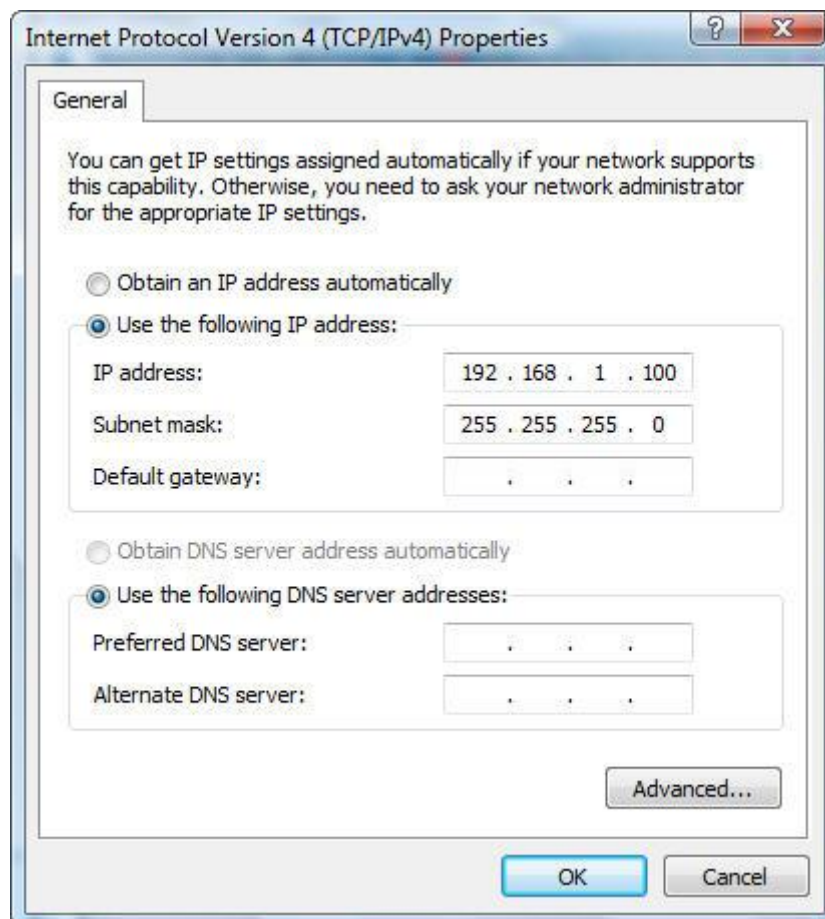


Figure 3-2 TCP/IP Setting

Now click **OK** to save your settings.

Now, you can run the ping command in the **command prompt** to verify the network connection between your PC and the AP. The following example is in **Windows 11** OS. Please follow the steps below:

1. Click on **Start > Run**.
2. Type "**cmd**" in the Search box.

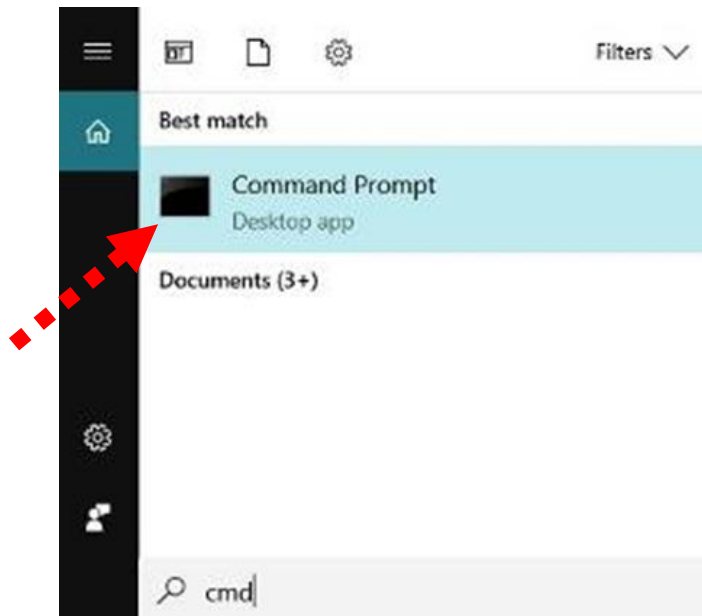


Figure 3-3 Windows Start Menu

3. Open a command prompt, type ping **192.168.1.253** and then press **Enter**.
 - ◆ If the result displayed is similar to [Figure 3-4](#), it means the connection between your PC and the AP has been established well.

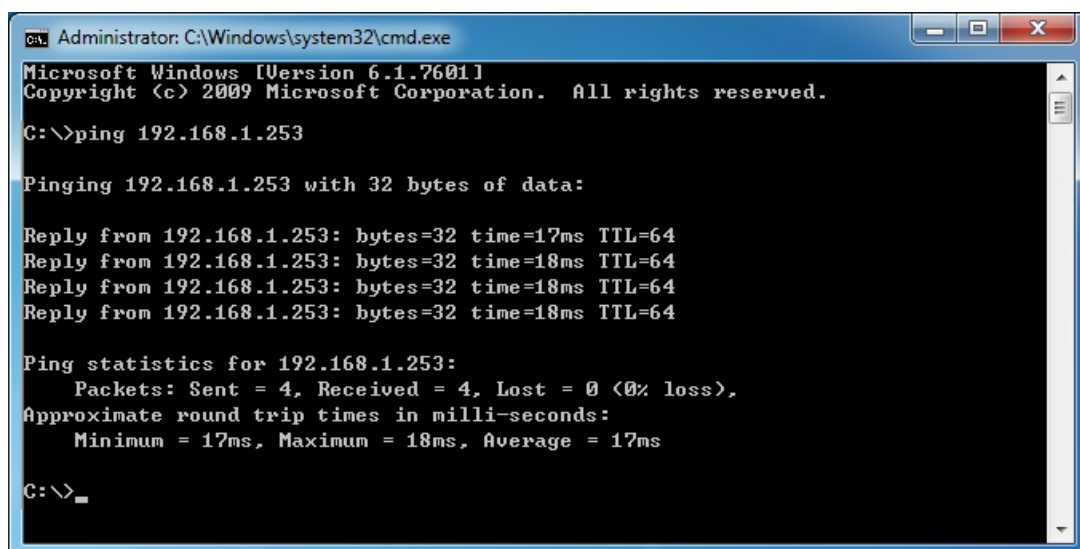
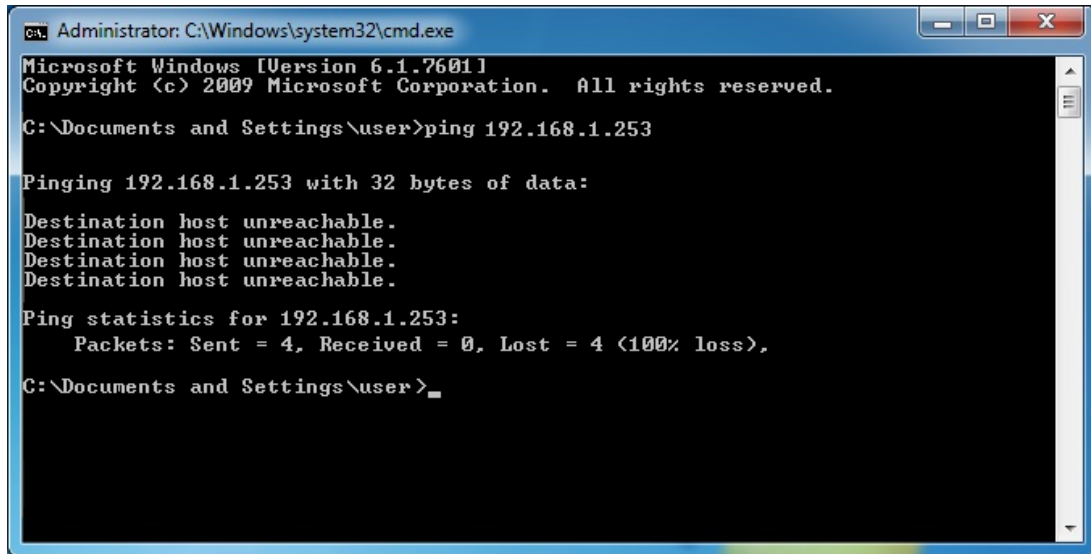


Figure 3-4 Successful Result of Ping Command

- ◆ If the result displayed is similar to **3-5**, it means the connection between your PC and the HLB-100 has failed.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Documents and Settings\user>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\user>
```

Figure 3-5 Failed Result of Ping Command

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your HLB-100. Some firewall software programs may block a DHCP request on newly installed adapters.

3.4 Logging on to the HaLow Network Device

1. Use Chrome or another Web browser to enter the default IP address <https://192.168.1.253> to access the Web interface.
2. When the following dialog box appears, please enter the default user name “**admin**” and the password. Refer to the following to determine your initial login password.

Default IP Address: **192.168.1.253**

Default Username: **admin**

Default Password: **hl+ the last 6 characters of the MAC ID in lowercase**

Default 1GHz SSID: **PLANET_AH**

Default Mode: **AP mode**

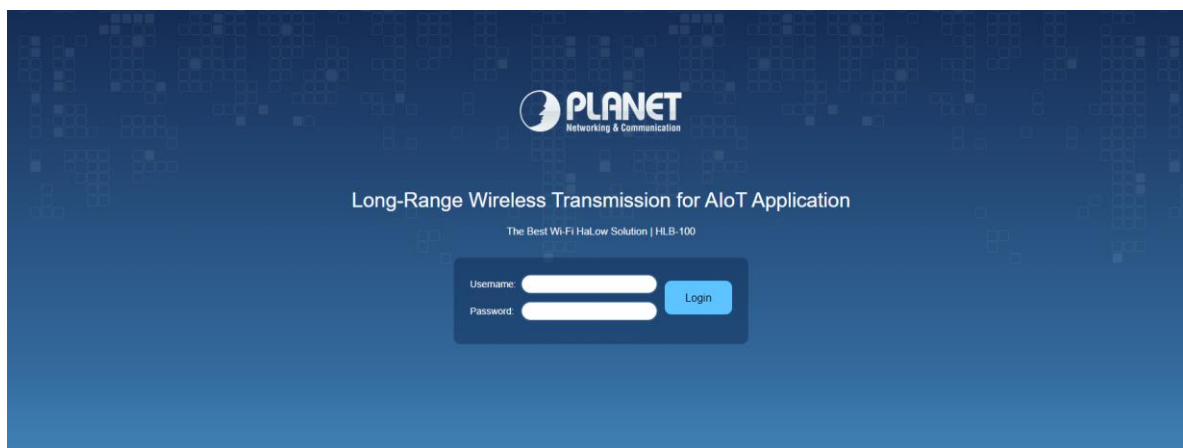


Figure 3-6: Web Login Screen

3. The HaLow Network Device supports three operation modes:

- **Gateway Mode**
- **AP Mode (Default)**
- **Station Mode**



The single RJ45 port can be configured by the user to function as either a **LAN** port or a **WAN** port. If you log in to the web user interface using the LAN IP address 192.168.1.253 in the default AP mode, **changing the operation mode to Gateway mode and applying the configuration will result in the web disconnection.**

If this occurs, you will need another HaLow device configured in Station mode to establish a HaLow wireless connection and remotely log in to the HaLow Router to complete the configuration.

Please follow the wizard to do the first-time setup and select the mode preferred.

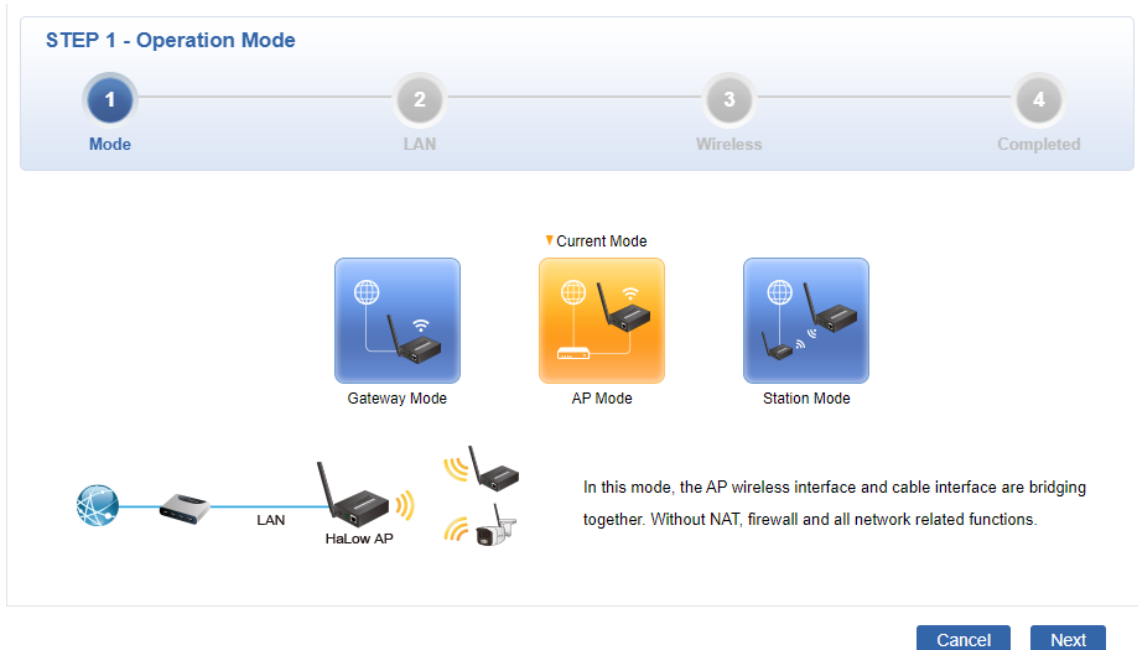


Figure 3-7: Web Wizard Operation Mode of HaLow Network Device

Once Web setup wizard is completed, enter the new username and password. The main screen appears as Figure 3-11 shows.



Figure 3-8: Web Main Screen of HaLow Network Device

Now you can use the Web management interface to continue the **HaLow Network Device** management.



MAC ID: A8F7E0XXXXXX
Default Password: **apxxxxxx**
("x" means the last 6 digits of the MAC address.
All characters should be in lowercase.)

3.5 Planet Smart Discovery Utility

To easily list the HLB-100 in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution.

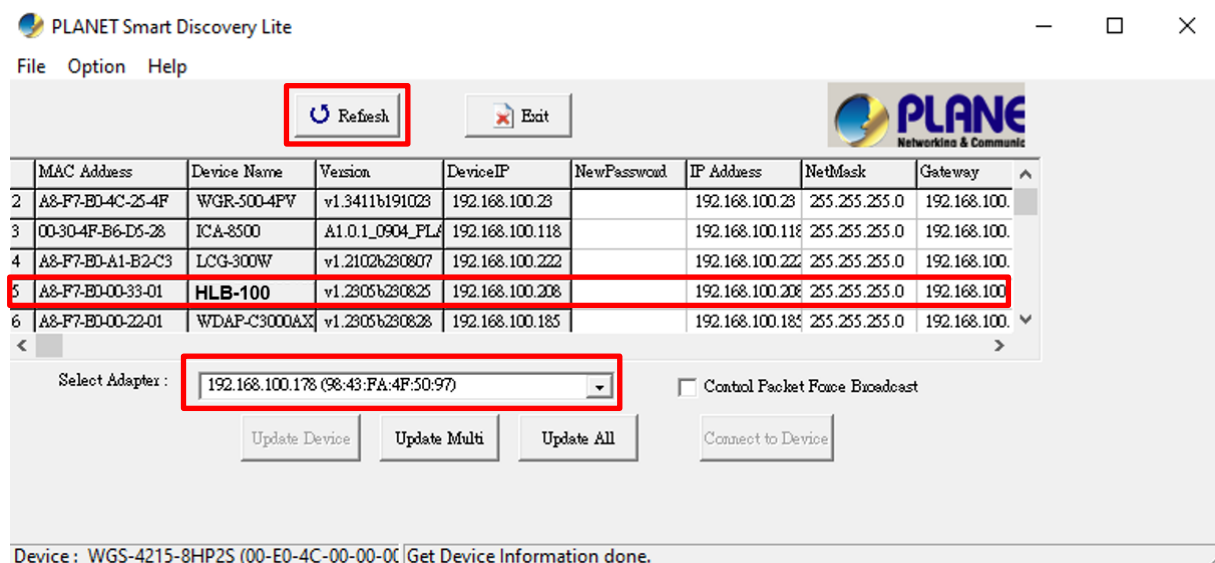
The following installation instructions guide you to running the Planet Smart Discovery Utility.

Step 1: Download the **Planet Smart Discovery Utility** to administrator PC.

Step 2: Run this utility and the following screen appears.



Step 3: Press **“Refresh”** for the current connected devices in the discovery list as shown in the following screen:



Step 4: Press **“Connect to Device”** and then the Web login screen appears.



The fields in the white background can be modified directly and then you can apply the new setting by clicking **“Update Device”**.

3.6 Pair Button Connection Setup (To Be Supported in Future Firmware)

To quickly establish a wireless connection between two HLB-100 units, you can use the Pair button on the devices without logging into the web interface.

This method is ideal for simple point-to-point wireless deployment between a Gateway or AP and a Station.

Step 1: Configure one HLB-100 to AP/Gateway Mode and the other to Station Mode, then power both devices on.

Step 2: On the device that will act as the AP, press and hold the Pair button for 1 second.

Step 3: Within 30 seconds, go to the device that will act as the Station and press and hold the Pair button for 1 second as well.

Step 4: Wait for both devices' Signal LED to turn solid ON, indicating a successful pairing and connection.

Step 5: Once paired, the devices will automatically communicate wirelessly via HaLow. You can proceed with further configuration if needed.



If pairing fails, please wait for about 1 minute and try the pairing process again from Step 2

The paired connection will persist after reboot unless factory reset is performed.

Make sure no firewall or DHCP conflict exists in the same network.

Chapter 4. Web-based Management

This chapter delivers a detailed presentation of HLB-100's functionalities and allows you to manage the HaLow device with ease.

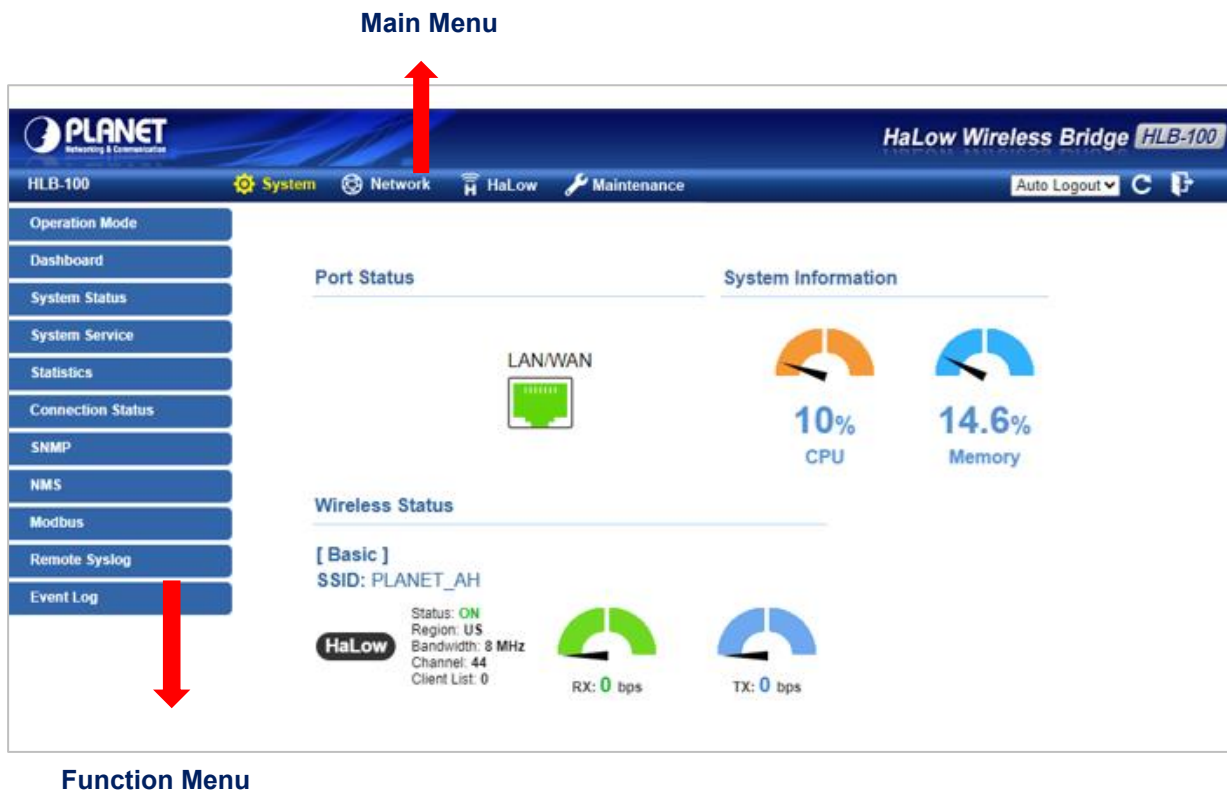


Figure 4-1 Main Web Page

Main Menu

The main menu displays the product name, function menu, and main information in the center. Via the Web management, the administrator can set up the device by selecting the functions those listed in the function menu and button as shown in [Figures 4-2 and 4-3](#).



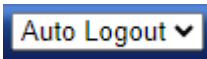


Figure 4-2: Function Menu

Object	Description
System	Provides system information of the router.
Network	Provides WAN, LAN and network configuration of the router.
Security	Provides firewall and security configuration of the router.
HaLow	Provides HaLow configuration of the router.
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the router.



Figure 4-3: Function Button

Object	Description
	Click the " Refresh button " to refresh the current web page.
	Click the " Logout button " to log out the web UI of the router.
	Set "Auto Logout" to log out the web UI of the router. <div data-bbox="443 1713 635 1953"> Auto Logout ▾ Auto Logout Off 3 min 5 min 10 min 15 min </div>

4.1 System

Use the system menu items to display and configure basic administrative details of the router. The System menu shown in [Figure 4-4](#) provides the following features to configure and monitor system.

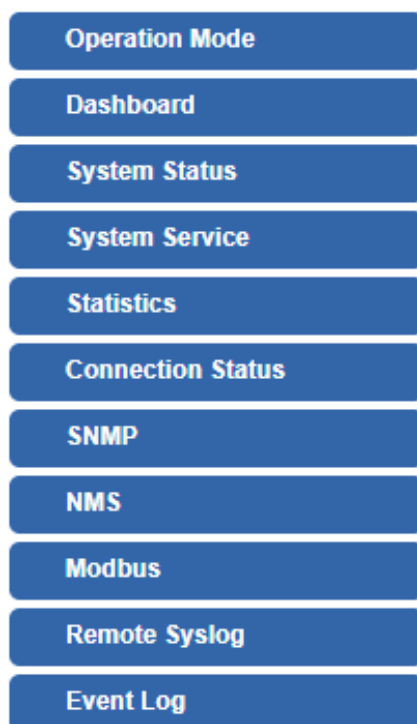


Figure 4-4: System Menu

Object	Description
Operation Mode	The Wizard will guide the user to configuring the router easily and quickly.
Dashboard	The overview of system information includes connection, port, and system status.
System Status	Display the status of the system, Device Information, LAN and WAN.
System Service	Display the status of the system, Secured Service and Server Service.
Statistics	Display statistics information of network traffic of LAN and WAN.
Connection Status	Display the DHCP client table and the ARP table.
SNMP	Display SNMP system information.
NMS	Enable/Disable NMS on routers.
Modbus	Configure the Modbus TCP Mode on this page.
Remote Syslog	Enable Captive Portal on routers.
Event Log	Display Event Log information.

4.1.1 Operation Mode

The Wizard allows you to configure the HLB-100 in different operation modes, including AP Mode, Station Mode, and Gateway Mode, depending on your network application.



Figure 4-5 Operation Mode



The default operation mode is AP Mode.

4.1.2 Gateway Mode (Router)

Click **“Wizard”** → **“Gateway Mode”** and the following page will be displayed. This section allows you to configure the Gateway mode.

Step 1: Operation Mode

Select operation mode.



Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in [Figure 5-5](#).

STEP 2 - Network Interface LAN

1 Mode 2 LAN 3 WAN 4 Wireless 5 Security 6 Completed

IP Address 192.168.1.253

Netmask 255.255.255.0

DHCP Server ☒

Start IP Address 192.168.100.100

Maximum DHCP Users 101

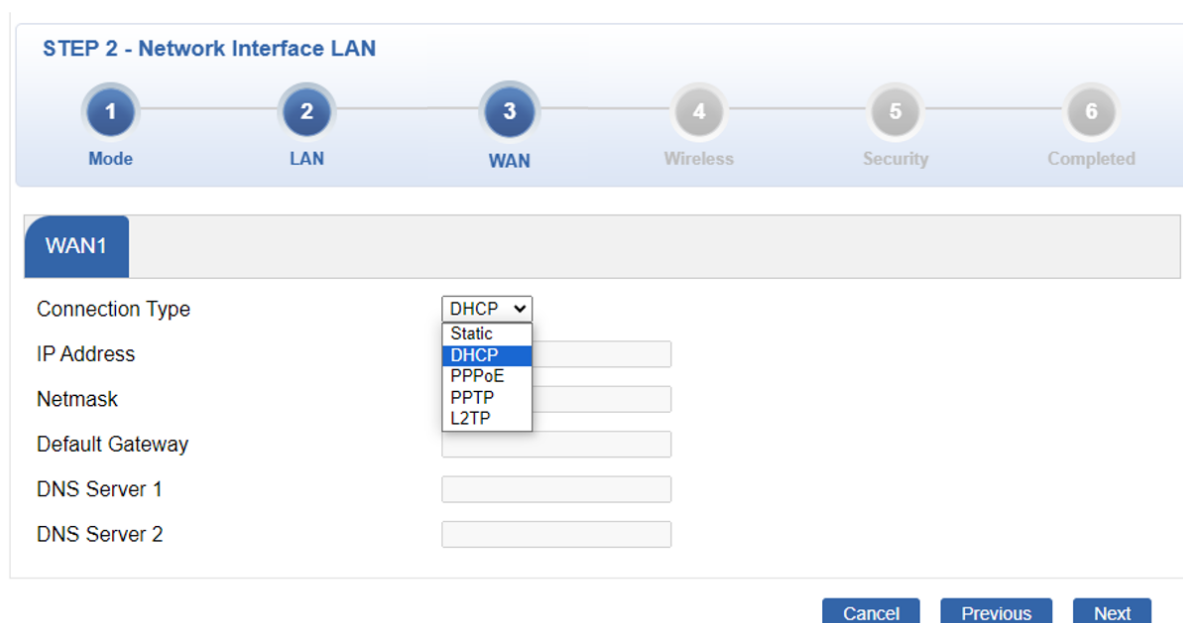
Cancel Previous Next

Figure 4-6: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your router. The default is 192.168.1.1.
Subnet Mask	An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
DHCP Server	By default, the DHCP Server is enabled. If user needs to disable the function, please uncheck the box.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the router will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Next	Press this button to the next step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 3: WAN Interface

The router supports two access modes on the WAN side shown in [Figure 4-9](#)



STEP 2 - Network Interface LAN

1 Mode 2 LAN 3 **WAN** 4 Wireless 5 Security 6 Completed

WAN1

Connection Type: DHCP (Static, DHCP, PPPoE, PPTP, L2TP)

IP Address:

Netmask:

Default Gateway:

DNS Server 1:

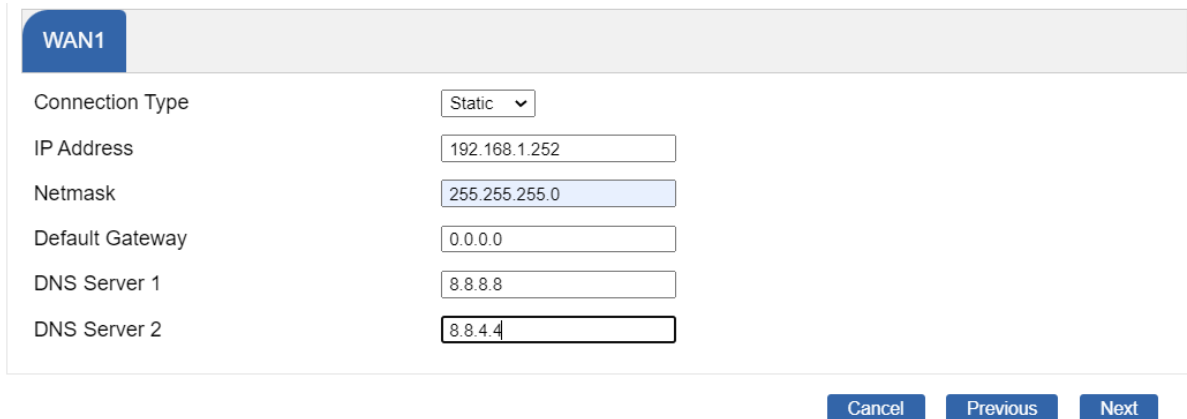
DNS Server 2:

Cancel Previous Next

Figure 4-7: Setup Wizard – WAN 1 Configuration

Mode 1 -- Static IP

Select **Static IP Address** if all the Internet port's IP information is provided to you by your ISP. You will need to enter the **IP Address**, **Netmask**, **Default Gateway** and **DNS Server** provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format. The setup is shown in [Figure 4-8](#).



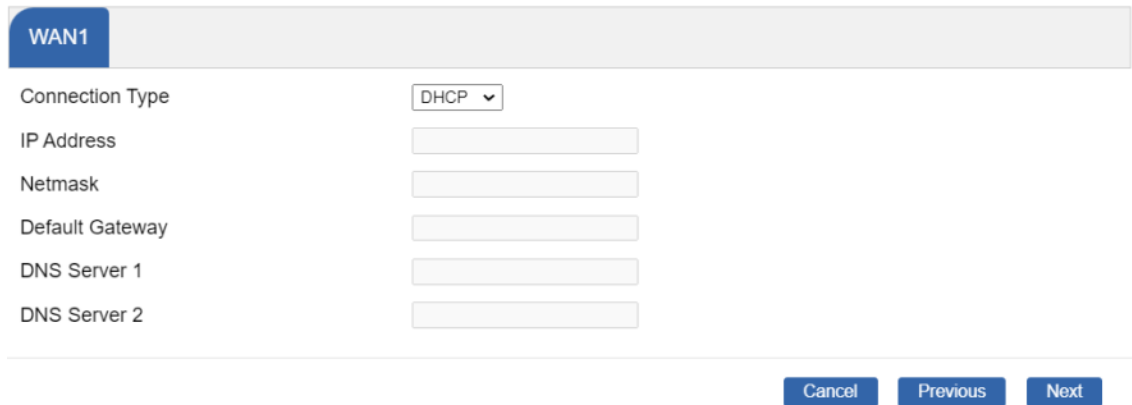
The screenshot displays the WAN1 configuration page for a static IP setup. The 'Connection Type' is set to 'Static'. The 'IP Address' field contains '192.168.1.252', 'Netmask' contains '255.255.255.0', 'Default Gateway' contains '0.0.0.0', 'DNS Server 1' contains '8.8.8.8', and 'DNS Server 2' contains '8.8.4.4'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

Figure 4-8: WAN Interface Setup – Static IP Setup

Object	Description
IP Address	Enter the IP address assigned by your ISP.
Netmask	Enter the Netmask assigned by your ISP.
Default Gateway	Enter the Gateway assigned by your ISP.
DNS Server	The DNS server information will be supplied by your ISP.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Mode 2 -- DHCP Client

Select DHCP Client to obtain IP Address information automatically from your ISP. The setup is shown in [Figure 4-9](#).

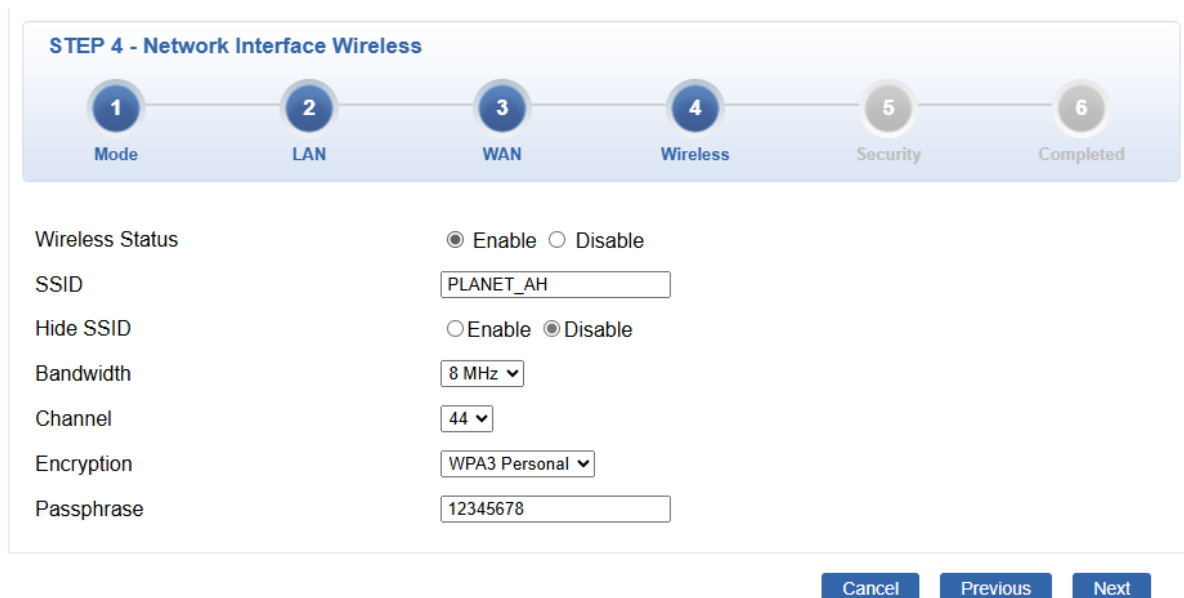


The screenshot shows the 'WAN1' configuration page. The 'Connection Type' is set to 'DHCP'. Below this, there are input fields for 'IP Address', 'Netmask', 'Default Gateway', 'DNS Server 1', and 'DNS Server 2', all of which are currently empty. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

Figure 4-9: WAN Interface Setup – DHCP Setup

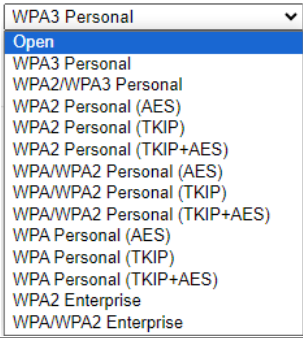
Step 4: Network Interface Wireless Connection

Set up the Security Settings as shown in [Figure 5-9](#).



The screenshot shows the 'STEP 4 - Network Interface Wireless' configuration page. At the top, there is a progress bar with six steps: 1 Mode, 2 LAN, 3 WAN, 4 Wireless (current step), 5 Security, and 6 Completed. Below the progress bar, the 'Wireless Status' is set to 'Enable'. The 'SSID' is 'PLANET_AH'. 'Hide SSID' is set to 'Disable'. 'Bandwidth' is '8 MHz'. 'Channel' is '44'. 'Encryption' is 'WPA3 Personal'. The 'Passphrase' is '12345678'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

Figure 4-10: Wireless Connection- set up

Object	Description
Wireless Status	Select to enable or disable the Wi-Fi HaLow wireless function.
SSID	Enter the SSID for the HaLow wireless network. This name will be broadcast for other HaLow stations to connect.
Hide SSID	Enable this option to prevent the SSID from being broadcast publicly. When disabled, the SSID will be visible.
Bandwidth	Select the channel bandwidth for the HaLow interface. Available options include 1 MHz, 2 MHz, 4 MHz, and 8 MHz.
Channel	Select the specific channel number for Wi-Fi HaLow operation. Please ensure the selected channel complies with local regulatory settings.
Encryption	<p>Selector is for the encryption for the sake of security.</p> 
Passphrase	Enter the password used to connect to the HaLow SSID. The default is empty; users must configure a secure password manually.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 5: Security Setting

Set up the Security Settings as shown in Figure 4-11.

STEP 5 - Security Settings

1

Mode

2

LAN

3

WAN

4

Wireless

5

Security

6

Completed

SPI Firewall

☒ Enable
 ☐ Disable

Block SYN Flood

☒ Enable
 ☐ Disable

Block ICMP Flood

☐ Enable
 ☒ Disable

Block WAN Ping

☐ Enable
 ☒ Disable

Remote Management

☐ Enable
 ☒ Disable

Cancel

Previous

Next

Figure 4-11: Setup Wizard –Security Setting

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.
Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack. The default configuration is disabled.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.

Remote Management	Enable the function to allow the web server access of the router from the Internet network. The default configuration is disabled.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 6: Setup Completed

The page will show the summary of LAN, WAN and Security settings as shown in [Figure 4-12](#).

STEP 6 - Setup Completed

1

Mode

2

LAN

3

WAN

4

Wireless

5

Security

6

Completed

Operation Mode

Gateway Mode

LAN

Enable: Static IP: 192.168.1.253 / 255.255.255.0

WAN

Enable: DHCP

Halow WiFi

Enable: ON SSID: PLANET_AH Bandwidth: 8 MHz Channel: 44
Encryption: WPA3 Personal Hide SSID: Disable

Security Settings

SPI Firewall: ON
Block SYN Flood: ON
Block ICMP Flood: OFF
Block WAN Ping: OFF
Remote Management: OFF

Previous

Finish

Figure 4-12: Setup Wizard – Setup Completed

Object	Description
Finish	Press this button to save and apply changes.
Previous	Press this button for the previous step.

4.1.3 Dashboard

The dashboard provides an overview of system information including connection, port, and system status as shown in Figure 4-13.

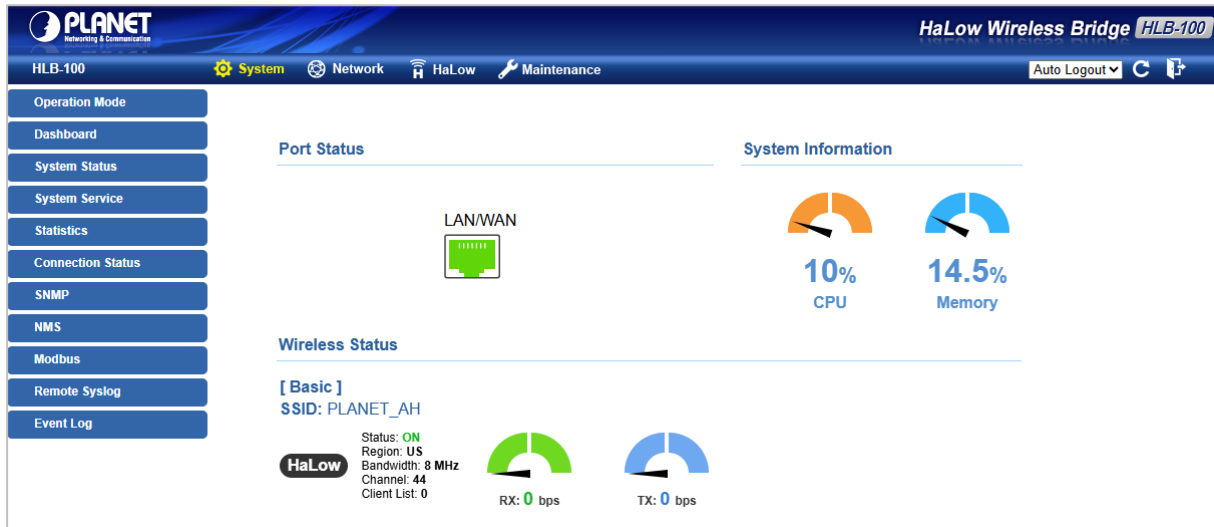


Figure 4-13: Dashboard

Port Status

Object	Description
	Ethernet port is in use.
	Ethernet port is not in use.

Wireless Status

Object	Description
	Wireless is in use.
	Wireless is not in use.

System Information

Object	Description
CPU	Display the CPU loading
Memory	Display the memory usage

4.1.4 System Status

This page displays system information as shown in [Figure 4-14](#).

Device Information	
Model Name	HLB-100
Firmware Version	v1.2203b250117
Region	ETSI
Current Time	2023-04-28 Friday 06:54:49
Running Time	0 day, 02:26:51

LAN	
MAC Address	A8:F7:E0:00:16:01
Connection Type	Static
IP Address	192.168.1.253
Netmask	255.255.255.0
Gateway	192.168.1.254

Halow WiFi	
Status	ON
SSID	PLANET_AH
Channel	44
Encryption	WPA3 Personal
MAC Address	A8:F7:E0:00:16:02

Figure 4-14: Status

4.1.5 System Service

This page displays the number of packets that pass through the router on the WAN and LAN. The statistics are shown in [Figure 4-15](#).

Server Service			
#	Action	Service	Status
1	✓ Enabled	DHCP Service	DHCP Table: 5
2	✗ Disabled	DDNS Service	Not enabled
3	✗ Disabled	Quality of Service	
4	✗ Disabled	RADIUS Service	
5	✗ Disabled	Captive Portal	
6	✓ Enabled	HaLow WiFi	SSID: PLANET_AH

Secured Server Service			
#	Action	Service	Status
1	✓ Enabled	Cybersecurity	TLS 1.1, TLS 1.2, TLS 1.3
2	✓ Enabled	SPI Firewall	
3	✗ Disabled	MAC Filtering	(Active / Maximum Entries) 0 / 32
4	✗ Disabled	IP Filtering	(Active / Maximum Entries) 0 / 32
5	✗ Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32

Figure 4-15: Service

4.1.6 Statistics

This page displays the number of packets that pass through the router on the WAN and LAN. The statistics are shown in [Figure 4-16](#).

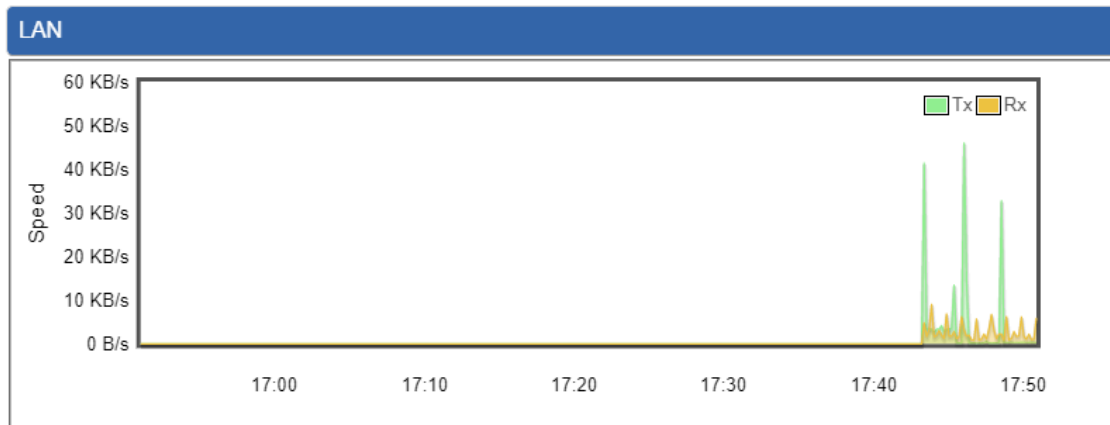


Figure 4-16: Statistics

4.1.7 Connection Status

The page will show the DHCP Table and ARP Table. The status is shown in [Figure 4-17](#).

DHCP Table			
Name	IP Address	MAC Address	Expiration Time

ARP Table		
IP Address	MAC Address	ARP Type
192.168.1.11	00:30:4f:9e:b7:df	dynamic
192.168.1.188	00:05:1b:c5:51:14	dynamic
192.168.1.239	a8:f7:e0:6a:a3:a4	dynamic
192.168.1.1	00:e0:53:00:12:01	dynamic

Figure 4-17: Connection Status

4.1.8 SNMP

This page provides SNMP setting of the router as shown in Figure 4-18.

SNMP

SNMP ☒ Enable ☐ Disable

SNMP Versions SNMP v1,v2c

Read Community public

Write Community private

Engine ID

SNMP v3 Security Level AuthPriv

SNMP v3 User Name

SNMP v3 Auth Protocol MD5

SNMP v3 Auth Password

SNMP v3 Privacy Protocol DES

SNMP v3 Privacy Password

System Identification

System Name HLB-100

System Description

System Location Default Location

System Contact Default Contact

SNMP Trap Receiver Configuration

SNMP Trap ☐ Enable ☒ Disable

SNMP Trap Destination 1

SNMP Trap Destination 2

Apply Settings
Cancel Changes

Figure 4-18: SNMP

Object	Description
Enable SNMP	Disable or enable the SNMP function. The default configuration is enabled.
Read/Write Community	Allows entering characters for SNMP Read/Write Community of the router.
System Name	Allows entering characters for system name of the router.
System Location	Allows entering characters for system location of the router.
System Contact	Allows entering characters for system contact of the router.
Apply Settings	Press this button to save and apply changes.
Cancel Changes	Press this button to undo any changes made locally and revert to previously saved values.

4.1.9 NMS

The CloudViewer Server – Internet screens – is shown in [Figure 4-19](#).

NMS Configuration

NMS	PLANET CloudViewer Server - Internet ▼
Email	
Password	
Connection Status	Not enabled

Apply Settings
Cancel Changes

Figure 4-19: CloudViewer Server

Object	Description
Email	The email is registered on CloudViewer Server.
Password	The password of your CloudViewer account.
Connection Status	Indicates the status of connecting CloudViewer Server.

4.1.10 Remote Syslog

Remote Syslog	
Enable	<input type="checkbox"/>
Syslog Server	<input type="text"/>
Port Destination	<input type="text"/> (1~65535)

Figure 4-20: Remote Syslog

Object	Description
Enable Remote Syslog	Enable Captive Portal on routers.

4.1.11 Event Log

Event Log			
1			
No.	Date Time	Uptime	Message
1	2021-04-22 16:14:19	0d 00:03:19	Wireless configure change
2	2021-04-22 16:14:19	0d 00:03:19	Firewall configure change
3	2021-04-22 16:14:19	0d 00:03:19	Network configure change
4	2021-04-22 16:14:19	0d 00:03:19	DHCP configure change
5	2021-04-22 16:14:19	0d 00:03:19	Network configure change
6	2021-04-22 16:14:19	0d 00:03:19	Network configure change
7	2021-04-22 16:13:14	0d 00:02:15	Web configure change
8	2021-04-22 16:13:06	0d 00:02:07	Web configure change
9	2021-04-22 16:13:05	0d 00:02:05	RADIUS configure change
10	2021-04-22 16:13:05	0d 00:02:05	Wireless configure change
11	2021-04-22 16:13:05	0d 00:02:05	Firewall configure change
12	2021-04-22 16:13:05	0d 00:02:05	Network configure change
13	2021-04-22 16:13:05	0d 00:02:05	DHCP configure change
14	2021-04-22 16:13:05	0d 00:02:05	Network configure change
15	2021-04-22 16:13:05	0d 00:02:05	Network configure change
16	2021-04-22 16:13:05	0d 00:02:05	System configure change
17	2021-04-22 16:11:33	0d 00:00:33	UPnP configure change
18	2021-04-22 16:11:27	0d 00:00:27	Wireless configure change
19	2021-04-22 08:11:27	0d 00:00:27	Network configure change
20	2021-04-22 08:11:27	0d 00:00:27	Web configure change

Clear All Event Logs

Figure 4-21: Event Log

Object	Description
Event Log	Display Event Log information.

4.2 Network

The Network function provides WAN, LAN and network configuration of the router as shown in [Figure 4-22](#).



Figure 4-22: Network Menu

Object	Description
WAN	Allows setting WAN interface.
LAN	Allows setting LAN interface.
UPnP	Disable or enable the UPnP function. The default configuration is disabled.
Routing	Allows setting Route.
RIP	Disable or enable the RIP function. The default configuration is disabled.
OSPF	Disable or enable the OSPF function. The default configuration is disabled.
IGMP	Disable or enable the IGMP function. The default configuration is disabled.
IPv6	Allows setting IPv6 WAN interface.
DHCP	Allows setting DHCP Server.
DDNS	Allows setting DDNS and PLANET DDNS.
MAC Address Clone	Allows setting WAN MAC Address Clone.

4.2.1 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the router as shown in [Figure 4-23](#). Here you may select the access method by clicking the item value of WAN access type.

WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="Static"/> ▾
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="DHCP"/> ▾
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="PPPoE"/> ▾
Username	<input type="text"/>
Password	<input type="text"/>

WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="button" value="PPTP"/> ▾
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Enable MPPE Encryption	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Type	<input type="button" value="DHCP"/> ▾


WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="button" value="L2TP"/> ▾
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Connection Type	<input type="button" value="DHCP"/> ▾

Figure 4-23: WAN

Object	Description
WAN Access Type	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.
	<div>Static</div> <div> Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP. </div> <div> Each IP address entered in the fields must be in the appropriate IP form, where the four octets are separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format. </div> <div> IP Address Enter the IP address assigned by your ISP. </div> <div> Netmask Enter the Subnet Mask assigned by your ISP. </div>

Object	Description
	Gateway Enter the Gateway assigned by your ISP. DNS Server The DNS server information will be supplied by your ISP.
	DHCP Select DHCP Client to obtain IP Address information automatically from your ISP.
	PPPoE Select PPPOE if your ISP is using a PPPoE connection and provide you with PPPoE user name and password info.
	PPTP Enable or disable PPTP to pass through PPTP communication data.
	L2TP Enable or disable L2TP to pass through L2TP communication data.



WAN IP, whether obtained automatically or specified manually, should NOT be on the same IP net segment as the LAN IP; otherwise, the router will not work properly. In case of emergency, press the hardware-based "Reset" button.

4.2.2 LAN

This page is used to configure the parameters for local area network which connects to the LAN port of your router as shown in [Figure 4-24](#). Here you may change the settings for IP address, subnet mask, DHCP, etc.

LAN Configuration

IP Address	192.168.1.1
Netmask	255.255.255.0

Apply Settings
Cancel Changes

Figure 4-24: LAN Setup

Object	Description
IP Address	The LAN IP address of the router and default is 192.168.1.253 .
Net Mask	Default is 255.255.255.0 .

4.2.3 UPnP

UPnP Configuration

UPnP ☐ Enable ☒ Disable

Apply Settings **Cancel Changes**

Figure 4-25: UPnP

Object	Description
UpnP	Set the function as enable or disable

4.2.4 Routing

Please refer to the following sections for the details as shown in [Figures 5-28 and 29](#).

Routing Table Rules							
No.	Type	Destination	Netmask	Gateway	Interface	Comment	Action
Current Routing Table Information							
No.	Destination		Netmask	Gateway	Interface		
1	192.168.1.0		255.255.255.0	0.0.0.0	LAN		
<div>Add Routing Table Rule</div>							

Figure 4-26: Routing table

Routing Table Configuration	
Type	Host ▼
Destination	<input type="text"/>
Netmask	255.255.255.255 /32 ▼
Default Gateway	<input type="text"/>
Interface	LAN ▼
Comment	<input type="text"/>
<input type="button" value="Apply Settings"/> <input type="button" value="Cancel Changes"/>	

Figure 4-27: Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote router (or other network gateway) that the local router is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept.

Object	Description
Type	There are two types: Host and Net. When the Net type is selected, user does not need to input the Gateway.
Destination	The network or host IP address desired to access.
Net Mask	The subnet mask of destination IP.
Gateway	The gateway is the router or host's IP address to which the packet was sent. It must be the same network segment with the WAN or LAN port.
Interface	Select the interface that the IP packet must use to transmit out of the router when this route is used.
Comment	Enter any words for recognition.

4.2.5 RIP

RIP Configuration

Dynamic Route

☐ Enable ☒ Disable

RIP Versions

RIP 2 ▾

Apply Settings

Cancel Changes

Figure 4-28 RIP

Object	Description
Dynamic Route	Disable or enable the RIP function
RIP Versions	Set RIP Versions

4.2.6 OSPF

OSPF Configuration

OSPF

☐ Enable
 ☒ Disable

Router ID

Area ID

Apply Settings

Cancel Changes

Figure 4-29: OSPF

Object	Description
OSPF	Enable the OSPF function.
Router ID	Set Router ID
Area ID	Set Area ID

4.2.7 IGMP

IGMP Configuration

IGMP Proxy

☐ Enable ☒ Disable

IGMP Versions

Auto ▼

Apply Settings

Cancel Changes

Figure 4-30: IGMP

Object	Description
IGMP	Enable the IGMP function.
IGMP Versions	Select the GMP Versions

4.2.8 IPv6

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the router as shown in [Figure 4-36](#). It allows you to enable IPv6 function and set up the parameters of the router's WAN. In this setting you may change WAN connection type and other settings.

IPv6 - WAN1	
Connection Type	<input type="text" value="DHCP"/>
IPv6 Address	<input type="text"/>
Subnet Prefix Length	<input type="text" value="64"/>
Default Gateway	<input type="text"/>
IPv6 DNS Server 1	<input type="text"/>
IPv6 DNS Server 2	<input type="text"/>

IPv6 - LAN	
Type	<input checked="" type="radio"/> Delegate Prefix from WAN <input type="radio"/> Static
Static Address	<input type="text"/>
Subnet Prefix Length	<input type="text" value="64"/>

DHCPv6	
Address Assign	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful <input type="radio"/> Passthrough <input type="radio"/> Disable

IPv6 - WAN1

Connection Type
Static ▾

IPv6 Address

Subnet Prefix Length

Default Gateway

IPv6 DNS Server 1

IPv6 DNS Server 2

IPv6 - LAN

Type
☒ Delegate Prefix from WAN ☐ Static

Static Address

Subnet Prefix Length

DHCPv6

Address Assign
☒ Stateless ☐ Stateful ☐ Passthrough ☐ Disable

Apply Settings
Cancel Changes

Figure 4-31 IPv6 WAN setup

Object	Description
Connection Type	Select IPv6 WAN type either by using DHCP or Static.
IPv6 Address	Enter the WAN IPv6 address.
Subnet Prefix Length	Enter the subnet prefix length.
Default Gateway	Enter the default gateway of the WAN port.
IPv6 DNS Server 1	Input a specific DNS server.
IPv6 DNS Server 2	Input a specific DNS server.

4.2.9 DHCP

The DHCP service allows you to control the IP address configuration of all your network devices. When a client (host or other device such as networked printer, etc.) joins your network, it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP; this is something called "automatic network configuration" and is often the default setting. The setup is shown in [Figure 4-32](#).

DHCP Configuration

DHCP Server

☒ Enable ☐ Disable

Start IP Address

192.168.1.

Maximum DHCP Users

DNS Server

☒ Automatically ☐ Manually

Primary DNS Server

Secondary DNS Server

WINS

Lease Time

minutes

Domain Name

Static DHCP List

Index	Device Name	IP Address	MAC Address	Delete
		192.168.1.150	00:30:4F:00:00:01	<div style="border: 1px solid #ccc; padding: 2px 5px; background-color: #4a7ebb; color: white;">Add</div>

Apply Settings

Cancel Changes

Figure 4-32: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the router will assign IP addresses to the DHCP clients automatically. If user needs to disable the function, please set it as disable.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the router will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
DNS Server	By default, it is set Automatically, and the DNS server is the router's LAN IP address.

Object	Description
	If user needs to use specific DNS server, please set it Manually, and then input a specific DNS server.
Primary/Secondary DNS Server	Input a specific DNS server.
WINS	Input a WINS server if needed.
Lease Time	Set the time for using one assigned IP. After the lease time, the DHCP client will need to get new IP addresses from the router. Default is 1440 minutes.
Domain Name	Input a domain name for the router.

4.2.10 DDNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as **PLANET DDNS** (<http://www.planetddns.com>) and set up the domain name of your choice.

PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in [Figure 5-35](#).

PLANET DDNS

For example, you've just installed a PLANET IP camera with dynamic IP like 210.66.155.93 in the network. You can name this device as "Mycam1" and register a domain as Mycam1.planetddns.com at PLANET DDNS (<http://www.planetddns.com>). Thus, you don't need to memorize the exact IP address but just the URL link: Mycam1.planetddns.com.

PLANET Easy DDNS

PLANET Easy DDNS is an easy way to help user to get your Domain Name with just one click. You can just log in to the Web Management Interface of your devices, say, your router, and check the DDNS menu and just enable it. You don't need to go to <http://www.planetddns.com> to apply for a new account. Once you enabled the Easy DDNS, your PLANET Network Device will use the format PLxxxxxx where xxxxxx is the last 6 characters of your MAC address that can be found on the Web page or bottom label of the device. (For example, if the router's MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)

DDNS Configuration

Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Interface	<div style="border: 1px solid #ccc; padding: 2px;">WAN1 ▾</div>
DDNS Type	<div style="border: 1px solid #ccc; padding: 2px;">PLANET DDNS ▾</div>
PLANET Easy DDNS	<div style="border: 1px solid #ccc; padding: 2px;">Disable ▾</div>
User Name	<div style="border: 1px solid #ccc; height: 20px;"></div>
Password	<div style="border: 1px solid #ccc; height: 20px;"></div>
Host Name	<div style="border: 1px solid #ccc; height: 20px;"></div>
Interval	<div style="border: 1px solid #ccc; padding: 2px;">120</div> seconds
Connection Status	Not enabled

Apply Settings

Cancel Changes

Figure 4-33: PLANET DDNS

Object	Description
DDNS Service	By default, the DDNS service is disabled. If user needs to enable the function, please set it as enable.
Interface	User is able to select the interface for DDNS service. By default, the interface is WAN 1.
DDNS Type	There are three options: 1. PLANET DDNS: Activate PLANET DDNS service. 2. DynDNS: Activate DynDNS service. 3. NOIP: Activate NOIP service. Note that please first register with the DDNS service and set up the domain name of your choice to begin using it.
Easy DDNS	When the PLANET DDNS service is activated, user is able to select to enable or disable Easy DDNS. When this function is enabled, DDNS hostname will appear automatically. User doesn't go to http://www.planetddns.com to apply for a new account.
User Name	The user name is used to log in to DDNS service.
Password	The password is used to log in to DDNS service.
Host Name	The host name as registered with your DDNS provider.
Interval	Set the update interval of the DDNS function.
Connection Status	Show the connection status of the DDNS function.

4.2.11 MAC Address Clone

Clone or change the MAC address of the WAN interface. The setup is shown below.

MAC Address Clone - WAN1

Clone WAN MAC
☐ Enable ☒ Disable

MAC Address

MAC Address Clone - WAN2

Clone WAN MAC
☐ Enable ☒ Disable

MAC Address

Apply Settings
Cancel Changes

Figure 4-34 MAC Address Clone for WAN

Object	Description
Clone WAN MAC	Set the function as enable or disable.
MAC Address	Input a MAC Address, such as A8:F7:E0:00:06:62.

4.3 Security

The Security menu provides Firewall, Access Filtering and other functions as shown in [Figure 4-35](#).

Please refer to the following sections for the details.

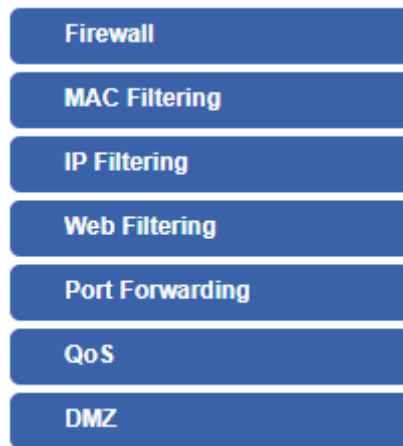


Figure 4-35: Security menu

Object	Description
Firewall	Allows setting DoS (Denial of Service) protection as enable.
MAC Filtering	Allows setting MAC Filtering.
IP Filtering	Allows setting IP Filtering.
Web Filtering	Allows setting Web Filtering.
Port Forwarding	Allows setting Port Forwarding.
QoS	Allows setting Qos.
DMZ	Allows setting DMZ.

4.3.1 Firewall

A "Denial-of-Service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service. The router can prevent specific DoS attacks as shown in Figure 4-36.

Firewall Protection

SPI Firewall

☒ Enable
 ☐ Disable

DDoS

Block SYN Flood	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	30	Packets/Second
Block FIN Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	30	Packets/Second
Block UDP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	30	Packets/Second
Block ICMP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	5	Packets/Second
Block IP Teardrop Attack	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block Ping of Death	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block TCP packets with SYN and FIN Bits set	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block TCP packets with FIN Bit set but no ACK Bit set	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block TCP packets without Bits set	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

System Security

Block WAN Ping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
HTTP Port		80
HTTPs Port		443
Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Temporarily block when login failed more than	0	(0 means no limit)
IP blocking period	0	minute(s) (0 means permanent blocking)
Blocked IP	0.0.0.0	

NAT ALGs

FTP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
TFTP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
RTSP ALG	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
H.323 ALG	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
SIP ALG	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

Apply Settings

Cancel Changes

Figure 4-36: Firewall

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.
Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block FIN Flood	If the function is enable and when the number of the current FIN packets is beyond the set value, the router will start the blocking function immediately. The default configuration is disabled.
Block UDP Flood	If the function is enabled and when the number of the current UDP-FLOOD packets is beyond the set value, the router will start the blocking function immediately. The default configuration is disabled.
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack. The default configuration is disabled.
IP TearDrop	If the function is enabled, the router will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.
Ping Of Death	If the function is enabled, the router will block Ping of Death attack that aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size causing the target machine to freeze or crash.
TCP Packets with SYN and FIN Bits set	Set the function as enable or disable
TCP Packets with FIN Bit set but no ACK Bit set	Set the function as enable or disable
TCP Packets without Bits set	Set the function as enable or disable
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
HTTP Port	The default is 80.
HTTPs Port	The default is 443.
Remote Management	Enable the function to allow the web server access of the router from the Internet network. The default configuration is disabled.
Temporarily block when login failed	The default is 0. (0 means no limit)

IP blocking period	The default is 0. (0 means permanent blocking)
Blocked IP	0.0.0.0
FTP ALG	Set the function as enable or disable.
TFTP ALG	Set the function as enable or disable.
RTSP ALG	Set the function as enable or disable.
H.323 ALG	Set the function as enable or disable.
SIP ALG	Set the function as enable or disable.

4.3.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network or Internet through the router. Use of such filters can be helpful in securing or restricting your local network as shown in [Figure 4-37](#).

MAC Filtering

MAC Filtering

☐ Enable
☒ Disable

Interface

☐ LAN
☐ WAN

MAC Filtering Rules


Index	Active	Device Name	MAC Address	Action
		<input type="text" value="abc"/>	<input type="text" value="00:30:4F:00:00:01"/>	<input type="button" value="Add"/>

Figure 4-37: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the router will block traffic of the MAC address on the list.
Interface	Select the function works on LAN, WAN or both. If you want to block a LAN device's MAC address, please select LAN, vice versa.
MAC Address	Input a MAC address you want to control, such as A8:F7:E0:00:06:62.
Add	When you input a MAC address, please click the "Add" button to add it into the list.

4.3.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in [Figure 4-38](#). To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.

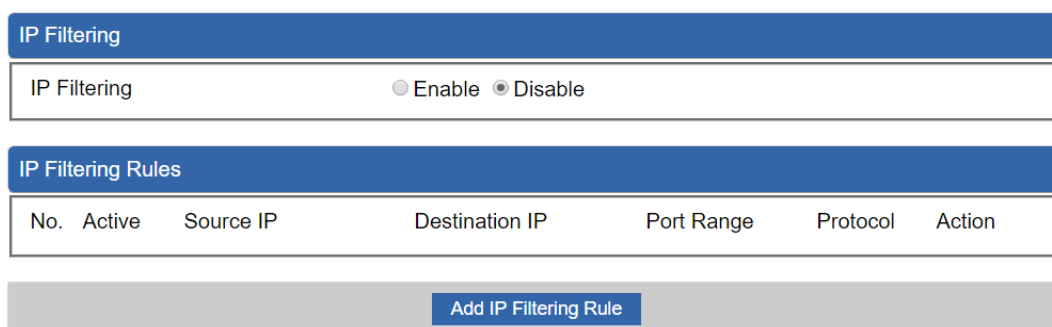


Figure 4-38: IP Filtering

Object	Description
IP Filtering	Set the function as enable or disable.
Add IP Filtering Rule	Go to the Add Filtering Rule page to add a new rule.

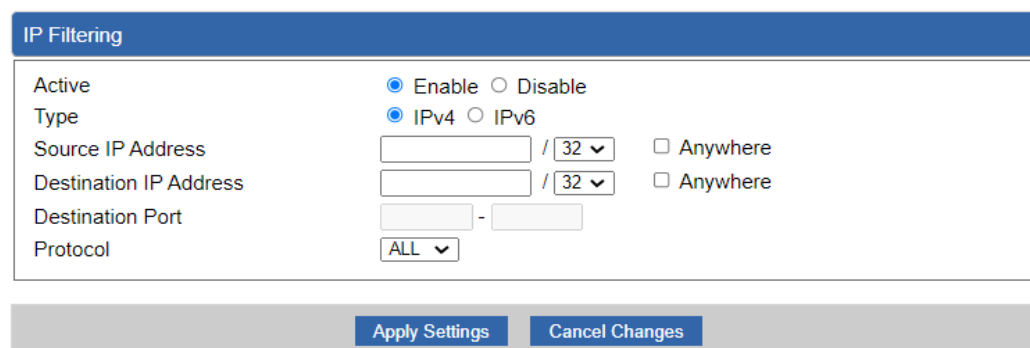


Figure 4-39: IP Filter Rule Setting

Object	Description
Enable	Set the rule as enable or disable.
Type	Set the type as IPv4 or IPv6
Source IP Address	Input the IP address of LAN user (such as PC or laptop) which you want to control.
Anywhere (of source IP Address)	Check the box if you want to control all LAN users.
Destination IP Address	Input the IP address of web site which you want to block.
Anywhere (of destination	Check the box if you want to control all web sites, meaning the

Object	Description
IP Address)	LAN user can't visit any web site.
Destination Port	Input the port of destination IP Address which you want to block. Leave it as blank if you want to block all ports of the web site.
Protocol	Select the protocol type (TCP, UDP or all). If you are unsure, please leave it to the default all protocol.

4.3.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in Figure 4-40. Block those URLs which contain keywords listed below.

Web Filtering

Web Filtering
☐ Enable
☒ Disable

Web Filtering Rules

No.	Active	Filter Keyword	Action
<div>Add Web Filtering Rule</div>			

Figure 4-40: Web Filtering

Object	Description
Web Filtering	Set the function as enable or disable.
Add Web Filtering Rule	Go to the Add Web Filtering Rule page to add a new rule.

Web Filter Settings

Status

Filter Keyword

Apply Settings

Cancel Changes

Figure 4-41: Web Filtering Rule Setting

Object	Description
Status	Set the rule as enable or disable.
Filter Keyword	Input the URL address that you want to filter, such as www.yahoo.com.

4.3.5 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall as shown in [Figure 4-42](#). These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Router's NAT firewall.

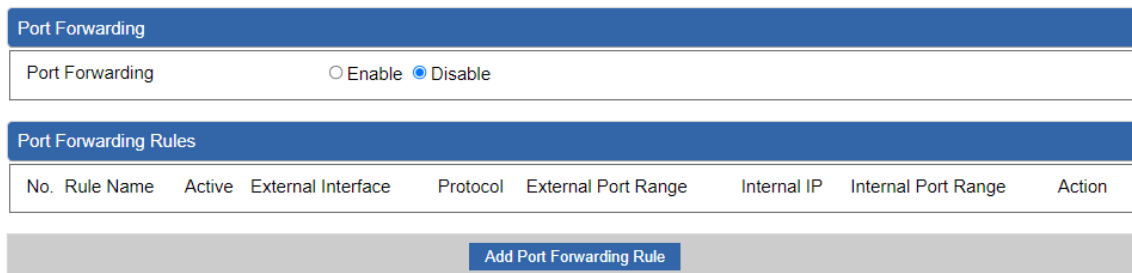


Figure 4-42: Port Forwarding

Object	Description
Port Forwarding	Set the function as enable or disable.
Add Port Forwarding Rule	Go to the Add Port Forwarding Rule page to add a new rule.

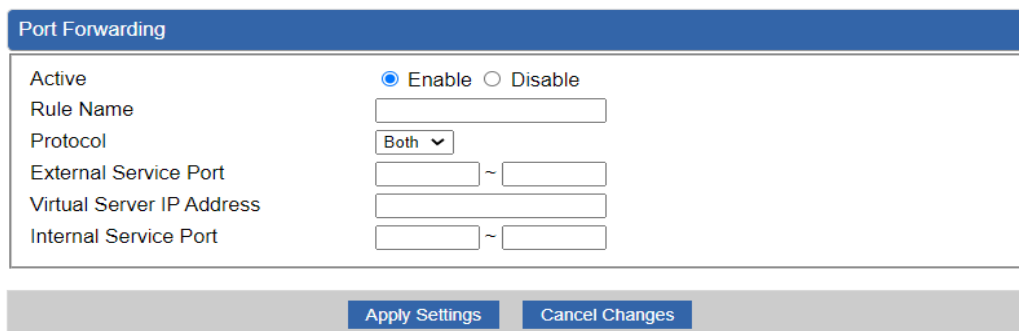


Figure 4-43: Port Forwarding Rule Setting

Object	Description
Active	Set the function as enable or disable
Rule Name	Enter any words for recognition.
Protocol	Select the protocol type (TCP, UDP or both). If you are unsure, please leave it to the default both protocols.
External Service Port	Enter the external ports you want to control. For TCP and UDP services, enter the beginning of the range of port numbers used by

Object	Description
	the service. If the service uses a single port number, enter it in both the start and finish fields.
Virtual Server IP Address	Enter the local IP address.
Internal Service Port	Enter local ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

4.3.6 QoS

QoS - WAN1

Quality of Service

☐ Enable
☒ Disable

Upstream

Kbps

Downstream

Kbps

Upstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
Express	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
Standard	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
Bulks	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps

Downstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
Express	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
Standard	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
Bulks	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps

Service Priority

Protocol	Description	Priority	Action
<input type="text" value="AOL(TCP:5190)"/> ▼	AOL Instant Messenger protocol	<input type="text" value="Premium"/> ▼	<input type="button" value="Add"/>

Network Priority

Source Network	Protocol	Destination Port Range	Priority	Action
<input type="text"/> / <input type="text"/>	<input type="text" value="ALL"/> ▼	<input type="text"/> -- <input type="text"/>	<input type="text" value="Premium"/> ▼	<input type="button" value="Add"/>

Figure 4-44: QoS Setting

Object	Description
QoS - WAN1	Enable/disable QoS function
Upstream Bandwidth	Setting Upstream Bandwidth
Downstream Bandwidth	Setting Downstream Bandwidth
Service Priority	Setting Service Priority
Network Priority	Setting Network Priority

4.3.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in [Figure 4-45](#). Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ - WAN1

DMZ

☐ Enable ☒ Disable

DMZ IP Address

Apply Settings

Cancel Changes

Figure 4-45: DMZ

Object	Description
DMZ	Set the function as enable or disable. If the DMZ function is enabled, it means that you set up DMZ at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/online game can have two way connections.
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.

4.4 Wireless

The Wireless menu provides the following features for managing the system

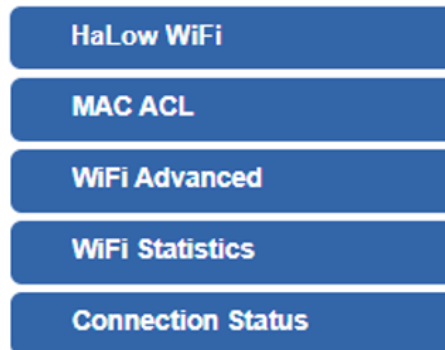


Figure 4-46: Wireless Menu

Object	Description
HaLow Wi-Fi	Allow to configure HaLow Wi-Fi.
MAC ACL	Allow configure MAC ACL.
Wi-Fi Advanced	Allow to configure advanced setting of Wi-Fi.
Wi-Fi Statistics	Display the statistics of Wi-Fi traffic.
Connection Status	Display the connection status.

4.4.1 HaLow Wi-Fi

This page allows the user to define HaLow Wi-Fi.

Halow WiFi Configuration

Basic

Wireless Status

☒ Enable
 ☐ Disable

Wireless Name (SSID)

PLANET_AH

Hide SSID

☐ Enable
 ☒ Disable

Wireless Mode

8 MHz

Channel

44

Encryption

WPA3 Personal

Passphrase

12345678

WiFi Multimedia

☒ Enable
 ☐ Disable

WiFi Analyzer

Scan

Apply Settings

Cancel Changes

Figure 4-47: HaLow Wi-Fi

Object	Description
Wireless Status	Allows user to enable or disable HaLow Wi-Fi.
Wireless Name (SSID)	It is the wireless network name. The default SSID is "PLANET_AH".
Hide SSID	Allows user to enable or disable SSID.
Wireless Mode	Select the operating wireless mode.
Channel	It shows the channel of the CPE. Default channel is 44.
Encryption	Select the wireless encryption. The default is "Open".
Passphrase	Enter the wireless password used for client authentication.
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function.
WiFi Analyzer	Launch a wireless scan tool to detect nearby HaLow SSIDs. Use this to assist in manual channel selection or connection analysis.

4.4.2 MAC ACL

This page allows the user to define MAC ACL.

MAC ACL

MAC ACL

☐ Enable
☒ Disable

MAC ACL Rules


Index	Active	Device Name	MAC Address	Action
		<input type="text" value="abc"/>	<input type="text" value="00:30:4F:00:00:01"/>	<div>Add</div> <div>Scan</div>

Figure 4-48: MAC ACL

Object	Description
Active	Allows the devices to pass in the rule.
Device Name	Set an allowed device name.
MAC Address	Set an allowed device MAC address.
Add	Press the “ Add ” button to add end-device that is scanned from wireless network and mark them.
Scan	Connect to client list.

4.4.3 Wi-Fi Advanced

This page allows the user to define advanced setting of Wi-Fi.

WiFi Advanced

Region	US ▼
Protected Management Frames	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Beacon Interval	100 (ms)
DTIM Period	1 ▼
Max Inactivity	300 (1-65536)
Maximum Associated Clients	32 (Range 1~32)

Apply Settings

Cancel Changes

Figure 4-49: Wi-Fi Advanced

Object	Description
Region	Select the regulatory domain for wireless channel availability and power limitations. This must match the deployment region to comply with local regulations.
Protected Management Frames	Enable this feature to protect wireless management frames (e.g., authentication, association) against spoofing or eavesdropping. Recommended to keep enabled.
Beacon Interval	Set the interval (in milliseconds) between beacon transmissions. Default is 100 ms. Adjusting this affects power saving and roaming behavior of clients.
DTIM Period	Set the Delivery Traffic Indication Message period. Defines how often broadcast/multicast data is sent. A higher DTIM conserves client power.
Max Inactivity	Define the maximum idle time (in seconds) before disconnecting an inactive client. Range: 1–65536.
Maximum Associated Clients	Set the maximum number of client devices allowed to connect to this HLB-100 unit. Range: 1–32

4.4.4 Wi-Fi Statistics

This page shows the statistics of Wi-Fi traffic.

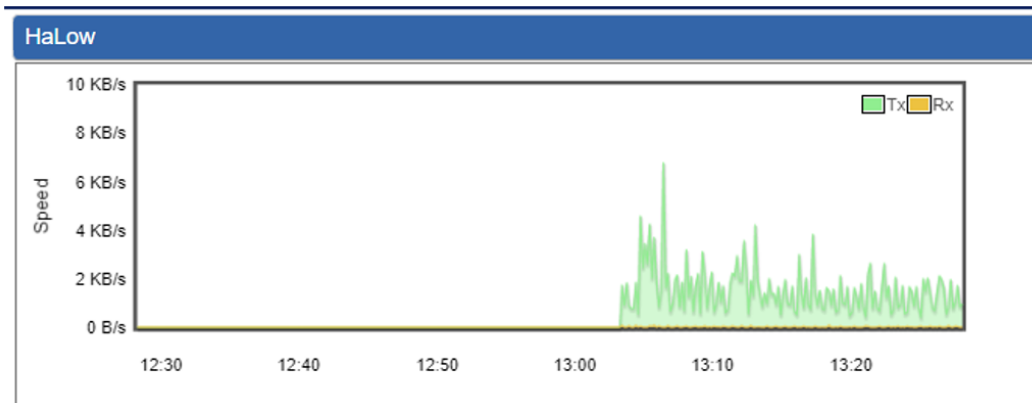


Figure 4-50: Wi-Fi Statistics

4.4.5 Connection Status

This page shows the host names and MAC address of all the clients in your network

Client List				
No.	Name	MAC Address	Signal	Connected Time

Figure 4-51: Connection Status

Object	Description
Name	Display the host name of connected clients.
MAC Address	Display the MAC address of connected clients.
Signal	Display the connected signal of connected clients.
Connected Time	Display the connected time of connected clients.

4.5 Maintenance

The Maintenance menu provides the following features for managing the system



Figure 4-52: Maintenance

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the router's configuration to local or USB sticker. Restore the router's configuration from local or USB sticker.
Firmware Upgrade	Upgrade the firmware from local or USB storage.
Reboot / Reset	Reboot or reset the system.
Auto Reboot	Allows setting auto-reboot schedule.
Diagnostics	Allows you to issue ICMP PING packets to troubleshoot IP.

4.5.1 Administrator

To ensure the router's security is secure, you will be asked for your password when you access the router's Web-based utility. The default user name and password are "**admin**". This page allows you to modify the user name and passwords as shown in [Figure 4-53](#).

Account Password

Username	admin
Password	
Confirm Password	

Apply Settings
Cancel Changes

Figure 4-53: Administrator

Object	Description
Username	Input a new username.
Password	Input a new password.
Confirm Password	Input the password again.

4.5.2 Date and Time

This section assists you in setting the system time of the router. You are able to either select to set the time and date manually or automatically obtain the GMT time from Internet as shown in [Figure 4-54](#).

Date and Time

Current Time

Year Month Day Hour Minute Second

Time Zone Select

NTP Client Update

☐ Enable ☒ Disable

NTP Server

Figure 4-54: Date and Time

Object	Description
Current Time	Show the current time. User is able to set time and date manually.
Time Zone Select	Select the time zone of the country you are currently in. The router will set its time based on your selection.
NTP Client Update	Once this function is enabled, router will automatically update current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.

4.5.3 Saving/Restoring Configuration

This page shows the status of the configuration. You may save the setting file to either USB storage or PC and load the setting file from USB storage or PC as [Figure 4-55](#) is shown below:

Save/Restore Configuration

Configuration Export

Export

Configuration Import


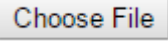

Choose File

No file chosen

Import

Figure 4-55: Save/Restore Configuration

■ Save Setting to PC

Object	Description
Configuration Export	Press the  button to save setting file to PC.
Configuration Import	Press the  button to select the setting file, and then press the  button to upload setting file from PC.

4.5.4 Firmware Upgrading

This page provides the firmware upgrade of the router as shown in [Figure 4-56](#).

Firmware Information	
Firmware Version	v2.2102b210922
Last Upgrade Date	N/A

Firmware Upgrade	
Select File	<input type="button" value="Choose File"/> No file chosen
<input type="button" value="Upgrade"/>	

Figure 4-56: Firmware upgrade

Object	Description
Choose File	Press the button to select the firmware.
Upgrade	Press the button to upgrade firmware to system.

4.5.5 Reboot / Reset

This page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, users have to re-log in to the Web interface as [Figure 4-57](#) is shown below:

Reboot / Reset

Reboot Button

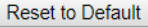
Reboot

Reset Button

Reset to Default

☐ I'd like to keep the network profiles.
Keep your current network profiles and reset all other configuration to factory defaults.

Figure 4-57: Reboot/Reset

Object	Description
Reboot	Press the button to reboot system.
Reset	Press the button to restore all settings to factory default settings.
I'd like to keep the network profiles.	Check the box and then press the  button to keep the current network profiles and reset all other configurations to factory defaults.

4.5.6 Auto Reboot

Auto Reboot

Auto Reboot
☐ Enable ☒ Disable

Reboot Type

☐ Daily based ☒ Selected Week Day

☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday

☐ Saturday ☐ Sunday

Time

 : (HH/MM)

Apply Settings
Cancel Changes

Figure 4-58: Auto Reboot

Object	Description
Auto Reboot	Disable or enable the Auto Reboot function.
Reboot Type	Set the function type.
Time	Select reboot time for clock.

4.5.7 Diagnostics

The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press “Ping”, ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The Page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping is shown in [Figure 4-59](#).

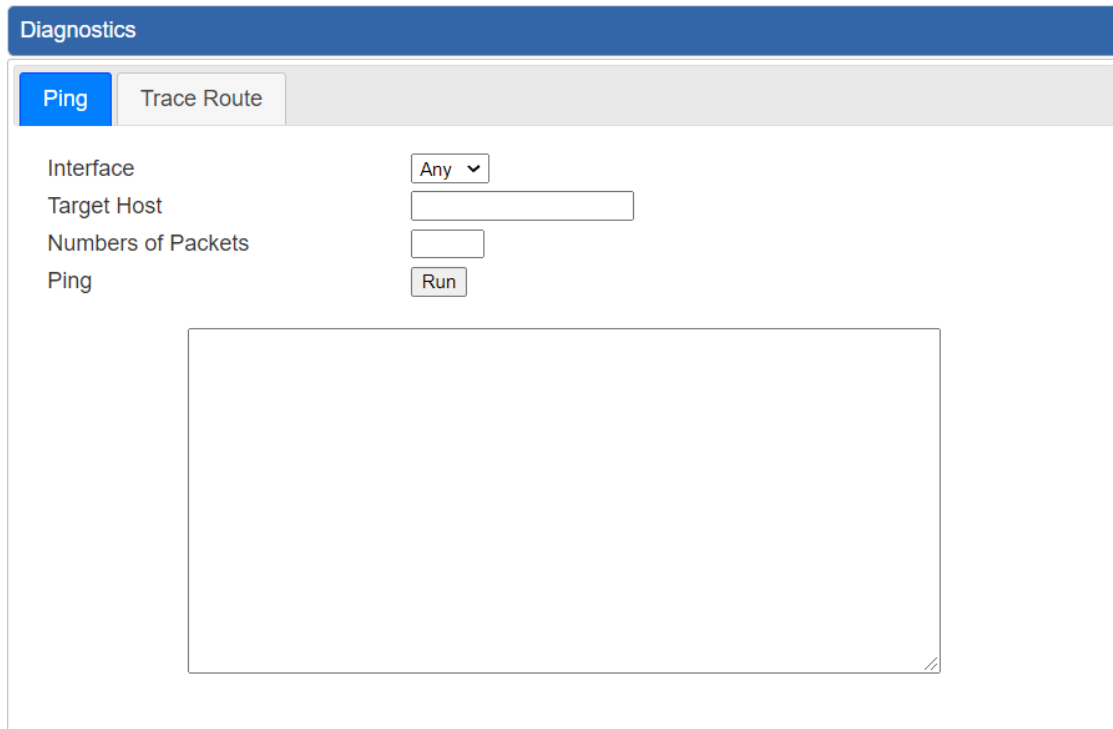


Figure 4-59: Ping

Object	Description
Interface	Select an interface of the router.
Target Host	The destination IP Address or domain.
Number of Packets	Set the number of packets that will be transmitted; the maximum is 100.
Ping	The time of ping

Diagnostics

Ping

Trace Route

Target Host

Trace

Run

Figure 4-60: Trace Route

Object	Description
Target Host	The destination IP Address or domain.
Trace	The time of ping



Be sure the target IP address is within the same network subnet of the router, or you have to set up the correct gateway IP address.

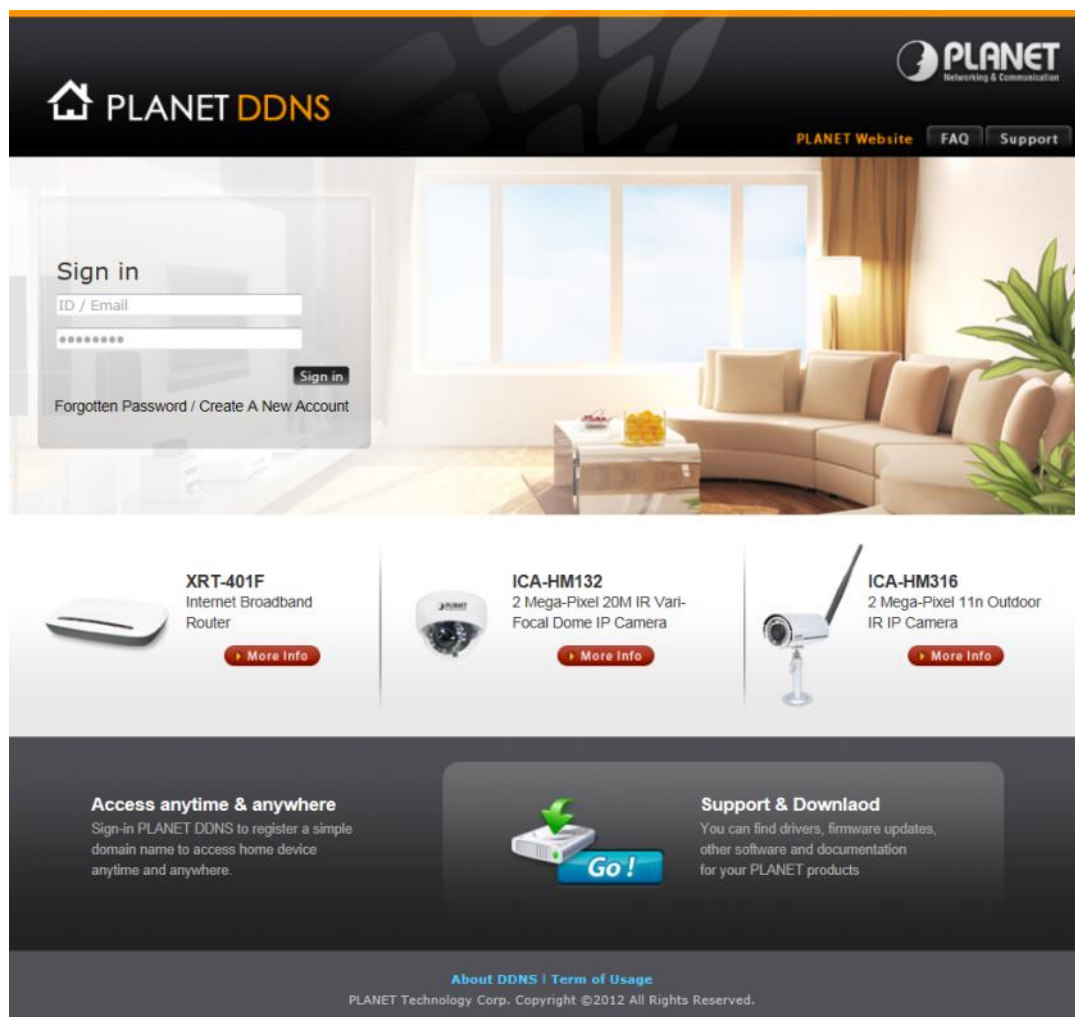
Appendix A: DDNS Application

Configuring **PLANET** DDNS steps:

Step 1: Visit DDNS provider's web site and register an account if you do not have one yet. For example, register an account at <http://planetddns.com>

Step 2: Enable DDNS option through accessing web page of the device.

Step 3: Input all DDNS settings.



Appendix B: Troubleshooting

If you find the HLB-100 is working improperly or stop responding to you, please read this troubleshooting first before contacting the dealer for help. Some problems can be solved by yourself within a very short time.

Scenario	Solution
The HLB-100 is not responding to me when I want to access it by Web browser.	<ul style="list-style-type: none"> a. Please check the connection of the power cord and the Ethernet cable of this HLB-100. All cords and cables should be correctly and firmly inserted into the HLB-100. b. If all LEDs on this HLB-100 are off, please check the status of power adapter, and make sure it is correctly powered. c. You must use the same IP address section which HLB-100 uses. d. Are you using MAC or IP address filter? Try to connect the HLB-100 by another computer and see if it works; if not, please reset the HLB-100 to the factory default settings by pressing the 'reset' button for over 7 seconds. e. Use the Smart Discovery Tool to see if you can find the HLB-100 or not. f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help. g. If all the solutions above don't work, contact the dealer for help.
I can't get connected to the Internet.	<ul style="list-style-type: none"> a. Go to 'Status' -> 'Internet Connection' menu on the router connected to the HLB-100, and check Internet connection status. b. Please be patient. Sometimes Internet is just that slow. c. If you've connected a computer to Internet directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. d. Check PPPoE / L2TP / PPTP user ID and password entered in the router's settings again. e. Call your Internet service provider and check if there's something wrong with their service.

Scenario	Solution
	<ul style="list-style-type: none"> f. If you just can't connect to one or more website, but you can still use other internet services, please check URL/Keyword filter. g. Try to reset the HLB-100 and try again later. h. Reset the device provided by your Internet service provider too. i. Try to use IP address instead of host name. If you can use IP address to communicate with a remote server, but can't use host name, please check DNS setting.
I can't locate my HLB-100 by my wireless device.	<ul style="list-style-type: none"> a. 'Broadcast ESSID' set to off? b. Both of the two antennas are properly secured. c. Are you too far from your HLB-100? Try to get closer. d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File downloading is very slow or breaks frequently.	<ul style="list-style-type: none"> a. Internet is slow sometimes. Please be patient. b. Try to reset the HLB-100 and see if it's better after that. c. Try to know what computers do on your local network. If someone's transferring big files, Internet access may be really slow. d. If this never happens before, call you Internet service provider to know if there is something wrong with their network.
I can't log in to the web management interface; the password is wrong.	<ul style="list-style-type: none"> a. Make sure you're connecting to the correct IP address of the HLB-100. b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard reset.
The HLB-100 becomes hot.	<ul style="list-style-type: none"> a. This is not a malfunction; don't keep your hand on the HLB-100's case. b. If you smell something wrong or see the smoke coming out from HLB-100 or A/C power adapter, please disconnect the HLB-100 and power source from utility power (make sure it's safe before you're doing this), and call the dealer where it is purchased for help.

Appendix C: Note on EU Regulatory Compliance

The HLB-100-EU868 is designed to comply with CE EN 300 220 requirements for sub-GHz wireless operation within the EU region.

No manual configuration is required under normal use, as the wireless parameters are automatically adjusted to meet applicable regional regulations.