



ALL02850N



WLAN N Access Point /Client Bridge



Table of Contents

1	INTRODUCTION	5
1.1	Features and Benefits	5
1.2	Package Contents	6
1.3	System Requirements	6
1.4	Applications	6
2	BEFORE YOU BEGIN	8
2.1	Considerations for Wireless Installation	8
2.2	Computer Settings (Windows XP/Windows Vista/Windows 7)	9
2.3	Apple Mac X OS	11
2.4	Hardware Installation	12
3	CONFIGURING YOUR CLIENT BRIDGE	14
3.1	Default Settings	14
3.2	Web Configuration	15
4	BUILDING A WIRELESS NETWORK	17
4.1	Client Bridge Mode	17
4.2	Access Point Mode	18
4.3	WDS AP Mode	19
4.4	WDS Bridge Mode	20
4.5	Router Mode	21
4.6	Repeater Mode	22
5	SYSTEM	23
5.1	Operation Mode	23
5.2	Status	24
5.3	DHCP	27
5.4	Schedule	29

5.5	Event Log.....	31
5.6	Monitor.....	32
6	WIRELESS.....	33
6.1	Status.....	33
6.2	Basic.....	35
6.3	Site Survey.....	39
6.4	Advanced.....	42
6.5	Security.....	45
6.6	Filter.....	49
6.7	WPS (Wi-Fi Protected Setup).....	50
6.8	Client List.....	52
6.9	VLAN.....	53
6.10	AP Profile.....	54
7	NETWORK.....	56
7.1	Status.....	56
7.2	LAN.....	57
7.3	Spanning Tree.....	59
7.4	WAN (Router mode).....	60
7.4.1	Static IP Address.....	60
7.4.2	Dynamic IP Address.....	61
7.4.3	PPP over Ethernet (PPPoE).....	62
7.4.4	Point-to-Point Tunneling Protocol (PPTP).....	62
8	FIREWALL.....	64
8.1	Enable.....	64
8.2	DMZ.....	65
8.3	DoS.....	66
8.4	MAC Filter.....	67
8.5	IP Filter.....	68
8.6	URL Filter.....	69



9	ADVANCED	70
9.1	Network Address Translation (NAT)	70
9.2	Port Mapping	71
9.3	Port Forwarding	72
9.4	Port Triggering	73
9.5	Application Layer Gateway (ALG)	74
9.6	Universal Plug and Play (UPnP)	75
9.7	Quality of Service (QoS)	76
9.8	Static Routing	78
9.9	Dynamic Routing	79
9.10	Routing Table	80
10	MANAGEMENT	81
10.1	Admin	81
10.2	SNMP	82
10.3	Firmware Upgrade	84
10.4	Configure	86
10.5	Reset	87
11	TOOLS	88
11.1	Time Setting	88
11.2	Diagnosis	89
12	LOGOUT	90
APPENDIX A – FCC INTERFERENCE STATEMENT		91
APPENDIX B – IC INTERFERENCE STATEMENT		92
APPENDIX C – CE INTERFERENCE STATEMENT		0



1 Introduction

The **ALL02850N** is a multi-function 802.11b/g/n product with 6 major multi-functions. The ALL02850N is designed to operate in every working environment including enterprises.

The ALL02850N is a Wireless Network device that delivers up to 6x faster speeds and 7x extended coverage than 802.11b/g devices. The ALL02850N supports use in the home network with superior throughput, performance, and significant wireless range. To protect data during wireless transmissions, the ALL02850N encrypts all wireless transmissions through WEP data encryption and supports WPA/WPA2 encryption. The ALL02850N has MAC address filtering to allow users to select differing stations to access the network. The ALL02850N is an ideal product to ensure network safety for both home and enterprise environments.

1.1 Features and Benefits

Features	Benefits
High Speed Data Rate Up to 300 Mbps	Capable of handling heavy data payloads such as HD multimedia streaming.
10/100 Fast Ethernet	Support up to 100Mbps networking speed.
IEEE 802.11n Draft Compliant and Backwards Compatible with 802.11b/g devices	Fully compatible with IEEE 802.11b/g/n devices.
Multi-Function	Allowing users to select Access Point, Client Bridge, WDS AP, WDS Bridge, Router or Universal Repeater mode in various applications.
Point-to-Point or Point-to-Multipoint Wireless Connectivity	Allows transfer of data from building to building.
Support Multiple SSID in AP mode (up to 4)	Allow clients to access different networks through a single access point and assign different policies and functions for each SSID through the built in software.
WPA/WPA2/IEEE 802.1x Support	Powerful data security.
MAC Address Filtering in AP Mode	Ensure a secure network connection.
User Isolation Support (AP mode)	Protect the private network between client users.

Power-over-Ethernet (IEEE802.3af)	Flexible Access Point locations.
Save User Settings	Firmware upgrade does not delete user settings.
SNMP Remote Configuration Management	Allows remote connection to configure or manage the ALL02850N easily.
QoS (WMM) support	Enhanced user performance and density.

1.2 Package Contents

The ALL02850N package contains the following items (all items must be in package to issue a refund):

- ALL02850N Wireless Long Range Multi-Function Client Bridge / Access Point
 - 12V/1A 100V~240V Power Adapter
 - RJ-45 Ethernet Cable
 - Detachable Antenna
 - CD with User's Manual
 - Quick Installation Guide
-
- Please use only the power supply unit that is delivered with the device.
 - Bitte verwenden Sie nur das mitgelieferte Netzteil.

1.3 System Requirements

The following are the minimum system requirements in order to configure the device.

- Computer with an Ethernet interface or Wireless Network.
- Windows, Mac OS, or Linux based operating systems.
- Web-Browsing Application (example: Internet Explorer, FireFox, Safari, or other similar software)

1.4 Applications

Wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) Difficult-to-Wire Environments

There are many situations where wires cannot be laid easily or cannot be hidden from view. Older buildings, sites with multiple buildings, and/or areas make the



installation of a Wired LAN impossible, impractical, and/or expensive.

b) Temporary Workgroups

Create temporary workgroups/networks in open areas such as parks, athletic arenas, exhibition centers, temporary offices, and construction sites where one wants a temporary Wireless LAN established and easily removed.

c) The Ability to Access Real-Time Information

Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information while dealing with patients, serving customers, and/or processing information.

d) Frequently Changing Environments

Set up networks in environments that change frequently (i.e.: Show Rooms, Exhibits, etc.).

e) Small Office and Home Office (SOHO) Networks

SOHO users need a cost-effective, easy and quick installation of a small network.

f) Wireless Extensions to Ethernet Networks

Extend network coverage where the network cannot reach (i.e.: There is no wired internet connection to reach certain location of the environment).

g) Wired LAN Backup

Implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational Facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

2 Before you Begin

This section will guide you through the installation process. Placement of the ENGNIUS ALL02850N is essential to maximize the ALL02850N's performance. Avoid placing the ALL02850N in an enclosed space such as a closet, cabinet, or wardrobe.

2.1 Considerations for Wireless Installation

The operating distance of all wireless devices cannot be pre-determined due to a number of unknown obstacles in the environment that the device is deployed in. These could be the number, thickness, and location of walls, ceilings, or other objects that the ALL02850N's wireless signals must pass through. Here are some key guidelines to allow the ALL02850N to have optimal wireless range.

- Keep the number of walls and/or ceilings between the ALL02850N and other network devices to a minimum. Each wall and/or ceiling can reduce the signal strength, resulting in lower signal strength.
- Building materials makes a difference. A solid metal door and/or aluminum studs may have a significant negative effect on the signal strength of the ALL02850N. Locate your wireless devices carefully so the signal can pass through a drywall and/or open doorways. Materials such as glass, steel, metal, concrete, water (example: fish tanks), mirrors, file cabinets, and/or brick can also lower your wireless signal strength.
- Interferences can also come from other electrical devices and/or appliances that generate RF noise. The most usual types are microwaves and cordless phones.

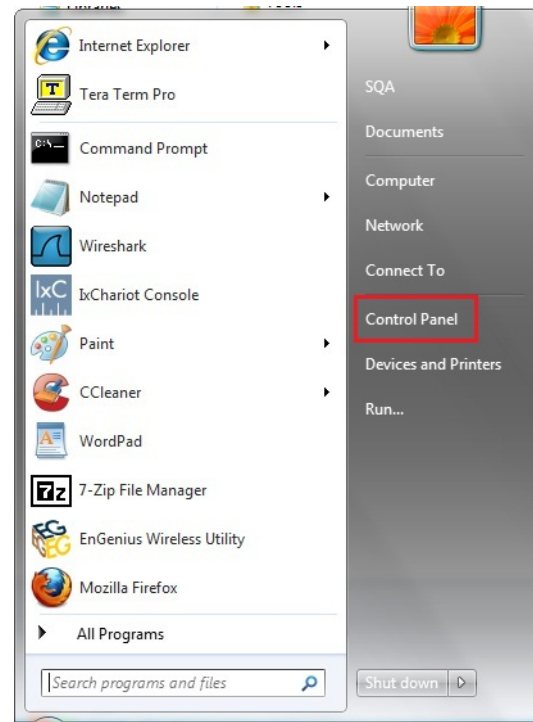
2.2 Computer Settings (Windows XP/Windows Vista/Windows 7)

In order to use the ALL02850N, you must first configure the TCP/IPv4 connection of your computer system.

- Click **Start** button and select **Control Panel**.



Windows XP



Windows Vista/Windows 7

- In **Windows XP**, click **Network Connections**

- In **Windows 7**, click **View Network Status and Tasks** in the **Network and Internet**

section, then

Change Adapter Settings



Network and Internet

View network status and tasks

Choose homegroup and sharing options



Network Connections

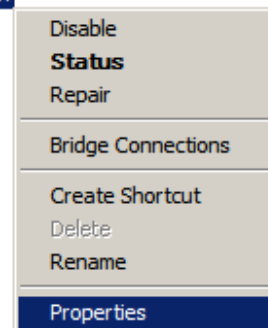
select

Control Panel Home

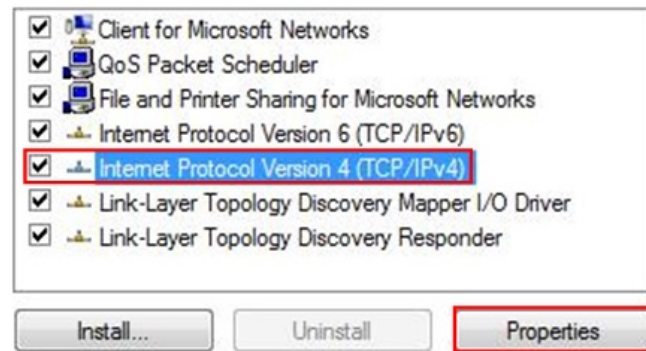
Change adapter settings

Change advanced sharing settings

- Right click on **Local Area Connection** and select **Properties**



- Highlight **Internet Protocol Version 4 (TCP/IPv4)** and select **Properties**



- Select **Use the following IP address** and enter IP address and subnet mask then press **OK**.

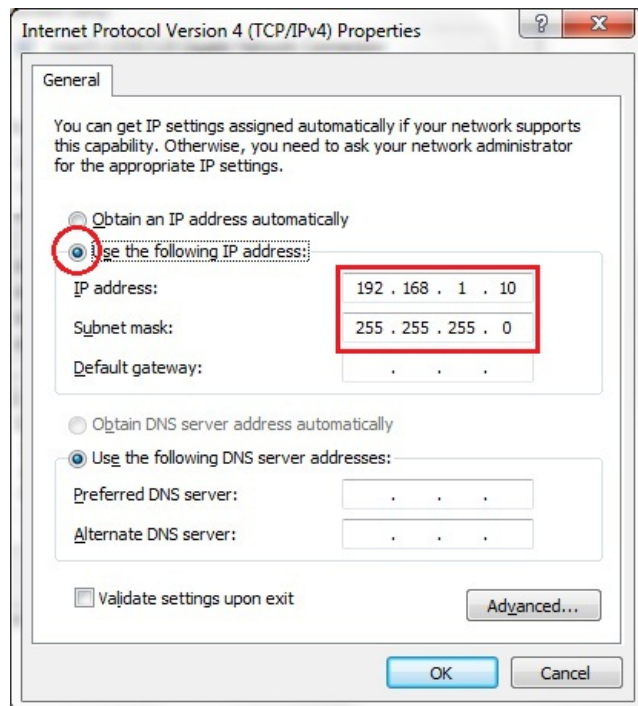
Note: Ensure that the IP address and subnet mask are on the same subnet as the device.

For example:

Device IP address: 192.168.1.1

PC IP address: 192.168.1.2 - 192.168.1.254

PC subnet mask: 255.255.255.0



2.3 Apple Mac X OS

- Open the **System Preferences** (can be opened in the **Applications** folder or selecting it in the Apple Menu)
- Select **Network** in the **Internet & Network** section
- Highlight **Ethernet**
- In **Configure IPv4**, select **Manually**
- Enter IP address and subnet mask then press **OK**.

Note: Ensure that the IP address and subnet mask are on the same subnet as the device.

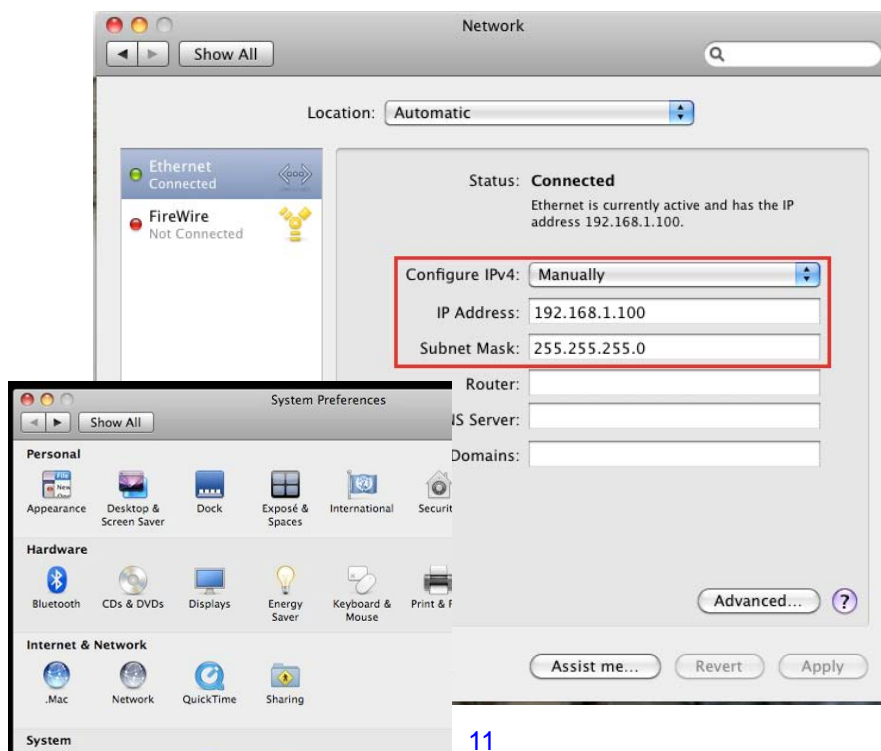
For example:

Device IP address: 192.168.1.1

PC IP address: 192.168.1.2 -
192.168.1.254

PC subnet mask: 255.255.255.0

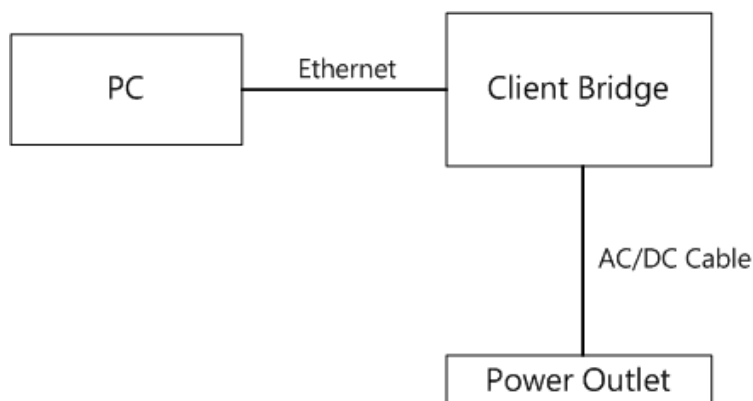
- Click **Apply** when done.

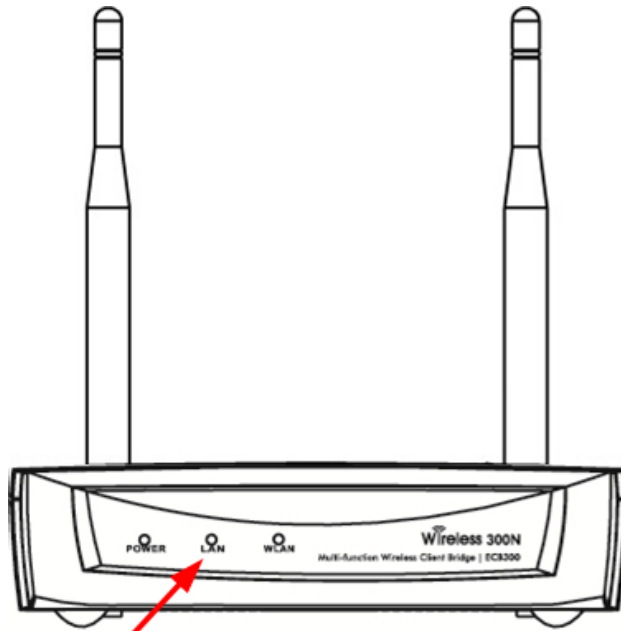


2.4 Hardware Installation

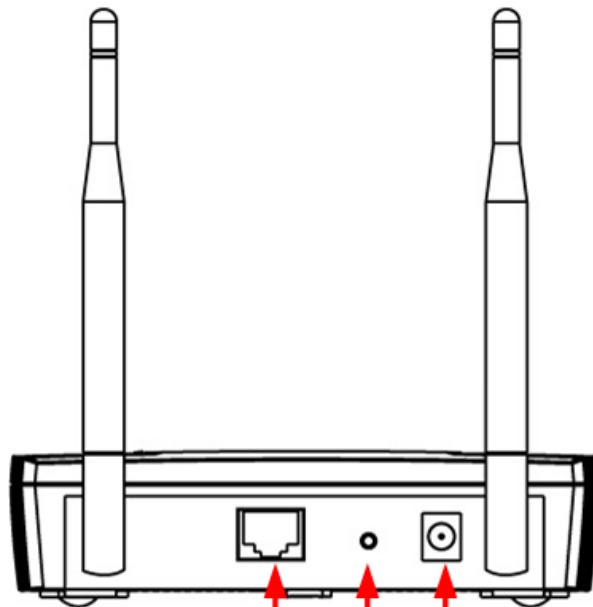
- 1) Ensure that the computer in use has an Ethernet Card (RJ-45 Ethernet Port). For more information, verify with our computer user manual.
- 2) Connect one end of the Category 5 Ethernet cable into RJ-45 port of the ALL02850N and the other end to the RJ-45 port on the computer that will use the ALL02850N. Ensure that the cable is securely connected to both the ALL02850N and the Computer.
- 3) Connect the Power Adaptor DC Inlet to the **DC-IN** port of the ALL02850N and the Power Adaptor to the electrical out. Once both connections are secure, verify the following:
 - a) Ensure that the **Power** light is on (it will be blue).
 - b) Ensure that the **Wireless** light is on (it will be blue).
 - c) Ensure that the **LAN (Computer/ALL02850N Connection)** light is on (it will be blue).
 - d) Once all three lights are on, proceed to setting up the computer.

This diagram depicts the hardware configuration.





LED Lights for Wireless,
Ethernet port and Power



Ethernet port for RJ-45 cable
Reset Button
DC IN for Power

Front

Panel

Rear Panel

Front Panel	
LED Lights	LED lights for Wireless, Ethernet port and Power.
Rear Panel	
DC IN	DC IN for Power.



Reset Button	One click for reset the device. Press over 10 seconds for reset to factory default.
Ethernet Port	Ethernet port for RJ-45 cable.

3 Configuring Your Client Bridge

This section will show you how to configure the device using the web-based configuration interface.

3.1 Default Settings

Please use your Ethernet port or wireless network adapter to connect the Client Bridge.

Default Settings

IP Address	192.168.1.1
Username / Password	admin / admin
Operation Mode	Client Bridge


3.2 Web Configuration

- Open a web browser (Internet Explorer/Firefox/Safari) and enter the IP Address:
http://192.168.1.1

Note: If you have changed the default LAN IP Address of the device, ensure you enter the correct IP Address.




- The default username and password are **admin**. Once you have entered the correct username and password, click the **Login** button to open the web-base configuration page.



The image shows a login form for the ALLNET device. At the top is the ALLNET logo, which consists of a stylized antenna icon and the word "ALLNET" in bold. Below the logo, there are two input fields. The first is labeled "Username:" and contains the text "admin". The second is labeled "Password:" and contains five dots, indicating a masked password. At the bottom of the form, there are two buttons: "Login" and "Cancel".

- If successful, you will be logging in and see the ALL02850N User Menu



2.4GHz Wireless-N Multi-function AP

Client Bridge Mode

- System
- Wireless
- Network
- Management
- Tools
- ▷ Logout

You can use the Status page to monitor the connection status for WLAN/LAN interfaces, firmware and hardware version numbers.

System	
Operation Mode	Client Bridge
System Time	2009/01/01 00:38:27
System Up Time	38 min 34 sec
Hardware Version	0.1.0
Serial Number	201107279
Firmware version	1.0.0

WLAN Station Information	
Connection Status	Fail
Channel	---
ESSID	---
Security	---
BSSID	---

4 Building a Wireless Network

The ALL02850N has the ability to operate in various operating modes. The ALL02850N is the ideal device in which you can build your WLAN. This chapter describes how to build a WLAN around your ALL02850N using the operating modes of the ALL02850N.

4.1 Client Bridge Mode

In Client Bridge Mode, the ALL02850N acts as a wireless dongle that connects to an Access Point to allow a system wireless access to the network. This mode requires you to connect the Ethernet port on your PC to the ALL02850N LAN port.

If you use the client bridge operating mode, use the ALL02850N Site Survey feature to scan for Access Points within range. When you find an Access Point, configure the ALL02850N to use the same SSID and Security Password as the Access Point to associate with it.



4.2 Access Point Mode

In Access Point Mode, ALL02850N behaves like a central connection for stations or clients that support IEEE 802.11b/g/n networks. The stations and clients must be configured to use the same SSID and security password to associate with the ALL02850N. The ALL02850N supports up to four SSIDs at the same time for secure guest access.



4.3 WDS AP Mode

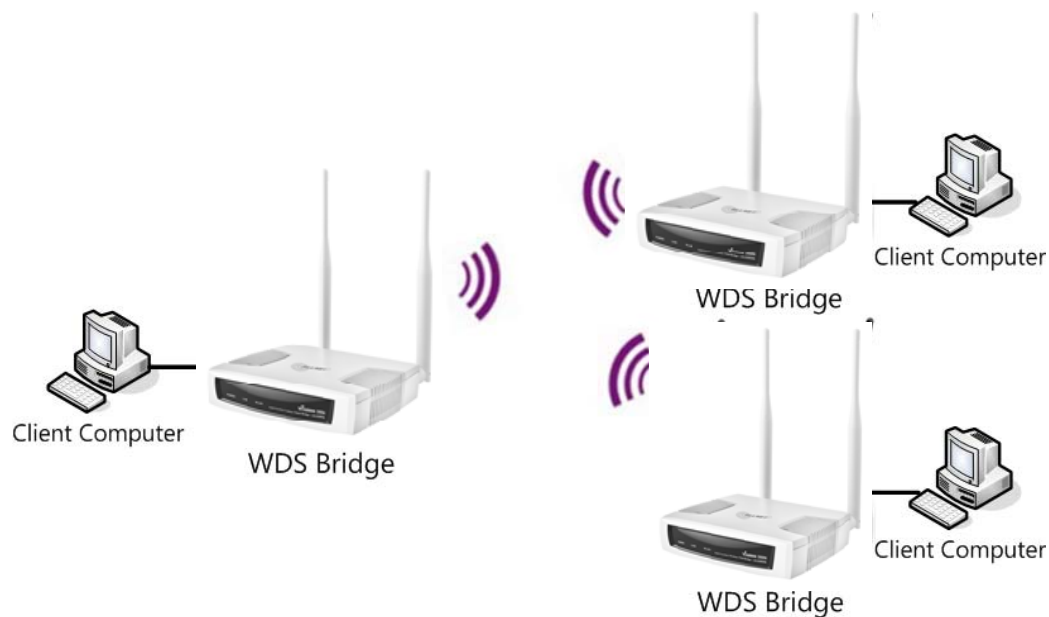
The ALL02850N also supports WDS AP mode. This operating mode allows wireless connections to the ALL02850N using WDS technology. In this mode, configure the MAC addresses in both Access Points to enlarge the wireless area by enabling WDS Link settings. WDS supports four AP MAC addresses.



4.4 WDS Bridge Mode

In WDS Bridge Mode, the ALL02850N can wirelessly connect different LANs by configuring the MAC address and security settings of each ALL02850N device. Use this mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to use the ALL02850N to wirelessly connect two wired LANs, as shown in the following figure.

WDS Bridge Mode can establish four WDS links, creating a star-like network.

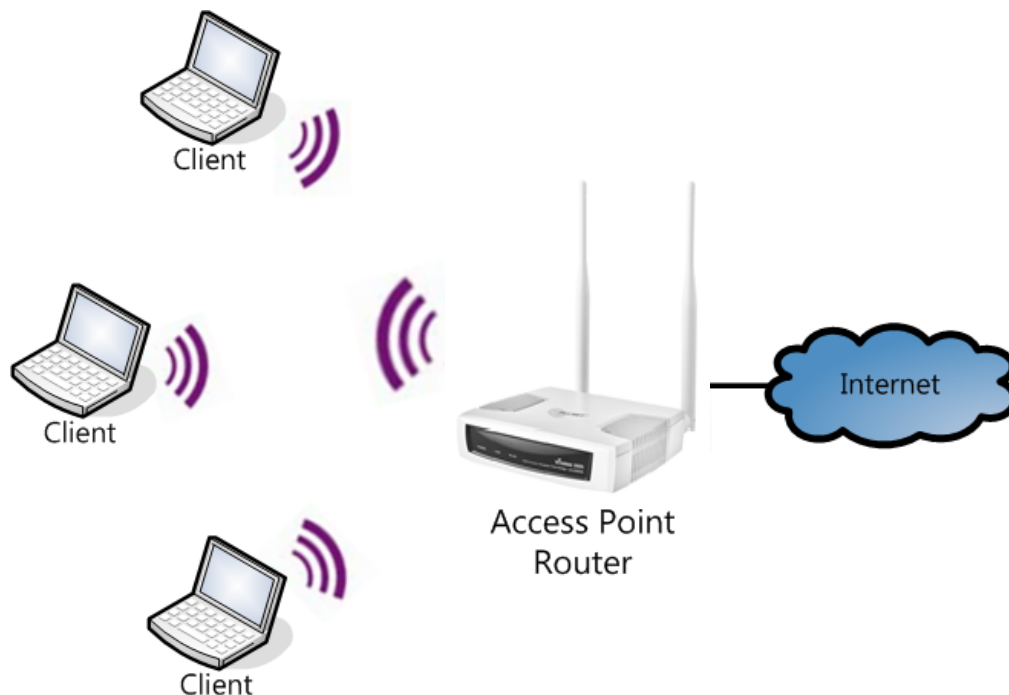


Note: WDS Bridge Mode does not act as an Access Point. Access Points linked by WDS are using the same frequency channel. More Access Points connected together may lower throughput. Please be aware to avoid loops in your wireless connection, otherwise enable Spanning Tree Function.

4.5 Router Mode

In Access Point Router Mode, ALL02850N grants Internet access to multiple wireless clients. In this mode, the ALL02850N's internal Dynamic Host Configuration Protocol (DHCP) server automatically allocates ranges of IP addresses to each wireless client that will access the Internet through the ALL02850N.

This mode requires you to connect the ALL02850N's Ethernet port to a modem or router. And the wireless clients must be configured to use the same SSID and security password to associate with the ALL02850N. The ALL02850N supports up to four SSIDs at the same time for secure guest access.



Please Note:

You have to configure WLAN interface before you change to this mode.

After you change to *Access Point Router-mode*, you have to connect via WLAN to the ALL02850N, because the device will change the LAN Port to WAN Port with an dynamic IP-address configuration (DHCP).

This means you can't connect to the device via LAN anymore, only with WLAN.

4.6 Repeater Mode

Repeater is used to regenerate or replicate signals that are weakened or distorted by transmission over long distances and through areas with high levels of electromagnetic interference (EMI).



5 System

5.1 Operation Mode

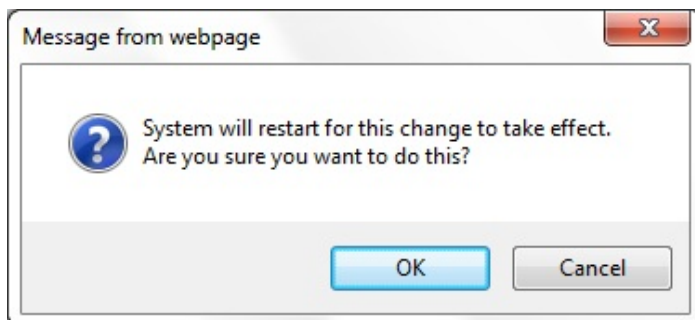
Each operating mode offers different features. In order to switch the operating mode, select it from the **Operation Mode** from the **System Menu**. There are six operation modes: **Access Point**, **Client Bridge**, **WDS AP**, **WDS Bridge**, **Access Point Router** and **Universal Repeater**.

Operation Mode

Operation Mode :	<input type="radio"/> Access Point <input checked="" type="radio"/> Client Bridge <input type="radio"/> WDS AP <input type="radio"/> WDS Bridge <input type="radio"/> Access Point Router <input type="radio"/> Universal Repeater
------------------	---

Apply Cancel

A dialog box will appear to notify you that the system will restart in order for the changes to take effect. Click on the **OK** button to continue.



The ALL02850N will display how much time it will take to restart the device in the new operating mode as shown below.

System mode is changed and module is reloading, please wait seconds.

5.2 Status

This page will display status of the device.

System

Operation Mode Client Bridge
 System Time 2009/01/01 01:01:47
 System Up Time 1 hours 1 min 52 sec
 Hardware Version 0.1.0
 Serial Number 201107279
 Firmware version 1.0.0

System	
Operation Mode	Displays the current mode of operation of the ALL02850N.
System Time	Displays the current time of the ALL02850N.
System Up Time	The elapsed time of operation of the ALL02850N.
Hardware Version and Serial Number	Hardware information of the ALL02850N.
Firmware Version	The current firmware version of the ALL02850N.

WAN Settings

Attain IP Protocol Dynamic IP Address
 IP Address 192.168.7.162
 Subnet Mask 255.255.255.0
 Default Gateway 192.168.7.10
 MAC Address 00:02:6F:30:0A:24
 Primary DNS 192.168.7.10
 Secondary DNS ---

Renew

WAN Settings (Router mode)	
Attain IP Protocol	Method used to connect to the Internet. This is your WAN connection type.
IP Address	The WAN IP address of the Router.
Subnet Mask	The WAN subnet mask of the Router.
Default Gateway	The default gateway of the Router.
MAC Address	The WAN MAC address of the Router.
Primary and Secondary DNS	The IP addresses of the Primary and Secondary DNS servers assigned to the WAN connection.

WLAN Station Information

Connection Status Fail
 Channel ---
 ESSID ---
 Security ---
 BSSID ---

WLAN Station Information (Client Bridge mode)	
Connection Status	The connection status: Successful or Fail .
Channel	The wireless channel in use.
ESSID	The SSID (Network Name) of the wireless network which ALL02850N connected.
Security	The wireless encryption in use.
BSSID	The MAC address of this SSID which ALL02850N connected.

WLAN Repeater Information

Connection Status Successful
 ESSID Test2013
 Security WPA2 pre-shared key
 BSSID 88:DC:96:07:3A:4D

WLAN Repeater Information (Repeater mode)	
Connection Status	The connection status: Successful or Fail .
Channel	The wireless channel in use.
ESSID	The SSID (Network Name) of the wireless network.
Security	Wireless encryption for this SSID.
BSSID	The MAC address of this SSID.

View the current wireless connection status and related information.

WLAN Settings

Channel 11

SSID_1

ESSID ALL02850N
 Security WPA2 pre-shared key
 BSSID 88:DC:96:07:3A:4C

WLAN Settings (Access Point / WDS AP / Repeater / Router mode)	
Channel	Displays the current Wireless Channel in use by the ALL02850N.
ESSID	The SSID (Network Name) of the wireless network (up to 4 SSIDs supported).
Security	Current wireless encryption for the corresponding SSID.
BSSID	The MAC address of the corresponding SSID.

5.3 DHCP

The **DHCP** option in the **System** menu displays the client IP address assigned by the DHCP Server. You can also set the IP Addresses of the connected devices manually.

Note: Only in Access Point / Router mode.

DHCP Client Table :

This DHCP Client Table shows client IP address assigned by the DHCP Server.

IP Address	MAC Address	Expiration Time
192.168.1.10	00:C0:9F:26:64:EE	Forever

Refresh

You can assign an IP address to the specific MAC address.

☒ **Enable Static DHCP IP**

IP Address	MAC Address
192.168.1.100	80E3A39B703A

Add

Reset

Current Static DHCP Table :

NO.	IP Address	MAC Address	Select
1	192.168.1.50	00:24:E8:C7:41:0D	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

The DHCP Client Table shows the LAN clients that have been allocated an IP address from the DHCP Server.

DHCP Client Table :

This DHCP Client Table shows client IP address assigned by the DHCP Server.

IP Address	MAC Address	Expiration Time
192.168.1.10	00:C0:9F:26:64:EE	Forever

Refresh



DHCP Client Table	
IP address	Displays the IP Address of the client on the LAN.
MAC address	Displays the MAC Address of the client on the LAN.
Expiration Time	Displays the time of expiration of the IP Address of the client.
Refresh	Click this button to update the DHCP Client Table.

5.4 Schedule

The **Schedule** option of the **System** menu allows you to set a schedule when the ALL02850N's Wireless is active.

The **Schedule Table** will display:

- **NO.:** The entry number of the schedule.
- **Description:** The name given to the schedule.
- **Service:** Displays whether the wireless service will be activate or not during the scheduled time.
- **Schedule:** Displays when the schedule will execute.

You will also be able to **Add** new schedules (at most 10), **Edit** schedules, **Delete Selected** schedules, or **Delete All** schedules.

☐ **Enabled Schedule Table (up to 10)**

NO.	Description	Service	Schedule	Select
1	schedule 01	Wireless Active	From 11:00 To 12:00--- Mon, Wed	<input type="checkbox"/>

Add

Edit

Delete Selected

Delete All

Apply

Cancel

After selecting **Add** or **Edit**, the following form will show up. Fill in the form to set the schedule you want.



Schedule Description :	<input type="text" value="schedule 01"/>
Service :	<input checked="" type="checkbox"/> Wireless Active
Days :	<input type="checkbox"/> Every Day <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Time of day :	<input type="checkbox"/> All Day (use 24-hour clock) From <input type="text" value="11"/> : <input type="text" value="0"/> To <input type="text" value="12"/> : <input type="text" value="0"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Schedule	
Schedule Description	Assign a name to the schedule.
Service	The service provided for the schedule.
Days	Set which days the schedule will be active.
Time of day	Set what time of the selected days the schedule will be active.

5.5 Event Log

The **Event Log** of the **System** menu displays the system events and actions of the ALL02850N. When powered down or rebooted, the **Event Log** will be cleared.

View the system operation information.

```

day 1 00:00:07 [SYSTEM]: WLAN, start LLTD
day 1 00:00:06 [SYSTEM]: TELNETD, start Telnet-cli Server
day 1 00:00:06 [SYSTEM]: HTTPS, start
day 1 00:00:06 [SYSTEM]: HTTP, start
day 1 00:00:05 [SYSTEM]: UPnP, Start
day 1 00:00:05 [SYSTEM]: SNMP, start SNMP server
day 1 00:00:05 [SYSTEM]: SCHEDULE, Wireless Radio On
day 1 00:00:04 [SYSTEM]: NTP, start NTP Client
day 1 00:00:04 [SYSTEM]: DHCP, DHCP Server Stopping
day 1 00:00:03 [SYSTEM]: WLAN[2.4G], Channel = 11
day 1 00:00:03 [SYSTEM]: LAN, IP address=192.168.1.1
day 1 00:00:03 [SYSTEM]: LAN, start
day 1 00:00:01 [SYSTEM]: BR, start
day 1 00:00:01 [SYSTEM]: SYS, Application Version: 1.0.0
day 1 00:00:01 [SYSTEM]: Start Log Message Service!

```

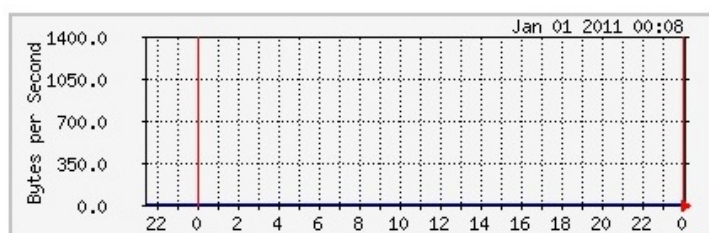
Event Log	
Save	Save the log to a .txt file.
Clear	Clear the log.
Refresh	Update the log.

5.6 Monitor

The **Monitor** option of the **System** menu displays 2 histogram graphs. The histograms represent the bandwidth usage of both the daily use of the Ethernet and the daily use of the WLAN. If you click on **Detail**, a new browser window will open with 4 additional histograms (6 total). In the new browser window, you will be able to view the weekly and monthly bandwidth usage for both the Ethernet and WLAN.

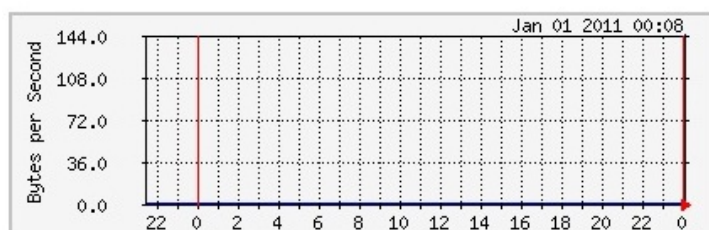
Ethernet Daily Graph (5 Minute Average)

[Detail](#)



	Maximum	Average	Current
RX	293 B/sec	293 B/sec	293 B/sec
TX	1365 B/sec	1365 B/sec	1365 B/sec

WLAN Daily Graph (5 Minute Average)



	Maximum	Average	Current
RX	0 B/sec	0 B/sec	0 B/sec
TX	144 B/sec	144 B/sec	144 B/sec

6 Wireless

6.1 Status

The **Status** of the **Wireless** menu displays the current status of the ALL02850N's wireless configuration.

Client Bridge mode:

View the current wireless connection status and related information.

WLAN Station Information

Connection Status	Successful
ESSID	Test2013
Security	WPA2 pre-shared key
BSSID	00:08:54:A2:B2:C6
Channel	13
Link Quality	100/100

Access Point / Router mode:

View the current wireless connection status and related information.

WLAN Settings

Channel 11

SSID_1

ESSID	ALL02850N
Security	WPA2 pre-shared key
BSSID	88:DC:96:07:3A:4C

Repeater mode:

View the current wireless connection status and related information.

WLAN Repeater Information

Connection Status	Successful
ESSID	Test2013
Security	WPA2 pre-shared key
BSSID	88:DC:96:07:3A:4D
Channel	13

WLAN Settings

Channel	13
---------	----

SSID_1

ESSID	Test2013
Security	WPA2 pre-shared key
BSSID	88:DC:96:07:3A:4C

6.2 Basic

The **Basic** option of the **Wireless** menu displays the basic wireless options of the ALL02850N.

Client Bridge:

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless device move to a clean Wireless Channel automatically.

Radio : ☒ Enable ☐ Disable

Mode :

Band :

Enabled SSID#:

ESSID1 :

Auto Channel: ☐ Enable ☒ Disable

Channel :

Basic (Client Bridge mode)	
Radio	Enable or Disable the device's wireless signal.
Band	Select the types of wireless clients that the device will accept.
Site Survey	Click on [Site Survey] to search the existing AP.

Access Point / Router mode:

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless device move to a clean Wireless Channel automatically.

Radio : ☒ Enable ☐ Disable

Mode :

Band :

Enabled SSID#:

ESSID1 :

Auto Channel: ☐ Enable ☒ Disable

Channel :

Basic (Access Point / Router mode)	
Radio	Enable or Disable the ALL02850N's wireless signal.
Mode	Select between Access Point or Wireless Distribution System (WDS) modes.
Band	Select the types of wireless clients that the device will accept.
Enable SSID#	Select the number of SSID's (Wireless Network names) you would like (up to 4).
SSID#	Enter the name of your wireless network. You can use up to 32 characters.
Auto Channel	When enabled, the device will scan the wireless signals around your area and select the channel with the least interference.
Channel	Manually select which channel the wireless signal will use.
Check Channel Time	When Auto Channel is Enabled , you can specify the period of device will scan the wireless signals around your area.

WDS AP / WDS Bridge mode:

Wireless Distribution System (WDS)

Using a WDS to connect Access Points wirelessly extends a wired infrastructure to locations where cabling is not possible or inefficient to implement.

Note: Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that a WDS network be created using the same Access Point models for maximum compatibility.

Also, all Access Points in the WDS network need to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four access points.

Radio :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode :	WDS ▾
Band :	2.4 GHz (B+G+N) ▾
Channel :	11 ▾
MAC Address 1 :	000000000000
MAC Address 2 :	000000000000
MAC Address 3 :	000000000000
MAC Address 4 :	000000000000
WDS Data Rate :	300M ▾
Set Security :	<input type="button" value="Set Security"/>

Repeater mode:

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless device move to a clean Wireless Channel automatically.

Radio :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode :	Universal Repeater ▾
Band :	2.4 GHz (N) ▾
Enabled SSID#:	1 ▾
ESSID1 :	Test2013
Channel :	13 ▾
Site Survey :	<input type="button" value="Site Survey"/>

Basic (Repeater mode)	
Radio	Enable or Disable the device's wireless signal.
Band	Select the types of wireless clients that the device will accept. eg: 2.4 Ghz (B+G) Only 802.11b and 11g clients will be allowed.
ESSID1	Enter the name of your wireless network. You can use up to 32 characters.
Site Survey	Click on [Site Survey] to search the existing AP.

6.3 Site Survey

Client Bridge mode:

1. AP list after site survey.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	13	Test2013	00:08:54:A2:B2:C6	AES	WPA2PSK	70	b/g/n
2	<input type="radio"/>	6	ALLNET_ECB350	00:02:6F:E6:1C:18	TKIPAES	WPA2	68	b/g/n
3	<input type="radio"/>	6	ALLNET_EAP600	00:02:6F:EC:B2:D4	AES	WPAWPA2	68	b/g/n
4	<input type="radio"/>	6	ALLNET_350_2	02:02:6F:E8:08:4C	AES	WPA2	62	b/g/n
5	<input type="radio"/>	1	ALLNET-INT1	50:A7:33:1C:EC:58	AES	WPA2PSK	62	b/g/n
6	<input type="radio"/>	1	ALLNET-Guest	50:A7:33:5C:EC:58	AES	WPA2PSK	62	b/g/n
7	<input type="radio"/>	6	ALLNET_350	00:02:6F:E8:08:4C	AES	WPA2	60	b/g/n
8	<input type="radio"/>	9	ALL-Support	74:91:1A:11:76:C8	AES	WPA2PSK	56	b/g/n
9	<input type="radio"/>	9	ALL-Guest	74:91:1A:51:76:C8	NONE	OPEN	56	b/g/n
10	<input type="radio"/>	6	ALLPrint	00:11:E5:03:FC:4A	AES	WPA2PSK	54	b/g/n
11	<input type="radio"/>	4	Raubfischteam	34:08:04:24:79:10	WEP	AUTOWEP	14	b/g
12	<input type="radio"/>	12	AeroFlot	68:7F:74:41:FC:4F	TKIP	WPA2PSK	14	b/g

Refresh

Add to AP Profile

2. Select an AP and click on **[Add to AP Profile]**.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input checked="" type="radio"/>	13	Test2013	00:08:54:A2:B2:C6	AES	WPA2PSK	70	b/g/n
2	<input type="radio"/>	6	ALLNET_ECB350	00:02:6F:E6:1C:18	TKIPAES	WPA2	68	b/g/n
3	<input type="radio"/>	6	ALLNET_EAP600	00:02:6F:EC:B2:D4	AES	WPAWPA2	68	b/g/n
4	<input type="radio"/>	6	ALLNET_350_2	02:02:6F:E8:08:4C	AES	WPA2	62	b/g/n
5	<input type="radio"/>	1	ALLNET-INT1	50:A7:33:1C:EC:58	AES	WPA2PSK	62	b/g/n
6	<input type="radio"/>	1	ALLNET-Guest	50:A7:33:5C:EC:58	AES	WPA2PSK	62	b/g/n
7	<input type="radio"/>	6	ALLNET_350	00:02:6F:E8:08:4C	AES	WPA2	60	b/g/n
8	<input type="radio"/>	9	ALL-Support	74:91:1A:11:76:C8	AES	WPA2PSK	56	b/g/n
9	<input type="radio"/>	9	ALL-Guest	74:91:1A:51:76:C8	NONE	OPEN	56	b/g/n
10	<input type="radio"/>	6	ALLPrint	00:11:E5:03:FC:4A	AES	WPA2PSK	54	b/g/n
11	<input type="radio"/>	4	Raubfischteam	34:08:04:24:79:10	WEP	AUTOWEP	14	b/g
12	<input type="radio"/>	12	AeroFlot	68:7F:74:41:FC:4F	TKIP	WPA2PSK	14	b/g

Refresh

Add to AP Profile

3. Enter the correct security setting.

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server.

AP Profile Settings

Network Name (SSID) :	<input type="text" value="Test2013"/>
Encryption :	WPA pre-shared key ▾
Authentication Type :	WPA2(AES) ▾
Pre-shared Key :	<input type="text" value="entersavepwhere"/>

4. Add AP profile successfully, click on [Close] to close the browser.

Add to AP Profile successfully.

5. The AP profile is added in AP Profile Table.

AP Profile Table

NO.	SSID	MAC	Authentication	Encryption	Select
1	Test2013	00:02:6F:C7:EB:70	WPA2_PSK	AES	<input type="checkbox"/>

Repeater mode:

1. AP list after site survey.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	13	Test2013	00:08:54:A2:B2:C6	AES	WPA2PSK	70	b/g/n
2	<input type="radio"/>	6	ALLNET_EAP600	00:02:6F:EC:B2:D4	AES	WPAWPA2	68	b/g/n
3	<input type="radio"/>	6	ALLNET_ECB350	00:02:6F:E6:1C:18	TKIPAES	WPA2	66	b/g/n
4	<input type="radio"/>	1	ALLNET-INT1	50:A7:33:1C:EC:58	AES	WPA2PSK	62	b/g/n
5	<input type="radio"/>	1	ALLNET-Guest	50:A7:33:5C:EC:58	AES	WPA2PSK	60	b/g/n
6	<input type="radio"/>	9	ALL-Guest	74:91:1A:51:76:C8	NONE	OPEN	58	b/g/n
7	<input type="radio"/>	6	ALLNET_350	00:02:6F:E8:08:4C	AES	WPA2	58	b/g/n
8	<input type="radio"/>	6	ALLNET_350_2	02:02:6F:E8:08:4C	AES	WPA2	58	b/g/n
9	<input type="radio"/>	9	ALL-Support	74:91:1A:11:76:C8	AES	WPA2PSK	58	b/g/n
10	<input type="radio"/>	6	ALLPrint	00:11:E5:03:FC:4A	AES	WPA2PSK	46	b/g/n
11	<input type="radio"/>	4	Raubfischteam	34:08:04:24:79:10	WEP	AUTOWEP	16	b/g
12	<input type="radio"/>	12	AeroFlot	68:7F:74:41:FC:4F	TKIP	WPA2PSK	14	b/g
13	<input type="radio"/>	1	HEIM-NETZ	BC:05:43:50:56:9B	AES	WPAPSKWPA2PSK	10	b/g/n

2. Select an AP and click on [**Connect**].

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input checked="" type="radio"/>	13	Test2013	00:08:54:A2:B2:C6	AES	WPA2PSK	70	b/g/n
2	<input type="radio"/>	6	ALLNET_EAP600	00:02:6F:EC:B2:D4	AES	WPAWPA2	68	b/g/n
3	<input type="radio"/>	6	ALLNET_ECB350	00:02:6F:E6:1C:18	TKIPAES	WPA2	66	b/g/n
4	<input type="radio"/>	1	ALLNET-INT1	50:A7:33:1C:EC:58	AES	WPA2PSK	62	b/g/n
5	<input type="radio"/>	1	ALLNET-Guest	50:A7:33:5C:EC:58	AES	WPA2PSK	60	b/g/n

3. Enter the correct security setting.

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server.

AP Profile Settings

Network Name (SSID) :	<input type="text" value="Test2013"/>
Encryption :	WPA pre-shared key ▾
Authentication Type :	WPA2(AES) ▾
Pre-shared Key :	<input type="text" value="entersavepwhere"/>

Save

4. Connect AP successfully, click on [**Close**] to close the browser.

5. You can see the Connection Status in Status WEB page.

View the current wireless connection status and related information.

WLAN Repeater Information

Connection Status	Successful
ESSID	Test2013
Security	WPA2 pre-shared key
BSSID	88:DC:96:07:3A:4D
Channel	13

WLAN Settings

Channel	13
---------	----

SSID_1

ESSID	Test2013
Security	WPA2 pre-shared key
BSSID	88:DC:96:07:3A:4C

6.4 Advanced

The **Advanced** option of the **Wireless** menu displays the advanced wireless options of the ALL02850N.

It is recommended that the ALL02850N's default settings are used unless the user has experience with advanced networking.

Client Bridge mode:

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(1-2347)

Advanced (Client Bridge mode)	
Fragment Threshold	Specifies the maximum size of the packet per fragment. This function can reduce the chance of packet collision. However, when the fragment threshold is set too low, there will be increased overhead resulting in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, the packet will be sent without an RTS/CTS handshake, which may result in incorrect transmission.

Access Point / WDS AP / Router / Repeater mode:

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(1-2347)
Beacon Interval :	<input type="text" value="100"/>	(20-1024 ms)
DTIM Period :	<input type="text" value="1"/>	(1-255)
N Data Rate:	Auto ▾	
Channel Bandwidth	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz	
Preamble Type :	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
CTS Protection :	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power :	100 % ▾	

Advanced (Access Point / WDS AP / Router / Repeater mode)	
Fragment Threshold	Specifies the maximum size of the packet per fragment. This function can reduce the chance of packet collision. However, when the fragment threshold is set too low, there will be increased overhead resulting in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, the packet will be sent without an RTS/CTS handshake, which may result in incorrect transmission.
Beacon Interval	The time interval that the device broadcasts a beacon. This beacon is used to synchronize all wireless clients on the network.
DTIM Period	A Delivery Traffic Indication Message (DTIM) informs all wireless clients that the access point will be transmitting Multi-casted data.
N Data Rate	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
Channel Bandwidth	Set whether each channel uses 20Mhz or 40Mhz transmission frequency. To achieve 11n speeds, 40Mhz channels must be used.
Preamble Type	A preamble is a message that helps access points synchronize with the client. Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, resulting in decreased compatibility, but increased performance.
Tx Power	Set the power output of the wireless signal.

WDS Bridge mode:

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	<input type="text" value="2346"/> (256-2346)
RTS Threshold :	<input type="text" value="2347"/> (1-2347)
N Data Rate:	<input type="text" value="Auto"/>
Channel Bandwidth	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz
Preamble Type :	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble
CTS Protection :	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None
Tx Power :	<input type="text" value="100 %"/>

Apply

Cancel

Advanced (WDS Bridge mode)	
Fragment Threshold	Specifies the maximum size of the packet per fragment. This function can reduce the chance of packet collision. However, when the fragment threshold is set too low, there will be increased overhead resulting in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, the packet will be sent without an RTS/CTS handshake, which may result in incorrect transmission.
N Data Rate	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
Channel Bandwidth	Set whether each channel uses 20Mhz or 40Mhz transmission frequency. To achieve 11n speeds, 40Mhz channels must be used.
Preamble Type	A preamble is a message that helps access points synchronize with the client. Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, resulting in decreased compatibility, but increased performance.
Tx Power	Set the power output of the wireless signal.

6.5 Security

The **Security** option in the **Wireless** menu allows you to set the wireless security settings.

Note: Only in Access Point / WDS AP / Router and Repeater mode.

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server.

ESSID Selection :	ALL02850N ▼
Separate :	<input type="checkbox"/> SSID <input type="checkbox"/> STA
Broadcast ESSID :	Enable ▼
WMM :	Enable ▼
Encryption :	<div> Disable ▼ <div> Disable WEP WPA pre-shared key WPA RADIUS </div> </div>
<input type="checkbox"/> Enable 802.1x Authentication	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Security (Access Point / WDS AP / Router / Repeater mode)	
SSID Selection	Select the SSID that the corresponding security settings will apply to.
Separate	Separating the SSID from each other (or use of STA) prevents communication and data sharing between wireless stations associated with the SSIDs.
Broadcast SSID	If Disabled , the ALL02850N will not broadcast the SSID. It will be invisible to the clients.
WMM	<p>Wi-Fi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, and background.</p> <p>Note: In certain situations, WMM needs to be enabled to achieve 11n transfer speeds.</p>
Encryption	<p>The encryption method to be used on the corresponding SSID. You can choose between WEP, WPA Pre-Shared Key, or WPA RADIUS.</p> <ul style="list-style-type: none"> • Disabled - No data encryption is used. • WEP - Data is encrypted using the WEP standard. WEP is the Wired Equivalent Privacy security over a wireless network. • WPA-PSK - Data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. WPA-PSK is Wi-Fi Protected Access using a Pre-Shared Key. This is the equivalent of password protecting your wireless network.

	<ul style="list-style-type: none"> • WPA2-PSK - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption. • WPA-RADIUS - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard. <p>If this option is selected:</p> <ul style="list-style-type: none"> • This Access Point must have a Client Login on the Radius Server. • Each user must have a User Login on the Radius Server. • Each user's wireless client must support 802.1x and provide the login data when required. • All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.
--	--

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is then processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

☒ **Enable 802.1x Authentication**

RADIUS Server IP Address :

RADIUS Server Port :

RADIUS Server Shared Secret :

802.1x Authentication	
RADIUS Server IP Address	The IP Address of the RADIUS Server.
RADIUS Server port	The port number of the RADIUS Server.
RADIUS Server password	The RADIUS Server password.

WEP Encryption:

Encryption :	WEP ▼
Authentication Type :	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key <input type="radio"/> Auto
Key Length :	64-bit ▼
Key Type :	Hex (10 characters) ▼
Default Key :	Key 1 ▼
Encryption Key 1 :	1234567890
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

WEP Encryption	
Authentication Type	Please ensure that your wireless clients use the same authentication type.
Key type	ASCII: Using characters from the ASCII standard (recommended) HEX: Uses hexadecimal characters.
Key Length	The amount of bits the WEP key will use. <ul style="list-style-type: none"> • 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key .
Encryption Key #	Enter the key value or values you wish to use. Only the Key selected as Default is required. The others are optional.

WPA Pre-Shared Key Encryption:

Encryption :	WPA pre-shared key ▼
WPA Type :	<input type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input checked="" type="radio"/> WPA2 Mixed
Pre-shared Key Type :	Passphrase ▼
Pre-shared Key :	12345678

WPA Pre-Shared Key Encryption	
WPA type	<p>Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.</p> <ul style="list-style-type: none"> • WPA(TKIP): Uses a Pre-Shared Key with a dynamically generated key for each 128-bit packet. • WPA2(AES): Government standard of WPA2 encryption. • WPA2 Mixed: Allows the use of both WPA and WPA2 clients on the network.
Pre-shared Key Type	Pre-Shared Key format (ASCII or Hexadecimal).
Pre-shared Key	<p>Wireless clients must use the same key to associate the device to the ALL02850N.</p> <p>If using passphrase format, the Key must be from 8 to 63 characters in length.</p>

WPA RADIUS Encryption:

Encryption :	WPA RADIUS ▾
WPA Type :	<input type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input checked="" type="radio"/> WPA2 Mixed
RADIUS Server IP Address :	<input type="text"/>
RADIUS Server Port :	<input type="text" value="1812"/>
RADIUS Server Shared Secret :	<input type="text"/>

WPA RADIUS Encryption	
WPA type	<p>Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.</p> <ul style="list-style-type: none"> • WPA(TKIP): Uses a Pre-Shared Key with a dynamically generated key for each 128-bit packet. • WPA2(AES): Government standard of WPA2 encryption. • WPA2 Mixed: Allows the use of both WPA and WPA2 clients on the network.
RADIUS Server IP address	Enter the IP address of the RADIUS Server.
RADIUS Server Port	Enter the port number used for connections to the RADIUS server.
RADIUS Server password	Enter the password required to connect to the RADIUS server.

6.6 Filter

The **Filter** option in the **Wireless** menu allows users to allow clients with specific MAC Addresses to join the SSID.

Note: Only in Access Point / WDS AP / Router and Repeater mode.

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

☒ **Enable Wireless MAC Filtering**

Description	MAC Address
rule02	80A49E837BA2

Add

Reset

Only the following MAC Addresses can use network:

NO.	Description	MAC Address	Select
1	rule01	00:21:6A:78:8E:70	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

Wireless MAC Filter (Access Point / WDS AP / Router / Repeater mode)	
Enable Wireless Access Control	Enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
Description	Enter a name or description for this entry.
MAC Address	Enter the MAC address of the wireless client that you wish to allow connection.
Add	Click this button to add the entry.
Reset	Click this button if you have made a mistake and want to reset the MAC address and Description fields.
MAC Address Filtering Table	
Only clients listed in this table will be allowed access to the wireless network.	
Delete Selected	Delete the selected entries.
Delete All	Delete all entries.
Reset	Deselect all entries.

6.7 WPS (Wi-Fi Protected Setup)

The **WPS** feature in the **Wireless** menu follows the Wi-Fi Alliance WPS standard. It eases the set up of security-enabled Wi-Fi networks in homes and/or small office environments.

It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

Note: Only in Access Point / WDS AP and Router mode.

WPS:	<input checked="" type="checkbox"/> Enable
Wi-Fi Protected Setup Information	
WPS Current Status:	Configured <input type="button" value="Release Configuration"/>
Self Pin Code:	04736769
SSID:	ALL02850N
Authentication Mode:	WPA2 pre-shared key
Passphrase Key :	<input type="text" value="entersafepwhere"/>
WPS Via Push Button:	<input type="button" value="Start to Process"/>
WPS Via PIN:	<input type="text"/> <input type="button" value="Start to Process"/>

Wi-Fi Protected Setup (WPS)	
WPS	Check to Enable the WPS feature.
Wi-Fi Protected Setup Information	
WPS Current Status	Shows whether the WPS function is Configured or Un-configured . Configured means that WPS has been used to authorize connection between the ALL02850N and the wireless clients.
SSID	The SSID (network name) used when connecting using WPS.
Authentication Mode	Shows the encryption method used by the WPS process. This is set as the mode selected in the Security option in the Wireless menu.
Passphrase Key	This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempts to connect to the wireless network.
WPS Via Push Button	Activate WPS using a push button.
WPS Via PIN	Activate WPS using the PIN code from the WPS device.

6.8 Client List

The **Client List** option of the **Wireless** menu shows all the wireless clients that are currently connected to the ALL02850N.

Note: Only in Access Point / WDS AP / Router and Repeater mode.

WLAN Client Table :

This WLAN Client Table shows client MAC address associate to this device.

Interface	MAC Address	Rx	Tx	Signal(%)	Connected Time	Idle Time
ALL02850N	00:0F:C9:0C:D7:1A	3.5 KBytes	958 Bytes	51	2 min 31 secs	1 secs
ALL02850N	00:0F:C9:0D:92:BD	794 Bytes	1.0 KBytes	42	7 secs	0 secs

Refresh

6.9 VLAN

The **VLAN** option of the **Wireless** menu allows you to configure the VLAN (Virtual LAN).

Note: Only in Access Point mode.

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.

Virtual LAN :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSID 1 Tag:	<input type="text" value="100"/> (1~4094)
LAN VLAN MGMT :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MGMT Tag:	<input type="text" value="500"/> (1~4094)

VLAN (Access Point and WDS AP mode)	
Virtual LAN	Choose to Enable or Disable the VLAN feature.
SSID# Tag	Specify the VLAN tag for each SSID.
LAN VLAN MGMT	Choose to Enable or Disable the LAN VLAN MGMT feature.
MGMT Tag	Specify the VLAN tag for the LAN.

6.10AP Profile

This page allows you to configure the profile of the Client Bridge including Security Setting exactly the same as the Access Point. You can save three AP profiles at most.

Note: Only in Client Bridge mode.

AP Profile Table

NO.	SSID	MAC	Authentication	Encryption	Select
1	Test2013	00:02:6F:C7:EB:70	WPA2_PSK	AES	<input checked="" type="checkbox"/>

AP Profile Table (Client Bridge mode)	
Add / Edit	Select a profile to add or edit.
Move Up / Move Down	Select a profile to move up or move down.
Delete Selected	Delete the selected entries.
Delete All	Delete all entries
Connect	Select a profile to connect.

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server.

AP Profile Settings

Network Name (SSID) :

Encryption :



AP Profile Settings	
Network Name (SSID)	Enter the SSID (Network Name) of the wireless network which ALL02850N want to connect.
Encryption	The encryption method to be applied. You can choose from Disable, WEP, WPA pre-shared key and RADIUS. Please select the correct security type.

7 Network

7.1 Status

The **Status** option of the **Network** menu shows the current status of the ALL02850N's LAN and WAN (Router mode) connection.

View the current wireless connection status and related information.

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:02:6F:30:00:24

WAN Settings

Attain IP Protocol	Dynamic IP Address
IP Address	192.168.7.162
Subnet Mask	255.255.255.0
Default Gateway	192.168.7.10
MAC Address	00:02:6F:30:0A:24
Primary DNS	192.168.7.10
Secondary DNS	---

Renew

7.2 LAN

The **LAN** option of the **Network** menu allows you to modify the device's LAN settings.

The LAN setting in Router mode:

Bridge Type :	Static IP ▼
IP Address :	192.168.1.1
IP Subnet Mask :	255.255.255.0
DNS Type :	Static ▼
First DNS Address :	192.168.1.1
Second DNS Address :	192.168.1.1

There is additional setting **Default Gateway** in Access Point / Client Bridge / WDS AP / WDS Bridge and Repeater mode.

Bridge Type :	Static IP ▼
IP Address :	192.168.1.1
IP Subnet Mask :	255.255.255.0
Default Gateway :	
DNS Type :	Static ▼
First DNS Address :	192.168.1.1
Second DNS Address :	192.168.1.1

LAN IP	
Bridge Type	<p>Select the Bridge type of the LAN.</p> <p>Static IP: Manually specify an IP address and subnet mask for the ALL02850N to use.</p> <p>Dynamic IP: The IP address is received automatically from the external DHCP server.</p> <p>Note: The option: Dynamic IP is only in Access Point and WDS AP mode.</p>
IP Address	The LAN IP Address of this device.
IP Subnet Mask	The LAN Subnet Mask of this device.
Default Gateway	The Default Gateway of the device. Leave empty for default setting.

	Note: The option: Dynamic IP is only in Access Point / Client Bridge / WDS AP / WDS Bridge and Repeater mode.
DNS Type	Select the DNS type of the LAN. Static: Manually specify the DNS of the ALL02850N. Dynamic: The DNS is received automatically from the external DNS server. Note: The option: Dynamic is only in Access Point and WDS AP mode.
First / Second DNS Address	The first / second DNS address for this device.

The **DHCP Server** feature is only available in Access Point and Router mode.

DHCP Server

DHCP Server :	Enabled ▼
Lease Time :	Forever ▼
Start IP :	192.168.1.100
End IP :	192.168.1.200
Domain Name :	Test2013
First DNS Address :	
Second DNS Address :	

DHCP Server (Access Point / Router mode)	
DHCP Server	Enable or disable DHCP feature. The DHCP Server automatically allocates IP addresses to your LAN device. Disabled as default.
Lease Time	The duration of the DHCP server allocates each IP address to a LAN device.
Start / End IP	The range of IP addresses of the DHCP server will allocate to LAN device.
Domain name	The domain name for this LAN network.
First / Second DNS Address	The first / second DNS address for this LAN network.

7.3 Spanning Tree

The **Spanning Tree** option of the **Network** menu allows you to set the ALL02850N to use the Spanning Tree Protocol. Enabling Spanning Tree Protocol will prevent network loops in your LAN network.

Note: Only in Access Point / Client Bridge / WDS AP / WDS Bridge and Repeater mode.

Spanning Tree Settings

Spanning Tree Status :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bridge Hello Time :	<input type="text" value="2"/> seconds (1-10)
Bridge Max Age :	<input type="text" value="20"/> seconds (6-40)
Bridge Forward Delay :	<input type="text" value="15"/> seconds (4-30)
Bridge Priority :	<input type="text" value="32768"/> (0-65535)

Spanning Tree Settings	
Spanning Tree Status	Enable or disable the Spanning Tree Protocol.
Bridge Hello Time	The duration of the initial connection between two access points.
Bridge Max Age	The maximum amount of time the bridge is connected when transmitting.
Bridge Forward Delay	The delay between transmissions between access points.
Bridge Priority	The priority port of the Spanning Tree Protocol.

7.4 WAN (Router mode)

The WAN section allows you to manually set the WAN type connection and its related settings.

Note: Only in Router mode.

7.4.1 Static IP Address

If your ISP Provider has assigned you a fixed IP address, enter the assigned IP address, Subnet mask, Default Gateway IP address, and Primary DNS and Secondary DNS (if available) of your ISP provider.

Login Method:	Static IP Address ▼
IP Address:	0.0.0.0
IP Subnet Mask :	0.0.0.0
Default Gateway :	0.0.0.0
Primary DNS :	
Secondary DNS :	
Interface :	WAN

Static IP Address	
IP Address	Assign an IP address Manually.
IP Subnet Mask	Specify an IP address's subnet mask.
Default Gateway	Specify the gateway of your network.
Primary DNS	Specify the primary DNS server's IP address.
Secondary DNS	Specify the second DNS server's IP address.

7.4.2 Dynamic IP Address

The IP Address is allocated automatically. However some ISP's will also recognize the MAC address and will reject connections if the MAC address does not match.

If your ISP has recorded the MAC address of your computer's Ethernet LAN card, please connect only the computer with the authorized MAC address, and click the **Clone MAC** button.

Note: This will replace the WAN MAC address to the computer MAC address. The correct MAC address is used to initiate the connection to the ISP.

Login Method:	Dynamic IP Address ▾		
Hostname :	<input type="text"/>		
MAC Address:	<input type="text" value="000000000000"/>	<input type="button" value="Clone MAC"/>	<input type="button" value="Set Default"/>
Interface :	WAN		

Dynamic IP Address	
Hostname	This is optional. Only required if specified by ISP
MAC Address	The MAC Address that is used to connect to the ISP.

7.4.3 PPP over Ethernet (PPPoE)

This protocol is used by most DSL services worldwide. Select this option if you have a DSL connection. Enter the username and password provided by your ISP.

Login Method:	PPP over Ethernet ▼
Login :	<input type="text"/>
Password :	<input type="password"/>
Service Name	<input type="text"/>
MTU :	1492 (512<=MTU Value<=1492)
Type :	Keep Connection ▼
Idle Timeout :	10 (1-1000 Minutes)

PPP over Ethernet (PPPoE)	
Login	Username assigned to you by the ISP
Password	Password for this username.
Service Name	You can assign a name for this service. (Optional)
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.
Type	<p>You can choose the method that the router maintains connection with the ISP.</p> <p>Keep Connection: The device will maintain a constant connection with the ISP.</p> <p>Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device.</p> <p>Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.</p>
Idle Timeout:	When the connection type is Automatic Connection , when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

7.4.4 Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by very few ISPs.

Login Method :	PPTP ▼	
WAN Interface Settings :		
WAN Interface Type :	Dynamic IP Address ▼	
Hostname :	<input type="text"/>	
MAC address:	<input type="text" value="000000000000"/>	<input type="button" value="Clone MAC"/> <input type="button" value="Set Default"/>
PPTP Settings :		
Login :	<input type="text"/>	
Password :	<input type="text"/>	
Service IP Address :	<input type="text"/>	
Connection ID :	<input type="text" value="0"/>	(Optional)
MTU :	<input type="text" value="1400"/>	(512<=MTU Value<=1492)
Type :	Keep Connection ▼	
Idle Timeout :	<input type="text" value="10"/>	(1-1000 Minutes)

Point-to-Point Tunneling Protocol (PPTP)	
WAN Interface Type	Select whether the ISP is set to Static IP or will allocate Dynamic IP address.
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC Address that is used to connect to the ISP.
Login	Username assigned to you by the ISP
Password	Password for this username.
Service IP Address	The IP Address of the PPTP server.
Connection ID	This is optional. Only required if specified by ISP
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.
Type	<p>You can choose the method that the router maintains connection with the ISP.</p> <p>Keep Connection: The device will maintain a constant connection with the ISP.</p> <p>Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device.</p> <p>Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.</p>
Idle Timeout:	When the connection type is Automatic Connection , when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

8 Firewall

The Firewall section allows you to set the access control and Firewall settings.

Note: Only in Router mode.

8.1 Enable

This page allows you to Enable / Disable the Firewall features.

If enabled Firewall service, the Denial of Service (DoS) and SPI (Stateful Packet Inspection) features will also be enabled.

Firewall automatically detects and blocks Denial of Service (DoS) attacks. Website blocking, packet filtering and SPI (Stateful Packet Inspection) are also supported. The hackers attack will be recorded associated with timestamp in the security logging area.

Firewall : ☒ Enable ☐ Disable

Apply

8.2 DMZ

If enabled this feature, allows the DMZ computer on your LAN to be exposed to all users on the Internet.

- This allows almost any application to be used on the server.
- The "DMZ PC" will receive all Unknown connections and data.
- If the DMZ feature is enabled, please enter the IP address of the PC to be used as the "DMZ PC"

Note: The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

☐ **Enable DMZ**

Local IP Address :

192.168.1.100

Apply

Cancel

8.3 DoS

Denial of Service (Denial of Service) is a type of Internet attack that sends a high amount of data to you with the intent to overload your Internet connection.

Enable the DoS firewall feature to automatically detect and block these DoS attacks.

The Firewall can detect and block DOS attacks, DOS (Denial of Service) attacks can flood your Internet Connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Block DoS : ☒ Enable ☐ Disable

Apply

Cancel

8.4 MAC Filter

You can choose whether to Deny or only Allow those computers listed in the MAC Filtering table to access the Internet.

MAC Filters are used to deny or allow LAN computers from accessing the Internet.

☐ **Enable MAC Filtering**

☒ Deny all clients with MAC address listed below to access the network

☐ Allow all clients with MAC address listed below to access the network

Description	LAN MAC Address
rule02	00026F11AC93

Add

Reset

MAC Filtering table:

NO.	Description	LAN MAC Address	Select
1	rule01	00:13:64:78:41:CE	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

MAC Filter	
Enable MAC filtering	Tick this box to Enable the MAC filtering feature.
Deny all clients with MAC addresses listed below to access the network	When selected, the computers listed in the MAC Filtering table will be Denied access to the Internet.
Allow all clients with MAC addresses listed below to access the network	When selected, only the computers listed in the MAC Filtering table will be Allowed access to the Internet.

8.5 IP Filter

You can choose whether to Deny or only Allow, computer with those IP Addresses from accessing certain Ports.

This can be used to control which Internet applications the computers can access. You may need to have certain knowledge of what Internet ports the applications use.

IP Filters are used to deny or allow LAN computers from accessing the Internet.

- ☐ **Enable IP Filtering Table (up to 20 computers)**
- ☒ Deny all clients with IP address listed below to access the network
- ☐ Allow all clients with IP address listed below to access the network

Description :	<input type="text"/>
Protocol :	Both ▼
Local IP Address :	<input type="text"/> ~ <input type="text"/>
Port Range :	<input type="text"/> ~ <input type="text"/>

NO.	Description	Local IP Address	Protocol	Port Range	Select
1	rule01	192.168.1.100	BOTH	21-22	<input type="checkbox"/>

IP Filter	
Enable IP filtering	Tick this box to Enable the IP filtering feature.
Deny all clients with IP addresses listed below to access the network	When selected, the computers with IP addresses specified will be Denied access to the indicated Internet ports.
Allow all clients with IP addresses listed below to access the network	When selected, the computers with IP addresses specified will be Allowed access only to the indicated Internet ports.

8.6 URL Filter

You can deny access to certain websites by blocking keywords in the URL web address.

For example, "gamer" has been added to the URL Blocking Table. Any web address that includes "gamer" will be blocked.

You can limit access to certain sites on the Internet. The Website filter will check each Web Site access. If the address, or part of the address, is included in the block site list, access will be denied. To filter a specific site, enter the Website for that site. For example, to stop your users from browsing a site called www.badsite.com, enter www.badsite.com or badsite.com in Website block fields.

☐ **Enable Website Blocking**

Website/keyword

Current Website Blocking Table:

NO.	Website/keyword	Select
1	test123	<input type="checkbox"/>

9 Advanced

The **Advanced** section allows you to configure the Advanced settings of the router.

Note: Only in Access Point Client Router mode.

9.1 Network Address Translation (NAT)

This page allows you to Enable / Disable the Network Address Translation (NAT) feature. The NAT is required to share one Internet account with multiple LAN users.

NAT(Network Address Translation) involves re-writing the source and/or destination addresses of IP packets as they pass through a Router or firewall, NAT enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT : ☒ Enable ☐ Disable

Apply

9.2 Port Mapping

Port Mapping allows you to redirect a particular range of ports to a computer on your LAN network.

This helps you host servers behind the NAT and Firewall.

In the example below, there is a FTP Server that requires ports 21 to 22.

When there is a connection from the Internet on those ports, it will be redirected to the FTP Server at IP address 192.168.1.100.

Port Mapping allows you to redirect common network services to a specific Client PC behind the NAT firewall.

☒ **Enable Port Mapping**

Description :	<input type="text"/>
Local IP :	<input type="text"/>
Protocol :	Both ▼
Port Range :	<input type="text"/> ~ <input type="text"/>

Current Port Mapping Table:

NO.	Description	Local IP	Type	Port Range	Select
1	rule01	192.168.1.100	BOTH	21-22	<input type="checkbox"/>

Port Mapping	
Enable Port Mapping	Check this box to enable the Port Mapping feature.
Description	Enter a name or description for this entry.
Local IP	The local IP address of the computer the server is hosted on.
Protocol	Select to apply the feature to TCP, UDP or Both types of packet transmissions.
Port Range	The range of ports that this feature will be applied to.

9.3 Port Forwarding

Port Forwarding allows you to redirect a particular public port to a computer on your LAN network. This helps you host servers behind the NAT and Firewall.

In the example below, there is a Web Server running on port 80 on the LAN.

For security reasons, the Administrator would like to provide this server to Internet connection on port 100.

Port Forwarding, also called Virtual Server. Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it.

☒ **Enable Port Forwarding**

Description :	<input type="text"/>
Local IP :	<input type="text"/>
Protocol :	Both ▾
Local Port :	<input type="text"/>
Forwarded Port :	<input type="text"/>

Current Port Forwarding Table :

NO.	Description	Local IP	Local Port	Type	Forwarded Port	Select
1	rule01	192.168.1.150	80	BOTH	100	<input type="checkbox"/>

Therefore when there is a connection from the Internet on port 100, it will be forwarded to the computer with the IP address 192.168.1.150 and changed to port 80.

Port Forwarding	
Enable Port Forwarding	Check this box to enable the Port Forwarding feature.
Description	Enter a name or description for this entry.
Local IP	The local IP address of the computer the server is hosted on.
Protocol	Select to apply the feature to TCP, UDP or Both types of packet transmissions.
Local Port	The port that the server is running on the local computer.
Forwarded Port	When a connection from the Internet is on this port, it will be forwarded to the indicated local IP address.

9.4 Port Triggering

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. Port Triggering will be required for these applications to work.

Port Triggering, also called Special Applications allows you to use Internet applications which normally do not function when used behind a firewall.

☒ **Enable Trigger Port**

Description :	PC-to-Phone	
Popular Applications :	PC-to-Phone	<input type="button" value="Add"/>
Trigger Port :	12053 ~	
Trigger Type :	Both	
Forwarded Port :	12120,12122,24150-24220	
Public Type :	Both	

Current Trigger-Port Table:

NO.	Trigger Port	Trigger Type	Forwarded Port	Public Type	Name	Select
1	28800	BOTH	2300-2400,47624	BOTH	MSN Gaming Zone	<input type="checkbox"/>

Port Triggering	
Enable Port Triggering	Check this box to enable the Port Trigger feature.
Popular Applications	This is a list of some common applications with preset settings. Select the application and click Add to automatically enter the settings.
Trigger Port	This is the outgoing (outbound) port numbers for this application.
Trigger Type	Select whether the application uses TCP, UDP or Both types of protocols for outbound transmissions.
Forwarded Port	These are the inbound (incoming) ports for this application.
Public Type	Select whether the application uses TCP, UDP or Both types of protocols for inbound transmissions.

9.5 Application Layer Gateway (ALG)

Certain applications may require the use of the ALG feature to function correctly. If you use any of the applications listed on the table below, select the feature and click Apply.

The ALG (Application Layer Gateway) serves the purpose of a window between correspondent application processes so that they may exchange information on the open environment.

Description	Select
H323	<input type="checkbox"/>
MMS	<input type="checkbox"/>
TFTP	<input type="checkbox"/>
Egg	<input type="checkbox"/>
IRC	<input type="checkbox"/>
Amanda	<input type="checkbox"/>
Quake3	<input type="checkbox"/>
Talk	<input type="checkbox"/>
IPsec	<input type="checkbox"/>
FTP	<input type="checkbox"/>

9.6 Universal Plug and Play (UPnP)

The UPnP function allows automatic discovery and configuration of UPnP enabled devices on your network. It also provides automatic port forwarding for supported applications to seamlessly bypass the Firewall.

UPnP allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments.

UPnP : ☒ Enable ☐ Disable

Apply

9.7 Quality of Service (QoS)

QoS allows you to control the priority that the data is transmitted over the Internet, or to reserve a specific amount of Internet bandwidth. This is to ensure that applications get enough Internet bandwidth for a good user experience.

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS : ☐ Priority Queue ☐ Bandwidth Allocation ☒ Disabled

QoS	
Priority Queue	Sets the QoS method to Priority Queue.
Bandwidth Allocation	Sets the QoS method to Bandwidth Allocation.
Disabled	Disables the QoS feature.

Priority Queue Method

Bandwidth priority is set to either High or Low. The data transmissions in the High Priority queues will be processed first.

QoS : ☒ Priority Queue ☐ Bandwidth Allocation ☐ Disabled

Unlimited Priority Queue

IP Address	Description
<input type="text"/>	The IP address will not be bounded in the QoS limitation

High/Low Priority Queue

Protocol	High Priority	Low Priority	Specific Port
FTP	<input type="radio"/>	<input checked="" type="radio"/>	20,21
HTTP	<input type="radio"/>	<input checked="" type="radio"/>	80
TELNET	<input type="radio"/>	<input checked="" type="radio"/>	23
SMTP	<input type="radio"/>	<input checked="" type="radio"/>	25
POP3	<input type="radio"/>	<input checked="" type="radio"/>	110
Name <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="0"/>
Name <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="0"/>
Name <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="0"/>

Unlimited Priority Queue	
IP Address	The computer with this IP Address will not be bound by the QoS rules.
High / Low Priority Queue	
Protocol	The type of network protocol.
High / Low Priority	Sets the protocol to High or Low priority.
Specific Port	Each protocol uses a specific port range. Please specify the ports used by this protocol.

Bandwidth Allocation Method

You can set the maximum amount of bandwidth a certain protocol will use at one time. Or you can set a minimum amount of bandwidth that will be guaranteed to a certain protocol.

QoS : ☐ Priority Queue ☒ Bandwidth Allocation ☐ Disabled

Type : download

IP range : ~

Protocol : All

Port Range : 1 ~ 65535

Policy : Min

Rate(bps) : FULL

Add Reset

Current QoS Table:

NO.	Type	IP range	Protocol	Port Range	Policy	Rate (bps)	Select
1	download	192.168.1.100 ~ 192.168.1.101	ALL	1 ~ 65535	Max	2M	<input type="checkbox"/>

Delete Selected Delete All Reset

Apply Cancel

Bandwidth Allocation	
Type	Set whether the QoS rules apply to transmission that are Download, Upload or Both directions.
IP range	Enter the IP address range of the computers that you would like the QoS rules to apply to.
Protocol	Select from this list of protocols to automatically set the related port numbers.
Port Range	Each protocol uses a specific port range. Specify the ports used by this protocol.
Policy	Choose whether this rule is to set a limit on the Maximum amount of bandwidth allocated to the specified protocol, or to set the guaranteed Minimum amount of bandwidth for the protocol.

9.8 Static Routing

If your wireless router is connected to a network with different subnets, this feature will allow the different subnets to communicate with each other.

Note: The NAT function needs to be disabled for the Routing feature to be enabled.

You can enable Static Routing to power off the NAT function of the router and let the router forward packets by your routing policy.

To take Static Route effect, please disable NAT function.

☐ Enable Static Routing

Destination LAN IP:

Subnet Mask:

Default Gateway:

Current Static Routing Table:

NO.	Destination LAN IP	Subnet Mask	Default Gateway	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>				

Static Routing	
Enable Static Routing	Check this box to enable the Static Router feature.
Destination LAN IP	Enter the IP address of the destination LAN.
Subnet Mask	Enter the Subnet Mask of the destination LAN IP address
Default Gateway	Enter the IP address of the Default Gateway for this destination IP and Subnet.

9.9 Dynamic Routing

Dynamic routing allows routing tables in routers to change as the possible routes change. This device use RIP to support dynamic routing.

The Router supports the Routing Information Protocol (RIP). RIP allows you to set up routing information on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network.

☐ **Dynamic Routing**

RIP Transferring:

RIPv1/RIPv2 ▼

RIP Receiving:

RIPv1/RIPv2 ▼

Password:

Apply

Cancel

9.10 Routing Table

This page allows you to observe the current routing table.

Current Routing Table

Destination LAN IP	Subnet Mask	Default Gateway
192.168.66.1	255.255.255.255	192.168.66.1
192.168.1.0	255.255.255.0	0.0.0.0
192.168.66.0	255.255.255.0	0.0.0.0
0.0.0.0	0.0.0.0	192.168.66.1

Refresh

10 Management

10.1Admin

The **Admin** section of the **Management** menu allows you to change the ALL02850N default password and to configure remote management (Router mode). By default, the password is: **admin**. The password can contain 0 to 12 alphanumeric characters and is case sensitive.

You can change the password that you use to access the device, this is not you ISP account password.

Old Password :	<input type="text"/>
New Password :	<input type="text"/>
Confirm password :	<input type="text"/>
Idle Timeout :	<input type="text" value="10"/> (1~10 Minutes)

Change Password	
Old Password	Enter the current password.
New Password	Enter your new password.
Confirm Password	Re-enter your new password.
Idle Timeout	Enter Administration Page timeout time (minutes).

There is additional setting **Remote Management** in Router mode.

Remote management allows the router to be configured from the Internet by a web browser, A username and password is still required to access the Web-Management interface.

Host Address	Port	Enable
<input type="text" value="0.0.0.0"/>	<input type="text" value="8080"/>	<input type="checkbox"/>

Remote Management (Router mode)	
Host Address	You can only perform remote management from the specified IP address. Leave blank to allow any host to perform remote management.
Port	Enter the port number you want to accept remote management connections.
Enable	Tick to Enable the remote management feature.

10.2SNMP

The **SNMP** section of the **Management** menu allows you to assign the contact details, location, community name, and trap settings for the Simple Network Management Protocol (SNMP). The SNMP is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (Agents) return data stored in their Management Information Bases.

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP Active	Enabled ▾
SNMP Version	All ▾
SNMP Manager IP	0.0.0.0
Read Community	public
Set Community	private
System Location	ALLNET GmbH
System Contact	ALLNET GmbH
Trap Active	Disabled ▾
Trap Manager IP	192.168.1.100
Trap Community	public

SNMP	
SNMP Active	Enable or disable the SNMP feature.
SNMP Version	<p>You may select the SNMP version you want to deploy.</p> <p>All: Interoperability between SNMPv1 and SNMPv2c devices.</p> <p>v1: The standard SNMP version.</p> <p>v2c: Improvement in performance and security of SNMPv1.</p>
Read Community	Specify the password for access the SNMP community for read only access.
Set Community	Specify the password for access to the SNMP community with read/write access.
System Location	Specify the location of the device.
System Contact	Specify the contact details of the device

Trap	
Trap Active	Enable or disable SNMP trapping feature.
Trap Manager IP	Specify the IP address of the computer that will receive the SNMP traps.
Trap Community	Specify the password for the SNMP trap community.

10.3 Firmware Upgrade

The **Firmware Upgrade** section of the **Management** allows you to upgrade the ALL02850N's firmware.

You can upgrade the firmware of the device in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update.

To perform the Firmware Upgrade:

1. Download the firmware version that you want to install into the ALL02850N and place it in a known location.
2. Click the **Browse** button and navigate to the location of the firmware upgrade file.
3. Select the firmware upgrade file. Its name will appear in the **Upgrade File** field.
4. Click the **Apply** button to commence the firmware upgrade.

Note: The device is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the device will be lost.

1. Click the **Browse** button and navigate to the location of the upgrade file and then click **Upload**.

Emergency Web Server

File

2. Wait for 60 seconds for firmware upgrade and reboot the device.

Updating File.....

Don't Power Down.

Please wait for **58** seconds ...

3. You can access the device again.



Username:

Password:

10.4Configure

The **Configure** option of the **Management** menu allows you to save the current device configurations. When you save the configurations, you also can re-load the saved configurations into the device through the **Restore Settings**. If extreme problems occur press the **Reset** button of the **Restore to Factory Defaults** option to set all configurations to its original default settings.

The current system settings can be saved as a file onto the local hard drive. The saved file can be loaded back on the device. To reload a system settings file, click on BROWSE to locate the system file to be used. You may also reset the device back to factory default settings by clicking RESET.

Restore To Factory Default :	<input type="button" value="Reset"/>
Backup Settings :	<input type="button" value="Save"/>
Restore Settings :	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>

Configure	
Restore to Factory Default	Restores the device to factory default settings.
Backup Settings	Save the current configuration settings to a file.
Restore Settings	Restores a previously saved configuration file. Click Browse to select the file. Then Upload to load the settings.

10.5Reset

In some circumstances it may be required to force the device to reboot. Click on **Apply** to reboot of the **Reset** option of the **Management** menu.

In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking.

Apply

11 Tools

11.1 Time Setting

The **Time Setting** section of the **Tools** menu allows you to set the ALL02850N's time.

The device reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option merely advances the system clock by one hour. The time zone setting is used by the system clock when displaying the correct time in schedule and the log files.

Time Setup :	Synchronize with the NTP Server ▼
Time Zone :	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
NTP Time Server :	<input type="text"/>
Daylight Saving :	<input type="checkbox"/> Enable From <input type="text" value="January"/> <input type="text" value="1"/> To <input type="text" value="January"/> <input type="text" value="1"/>

Time	
Time Setup	Select the method you want to set the time.
Time Zone	Select the time zone for your current location.
NTP Time Server	Enter the address of the Network Time Protocol (NTP) Server to automatically synchronize with a server on the Internet.
Daylight Savings	Check whether daylight savings applies to your area.

11.2Diagnosis

The **Diagnosis** section of the **Tools** menu allows you to test your network. Type in the IP Address of the device for diagnosis.

This page can diagnose the current network status.

Address to Ping :	<input type="text"/>
Ping Frequency :	<input type="text" value="1"/> <input type="button" value="Start"/>

Diagnosis	
Address to Ping	Enter the IP address you like to see if a successful connection can be made.
Ping Frequency	Select the frequency for Ping test.
Ping Result	The results of the Ping test.

12 Logout

Click on **Logout** button to logout of the ALL02850N.

This page is used to logout this device.

Logout

Appendix A – FCC Interference Statement

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 the 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 of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV 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 this equipment.

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, and (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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Appendix B – IC Interference Statement

Industry Canada statement:

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

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE IMPORTANTE: (Pour l'utilisation de dispositifs mobiles)

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This device has been designed to operate with a **diopole** antenna have a maximum gain of **[5]** dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (**IC: 10103A-ALL02850N / Model: ALL02850N**) has been approved by Industry Canada to operate with the antenna type, maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this user's manual, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de **diopole** antenne avec dB **[5]**. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie

Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteur radio (IC: 10103A-ALL02850N / Modèle: ALL02850N) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Appendix C – CE Interference Statement

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN60950-1:2006 A11:2009+A1:2010
- Safety of Information Technology Equipment

- EN50385 : 2002
- Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)

- EN 300 328 V1.7.1: 2006-10
- Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

- EN 301 489-1 V1.8.1: 2008-04
- Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- EN 301 489-17 V2.1.1 2009-05
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment








This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member










states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

C € 0560 !

 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ

	KAI TIS ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
 Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoja, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.



ALL02850N User's Manual

<input checked="" type="checkbox"/> Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
--	--



CE-Declaration of Conformity

For the following equipment:

Germering, 1st of August, 2013

WLAN N Access Point /Client Bridge

ALL02850N



The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The ALLNET ALL02850N conforms to the Council EMC Directives of 2006/95/EC.

This equipment meets the following conformance standards:

EN 60950-1:2006 +A11:2009 + A1:2010 + A12:2011

This equipment is intended to be operated in all countries.

This declaration is made by
ALLNET Computersysteme GmbH
Maistraße 2
82110 Germering
Germany

Germering, 01.08.2013



Wolfgang Marcus Bauer
CEO