

EnGenius®

300Mbps Wireless N Range Extender

ERB9260

300Mbps Wireless N Range Extender

V1.0



Table of Contents

1	Package Contents	5
2	Introduction	5
3	Hardware Overview	6
4	Before you Begin	8
4.1	Considerations for Wireless Installation	8
4.2	Computer Settings (Windows XP/Windows Vista/Windows 7).....	9
4.3	Apple Mac X OS.....	13
5	Hardware Installation	14
6	Configuring Range Extender	16
7	Quick Setup Range Extender	17
7.1	Manual Setup	17
7.2	One-Touch Setup (WPS).....	20
8	System	24
8.1	Operation Mode.....	24
8.2	Status.....	25
8.3	DHCP (Client Router mode)	30
8.4	Schedule (Client Router mode).....	33
8.5	Even Log.....	35
8.6	Monitor.....	36
9	Wireless	37
9.1	Status.....	37
9.2	Basic.....	39
9.3	Advanced	44

9.4	Security (Repeater mode)	47
9.5	Filter (Repeater mode)	50
9.6	WPS.....	52
9.7	Client List (Repeater mode).....	56
9.8	AP Profile.....	57
10	Network	59
10.1	Status.....	59
10.2	LAN.....	60
10.3	WAN (Client Router mode)	62
10.3.1	Static IP Address	62
10.3.2	Dynamic IP Address.....	63
10.3.3	PPP over Ethernet (PPPoE)	64
10.3.4	Point-to-Point Tunneling Protocol (PPTP).....	65
11	Firewall (Client Router mode)	67
11.1	Enable.....	67
11.2	DMZ	68
11.3	DoS.....	69
11.4	MAC Filter	70
11.5	IP Filter	71
11.6	URL Filter.....	73
12	Advanced (Client Router mode)	74
12.1	Network Address Translation (NAT).....	74
12.2	Port Mapping	75
12.3	Port Forwarding.....	76
12.4	Port Triggering.....	77
12.5	Application Layer Gateway (ALG).....	78
12.6	Universal Plug and Play (UPnP).....	79

12.7	Quality of Service (QoS).....	80
12.8	Static Routing.....	83
12.9	Dynamic Routing.....	84
12.10	Routing Table.....	85
13	Management	86
13.1	Admin.....	86
13.2	Firmware.....	87
13.3	Configure	90
13.4	Reset	91
14	Tools	92
14.1	Time Setting.....	92
14.2	Dynamic DNS (DDNS) (Client Router mode).....	93
14.3	Diagnosis.....	94
15	Wizard (Repeater mode).....	95
16	Logout.....	96
17	Building a Wireless Network.....	97
17.1	Repeater Mode	97
17.2	Client Bridge Mode	98
17.3	Client Router Mode.....	99
	Appendix A – FCC Interference Statement	100
	Appendix B – Industry Canada statement	101

Revision History

Version	Date	Notes
1.0	2011/06/24	First Release
1.1	2011/08/19	Add Client Bridge and Client Router mode

1 Package Contents

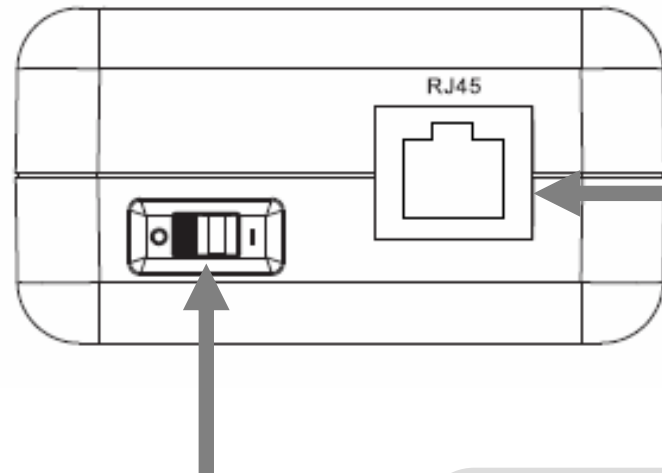
- EnGenius Range Extender
- AC Plug
- RJ45 Ethernet Cable
- CD-ROM with User Manual and Setup Utility
- Quick Installation Guide

2 Introduction

ERB9260 is a 2.4GHz 802.11b/g/n 300Mbps Repeater Extender. Range Extender solves the signal attenuation (limited coverage) problem by literally repeating / extending AP radio signal to dead-spots. Repeater clones AP and serves as a subsidiary entity to its clients. It supports latest industrial standard security settings WEP, WPA & WPA2.

ERB9260 offers an easy way to extend your wireless AP coverage without changing IP address settings. It is truly user friendly network gear for home users.

3 Hardware Overview



On/Off Switch







You can manually turn on/off the device using this slide switch.

O: Off **I:** ON

RJ45

This is RJ45 LAN port.

LAN: Connect to a computer, switch or hub.

LED Lights	icon	Description
Wireless LAN		Color – Blue Lights when Wireless signal is activated. Blinks when Wireless data transfer.
WPS		Color – Blue Blinks when WPS handshake is initialized.
LAN		Color – Blue Lights when wired network device is connected to RJ45 port. Blinks when data transfer occurs on RJ45 port.
Power		Color – Blue Lights when device is powered ON. Blinks device is Reset.
Signal Strength		Signal indicator shows AP signal strength. Green – Strong Yellow – Normal Red – Weak
Buttons	icon	Description
WPS		Press this button to initialize WPS process. Hold this button for 15 seconds to Reset to Factory Defaults.

4 Before you Begin

This section will guide you through the installation process. Placement of the Range Extender is very important to avoid poor signal reception and performance. Avoid placing the device in enclosed spaces such as a closet, cabinet or wardrobe.

4.1 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. These could be the number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through. Here are some key guidelines to ensure that you have the optimal wireless range.

1. Keep the number of walls and ceilings between the EnGenius access point and other network devices to a minimum. Each wall or ceiling can reduce the signal strength, the degradation depends on the building's material.
2. Building materials makes a difference. A solid metal door or aluminum studs may have a significant negative effect on range. Locate your wireless devices carefully so the signal can pass through a drywall or open doorways. Materials such as glass, steel, metal, concrete, water (fish tanks), mirrors, file cabinets and brick will also degrade your wireless signal.
3. Interferences can also come from your other electrical devices or appliances that generate RF noise. The most usual types are microwaves, or cordless phones.



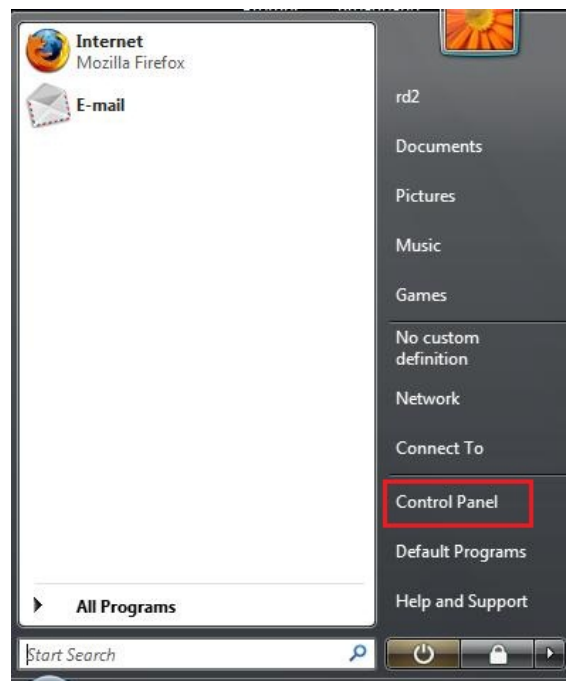
4.2 Computer Settings (Windows XP/Windows Vista/Windows 7)

This device can be configured as a Repeater, Client Bridge and Client Router. The default IP address of the device is **192.168.1.2** (In Repeater Mode as default). In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

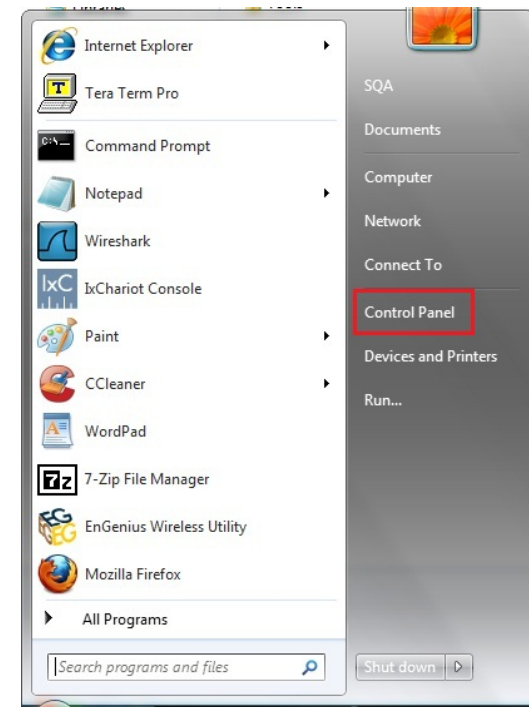
- Click Start button and open Control Panel.



Windows XP



Windows Vista

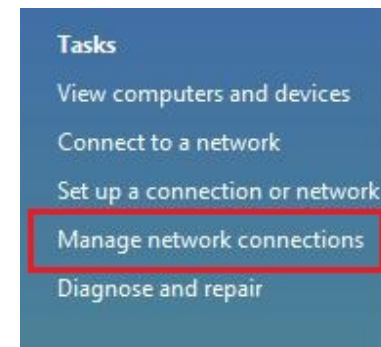
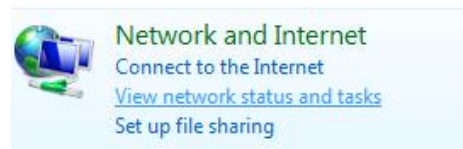


Windows 7

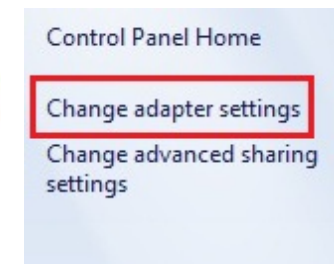
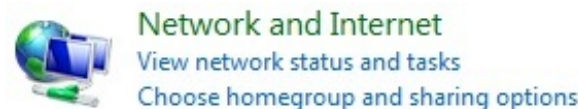
- Windows XP, click [Network Connection]



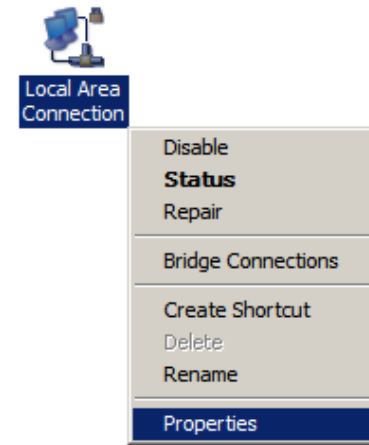
- Windows Vista, click [View Network Status and Tasks] then [Manage Network Connections]



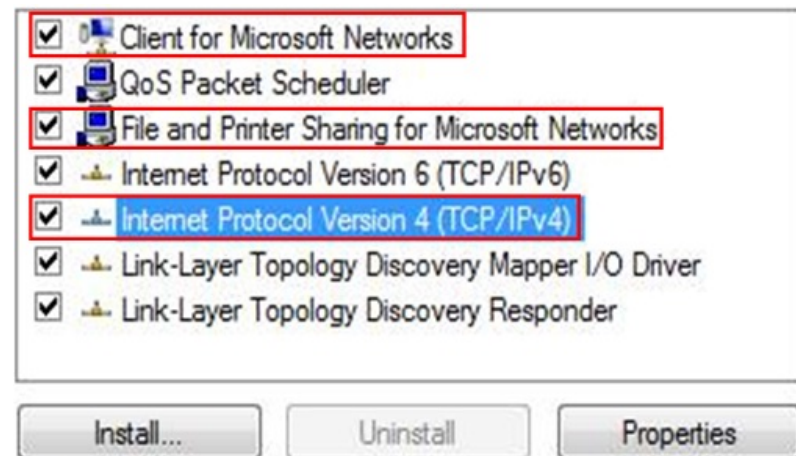
- Windows 7, click [View Network Status and Tasks] then [Change adapter settings]



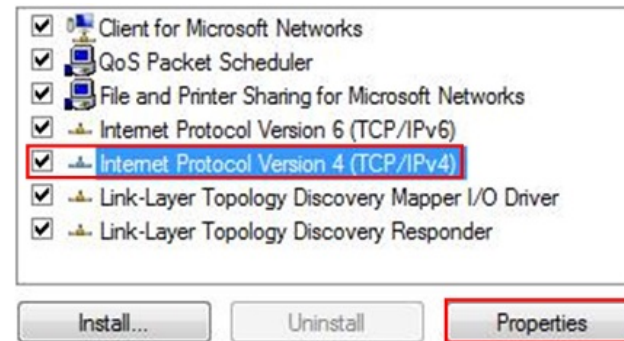
- Right click on [Local Area Connection] and select [Properties].



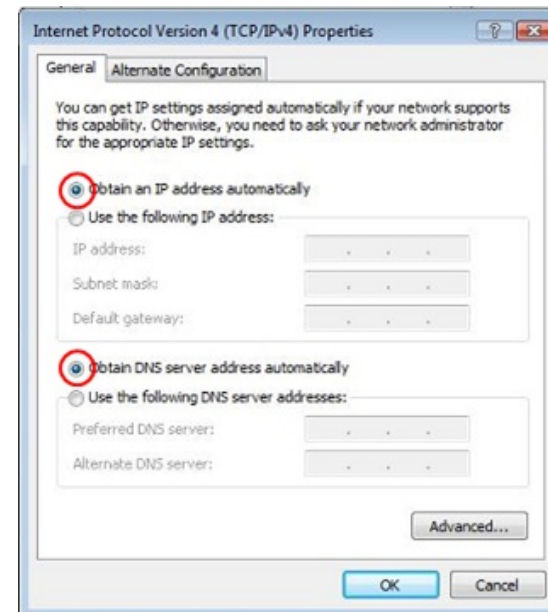
- Check "**Client for Microsoft Networks**", "**File and Printer Sharing for Microsoft Networks**", and "**Internet Protocol (TCP/IP)**" is ticked. If not, please install them.



- Select **“Internet Protocol (TCP/IP)”** and click [Properties]



- Select **“Obtain an IP Address automatically”** and **“Obtain DNS server address automatically”** then click [OK].

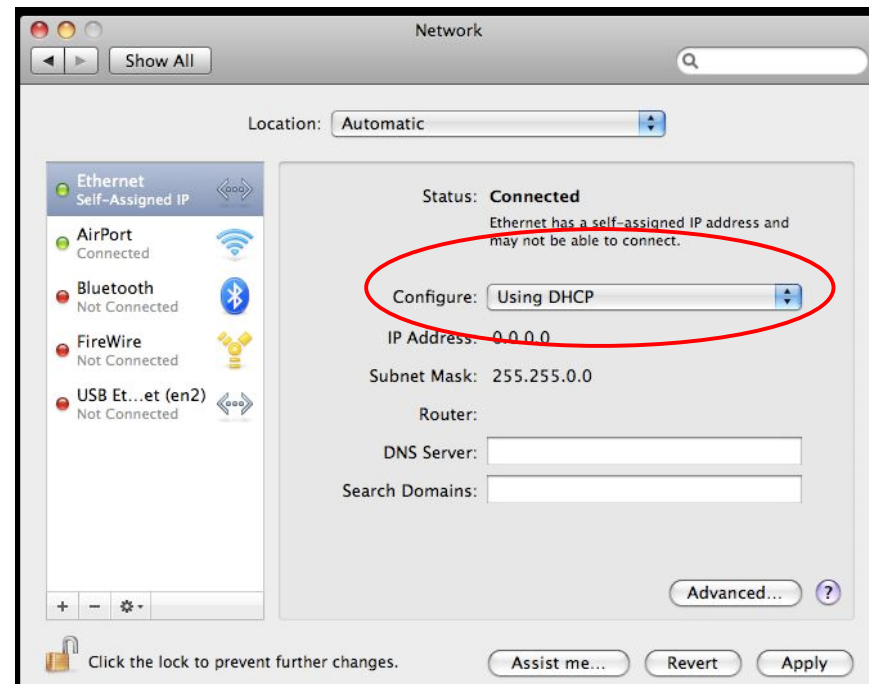


4.3 Apple Mac X OS

- Go to **System Preferences > Network**



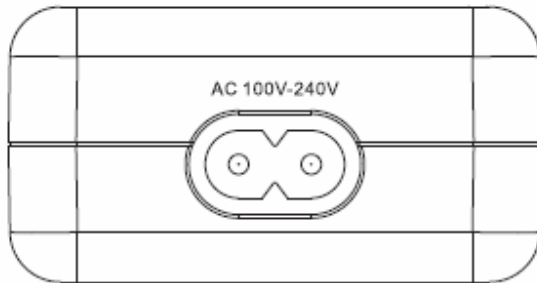
- Under Network setting, select Using **DHCP**.
- Click **Apply** when done.



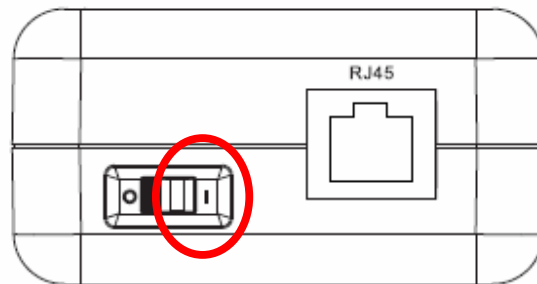
5 Hardware Installation

Power On:

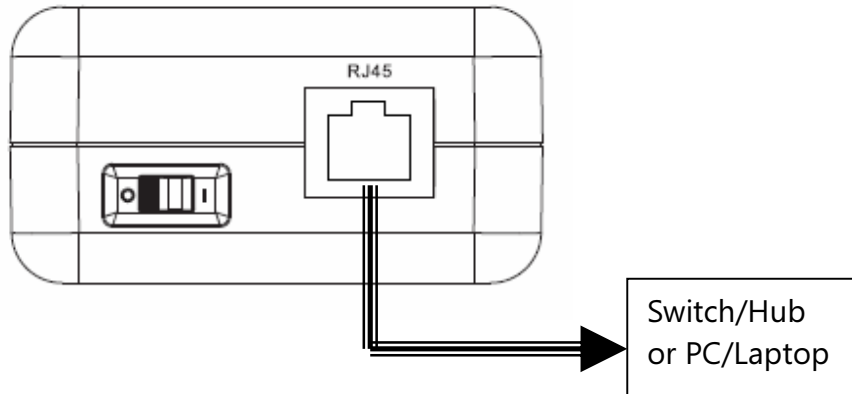
Use the AC Power cord to connect the device and outlet or any other power supplies to provide the electricity to the device.



Make sure On/Off switch is on the right side where the symbol indicates "I".



Connect the network cable to the RJ45 port.



6 Configuring Range Extender

This section will show you how to configure the device using the web-based configuration interface. Please use your wireless network adapter to connect the Range Extender.

Default Settings

IP Address	192.168.1.2
Username / Password	admin / admin
Wireless Mode	Enable
Wireless SSID	EnGeniusxxxxxx
Wireless Security	None

There are two ways to setup Range Extender.

1. Quick Setup

2. Smart Setup.

Please refer to **Section 7** for detail information.

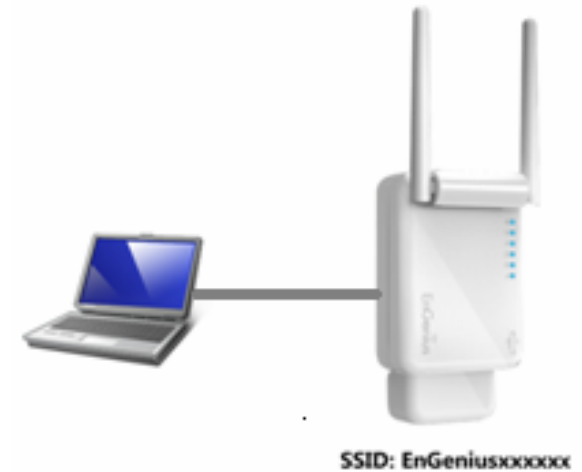
For expert users, if you need to configure advanced settings, please make use of the “**expert mode**” under **Section 8**.

Note: xxxxxx mentioned in the wireless SSID above is the last 6 characters of your device MAC Address. This can be found on the device body label and is unique for each device.

7 Quick Setup Range Extender

7.1 Manual Setup

1. Plug ERB9260 into power outlet.
2. Disable or turn off any wireless connections present on the computer being used to configure the Range Extender before setting up ERB9260.
3. Connect one end of the supplied Ethernet cable to the **Ethernet/RJ45** connector on the top of the Range Extender and the other end to Ethernet port on your PC/ laptop.
4. Open a web browser and enter the default IP Address of the Range Extender **http://192.168.1.2**



5. Click **Scan Now** and you will see all of the wireless networks in the range of the ERB9260.

START:

- Select your AP (router) to extend the wireless coverage.
- Show me a list of available AP list.

Click on [Expert Mode] to configure advanced settings

6. Select the target router and click **Connect**

- Please select one from the list and press [Connect] to proceed.
- If your AP is not found on the list please press [Refresh] again to get updated list.
- If you have enabled "Hidden SSID" or "Do not broadcast beacon" on your AP, you will have to enter correct SSID on the next page.

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	1	SENAOWL	00:02:6F:52:8C:D3	WEP	AUTOWEP	86	11b/g
2	<input type="radio"/>	1	SENAOWL	00:97:53:AA:11:1C	WEP	AUTOWEP	20	11b/g/n
3	<input type="radio"/>	1	ap51_memleak	00:02:6F:00:00:20	NONE	OPEN	50	11b/g
4	<input type="radio"/>	8	SQA_M36	00:02:6F:6B:D2:25	TKIPAES	WPA1PSKWPA2PSK	100	11b/g
5	<input type="radio"/>	2	belkin.nelson	94:44:52:B4:C0:D3	AES	WPA2PSK	65	11b/g/n
6	<input type="radio"/>	4	RD_ADSL	00:02:6F:11:22:A0	WEP	AUTOWEP	60	11b/g/n
7	<input checked="" type="radio"/>	4	HomeAP	00:02:6F:64:C9:F0	AES	WPA2PSK	100	11b/g/n
8	<input type="radio"/>	4	556-@@@	00:AA:BB:33:52:12	TKIPAES	WPA1PSKWPA2PSK	60	11b/g
9	<input type="radio"/>	5	RD2esr9850	00:AA:CC:DD:10:14	AES	WPA2PSK	60	11b/g/n
10	<input type="radio"/>	7	RAIDER ADSL`	00:0C:F6:54:A9:78	TKIPAES	WPA1PSKWPA2PSK	81	11b/g/n

7. Enter the password if your target router is encrypted. Click **Connect**.

- The following security settings are automatically entered for you in accords to the selected AP.
- Change it ONLY IF you found it mismatched.
- Usually you are only required to enter the password (security key).
- If your AP does not have security, please ignore this page and press [connect] to proceed.

Network Name (SSID) :	<input type="text" value="HomeAP"/>
Encryption :	<input type="text" value="WPA pre-shared key"/>
Authentication Type :	<input type="text" value="WPA2(AES)"/>
Pre-shared Key :	<input type="text" value="12345678"/>

8. The connection is established successfully between your AP/Router and ERB9260. Now the ERB9260's SSID is identical to with the router's SSID.

**Establishing connection with the selected AP...
Please Wait**

**Congratulations! You have successfully extended your AP signal with range extender.
Please read the following note carefully.**

- Your range extender has cloned your AP "**HomeAP**"; therefore, you will now find two APs with the same name (SSID) "**HomeAP**".
- You can now roam and your wireless interface card will pick up the most suitable AP signal as you move.
- Please reconnect to wireless network "**HomeAP**" with the password (security key) "**12345678**".

Note: Remove the Ethernet cable from ERB9260 and the computer and enable your wireless interface before using.

7.2 One-Touch Setup (WPS)

1. Click [WPS] button on ERB9260



SSID: EnGeniusxxxxxx



SSID: HomeAP

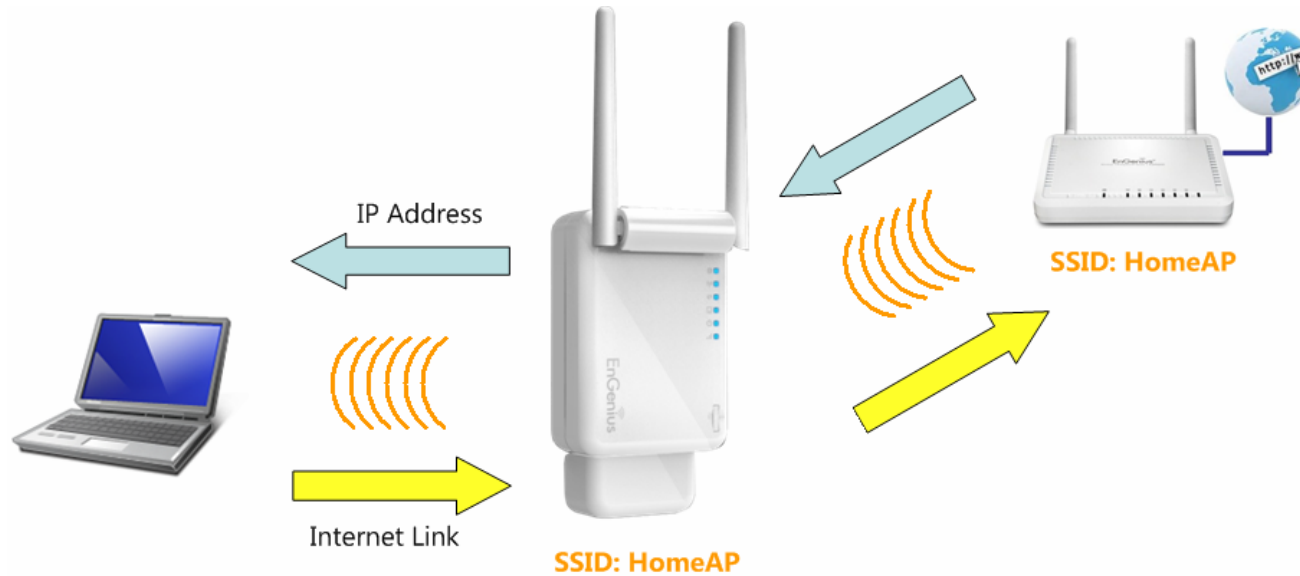
2. Click **[WPS]** button on the Access Point.



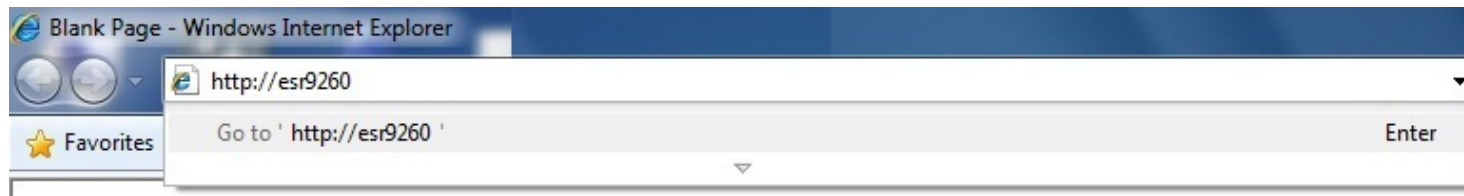
Note:

- It may take up to 60 seconds for ERB9260 to clone the AP. Please wait until **WPS led** stops blinking and stay **ON**.
- If the connection is successful. There will be **TWO** HomeAP in the environment.

3. Please **rescan** the APs and **reconnect** to the HomeAP closest to you. Your wireless card should pick up the AP with **strongest** signal as you roam.



Note: To re-configure the extender you can enter <http://erb9260> to enter the WEB configurator or reset the extender to default by press the WPS button for 15 seconds.



Expert Mode

8 System

8.1 Operation Mode

Each of the operating modes offers different features. In order to switch the operating mode, select it from the System >> Operation Mode. There are three operation modes: Repeater, Client Bridge and Client Router.

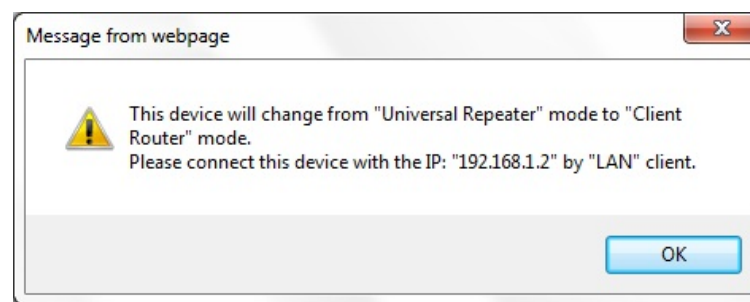
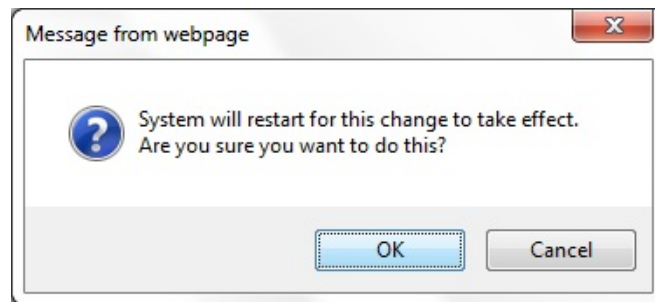
Operation Mode

Operation Mode : Universal Repeater ▾

Router Function : Enable Disable

Apply Cancel

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



Please wait while the device counts down and restarts into the new operating mode.

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

8.2 Status

This page allows you to monitor the status of the device.

System

Operation Mode Universal Repeater
 System Time 2009/01/01 00:28:10
 System Up Time 27 min 46 sec
 Hardware Version 1.0.0
 Serial Number 106291603
 Kernel Version 1.1.0
 Application Version 1.1.0

System	
Operation Mode	The device is currently in which mode.
System Time	The device's system time. If this is incorrect, please set the time in the Tools / Time page.
System Up Time	The duration about the device has been operating without powering down or reboot.
Hardware Version and Serial Number	Hardware information for this device.
Kernel and Application version	Firmware information for this device.

WLAN Repeater Information

Connection Status Successful
 Channel 4
 ESSID HomeAP
 Security WPA2 pre-shared key
 BSSID 00:02:6F:88:55:ED
 Frequency 2.427 GHz
 Data Rate 300 Mbps

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.
Data Rate	The Data Rate in use.

WLAN Settings

Channel 4

SSID_1

ESSID HomeAP

Security WPA2 pre-shared key

BSSID 00:02:6F:88:55:EC

WLAN Settings (Repeater mode)	
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.

WAN Settings

Attain IP Protocol Dynamic IP Address
 IP Address 192.168.66.104
 Subnet Mask 255.255.255.0
 Default Gateway 192.168.66.1
 MAC Address 00:02:6F:88:52:DA
 Primary DNS 192.168.66.1
 Secondary DNS ---

WAN Settings (Client Router)	
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 Successful
 Channel 4
 ESSID HomeAP
 Security WPA2 pre-shared key
 BSSID 00:BB:77:50:02:A0

 Frequency 2.427 GHz
 Data Rate 130 Mbps
 Link Quality 100/100
 Signal Level -23 dBm
 Noise Level -69 dBm

WLAN Station Information (Client Bridge / Client Router 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 ESR1221AN connected.
Security	The wireless encryption in use.
BSSID	The MAC address of this SSID which ESR1221AN connected.

8.3 DHCP (Client Router mode)

This page shows the status of the DHCP server and also allows you to control how the IP addresses are allocated.

DHCP Client Table :

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

IP Address	MAC Address	Expiration Time
192.168.1.100	00:24:E8:C7:41:0D	0 Days 00:18:47

Refresh

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

Enable Static DHCP IP

IP Address	MAC Address
192.168.1.200	0029E29A5FE9

Add

Reset

Current Static DHCP Table :

NO.	IP Address	MAC Address	Select
1	192.168.1.150	00:13:64:78:41:CE	<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
192.168.1.100	00:24:E8:C7:41:0D	0 Days 00:18:47

Refresh

DHCP Client Table (Client Router mode)	
IP Address	The LAN IP address of the client.
MAC Address	The MAC address of the client's LAN interface.
Expiration Time	The time that the allocated IP address will expire.
Refresh	Click this button to update the DHCP Client Table.

Enable Static DHCP IP

IP Address	MAC Address
192.168.1.200	0029E29A5FE9

Add Reset

Current Static DHCP Table :

NO.	IP Address	MAC Address	Select
1	192.168.1.150	00:13:64:78:41:CE	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

You can also manually specify the IP address that will be allocated to a LAN client by associating the IP address with its MAC address.

Type the IP address you would like to manually assign to a specific MAC address and click **Add** to add the condition to the Static DHCP Table.

8.4 Schedule (Client Router mode)

This page allows you to schedule times that the Firewall feature will be activated / deactivated.

Click **Add** to create a Schedule entry.

You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

Enabled Schedule Table (up to 8)

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

Add

Edit

Delete Selected

Delete All

Apply

Cancel

You can use the Schedule page to Start/Stop the Services regularly. The services will start at the time in the following Schedule Table or it will stop.

Schedule Description :	<input type="text" value="schedule 01"/>
Service :	<input checked="" type="checkbox"/> Firewall
Days :	<input type="checkbox"/> Every Day <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" 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 (Client Router mode)	
Schedule Description	Assign a name to the schedule.
Service	Type of service
Days	Define the Days to activate or deactivate the scheduled service.
Time of day	Define the Time of day to activate or deactivate the scheduled service. Note: Use 24-hour clock format.

8.5 Even Log

This page displays the system log of the device. When powered down or rebooted, the log will be cleared.

View the system operation information.

```

day 1 00:00:04 [SYSTEM]: WLAN, start LLTD
day 1 00:00:04 [SYSTEM]: HTTP, start
day 1 00:00:03 [SYSTEM]: NET, Firewall Disabled
day 1 00:00:03 [SYSTEM]: NET, NAT Disabled
day 1 00:00:03 [SYSTEM]: NTP, start NTP Client
day 1 00:00:01 [SYSTEM]: LAN, IP address=192.168.1.2
day 1 00:00:01 [SYSTEM]: LAN, start
day 1 00:00:01 [SYSTEM]: BR, start
day 1 00:00:01 [SYSTEM]: SYS, Kernel Version: 1.1.0
day 1 00:00:01 [SYSTEM]: SYS, Application Version: 1.1.0
day 1 00:00:01 [SYSTEM]: Start Log Message Service!

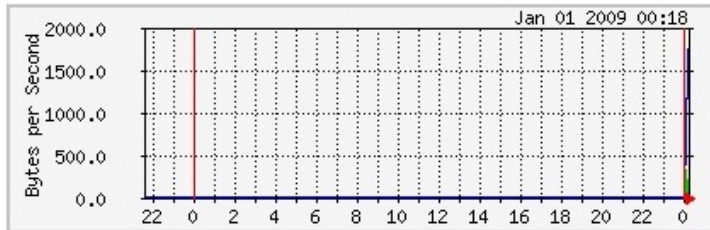
```


Log	
Save	Save the log to a file.
Clear	Clears the log.
Refresh	Updates the log.

8.6 Monitor

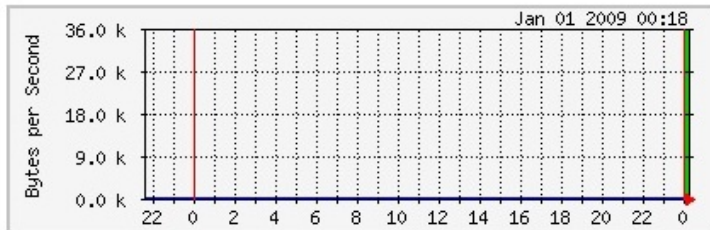
This page shows a histogram of the Ethernet and Wireless LAN traffic. Click on **[Detail]** to get the detail information.

Ethernet Daily Graph (5 Minute Average)

[Detail](#)


	Maximum	Average	Current
RX	338 B/sec	251 B/sec	207 B/sec
TX	1899 B/sec	1410 B/sec	1899 B/sec

WLAN Daily Graph (5 Minute Average)



	Maximum	Average	Current
RX	35399 B/sec	33343 B/sec	33087 B/sec
TX	278 B/sec	123 B/sec	18 B/sec

9 Wireless

9.1 Status

This page shows the current status of the device's Wireless settings.

Repeater mode:

View the current wireless connection status and related information.

WLAN Repeater Information

Connection Status	Successful
ESSID	HomeAP
Security	WPA2 pre-shared key
BSSID	00:02:6F:88:55:ED
Channel	4
Frequency	2.427 GHz
Data Rate	300 Mbps

WLAN Settings

Channel 4

SSID_1

ESSID	HomeAP
Security	WPA2 pre-shared key
BSSID	00:02:6F:88:55:EC

Client Bridge / Client Router mode:

View the current wireless connection status and related information.

WLAN Station Information

Connection Status	Successful
ESSID	HomeAP
Security	WPA2 pre-shared key
BSSID	00:02:6F:01:50:10
Channel	4
Frequency	2.427 GHz
Data Rate	270 Mbps
Link Quality	100/100
Signal Level	-19 dBm
Noise Level	-69 dBm

9.2 Basic

This page shows the current status of the device's Wireless settings.

Repeater mode:

Radio : Enable Disable

Mode : Universal Repeater ▾

Band : 2.4 GHz (B+G+N) ▾

Enabled SSID#: 1 ▾

ESSID1 : HomeAP

Channel : 4 ▾

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.

Client Bridge / Client Router mode:

Radio : Enable Disable

Mode : Client ▾

Band : 2.4 GHz (B+G+N) ▾

Site Survey :

Basic (Client Bridge / Client Router 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.

Site Survey (Client Bridge / Client Router mode)

1. AP list after site survey.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	1	ECB350_AP	00:03:7F:BE:F0:05	NONE	OPEN	86	11b/g/n
2	<input type="radio"/>	1	sqa-dlink-test	00:02:6F:61:51:16	TKIPAES	WPA1PSKWPA2PSK	91	11b/g/n
3	<input type="radio"/>	3	SQA_300H	00:02:6F:01:50:10	TKIPAES	WPA1PSKWPA2PSK	76	11b/g/n
4	<input type="radio"/>	4	RD_ADSL	00:02:6F:11:22:A0	WEP	AUTOWEP	76	11b/g/n
5	<input type="radio"/>	4	HomeAP	00:BB:77:50:02:A0	AES	WPA2PSK	100	11b/g/n
6	<input type="radio"/>	4	RAIDER ADSL`	00:0C:F6:54:A9:78	TKIPAES	WPA1PSKWPA2PSK	70	11b/g/n
7	<input type="radio"/>	4		00:0C:F6:54:A9:79	AES	WPA2PSK	70	11b/g/n
8	<input type="radio"/>	6	sqa-202-1	00:02:6F:B5:36:F0	TKIPAES	WPAPSK	86	11b/g/n
9	<input type="radio"/>	6	sqa-202-3	0A:02:6F:B5:36:F0	TKIPAES	WPA1PSKWPA2PSK	96	11b/g/n
10	<input type="radio"/>	6	sqa-202-4	0E:02:6F:B5:36:F0	NONE	OPEN	86	11b/g/n
11	<input type="radio"/>	8	SQA_M36	00:02:6F:6B:D2:25	TKIPAES	WPA1PSKWPA2PSK	100	11b/g
12	<input type="radio"/>	9	Please_remove_it	00:02:6F:00:00:20	NONE	OPEN	34	11b/g
13	<input type="radio"/>	11	EnGenius51F938	00:02:6F:51:F9:38	NONE	OPEN	55	11b/g/n

Refresh

Add to AP Profile

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

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	1	ECB350_AP	00:03:7F:BE:F0:05	NONE	OPEN	86	11b/g/n
2	<input type="radio"/>	1	sqa-dlink-test	00:02:6F:61:51:16	TKIPAES	WPA1PSKWPA2PSK	91	11b/g/n
3	<input type="radio"/>	3	SQA_300H	00:02:6F:01:50:10	TKIPAES	WPA1PSKWPA2PSK	76	11b/g/n
4	<input type="radio"/>	4	RD_ADSL	00:02:6F:11:22:A0	WEP	AUTOWEP	76	11b/g/n
5	<input checked="" type="radio"/>	4	HomeAP	00:BB:77:50:02:A0	AES	WPA2PSK	100	11b/g/n
6	<input type="radio"/>	4	RAIDER ADSL`	00:0C:F6:54:A9:78	TKIPAES	WPA1PSKWPA2PSK	70	11b/g/n
7	<input type="radio"/>	4		00:0C:F6:54:A9:79	AES	WPA2PSK	70	11b/g/n
8	<input type="radio"/>	6	sqa-202-1	00:02:6F:B5:36:F0	TKIPAES	WPAPSK	86	11b/g/n
9	<input type="radio"/>	6	sqa-202-3	0A:02:6F:B5:36:F0	TKIPAES	WPA1PSKWPA2PSK	96	11b/g/n
10	<input type="radio"/>	6	sqa-202-4	0E:02:6F:B5:36:F0	NONE	OPEN	86	11b/g/n
11	<input type="radio"/>	8	SQA_M36	00:02:6F:6B:D2:25	TKIPAES	WPA1PSKWPA2PSK	100	11b/g
12	<input type="radio"/>	9	Please_remove_it	00:02:6F:00:00:20	NONE	OPEN	34	11b/g
13	<input type="radio"/>	11	EnGenius51F938	00:02:6F:51:F9:38	NONE	OPEN	55	11b/g/n

- Enter the correct security setting.

AP Profile Settings

Network Name (SSID) :	<input type="text" value="HomeAP"/>
Encryption :	<input type="text" value="WPA pre-shared key"/>
Authentication Type :	<input type="text" value="WPA2(AES)"/>
Pre-shared Key :	<input type="text" value="12345678"/>

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

Add to AP Profile successfully.

Close

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

AP Profile Table

NO.	SSID	MAC	Authentication	Encryption	Select
1	HomeAP	00:BB:77:50:02:A0	WPA2_PSK	AES	<input type="checkbox"/>

Add Edit Move Up Move Down Delete Selected Delete All
Connect

9.3 Advanced

This page allows you to configure wireless advance settings. It is recommended the default settings are used unless the user has experience with these functions.

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:	<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 %"/>	

Advanced (Repeater mode)	
Fragment Threshold	<p>Specifies the size of the packet per fragment. This function can reduce the chance of packet collision.</p> <p>However when this value is set too low, there will be increased overheads resulting in poor performance.</p>
RTS Threshold	When the packet size is smaller than the RTS Threshold, then the packet will be sent without 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 informs all wireless clients that the access point will be sending 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	<p>Set whether each channel uses 20 or 40Mhz.</p> <p>To achieve 11n speeds, 40Mhz channels must be used.</p>
Preamble Type	<p>A preamble is a message that helps access points synchronize with the client.</p> <p>Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, so it decreases compatibility but increases performance.</p>
CTS Protection	When Enabled, the performance is slightly lower however the chances of packet collision is greatly reduced.
Tx Power	Set the power output of the wireless signal.

Client Bridge / Client Router 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 : (256-2346)

RTS Threshold : (1-2347)

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

9.4 Security (Repeater mode)

This page allows you to set the wireless security settings.

Note: Only in Repeater mode.

ESSID Selection :	HomeAP ▾
Broadcast ESSID :	Enable ▾
WMM :	Enable ▾
Encryption :	Disable ▾

Security (Repeater mode)	
SSID Selection	Select the SSID that the security settings will apply to.
Broadcast SSID	If Disabled, then the device will not be broadcasting the SSID. Therefore it will be invisible to wireless clients.
WMM	WiFi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, and background. Note that in certain situations, WMM needs to be enabled to achieve 11n transfer speeds.
Encryption	The encryption method to be applied. You can choose from WEP, WPA pre-shared key. <ul style="list-style-type: none"> • Disable - no data encryption is used. • WEP - data is encrypted using the WEP standard. • WPA-PSK (TKIP) - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP. • WPA2-PSK (AES) - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.

WEP Encryption:

Encryption :	WEP ▾
Authentication Type :	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key
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 Length	Select the desired option, and ensure the wireless clients use the same setting. <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 :	WPA2(AES) ▾
Pre-shared Key Type :	Passphrase ▾
Pre-shared Key :	12345678

WPA Pre-Shared Key Encryption	
WPA type	Select the WPA encryption you would like. You can choose WPA(TKIP), WPA2(AES), WAP(AES) or WAP2(TKIP). Please ensure that your wireless clients use the same settings.
Pre-shared Key Type	Select whether you would like to enter the Key in HEX or Passphrase format.
Pre-shared Key	Wireless clients must use the same key to associate the device. If using passphrase format, the Key must be from 8 to 63 characters in length.

9.5 Filter (Repeater mode)

This page allows you to create filters to control which wireless clients can connect to this device by only allowing the MAC addresses entered into the Filtering Table.

Note: Only in Repeater mode.

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

Enable Wireless MAC Filtering

Description	MAC Address
<input type="text"/>	<input type="text"/>

Only the following MAC Addresses can use network:

NO.	Description	MAC Address	Select
1	Rule01	00:02:6F:00:00:01	<input type="checkbox"/>

Wireless Filter (Repeater mode)	
Enable Wireless MAC Filtering	Tick the box to 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	Un-tick all selected entries.

9.6 WPS

WPS feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

It reduces the user steps required to configure a network and enable security.

WPS: Enable

Wi-Fi Protected Setup Information

WPS Via Push Button:

Wi-Fi Protected Setup (WPS)	
WPS	Tick to Enable the WPS feature.
WPS Via Push Button	Click this button to initialize WPS feature using the push button method.

Step 1: Click **[WPS]** button on ERB9260.



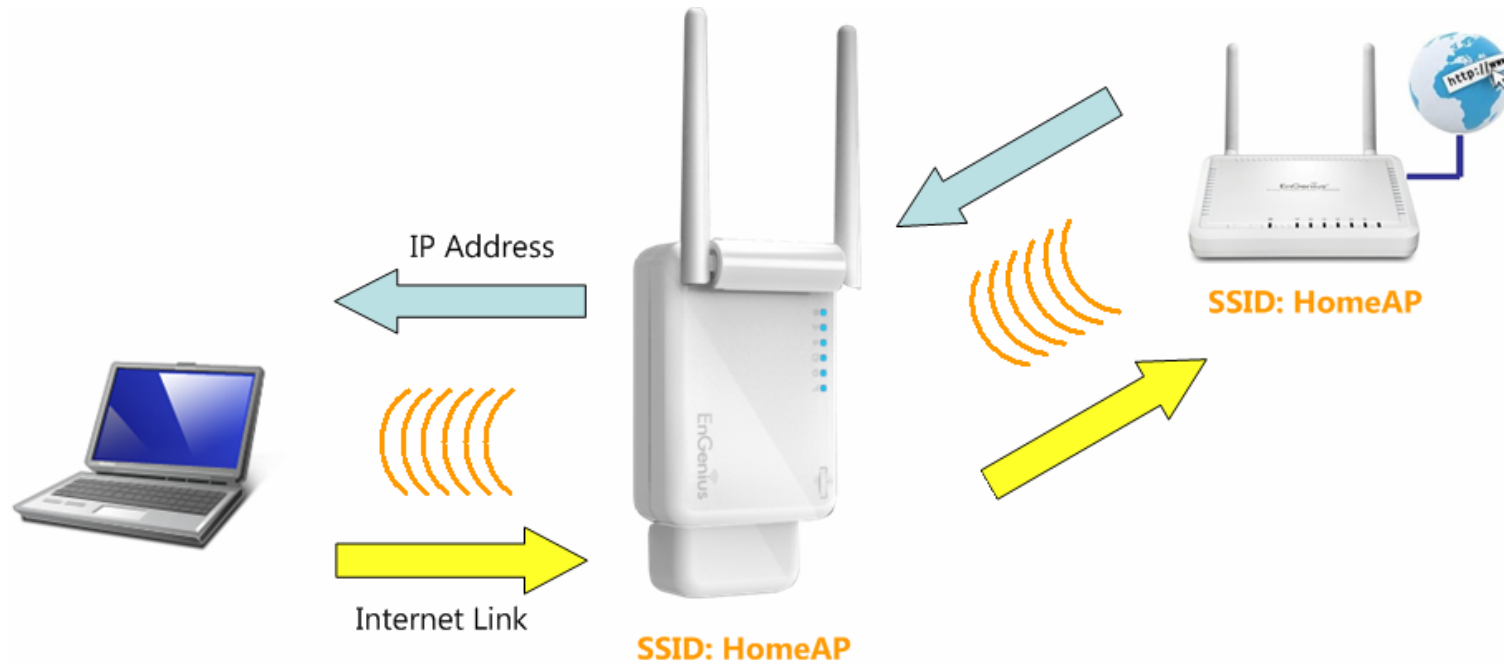
Step 2: Click **[WPS]** button on the Access Point



Note:

- It may take up to 60 seconds for ERB9260 to clone the AP. Please wait until **WPS led** stops blinking and stay **ON**.
- If the connection is successful, there will be **TWO** HomeAP in the environment.

Step 3: Please **rescan** the APs and **reconnect** to the HomeAP closest to you. Your wireless card should pick up the AP with **strongest** signal as you roam.



9.7 Client List (Repeater mode)

This page shows the wireless clients that are connected to the device. Click on **[Refresh]** to get the latest user list and information update.

Note: Only in 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
HomeAP	00:02:6F:47:65:CA	3.6 KBytes	8.0 KBytes	100	1 min 38 secs	0 secs
HomeAP	00:02:6F:11:AC:93	3.5 KBytes	7.5 KBytes	100	1 min 36 secs	0 secs
HomeAP	00:02:6F:63:69:19	254 Bytes	2.0 KBytes	100	14 secs	0 secs

Refresh

9.8 AP Profile

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

Note: Only in Client Bridge and Client Router mode.

AP Profile Table

NO.	SSID	MAC	Authentication	Encryption	Select
1	HomeAP	00:BB:77:50:02:A0	WPA2_PSK	AES	<input type="checkbox"/>

AP Profile Table (Client Bridge / Client Router 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.

AP Profile Settings

Network Name (SSID) :	<input type="text" value="HomeAP"/>	
Encryption :	<div style="border: 1px solid black; padding: 2px;"><div style="background-color: #e0e0e0; padding: 2px;">Disable ▾</div><div style="background-color: #0070c0; color: white; padding: 2px;">Disable</div><div style="padding: 2px;">WEP</div><div style="padding: 2px;">WPA pre-shared key</div><div style="padding: 2px;">RADIUS</div></div>	<input type="button" value="Save"/>

AP Profile Settings	
Network Name (SSID)	Enter the SSID (Network Name) of the wireless network which ERB9260 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.

10 Network

10.1 Status

This page shows the current status of the device's LAN and WAN (Client Router mode) connection.

Note: DHCP Server and WAN Settings are only in Client Router mode.

View the current wireless connection status and related information.

LAN Settings

IP Address	192.168.1.2
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:02:6F:88:55:EC

WAN Settings

Attain IP Protocol	Dynamic IP Address
IP Address	192.168.66.104
Subnet Mask	255.255.255.0
Default Gateway	192.168.66.1
MAC Address	00:02:6F:88:52:DA
Primary DNS	192.168.66.1
Secondary DNS	---

Renew

10.2 LAN

This page allows you to modify the device's LAN settings.

The LAN setting in Client Router mode.

Bridge Type :	Static IP ▾
IP Address :	192.168.1.2
IP Subnet Mask :	255.255.255.0
802.1d Spanning Tree :	Disabled ▾

There is additional setting **Default Gateway** in Repeater and Client Bridge mode.

Bridge Type :	Static IP ▾
IP Address :	192.168.1.2
IP Subnet Mask :	255.255.255.0
Default Gateway :	
802.1d Spanning Tree :	Disabled ▾

LAN IP	
Bridge Type	Select Static IP or Dynamic IP from the drop-down list. If you select Static IP, you will be required to specify an IP address and subnet mask. If Dynamic IP is selected, then the IP address is received automatically from the external DHCP server. Note: The option: Dynamic IP is only in Repeater mode.
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 this device. Leave it blank if you are unsure of this setting.
802.1d Spanning Tree	When Enabled, the Spanning Tree protocol will prevent network loops in your LAN network.

DHCP Server feature is only in Client Router mode.

DHCP Server

DHCP Server :	Enabled ▾
Lease Time :	Half hour ▾
Start IP :	192.168.1.100
End IP :	192.168.1.120
Domain Name :	erb9260
First DNS Address :	
Second DNS Address :	

DHCP Server (Client Router mode)	
DHCP Server	Enable or disable DHCP feature. The DHCP Server automatically allocates IP addresses to your LAN device.
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.

10.3 WAN (Client Router mode)

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

Note: Only in Client Router mode.

10.3.1 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 :	WLAN

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.

10.3.2 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 :	WLAN	

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.

10.3.3 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="text"/>
Service Name	<input type="text"/>
MTU :	<input type="text" value="1492"/> (512<=MTU Value<=1492)
Type :	Keep Connection ▾
Idle Timeout :	<input type="text" value="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	You can choose the method that the router maintains connection with the ISP. Keep Connection: The device will maintain a constant connection with the ISP. Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.
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.

10.3.4 Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by very few ISPs.

Login Method :	<input type="text" value="PPTP"/>
WAN Interface Settings :	
WAN Interface Type :	<input type="text" value="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 :	<input type="text" value="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	You can choose the method that the router maintains connection with the ISP. Keep Connection: The device will maintain a constant connection with the ISP. Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.
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.

11 Firewall (Client Router mode)

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

Note: Only in Client Router mode.

11.1 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

11.2 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 :

11.3 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

11.4 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

MAC Filtering table:

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

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.

11.5 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"/>

Add

Reset

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

Delete Selected

Delete All

Reset

Apply

Cancel

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.

11.6 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

Add

Reset

Current Website Blocking Table:

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

Delete Selected

Delete All

Reset

Apply

Cancel

12 Advanced (Client Router mode)

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

Note: Only in Client Router mode.

12.1 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

12.2 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 :

Local IP :

Protocol : Both ▾

Port Range : ~

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.

12.3 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.

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, 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 :

Local IP :

Protocol : Both ▾

Local Port :

Forwarded Port :

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"/>

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.

12.4 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 ~ <input type="text"/>
Trigger Type :	Both <input type="button" value="v"/>
Forwarded Port :	12120,12122,24150-24220
Public Type :	Both <input type="button" value="v"/>

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.

12.5 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"/>

12.6 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

12.7 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

Apply Cancel

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"/>	0 <input type="text"/>
Name <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	0 <input type="text"/>
Name <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	0 <input type="text"/>

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 :	<input type="text"/> ~ <input type="text"/>
Protocol :	All ▾
Port Range :	1 ~ 65535
Policy :	Min ▾
Rate(bps) :	FULL ▾

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"/>

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.

12.8 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
-----	--------------------	-------------	-----------------	--------

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.

12.9 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:	<input type="text"/>

12.10 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

13 Management

13.1 Admin

You can change the password required to log into the system web-based management. By default, the password is: **admin**. Password can contain 0 to 12 alphanumeric characters and are 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"/>
System Name :	<input type="text" value="ERB9260"/>
Idle Timeout :	<input type="text" value="10"/> (1~10 Minutes)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Change Password	
Old Password	Enter the current password.
New Password	Enter your new password.
Confirm Password	Enter your new password again for verification.
System Name	The system name of this device. You can use this System Name to access your device. Ex. http://erb9260
Idle Timeout	Enter Administration Page timeout time.

13.2 Firmware

This page allows you to upgrade the device'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. Click the [**Browse**] button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. 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.

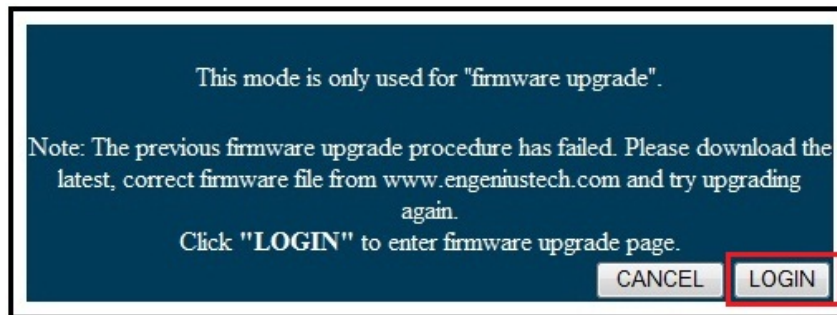
Emergency Upgrade

If you upgrade fail, you may enter Emergency Upgrade WEB page.

1. Enter IP address: **192.168.1.2** and enter Emergency Upgrade WEB page.



2. Select [**LOGIN**] to enter firmware upgrade WEB page.



3. Click the [**Browse**] button and navigate to the location of the upgrade file and then click [**UPLOAD**].



4. Wait for 100 seconds for firmware upgrade and reboot the device.

It takes for about 100 seconds to upgrade the firmware and reboot the device.
Upgrading, please wait....
Note: Do not do anything while firmware is upgrading!!

5. You can access the device again.



13.3 Configure

This page 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 you can use the [**Restore to Factory Defaults**] 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 style="width: 150px;" 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.

13.4 Reset

In some circumstances it may be required to force the device to reboot. Click on **[Apply]** to reboot.

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

14 Tools

14.1 Time Setting

This page allows you to set the system 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	Synchronize with the NTP Server or Synchronize with PC
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 Saving	Check whether daylight savings applies to your area.

14.2 Dynamic DNS (DDNS) (Client Router mode)

This free service is very useful when combined with the *Virtual Server (Port Forwarding)* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

Note: Only in Client Router mode.

DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, follow the Service provider's procedure to obtain your desired Domain name.
3. Enter your DDNS data on the device's DDNS screen, and enable the DDNS feature.
4. The Wireless Router will automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

The most common use for DDNS is in allowing an Internet domain name to be assigned to a computer with a varying (dynamic) IP address. This makes it possible for other sites on the Internet to establish connections to the machine without needing to track the IP address themselves.

Dynamic DNS :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Server Address :	DynDNS ▾
Host Name :	test.dyndns.biz
Username :	username
Password :	••••••••

Apply Cancel

Dynamic DNS	
Dynamic DNS	Tick this box to Enable the DDNS feature.
Server Address	Select the list of Dynamic DNS homes you would like to use from this list.
Username / Password	Enter the Username and Password of your DDNS account.

14.3 Diagnosis

This page allows you to test your network. Type in the address for diagnosis.

This page can diagnose the current network status.

Address to Ping :

Ping Frequency :

```
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: seq=0 ttl=128 time=0.001 ms
64 bytes from 192.168.1.100: seq=1 ttl=128 time=0.001 ms
64 bytes from 192.168.1.100: seq=2 ttl=128 time=0.001 ms
64 bytes from 192.168.1.100: seq=3 ttl=128 time=0.001 ms
64 bytes from 192.168.1.100: seq=4 ttl=128 time=0.001 ms

--- 192.168.1.100 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.001/0.001/0.001 ms
ping-finished
```

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.

15 Wizard (Repeater mode)

This page allows you to go to **Wizard Mode** setting WEB page.

Note: Only in Repeater mode.

Important Notice

You are about to enter Wizard Mode. This means you will lose your current connection with the AP. The previously configured wireless security settings on the range-extender will be erased. However, you can decide whether to keep the advanced (RTS Threshold / Transmit Power) settings.

- Reset the range-extender to factory default
- Keep the other advanced settings

Enter Wizard Mode

Wizard (Repeater mode)	
Reset the rang-extender to factory default	It will reset the device to factory default and go to Easy Setup WEB page again.
Keep the other advanced settings	It allows you to go to Easy Setup WEB page again and keep the other settings.

16 Logout

Click on [**Logout**] button to logout.

This page is used to logout this device.

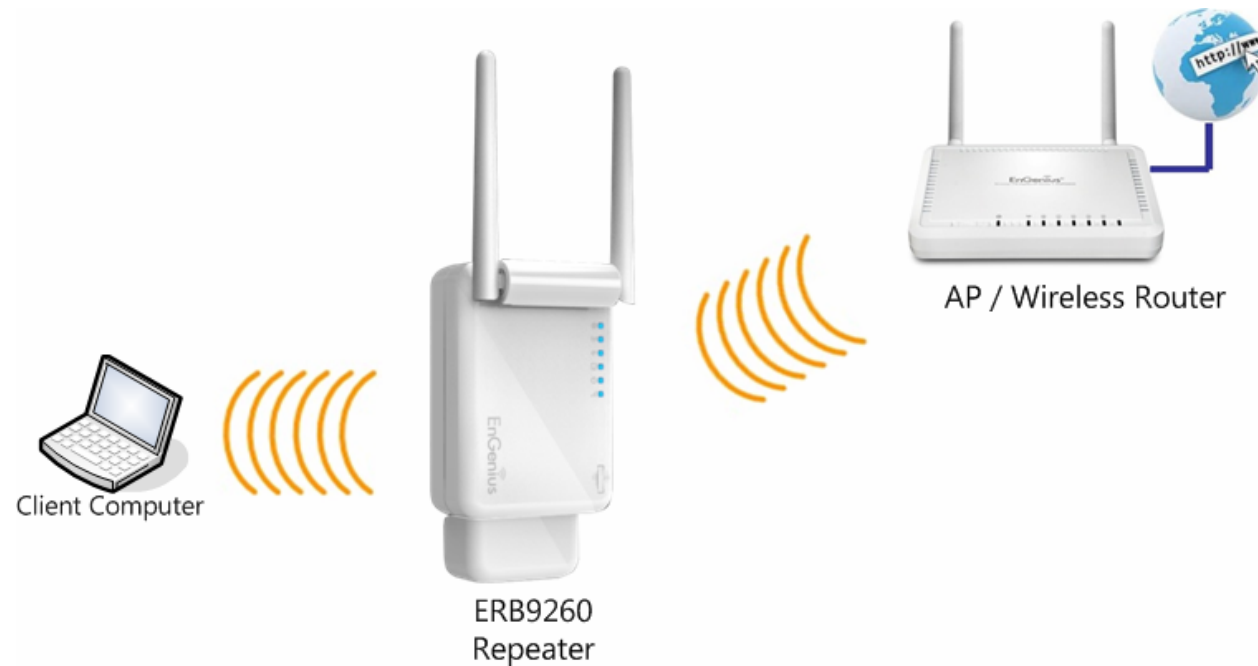
Logout

17 Building a Wireless Network

With its ability to operate in various operating modes, your ERB9260 is the ideal device around which you can build your WLAN. This appendix describes how to build a WLAN around your ERB9260 using the device's operating modes.

17.1 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).



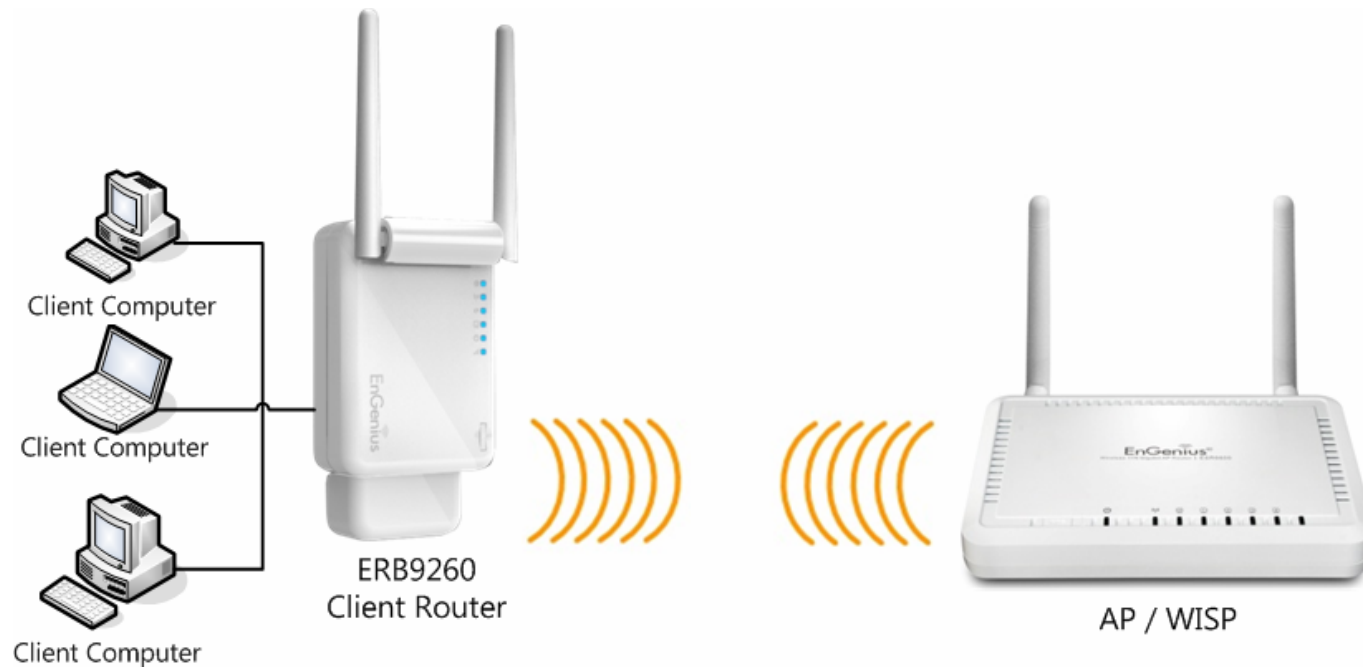
17.2 Client Bridge Mode

In Client Bridge Mode, the ERB9260 behaves like a wireless client that connects to an Access Point wirelessly and allows users to surf the Internet whenever they want. In this mode, use the ERB9260 Site Survey to scan for Access Points within range. Then configure the ERB9260 SSID and security password accordingly to associate with the Access Point. In this configuration, the station has a wired Ethernet connection to the EBR9260 LAN port.



17.3 Client Router Mode

In Client Router Mode, the EBR9260's internal DHCP server allows a number of LANs to automatically generate IP addresses to share the same Internet. In this mode, connect an AP/WISP wirelessly and connect to LANs via a wired connection.



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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

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

Appendix B – 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.

[French translation:](#)

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.

[French translation:](#)

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.